



User Guide

DeltaStream PON Management System

1900002905 REV1.2.0

APR 2026

© 2026 TP-Link

About this Guide

This User Guide provides information for centrally managing TP-Link DeltaStream GPON OLT (Optical Line Terminal) devices via DPMS (DeltaStream PON Management System). Please read this guide carefully before operation.

Intended Readers

This User Guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

When using this guide, notice that:

- Features available in DPMS and GPON OLT devices may vary due to your region, software version, and device model. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.
- The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.
- This guide uses the specific formats to highlight special messages. The following table lists the notice icons that are used throughout this guide.



Remind to take notice. The note contains the helpful information for a better use of the product.



Configuration Guidelines

Provide tips for you to learn about the feature and its configurations.

More Information

- For technical support, the latest version of the User Guide and other information, please visit <https://service-provider.tp-link.com/>.
- To ask questions, find answers, and communicate with TP-Link users or engineers, please visit <https://community.tp-link.com> to join TP-Link Community.

CONTENTS

About this Guide

Overview

Overview of DeltaStream GPON Solution	2
GPON Network Component.....	3

Get Started with DPMS

Deployment Requirements	6
Installation DPMS on Windows	7
Installation.....	7
Verification	7
Installation DPMS on Linux.....	8
Installation on Ubuntu	8
Installation on Debian	11
Installation on Red Hat.....	13
Verification for Linux	15
Basic Configurations	16
Log In to the Management Interface	19

Manage Devices and Sites

Create Sites	21
Manage OLT Devices	24
Manage ONU Devices	28
Network Tools	36

Configure DPMS

General Settings.....	40
Basic Settings.....	40
Services	40
Mail Server	41
Access Configuration	42
HTTPS Certificate.....	43
Manage DPMS Remotely via Cloud Access	44
Maintenance	45
User Interface	45

Backup & Restore	46
Auto Backup.....	47
Task.....	49
Create Task.....	49
Manage Task.....	54
Notification Strategy	55
Enable Notification.....	55
Email.....	55
Remote Logging.....	55
SNMP.....	56
Webhook.....	59

Monitor the Network

View the Status of Network with Dashboard.....	61
Page Layout of Dashboard	61
Explanation of Widgets.....	62
View the Statistics of the Network	64
Performance.....	64
Traffic/DDM Statistics	65
View and Manage Logs.....	68
Alerts.....	68
Events	69
Notifications.....	71

Manage User Accounts of DPMS

Introduction to User Accounts	77
Manage Roles	79
Understanding Permissions	79
Role-Based Security Policies.....	80
Default System Roles.....	81
Managing Custom Roles	81
Manage Local User Accounts	85
Create a New Local User	85
Edit, Block, and Delete Local Users.....	86
Manage Cloud User Accounts	90
Adding A Cloud User	90
Edit, Block, and Delete Cloud Users.....	92

Quick Config

Overview 96

Quick Config Create 97

 Quick Config File Create..... 97

 Quick Config Profile Create 99

Quick Config Apply 101

 Single OLT Device Apply Quick Config..... 101

 Batch Configuration Provisioning for OLT Devices 102

Quick Config History 103

 Quick Config File History..... 103

 Quick Config Profile History..... 104



Overview

The chapter includes the following sections:

- [1. 1 Overview of DeltaStream GPON Solution](#)
- [1. 2 GPON Network Component](#)

The following table shows the technical terminologies used in this chapter.

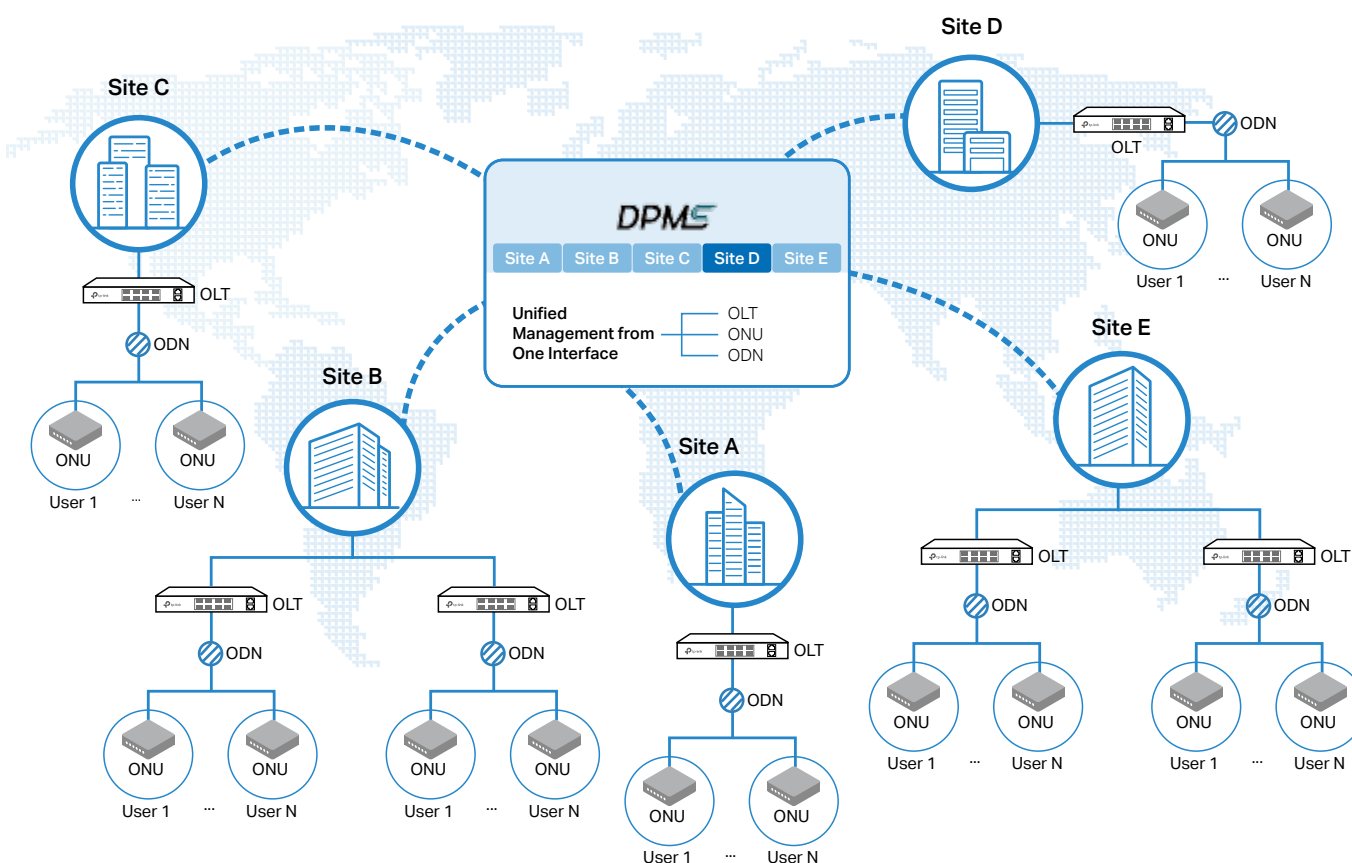
Acronym	Full Name
DPMS	DeltaStream PON Management System
GPON	Gigabit-Capable Passive Optical Network
ISP	Internet Service Provider
OLT	Optical Line Terminal
ONU	Optical Network Unit
ONT	Optical Network Terminal
FTTH	Fiber To The Home
FTTB	Fiber To The Building

♥ 1.1 Overview of DeltaStream GPON Solution

DeltaStream GPON Solution is designed for the ISP to provide business-class networking services for its customers via GPON, which comprises OLTs in the ISP's side, ONUs in the users' side, and the ODN between them.

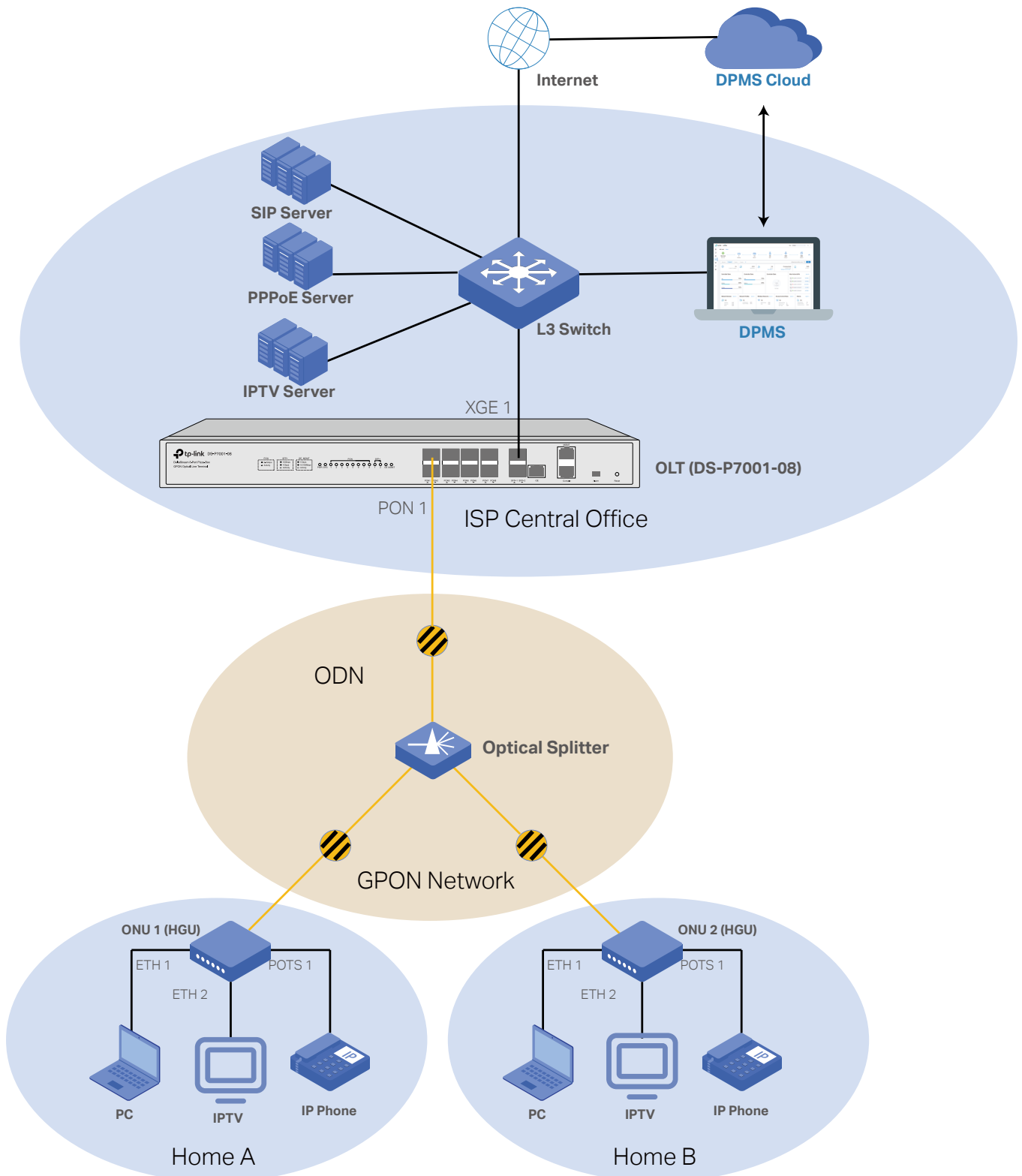
DPMS offers centralized management for configuring GPON of the ISP. DPMS simplifies deploying, configuring and monitoring the GPON networks by managing all the GPON-related devices at multiple sites from one central platform. This unleashes new levels of management to avoid complex and costly overprovisioning. With the help of DPMS, you can develop reliable to meet diverse demands of the customers in each scenario.

The following figure shows a simple architecture of GPON and DPMS.



♥ 1.2 GPON Network Component

The following figure shows a typical network topology of FTTH (Fiber to the Home) service.



The GPON Network consists of the following components.

Component	Description
DPMS	DPMS is the centralized management platform of all the GPON-related devices. To make sure that the DPMS can detect and adopt the OLTs, DPMS should have network access to those devices.
OLT	OLT, such as DS-P7001-08, is the core GPON network device, located at the ISP's central office. GPON networks are extended from the PON ports of OLT, and oriented to the locations of ISP's end users. OLT is uplinked, via the SFP+/SFP/GE ports, to the ISP's L3 Switch, connected to the ISP central network and internet.
ONU	ONU is deployed at the end user's location, and used to access the GPON network of ISP. ONU is uplinked to the GPON network and have downlink ports connected to the user's local network. The user's devices, such as PC, IPTV, and IP Phone, enjoy multiple ISP's services via the connection between ONU and OLT. ONUs are managed and controlled by the OLT via OMCI (ONT Management and Control Interface). There are different types of ONUs, such as HGU (Home Gateway Unit) and SFU (Single Family Unit).
ODN	ODN is a network that consists of optical fibers and passive optical components, such as one or more optical splitters. The ODN network provides highly reliable optical paths to connect ONUs to an OLT.
L3 Switch of ISP	The layer 3 switch is the core component of the ISP's central network, which is used to distribute traffic various services.
Servers of ISP	The servers of ISP provide multiple services for the users' client via the GPON network. The servers include the PPPoE server (for internet access service), the IPTV server, the SIP server (for VOIP service), and so on.
Clients of Users	Clients of users include PC, IPTV, IP Phone, and so on.

2

Get Started with DPMS

This chapter guides you on how to get started with DPMS to configure the GPO, including the initial setup steps, building your network topology, deploying your DPMS, and logging in to the DPMS. The chapter includes the following sections:

- [2.1 Deployment Requirements](#)
- [2.2 Installation DPMS on Windows](#)
- [2.3 Installation DPMS on Linux](#)
- [2.4 Basic Configurations](#)
- [2.5 Log In to the Management Interface](#)

♥ 2.1 Deployment Requirements

DPMS can be hosted on any computers with Windows systems on your network. Make sure your PC's hardware and system meet the following requirements, then properly install the DPMS

■ Hardware Requirements

DPMS can manage up to 500 OLTs if the DPMS Host has enough hardware resources. To guarantee operational stability for managing 500 OLTs, we recommend that you use the hardware which meets or exceeds the following specifications:

CPU: Intel Core i3-8100, i5-6500, or i7-4700 with 2 or more cores and 4 or more threads.

Memory: 6 GB RAM or more.

■ System Requirements

Windows Operating System: Microsoft Windows 7/8/10/11Server. (We recommend that you deploy DPMS on a 64-bit operating system to guarantee the software stability.)

Web Browser: Mozilla Firefox 32 (or above), Google Chrome 37 (or above), Opera 24 (or above), or Microsoft Internet Explorer 11(or above).

Linux Operating System: (Only for DPMS 1.2.5.10)

Ubuntu 24.04, 22.04, 20.04, 18.04, 16.04

Debian 12, 13

Red Hat Enterprise Linux 9.5

■ Java Version Requirements

JRE Version: Java 8u261+

♥ 2.2 Installation DPMS on Windows

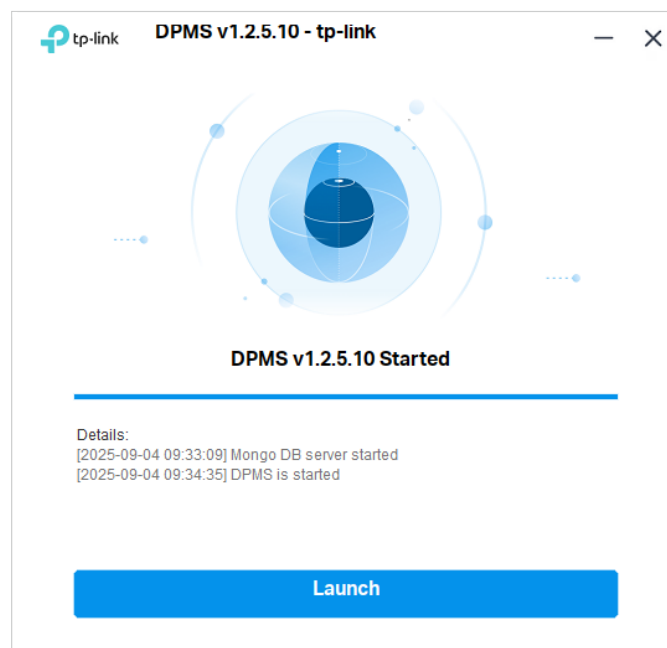
2.2.1 Installation

Ensure that the Java Runtime Environment (JRE) have been installed in your system. The DPMS requires that the system have Java 8 installed. Download the installation file of DPMS from the website. Then follow the instructions to properly install DPMS. After a successful installation, a shortcut icon of the DPMS will be created on your desktop.

2.2.2 Verification

➤ Launch DPMS

After a successful installation, a shortcut icon of the DPMS will be created on your desktop. Double click the icon  and the following window will pop up. After the initialization process, click Launch to open the webpage of DPMS in your web browser.



ⓘ Note:

- To open the webpage of DPMS, you can also launch a web browser and enter <https://127.0.0.1:8443> in the address bar.
- If your web browser opens but prompts a problem with the website's security certificate, click Continue.

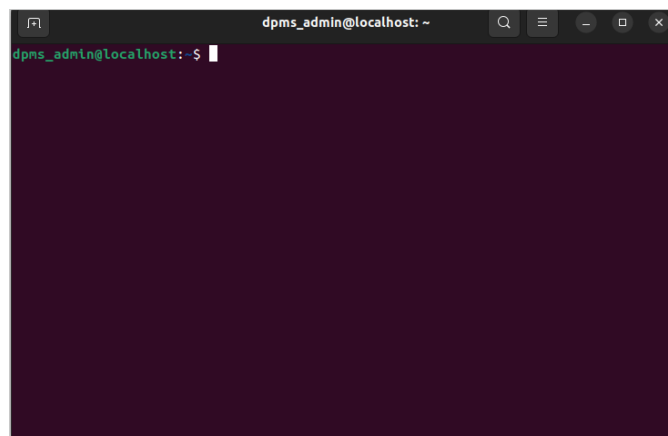
♥ 2.3 Installation DPMS on Linux

We will take Ubuntu, Debian, Red Hat as examples to show the installation process of the DPMS Controller. You can choose the matching process to follow according to your needs.

2.3.1 Installation on Ubuntu

You need to install OpenJDK, MongoDB, and other dependencies before installing your DPMS Controller. Here we use Ubuntu 22.04 as a sample to help you install these dependencies on Linux.

Firstly, you need to wake up a Command Line Window. For Ubuntu: Click Ctrl + Alt + T on your keyboard to wake up Command Line Window. Then you can input the commands in the following installation guides to install your DPMS Controller.



➤ Install OpenJDK

DPMS Controller for Linux only support Java-64bit version 8. Here we help you install the OpenJDK 8 on your system.

Step 1. Install OpenJDK-8 with the command.

```
sudo apt install openjdk-8-jre-headless -y
```

Step 2. Check version

```
java -version
```

➤ Install MongoDB

The following table lists the supported Ubuntu versions and MongoDB versions.

Platform	Version	Supported MongoDB version	MongoDB official guide
Ubuntu	16.04	4.4	https://www.mongodb.com/zh-cn/docs/v4.4/tutorial/install-mongodb-on-ubuntu/
	18.04	6.0	https://www.mongodb.com/zh-cn/docs/v6.0/tutorial/install-mongodb-on-ubuntu/
	20.04 / 22.04 / 24.04	8.0	https://www.mongodb.com/zh-cn/docs/manual/tutorial/install-mongodb-on-ubuntu/

❗ **Note:** You can also follow the MongoDB official guide below to install MongoDB.

1. For MongoDB v4.4. Here we help you install the MongoDB v4.4 on your system.

Step 1. Import the public key used by the package management system.

From a terminal, install **gnupg** and **curl** if they are not already available:

```
sudo apt-get install gnupg curl
```

To import the MongoDB public GPG key, run the following command:

```
curl -fsSL https://www.mongodb.org/static/pgp/server-4.4.asc | sudo gpg -o /usr/share/keyrings/mongodb-server-4.4.gpg --dearmor
```

Step 2. Create a list file for MongoDB.

Create the list file `/etc/apt/sources.list.d/mongodb-org-4.4.list` for Ubuntu 16.04.

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-4.4.gpg ] https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/4.4 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.4.list
```

Step 3. Reload local package database.

```
sudo apt-get update
```

Step 4. Install the MongoDB packages

```
sudo apt-get install mongodb-org
```

Step 5. Prohibit MongoDB from starting up automatically upon startup.

DPMS Controller is responsible for starting the mongod process, so we recommend that you configure it: prohibit MongoDB from starting up automatically upon startup.

```
sudo systemctl disable mongod 2>/dev/null
```

2. For MongoDB v6.0. Here we help you install the MongoDB v4.4 on your system.

Step 1. Import the public key used by the package management system.

From a terminal, install **gnupg** and **curl** if they are not already available:

```
sudo apt-get install gnupg curl
```

To import the MongoDB public GPG key, run the following command:

```
curl -fsSL https://www.mongodb.org/static/pgp/server-6.0.asc | sudo gpg -o /usr/share/keyrings/mongodb-server-6.0.gpg --dearmor
```

Step 2. Create a list file for MongoDB.

Create the list file `/etc/apt/sources.list.d/mongodb-org-6.0.list` for Ubuntu 18.04.

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-6.0.gpg ] https://repo.mongodb.org/apt/ubuntu bionic/mongodb-org/6.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list
```

Step 3. Reload local package database.

```
sudo apt-get update
```

Step 4. Install the MongoDB packages

```
sudo apt-get install mongodb-org
```

Step 5. Prohibit MongoDB from starting up automatically upon startup.

DPMS Controller is responsible for starting the mongod process, so we recommend that you configure it: prohibit MongoDB from starting up automatically upon startup.

```
sudo systemctl disable mongod 2>/dev/null
```

3. For MongoDB v8.0. Here we help you install the MongoDB v4.4 on your system.

Step 1. Import the public key used by the package management system.

From a terminal, install **gnupg** and **curl** if they are not already available:

```
sudo apt-get install gnupg curl
```

To import the MongoDB public GPG key, run the following command:

```
curl -fsSL https://www.mongodb.org/static/pgp/server-8.0.asc | sudo gpg -o /usr/share/keyrings/mongodb-server-8.0.gpg --dearmor
```

Step 2. Create a list file for MongoDB.

Create the list file /etc/apt/sources.list.d/mongodb-org-6.0.list for Ubuntu 18.04.

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-8.0.gpg ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/8.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-8.0.list
```

Step 3. Reload local package database.

```
sudo apt-get update
```

Step 4. Install the MongoDB packages

```
sudo apt-get install mongodb-org
```

Step 5. Prohibit MongoDB from starting up automatically upon startup.

DPMS Controller is responsible for starting the mongod process, so we recommend that you configure it: prohibit MongoDB from starting up automatically upon startup.

```
sudo systemctl disable mongod 2>/dev/null
```

➤ Install DPMS Controller

Go to the official website, download the installation package of Omada SDN Controller, and install it with the following command.

Step 1. Run the Terminal, change the directory to the folder where you save the installation package. Unzip the installation package.

```
tar -zxvf DPMS_Controller_v1.2.5.10_linux_x64_xxx.tar.gz
```

Step 2. Enter the unzipped folder.

```
cd DPMS_Controller_v1.2.5.10_linux_x64/bin/
```

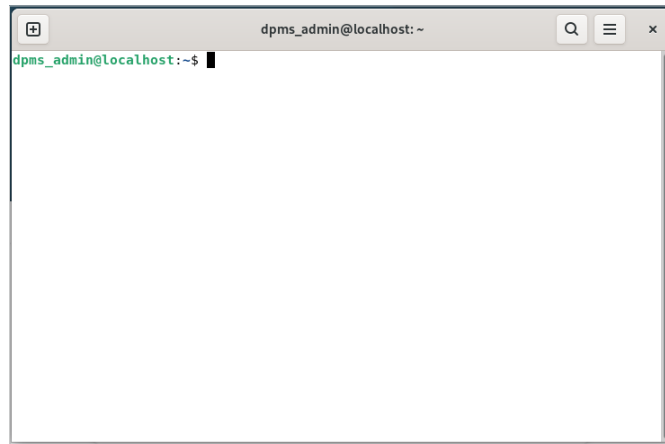
Step 3. Install the controller.

```
sudo ./install.sh
```

2.3.2 Installation on Debian

You need to install OpenJDK, MongoDB, and other dependencies before installing your DPMS Controller. Here we use Debian 12 as a sample to help you install these dependencies on Linux.

Firstly, you need to wake up a Command Line Window. For Debian: Click Ctrl + Alt + T on your keyboard to wake up Command Line Window. Then you can input the commands in the following installation guides to install your DPMS Controller.



➤ Install OpenJDK

DPMS Controller for Linux only support Java-64bit version 8. Here we help you install the OpenJDK 8 on your system.

Step 1. Add the repository

```
sudo apt update
```

```
sudo apt install gnupg ca-certificates curl
```

```
curl -s https://repos.azul.com/azul-repo.key | gpg --dearmor -o /usr/share/keyrings/azul.gpg
```

```
echo "deb [signed-by=/usr/share/keyrings/azul.gpg] https://repos.azul.com/zulu/deb stable main" | tee /etc/apt/sources.list.d/zulu.list
```

Step 2. Execute the installation

```
apt update
```

```
sudo apt install zulu8-jdk
```

Step 3. Check version

```
java -version
```

➤ Install MongoDB

The following table lists the supported Debian versions and MongoDB versions.

Platform	Version	Supported	MongoDB official guide
		MongoDB version	
Debian	12 / 13	8.0	https://www.mongodb.com/zh-cn/docs/manual/tutorial/install-mongodb-on-debian/

Here we help you install the MongoDB v8 on your system.

Step 1. Import the public key.

Install gnupg and curl from the terminal (if not already installed):

```
sudo apt-get install gnupg curl
```

To import the MongoDB public GPG key, run the following command:

```
curl -fsSL https://www.mongodb.org/static/pgp/server-8.0.asc | \  
sudo gpg -o /usr/share/keyrings/mongodb-server-8.0.gpg \  
--dearmor
```

Step 2. Create a list file

MongoDB support:

Take Debian 12 (bookworm) as an example.

```
echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-8.0.gpg ] \  
http://repo.mongodb.org/apt/debian bookworm/mongodb-org/8.0 main" | sudo tee /etc/  
apt/sources.list.d/mongodb-org-8.0.list
```

Step 3. Reload the local package database

Mandatory: Force update and ignore signature errors

```
sudo apt -o Acquire::AllowInsecureRepositories=true update
```

Step 4. Install MongoDB Community Server

```
# try sudo apt --fix-broken install --fix-missing if failed
```

```
sudo apt-get install mongodb-org
```

Step 5. Check version

```
which mongod
```

If the installation fails, you can execute the following command and then reinstall:

```
sudo apt --fix-broken install
```

➤ Install DPMS Controller

Go to the official website, download the installation package of Omada SDN Controller, and install it with the following command.

Step 1. Run the Terminal, change the directory to the folder where you save the installation package.

Unzip the installation package.

```
tar -zxvf DPMS_Controller_v1.2.5.10_linux_x64_xxx.tar.gz
```

Step 2. Enter the unzipped folder.

```
cd DPMS_Controller_v1.2.5.10_linux_x64/bin/
```

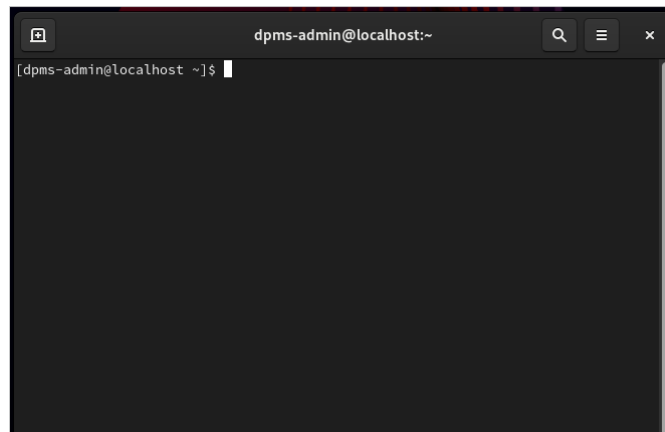
Step 3. Install the controller.

```
sudo ./install.sh
```

2.3.3 Installation on Red Hat

You need to install OpenJDK, MongoDB, and other dependencies before installing your DPMS Controller. Here we use Red Hat 9 as a sample to help you install these dependencies on Linux.

Firstly, you need to wake up a Command Line Window. For Red Hat: Click Ctrl + Alt + T on your keyboard to wake up Command Line Window. Then you can input the commands in the following installation guides to install your DPMS Controller.



➤ 2.3.4.1 Install OpenJDK

DPMS Controller for Linux only support Java-64bit version 8. Here we help you install the OpenJDK 8 on your system.

Step 1. Check available packages

```
sudo yum list java-1*
```

Step 2. Select the appropriate version to install

```
sudo yum install -y java-1.8.0-openjdk.x86_64
```

```
apt update
```

```
sudo apt install zulu8-jdk
```

Step 3. Check version

```
java -version
```

➤ Install MongoDB

Here we help you install the MongoDB v7 on your system.

Step 1. Configure the repository

Create the `/etc/yum.repos.d/mongodb-org-8.0.repo` file:

```
sudo vim /etc/yum.repos.d/mongodb-org-8.0.repo
```

Add the following content to the file:

```
[mongodb-org-8.0]  
name=MongoDB Repository  
baseurl=https://repo.mongodb.org/yum/redhat/9/mongodb-org/8.0/x86_64/  
gpgcheck=1  
enabled=1  
gpgkey=https://pgp.mongodb.com/server-8.0.asc
```

Step 2. Install MongoDB Community Server

To install the latest version (ensure it is 8.0):

```
sudo yum install -y mongodb-org
```

To install a specific version, such as v8.0.4:

```
sudo yum install -y mongodb-org-8.0.4 mongodb-org-database-8.0.4 \  
mongodb-org-server-8.0.4 mongodb-mongosh \  
mongodb-org-mongos-8.0.4 mongodb-org-tools-8.0.4
```

Note: When a new version becomes available, **yum** will automatically upgrade the packages. If you want to prevent MongoDB from upgrading, add the following **exclude** directive to the `/etc/yum.conf` file to pin the current packages:

```
exclude=mongodb-org,mongodb-org-database,mongodb-org-server,mongodb-  
mongosh,mongodb-org-mongos,mongodb-org-tools
```

Step 3. Check version

```
which mongod
```

Step 4. Disable MongoDB from starting automatically on boot

The DPMS Controller will be responsible for starting the mongod process when it starts up.

```
sudo systemctl disable mongod 2>/dev/null
```

➤ Install DPMS Controller

Go to the official website, download the installation package of Omada SDN Controller, and install it with the following command.

Step 1. Install chkconfig

```
sudo yum install chkconfig
```

Step 2. Run the Terminal, change the directory to the folder where you save the installation package. Unzip the installation package.

```
tar -zxvf DPMS_Controller_v1.2.5.10_linux_x64_xxx.tar.gz/
```

Step 3. Enter the unzipped folder.

```
cd DPMS_Controller_v1.2.5.10_linux_x64/bin/
```

Step 4. Install the controller.

```
sudo ./install.sh
```

2.3.4 Verification for Linux

In the Linux system, we provide a series of shortcut commands for operating the DPMS software. You can view all supported commands by entering “`tpdpms help`” in the command line terminal.

Here are 3 commands that can help you check/change the status of the DPMS Controller.

Step 1. Start the DPMS Controller

```
tpdpms start
```

Step 2. Show the status of Controller

```
tpdpms status
```

Step 3. Stop running the DPMS Controller

```
tpdpms stop
```

ⓘ Note:

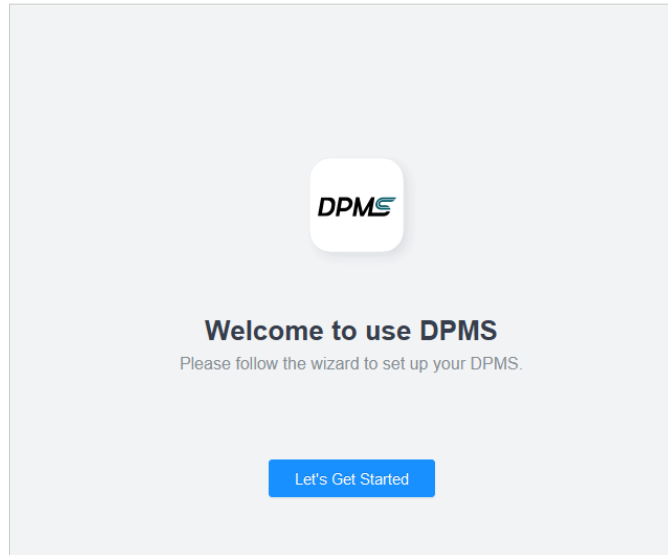
- By default, DPMS must be operated with administrator privileges (i.e., as the root user), including start, stop, restart, viewing software version, and checking operational status. However, you can operate DPMS as a non-root user by modifying the configuration.
- By default, DPMS will be automatically launched with [Root](#) privileges when the system boots up. You can disable the auto-start function at boot time by executing the following command:

```
sudo systemctl disable tdpms 2>/dev/null
```

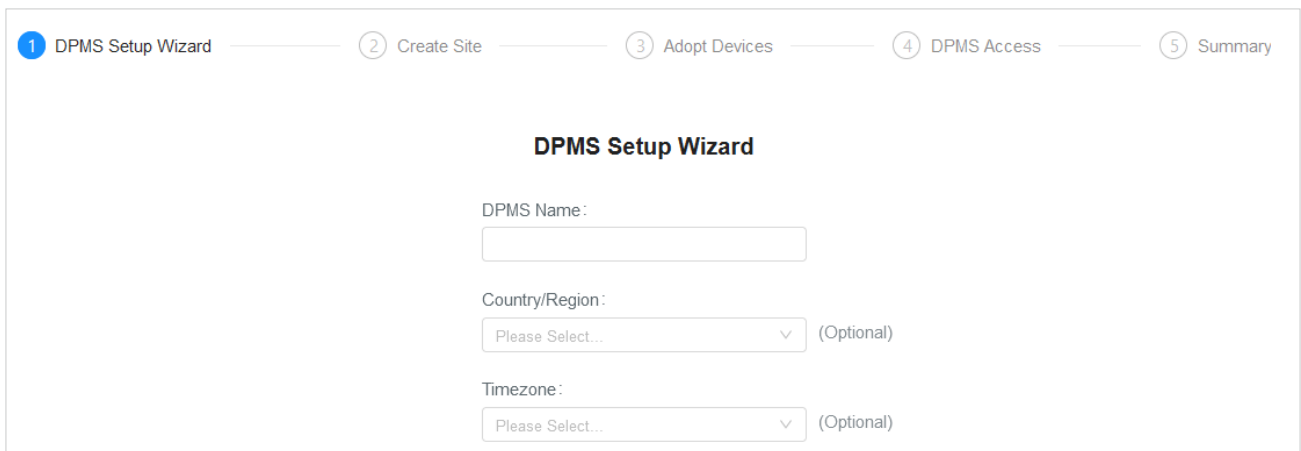
2.4 Basic Configurations

Follow the setup wizard to complete the basic settings for DPMS.

1. Click [Let's Get Started](#).



2. Specify a name for your DPMS, and set your region and timezone. Click [Next](#).

A screenshot of the DPMS Setup Wizard interface. At the top, there is a progress bar with five steps: 1. DPMS Setup Wizard (active), 2. Create Site, 3. Adopt Devices, 4. DPMS Access, and 5. Summary. The main content area is titled 'DPMS Setup Wizard'. It contains three input fields: 'DPMS Name:' with a text box, 'Country/Region:' with a dropdown menu showing 'Please Select...' and a '(Optional)' label, and 'Timezone:' with a dropdown menu showing 'Please Select...' and a '(Optional)' label.

3. You need to create sites to manage the devices. You can manage each region independently by assigning different administrators to each site.

1 DPMS Setup Wizard

2 Create Site

3 Adopt Devices

4 DPMS Access

5 Summary

Create Site

You need to create sites to manage the devices.
You can manage each area independently by
assigning different administrators to each site.

Site Name:

Address:
 (Optional)

Network Manager:
 (Optional)

Phone Number:
 (Optional)

E-mail:
 (Optional)

Note:
 (Optional)

4. The setup page displays all the discovered devices in the network. Select one or more devices to adopt and add to the site. Click [Next](#).

1 DPMS Setup Wizard

2 Create Site

3 Adopt Devices

4 DPMS Access

5 Summary

Adopt Devices

Please select the devices that you want to add to the site created in the last step.

i

DPMS will use the default Username and Password (admin/admin) to adopt devices. If you have changed the Username and Password of the devices, you need to re-adopt them later in the Device List.

Refresh

☐	DEVICE NAME	MODEL	IP ADDRESS	MAC ADDRESS	
☐	DS-P7001-08_000000	DS-P7001-08 1.0	192.168.1.1	00-00-00-00-00-00	The username and password have been changed

Showing 1-1 of 1 records < 1 > 10 / page

Note:

- DPMS will use the default [Username](#) and [Password \(admin/admin\)](#) to adopt devices. If you have changed the Username and Password of the devices, you need to re-adopt them later in the [Device List](#).
- You can click [Skip](#) to skip this step, and then adopt the devices in the [Device List](#).

5. Create an administrator username and password for local login to DPMS. Click [Next](#).

DPMS Setup Wizard — 2 Create Site — Adopt Devices — 4 DPMS Access — 5 Summary

DPMS Access

Create an administrator username and password for local login to DPMS.

Admin Name:

Password:

Confirm Password:

E-mail (Optional):

Alerts Emails: ☐

When enabled, alert emails are sent to the mailbox of network manager who manages the site.

6. Review your settings and click [Finish](#).

DPMS Setup Wizard — 2 Create Site — Adopt Devices — DPMS Access — 5 Summary

✓ Succeeded!

Please confirm the settings below. Once finished, you will be directed to the management interface.

DPMS Name: **TP-Link_DPMS**

Country/Region: **United States**

Timezone: **(UTC-08:00) Pacific Time (US & Canada)**

Site Name: **TP-Link**

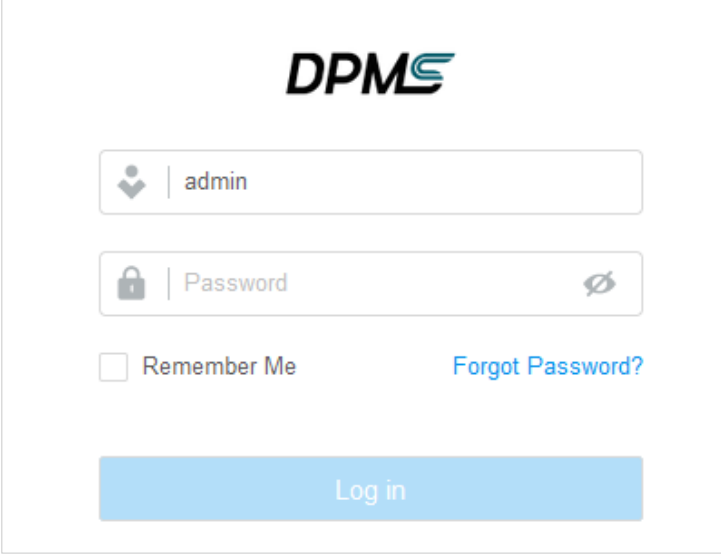
Admin Name: **admin**

2.5 Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page.

Log in to the management interface using the username and password you have set in the basic configurations.

If you forgot your password, click [Forgot Password?](#) and enter your TP-Link ID (email address). Then an email will be sent to you for password reset.



The image shows the DPMS login interface. At the top is the DPMS logo. Below it are two input fields: the first for the username, which contains 'admin', and the second for the password, which contains 'Password'. To the right of the password field is an eye icon for toggling visibility. Below the input fields is a checkbox labeled 'Remember Me' and a link labeled 'Forgot Password?'. At the bottom is a blue 'Log in' button.

3

Manage Devices and Sites

Start managing your network by creating sites and adopting devices so that you can configure and monitor your devices centrally while keeping things organized. The chapter includes the following sections:

- [3.1 Create Sites](#)
- [3.2 Manage OLT Devices](#)
- [3.3 Manage ONU Devices](#)
- [3.4 Network Tools](#)

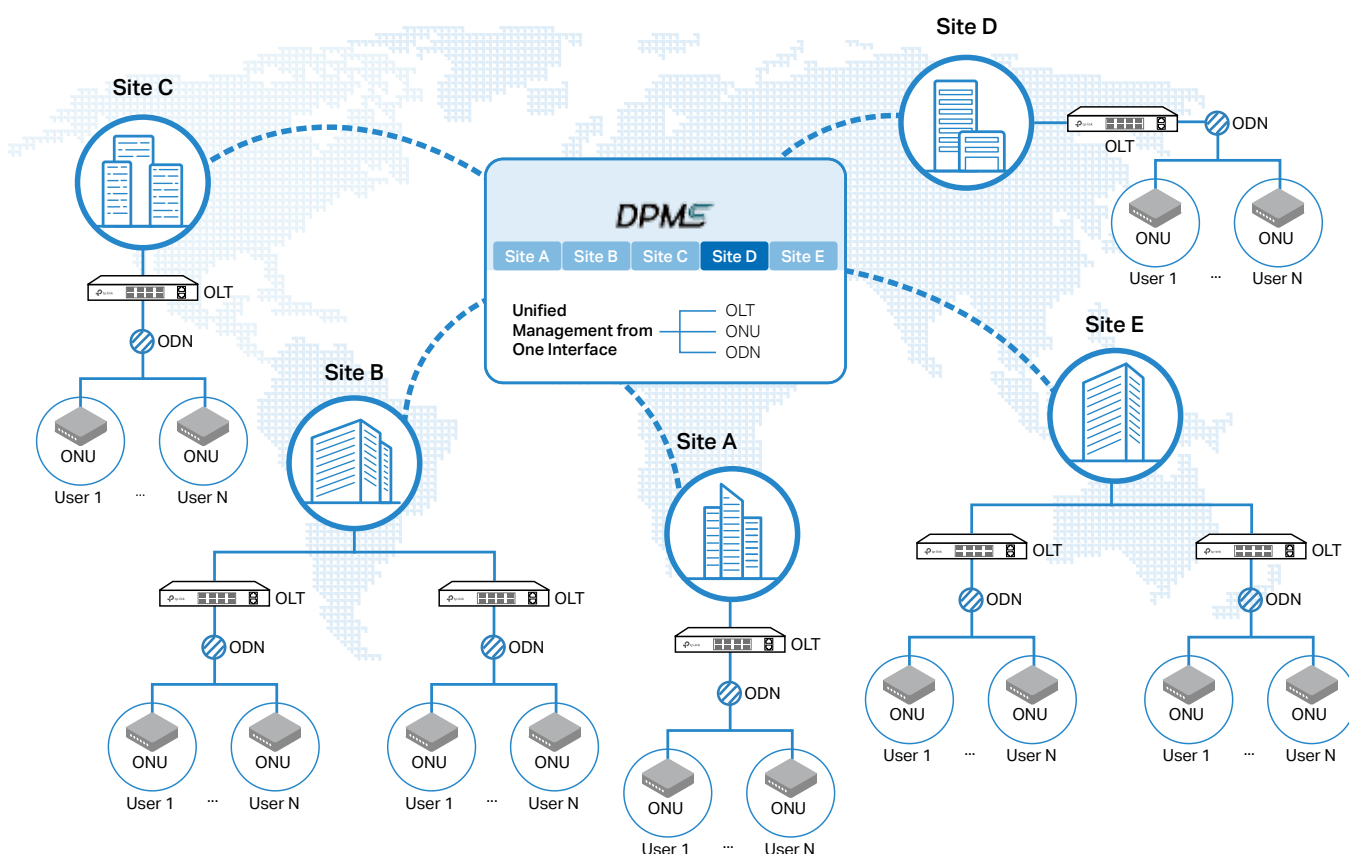
♥ 3.1 Create Sites

➤ Overview

Different sites are logically separated network locations, like different subsidiaries or offices of the ISP. It's best practice to create one site for each location and add all the devices within the network to the site, including the OLTs and ONUs.

Multi-level Site Management refers to the logical mapping of network structures to an organization's actual hierarchy (such as Group-Subsidiary-Department) through parent-child relationships. For instance, in a corporate network, the entire group can be set as the top-level site, subsidiaries as second-level sites, and specific departments or offices as third-level sites. This structure also enables regional and hierarchical partitioning in multi-branch scenarios like ISPs.

This feature supports the construction of a site hierarchy up to three levels, enabling hierarchical and role-based management of network equipment. Superior sites can access an aggregated view of all subordinate sites, while administrators of lower-level sites manage only the devices within their specific scope. This ensures a clear definition of responsibilities coupled with centralized management efficiency.



➤ Configuration

To create sites, follow these steps:

1. Go to [Site](#). Click [Add New Site](#). Configure the parameters and click [Apply](#).

Add Site

X

Site Name :

(1-32 characters)

Address :

(Optional, 1-128 characters)

Network Manager :

(Optional, 1-32 characters)

Phone Number :

(Optional, 1-32 characters)

E-mail :

(Optional, 1-128 characters)

Note :

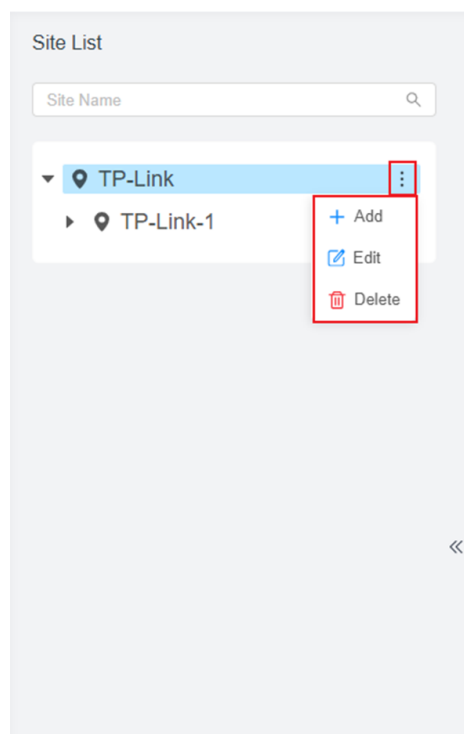
(Optional, 1-256 characters)

Apply

Cancel

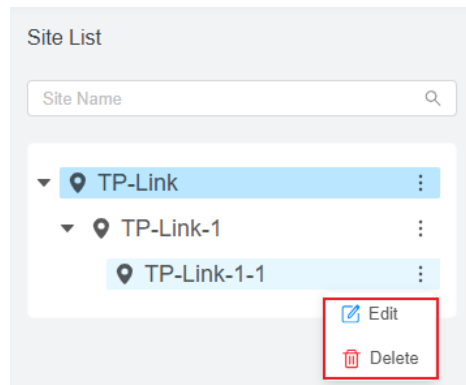
2. Click  in the site list, then you can:

- Click  Add to create a sub Site under the existing site.
- Click  Edit to edit the site's configuration.
- Click  Delete to delete the site and its sub sites.



Note:

- The site hierarchy supports a maximum of three levels. Second-level sites retain full administrative consistency with the first level, while third-level sites are restricted to edit and delete operations only, with no option to create further sub-sites.



♥ 3.2 Manage OLT Devices

➤ Adoption

1. To add a device to the site, go to [Devices](#). The devices which has been discovered by DPMS appear in the list and the status is [Pending](#).

DEVICE NAME	SITE	IP ADDRESS	MAC ADDRESS	STATUS	MODEL	VERSION	UPTIME	ACTION
DS-P7001-08_000000	--	192.168.1.1	00-00-00-00-00-00	Pending	DS-P7001-08 1.0	1.0.0 Build 20210604 Rel.13642	3h 44m 0s	✓ ✗

Showing 1-1 of 1 records < 1 > 10 / page

2. Select the device and click [✓](#). Select the desired site and enter the username and password to adopt the device. Then click [Apply](#).

Adopt

Site:

UserName:

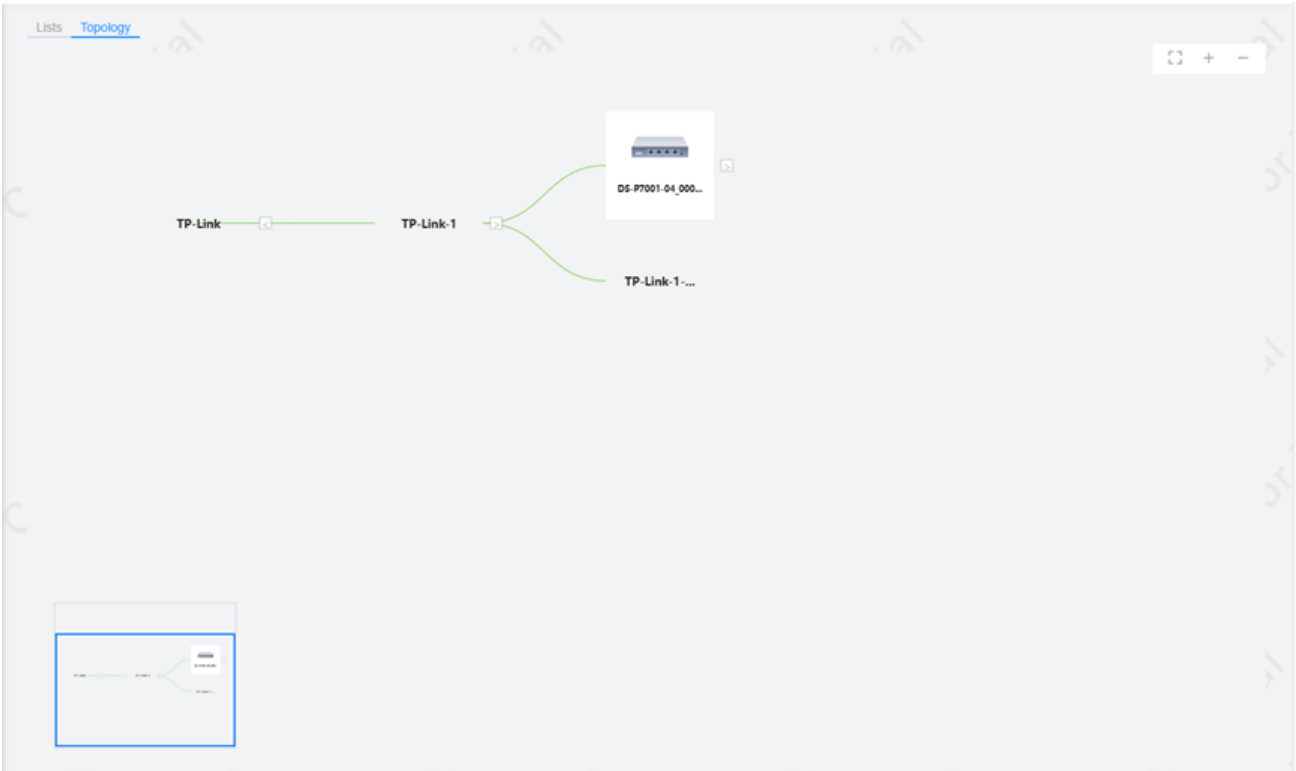
Password:

[Apply](#) [Cancel](#)

3. Go to [Site](#). Select the site from the site list, then the devices of the site and its sub-sites will be displayed in the device list.

The screenshot shows the DPMS interface with two main panels. On the left is the 'Site List' panel, which contains a search bar and a tree view showing a hierarchy: 'TP-Link' (selected), 'TP-Link-1', and 'TP-Link-1-1'. On the right is the 'Device List' panel, which displays a table of devices for the selected site. The table has columns for Device Name, Site, IP Address, MAC Address, Status, Model, Version, and Uptime. The first device shown is 'DS-P7001-04_000002' with status 'Online'. Red boxes highlight the 'SITE' column in the table and the 'TP-Link-1' sub-site in the tree view. Red text labels 'Sub-site' and 'Device List' are placed below the respective elements.

4. In the [Topology](#) tab, you can view all the connections between OLTs and ONUs, getting a clear overview of the network structure between the site and its sub-sites.



After you adopt the devices, you can view the basic information of the devices and perform basic operations on the devices according to your needs. You can go to the individual page of an OLT to configure its network.

➤ **Configuration**

1. Go to [Devices](#), you can view the basic information of the devices in a list. You can select which kinds of devices to display in the list, whether OLTs or ONUs. Also, you can choose to display the devices of a certain status by selecting a tab. If you have many devices, you can search the information of certain devices using the search bar.

OLT(1)

ONU(0)

All(1)

Online(1)

Pending(0)

Offline(0)

Search

Discard List

Batch

DEVICE NAME	SITE	IP ADDRESS	MAC ADDRESS	STATUS	MODEL	VERSION	UPTIME	ACTION
DS-P7001-08_000000	TP-Link	192.168.0.1	00-00-00-00-00-00	Online	DS-P7001-08 1.0	1.0.0 Build 20210604 Rel.13642	49m 51s	

Device Name	OLT Name.
Site	Site Name
IP Address	OLT Device IP Address
MAC Address	The deviceKey is the MAC address of OLT device

Status	OLT device detail status.		
	Online: The device has been adopted by DPMS and it is powered on and connected to the network.		
	Pending: The device has been discovered by DPMS and has not been adopted.		
	Offline: The device has been adopted by DPMS but it is powered off or disconnected from the network.		
Model	OLT model.		
Version	OLT Device firmware Version.		
Uptime	Time of the device running since this booting.		
Action	OLT Operation: rebooting, moving to another site, removing, denying, and editing the device.		

2. In the **ACTION** column, you can perform basic operations on the device, including upgrading, rebooting, moving to another site, removing, denying, and editing the device. Alternatively, you can click  **Batch** and select the operations to perform on devices in batches.

OLT(1) ONLINE(0) All(1) Online(1) Pending(0) Offline(0) Search									
Discard List Batch									
DEVICE NAME	SITE	IP ADDRESS	MAC ADDRESS	STATUS	MODEL	VERSION	UPTIME	ACTION	
DS-P7001-08_000000	TP-Link	192.168.0.1	00-00-00-00-00-00	Online	DS-P7001-08 1.0	1.0.0 Build 20210604 Rel.13642	49m 51s		



To manually upgrade the device, click the button and a window pops up. Click **Upload** to upload a firmware file and set the other parameters. Then click **Upgrade**.



To reboot the device, click the button and a window pops up. Set the parameters and click **Reboot**. It is recommended that you save the current configuration before reboot.



To move the device to another site, click the button and a window pops up. Select the desired site where you want to move the device and click **Apply**.



To remove, deny or edit the device, click the button and select the option according to your needs. If you remove the device, it is only deleted from the device list. If you deny the device, it is deleted from the device list and added to the deny list.

- You can click the device name to go to the individual page of the OLT and configure its network. For detailed configurations on this page, refer to the User Guide of OLTs.



DS-P7001-08_000000

[Back to Device List](#)

[Save the Configuration](#)

PON

PON Port

Profile

ONU Register

ONU Management

Service Port

L2 Feature

L3 Feature

Multicast

Qos Management

Security

Maintenance

System

[Port Information](#) [Port Config](#)

Line List

[Refresh](#)

PORT ID	STATUS	ONLINE ONU NUMBER	MAXIMUM AVAILABLE BANDWIDTH	BANDWIDTH IN USE	REMAINING BANDWIDTH	OPTICAL VCC	OPTICAL BIAS	OPTICAL POWER
PON 1/0/1	● Enable	0	1242432 kbps	0 kbps	1212928 kbps	3.36 V	14.98 mA	5.01 dBm
PON 1/0/2	● Enable	--	--	--	--	--	--	--
PON 1/0/3	● Enable	--	--	--	--	--	--	--
PON 1/0/4	● Enable	--	--	--	--	--	--	--
PON 1/0/5	● Enable	--	--	--	--	--	--	--
PON 1/0/6	● Enable	--	--	--	--	--	--	--
PON 1/0/7	● Enable	--	--	--	--	--	--	--
PON 1/0/8	● Enable	--	--	--	--	--	--	--

Showing 1-8 of 8 records < 1 > 10 / page

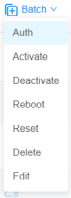
♥ 3.3 Manage ONU Devices

➤ ONU Operation

Go to [DPMS > Device](#) page, and select the ONU device list.

ONU Description	Serial Number	Connected OLT	Pon Port Id	ONU ID	Site	MAC Address	Online Status	Admin Status	Action
2	--	DS-PT001-08_13A23Ca	GPON 1/0/1	22	#	--	Offline	✓ A	⏻ ⌂ ⋮
--	--	DS-PT001-08_13A23Ca	GPON 1/0/2	3	#	--	Offline	✓ A	⏻ ⌂ ⋮
--	TPLG-7937EB40	DS-PT001-08_13A23Ca	GPON 1/0/3	3	#	--	Offline	✓ A	⏻ ⌂ ⋮
--	TPLG-54752498	DS-PT001-08_13A23Ca	GPON 1/0/5	2	#	--	Offline	✗ D	⏻ ⌂ ⋮
--	TPLG-12345677	DS-PT001-08_13A23Ca	GPON 1/0/3	#	--	--	Online	✗ D	⏻ ⌂ ⋮

ONU Description	The description of this ONU.
Serial Number	The Serial number of ONU.
Connected OLT	The name of the OLT to which the ONU is connected.
Pon Port Id	The PON port ID where the registered and online ONT is located.
ONU ID	(Optional) Specify the ONU ID. If not specified, the system automatically assigns the lowest available ONU ID under the current port.
Site	The name of the site where the OLT to which the ONU belongs is located.
MAC Address	The MAC Address of the ONU.
Online Status	The ONU online status. • ONLINE: Status before reboot or after successful reboot. • REBOOTING: Status during reboot (displayed briefly). • OFFLINE: Status when reboot fails and connection cannot be restored.
Config Status	The configuration status. • SUCCESS: The configuration is successfully issued and recognized by the ONU. • FAILED: The configuration delivery failed or ONU recognition failed.
Match Status	The ONU match status. • MATCH: The ONU hardware capability is consistent with the bound service profile. • MISMATCH: The ONU hardware capability is inconsistent with the bound service profile.
Active Status	The ONU Active status.
Model	ONU device model.
Action	Supported ONU operations: Auth, Activate, Deactivate, Reboot, Reset, Delete, Edit.

	Activate the currently inactive ONU device as needed.
	Deactivate the currently activated ONU device as needed.
	Restart the current online ONU device as needed.
	Edit the customer information of the current ONU device as needed.
	Perform the Edit/Delete/Auth operation on the ONU of the current model as needed. Edit: Edit the registered configuration profile. Auth: Issue registration profiles to unregistered ONUs. Delete: Delete registered and unregistered ONUs. Reset: Reset the current online ONU device as needed.
	According to the operation of multiple models, the ONU Batch operation can be selected to perform batch tasks of Auth/Activate/ Deactivate/Reboot/Reset/Delete/Edit on ONUs under the same OLT.

➤ ONU Single Operation

1. **Auth Current ONU:** Click  and select **Activate** to activate unregistered devices.

ONU Authentication ×

ONU ID :

(Optional, 0-127)

Authentication Method :

SN-Auth

▼

Line Profile :

0 (default)

▼

Service Profile :

0 (default)

▼

ONU Management Profile :

▼

(Optional)

Service Port Profile :

▼

(Optional)

Description :

(Optional,1-32 characters)

Apply

Cancel

ONU Authentication ×

ONU ID :

(Optional, 0-127)

Authentication Method :

Password-Auth

▼

Discovery Mode :

Always ON

▼

Line Profile :

0 (default)

▼

Service Profile :

0 (default)

▼

ONU Management Profile :

▼

(Optional)

Service Port Profile :

▼

(Optional)

Description :

(Optional,1-32 characters)

Apply

Cancel

ONU Authentication ×

ONU ID : (Optional, 0-127)

Authentication Method : ▾

Discovery Mode : ▾

Re-Register-Authentication : Loid-Auth

Line Profile : ▾

Service Profile : ▾

ONU Management Profile : ▾ (Optional)

Service Port Profile : ▾ (Optional)

Description : (Optional, 1-32 characters)

Apply

Cancel

ONU Authentication ×

ONU ID : (Optional, 0-127)

Authentication Method : ▾

Line Profile : ▾

Service Profile : ▾

ONU Management Profile : ▾ (Optional)

Service Port Profile : ▾ (Optional)

Description : (Optional, 1-32 characters)

Apply

Cancel

ONU Authentication

ONU ID :

(Optional, 0-127)

Authentication Method :

Loid-and-Password-Auth

Discovery Mode :

Always ON

Re-Register-Authentication :

Loid-Password-Auth

Line Profile :

0 (default)

Service Profile :

0 (default)

ONU Management Profile :

(Optional)

Service Port Profile :

(Optional)

Description :

(Optional,1-32 characters)

Apply

Cancel

ONU ID	(Optional) Specify the ONU ID. If not specified, the system automatically assigns the lowest available ONU ID under the current port.
Authentication Method	The authentication mode, including SN-Auth , Password-Auth , Loid-Auth , SN-and-Password-Auth , and Loid-and-Password-Auth .
Line Profile	The bound line profile for this ONU. The value should be the combination of the management profile's ID and name.
Service Profile	The bound service profile for this ONU. The value should be the combination of the management profile's ID and name.
ONU Management Profile	The bound management profile for this ONU. The value should be the combination of the management profile's ID and name.
Service Port Profile	The bound service port profile for this ONU. The value should be the combination of the management profile's ID and name.
Description	The description of this ONU.
SN-Value	The Serial number of ONU.
Password	The authentication password of ONU.
Loid	The authentication Loid of ONU.

Loid Password	The authentication Loid password of ONU.
Discovery Mode	Select the mode to discover the ONU when the ONU goes online again. Always-On: When the ONU goes online again, the OLT does not check the SN of the ONU. The ONU can still go online even though the ONU SN is changed. Once-On: The ONU is required to start authentication within the specified time, and cannot go online if the specified time period expires. The SN of the ONU cannot be modified once the ONU passes the authentication. Discovery Mode is only available for the Authentication Method of Password-Auth, LOID-Auth, and LOID-and-Password-Auth.
Re-Register-Authentication	Select the mode to re-authenticate the ONU when the ONU goes online again. SN: The ONU is re-authenticated using the SN. SN-Password: The ONU is re-authenticated using the SN and password. Re-Register-Auth-Mode is only available when the Authentication Method is Password-Auth and Discovery Mode is Once-On.

2. **Edit ONU Authentication Detail:** Click  and select **Edit** to edit the registered device.

Edit ONU Authentication

PON Port ID :

GPON 1/0/3

ONU ID :

12

Authentication Method :

SN-Auth

SN-Value :

TPLG-00F629C8

(12, 13, or 16 characters)

Line Profile :

0(default)

Service Profile :

0(default)

ONU Management Profile :

(Optional)

Service Port Profile :

(Optional)

Description :

22

(Optional,1-32 characters)

Apply

Cancel

3. **Edit Customer Information:** Click  and edit customer information.

×

Basic Information

Network Name :

(Optional, 1-64 characters)

User Name :

(Optional, 1-64 characters)

User Status :

▼

(Optional)

Phone Number :

(Optional, 1-20 characters)

Email :

(Optional, 1-64 characters)

Operator :

▼

(Optional)

City :

(Optional, 1-64 characters)

Address :

(Optional, 1-64 characters)

Subscription Plan

Download :

Mbps ▼

(Optional, 1-1024)

Upload :

Mbps ▼

(Optional, 1-1024)

Subscription Date :

(Optional)

Cancel

Clear

Save

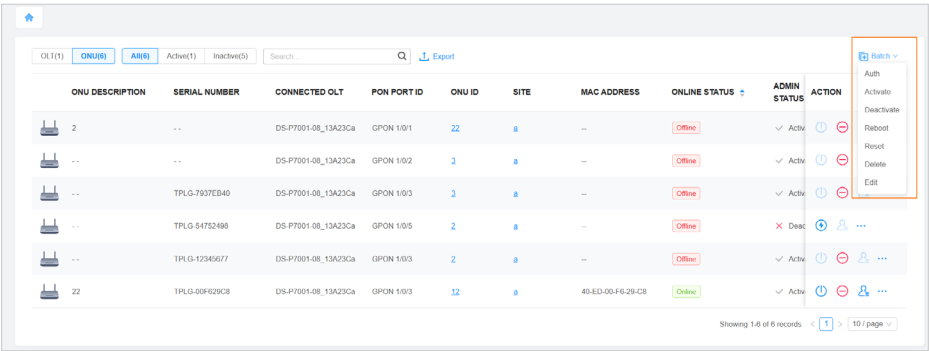
4. **Activate/Deactivate/Restart/Delete/Reset:** Click the corresponding button will take effect.

Network Name	The current network where ONU is located.
User Name	ONU subscriber name.
User Status	ONU subscriber status.
Phone Number	ONU subscriber phone number.
Email	ONU subscriber email.
Operator	Maintain the operator ID for this terminal network. The operator must be an existing account in DPMS.
City	ONU subscriber city.
Address	ONU subscriber home address.
Download	Subscriber plan download speed.

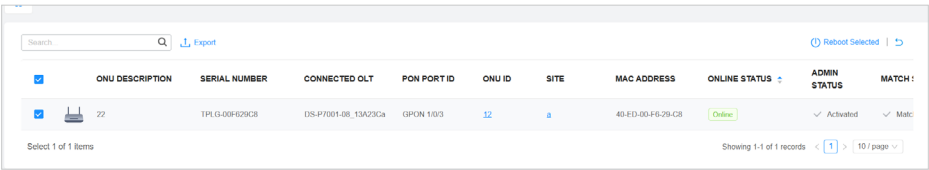
Upload	Subscriber plan upload speed.
Subscription Date	Subscriber plan activation time.

➤ **ONU Batch Operation**

1. Navigate to the ONU List homepage, click the **Batch** button, and then select **Auth/Activate/Deactivate/Reboot/Reset/Delete/Edit** as needed.



2. Check the box(es) for devices of the same model in the device list, and then click **Auth/Activate/Deactivate/Reboot/Reset/Delete/Edit Selected** as needed.



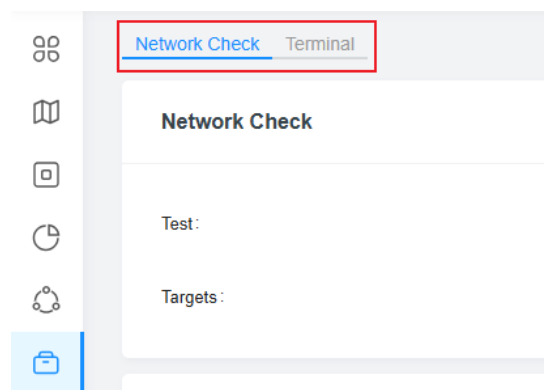
 Activate Selected	Batch activate ONUs under the same OLT.
 Edit Selected	Batch edit ONUs under the same OLT.
 Delete Selected	Batch delete ONUs under the same OLT.
 Deactivate Selected	Batch deactivate ONUs under the same OLT.
 Auth Selected	Batch auth ONUs under the same OLT.
 Reboot Selected	Batch reboot ONUs under the same OLT.
	Return to ONU list homepage.

♥ 3.4 Network Tools

The Network Tools section provides commonly used tools for network diagnostics tools and device access. You can run [Ping tests](#) or perform [Traceroute path tracing](#) directly against online devices to quickly verify network connectivity and troubleshoot latency and routing/path issues. In addition, on the [Terminal](#) tab, you can log in to a device's command-line interface (CLI) for advanced configuration and in-depth troubleshooting tasks.

➤ Network Check

1. Go to [Network Tools](#) page, including two tabs: [Network Check](#) and [Terminal](#).



2. Perform network check, taking Ping and Traceroute as an example: Go to the [Network Check](#) tab , configure the [Targets](#), [Packet Size](#), and [Count](#), then click [Run](#) to start the test.

A screenshot of the 'Network Check' configuration form. At the top, there are two tabs: 'Network Check' and 'Terminal'. The 'Network Check' tab is active. Below the tabs, the form is titled 'Network Check'. It contains two main sections. The first section has a 'Test:' dropdown menu set to 'Ping' and a 'Targets:' dropdown menu containing the IP address '00-00-00-00-01-03' with a close button 'X'. The second section is titled 'Advanced Test Settings' and contains two input fields: 'Packet Size:' with a value of '32' and a range '(10-1472)', and 'Count:' with a value of '4' and a range '(1-100)'. At the bottom left of this section is a blue 'Run' button.

Test Type	Select a test to run: Ping or Traceroute.
Target Device	Select one or more online target devices from the list.
Packet Size (Ping)	(Ping only) Specify the send buffer size.
Request Count (Ping)	(Ping only) Specify the number of Ping requests to send.
Max Hops (Traceroute)	(Traceroute only) Specify the maximum number of hops allowed when tracing the route to the target.

View Test Results: Test results are displayed in the [Device Output](#) section.

Multi-device tests: When multiple target devices are selected, the left pane displays results for each device as separate tabs. Click a tab to switch between devices and view the corresponding output.

Result interpretation: The output includes key diagnostic information such as per-packet round-trip time (RTT), TTL, and the response status of each hop/node along the path.

Advanced Test Settings

Packet Size:

32

(10-1472)

Count:

4

(1-100)

Run

Device Output

00-00-00-00-01-03

Output for the device: 00-00-00-00-01-03

```

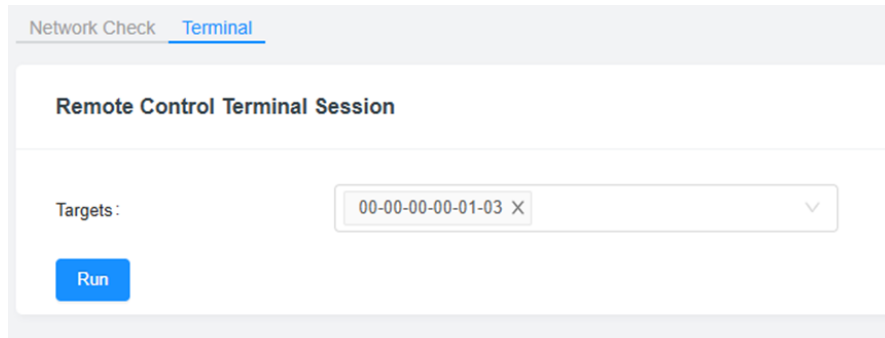
-----
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

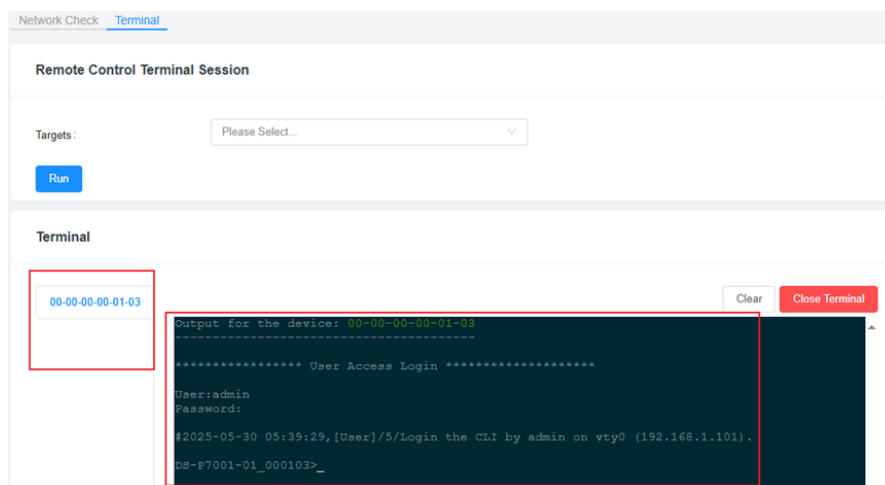
➤ Terminal

In the [Terminal](#) tab, you can connect to the selected device's command-line interface (CLI) directly via [Telnet](#), and run advanced configuration and troubleshooting commands.



Follow the steps:

1. **Select Devices and Start:** Select one or more target devices from the list, and click [Run](#).
2. **Start Terminal Sessions:** The system automatically opens a dedicated terminal page for each selected device.
3. **Log In to the Device:** Follow the prompts and enter the device username and password in the corresponding terminal to complete login.
4. **Run Commands:** After a successful login, enter commands in the CLI to interact with the device.
5. **Session Management:**
 - **Switch between devices:** If multiple device terminals are open, use the left pane tabs (named by the device MAC address) to switch between sessions.
 - **Clear output:** Click [Clear](#) to remove all output from the current terminal session.
 - **Close terminal:** Click [Close Terminal](#) to end the current session.



4

Configure DPMS

DPMS Settings control the appearance and behavior of DPMS and provide methods of data backup and restore. The chapter includes the following sections:

- [4. 1 General Settings](#)
- [4. 2 Manage DPMS Remotely via Cloud Access](#)
- [4. 3 Maintenance](#)
- [4. 4 Auto Backup](#)
- [4. 5 Task](#)
- [4. 6 Notification Strategy](#)

♥ 4. 1 General Settings

4. 1. 1 Basic Settings

Go to [Settings > General Settings](#). In [Basic Settings](#), configure the parameters and click [Apply](#).

Basic Settings

DPMS Server Name :

TP-Link_DPMS

Time Zone :

(UTC-08:00) Pacific Time (US & Canada)

▼

History Data Retention :

7 Days

▼

Apply

Cancel

DPMS Serever Name	Specify the DPMS Server Name to identify your DPMS.
Time Zone	Select the Time Zone of DPMS according to your region. For DPMS settings, time is displayed based on the Time Zone.
History Data Retention	Select how long DPMS retains its data. Any history data beyond the time range is dropped.

4. 1. 2 Services

Go to [Settings > General Settings](#). In [Services](#), configure the parameters and click [Apply](#).

Services

Alert Emails :

Send similar alerts within

60

seconds in one email.

Remote Logging :

Syslog Server IP / Host Name :

Syslog Server Port :

(1-65535)

Apply

Cancel

Alert Emails	Enable alert emails: When enabled, DPMS can send emails to notify the administrators, operators and viewers of the alert logs once generated. Send similar alerts within seconds in one email: When enabled, the similar alerts generated in each time period are collected and sent to administrators, operators and viewers in one email. To configure alert-level logs and enable email notifications on DPMS, refer to 5.3.3 Notifications
Remote Logging	With this feature configured, DPMS will send generated logs to the log server. When enabled, the following items are required: Syslog Server IP/Hostname: Enter the IP address or hostname of the log server. Syslog Server Port: Enter the port of the server.

4.1.3 Mail Server

With the Mail Server, DPMS can send emails for resetting your password, pushing notifications, and delivering the system logs. The Mail Server feature works with the SMTP (Simple Mail Transfer Protocol) service provided by an email service provider.

➤ Configuration

- 1. Log in to your email account and enable the SMTP (Simple Mail Transfer Protocol) Service. For details, refer to the instructions of your email service provider.
- 2. Go to [Settings > General Settings](#). In [Mail Server](#), enable SMTP Server and configure the parameters. Then click [Apply](#).

Mail Server

SMTP Server :

With the Mail Server, the DPMS Server can send emails for pushing notifications, and delivering the system logs. Configure Mail Server carefully.

SMTP :

Port :

25

(1-65535)

SSL :

Authentication :

Sender Address :

(Optional)

Test SMTP Server :

Test

Apply

Cancel

SMTP	Enter the URL or IP address of the SMTP server according to the instructions of the email service provider.
Port	Configure the port used by the SMTP server according to the instructions of the email service provider.
SSL	Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between DPMS and the SMTP server.
Authentication	Enable or disable Authentication according to the instructions of the email service provider. If Authentication is enabled, the SMTP server requires the username and password for authentication.
Username	When Authentication is enabled, enter your email address as the username.
Password	When Authentication is enabled, enter the authentication code as the password, which is provided by the email service provider when you enable the SMTP service.
Sender Address	(Optional) Specify the sender address of the email. If you leave it blank, DPMS uses your email address as the Sender Address.
Test SMTP Server	Test the Mail Server configuration by sending a test email to an email address that you specify.

4.1.4 Access Configuration

Go to [Settings > General Settings](#). In [Access Configuration](#), configure the parameters and click [Apply](#).

Access Configuration

DPMS Host Name / IP Address :

HTTPS Port : (443 or 1024-65535)



Once applying the change of HTTPS port, restart the DPMS Server to make the change effective. After restart, visit the URL `https://DPMS Server Host's IP Address or URL:port` number to log in to the DPMS Server.

Apply

Cancel

DPMS Host Name / IP Address	Enter the hostname or IP address of DPMS which will be used as the DPMS URL in the notification email for resetting your DPMS password.
HTTPS Port	Specify the HTTPS port used by DPMS for management. After setting the port, you can visit https://[DPMS Host's IP address or URL]:[Port] to log in to DPMS. Once applying the change of HTTPS port, restart DPMS to make the change effective.

4.1.5 HTTPS Certificate

If you have assigned a domain name to the controller for login, to eliminate the untrusted certificate error message that will appear in the login process, you can import the corresponding SSL certificate and private key. The certificate and private key are issued by the certificate authority.

 Note:

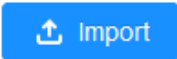
- You need to restart your controller for the imported SSL certificate to take effect.

 Configuration

Go to [Settings > General Settings](#). In [HTTPS Certificate](#), import your SSL certificate and configure the parameters. Click [Save](#).

HTTPS Certificate

SSL Certificate :



Keystore Password :

.....



Private Key Password :

Password

(Optional) 

Apply

Cancel

Keystore Password	Enter the keystore password if your SSL certificate has the keystore password.
Private Key Password	Enter the private key password if your SSL certificate has the private key password. Otherwise, leave it blank.

♥ 4.2 Manage DPMS Remotely via Cloud Access

With [Cloud Access](#), it's convenient for you to manage your DPMS from anywhere, as long as you have access to the internet.

➤ Configuration

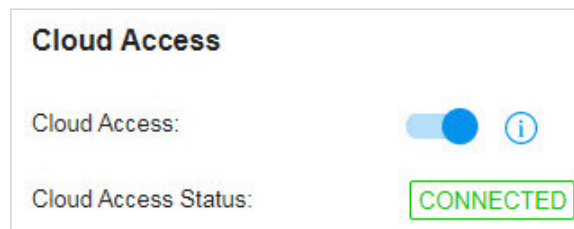
To manage your DPMS from anywhere, follow these steps:

1. Prepare your DPMS for Cloud Access.

ⓘ Note:

- Before you start, make sure your DPMS Host has access to the internet.
- If you have enabled Cloud Access and bound your TP-Link ID in the quick setup wizard, skip this step.

2. Go to [Settings](#) > [Cloud Access](#). Enable [Cloud Access](#).



3. Enter your TP-Link ID and password. Click [Login and Bind](#).

Log in and bind your TP-Link ID

ⓘ Enter the email address and password of your TP-Link ID, which is not the account that you have used to log in to DPMS Server.

TP-Link ID :

admin

No TP-Link ID? [Register now](#)

Password :

••••••••

Login and Bind

Cancel

4. After you have successfully bound the DPMS with your TP-Link ID, you can access the DPMS remotely and enjoy the cloud service on <https://dpms.tplinkcloud.com>.

♥ 4.3 Maintenance

4.3.1 User Interface

You can customize the User Interface settings of DPMS according to your preferences.

➤ Configuration

Go to [Settings > Maintenance](#). In [User Interface](#), configure the parameters and click [Apply](#).

User Interface

Use 24-hour time :

Log/ Statistic/ Dashboard Timezone :

DPMS Server's

▼

Show pending devices :

Refresh Button :

Refresh Interval :

2 minutes

▼

Apply

Cancel

Use 24-Hour Time	With Use 24-Hour Time enabled, time is displayed in a 24-hour format. With Use 24-Hour Time disabled, time is displayed in a 12-hour format.
Log/Statistic/Dashboard Timezone	Select which Timezone the time of statistics and the dashboard is based on. Browser's (PC): Browser's Timezone is synchronized with the browser configuration. DPMS Server's: DPMS Server's Timezone is set in General Settings of DPMS. UTC: UTC (Coordinated Universal Time) is the common time standard across the world.
Show Pending Devices	With this option enabled, the devices in Pending status will be shown, and you can determine whether to adopt them. With this option disabled, they will not be shown, thus you cannot adopt any new devices.
Refresh Button	Enable or disable Refresh Button in the upper right corner of the configuration page.
Refresh Interval	Select how often the controller automatically refreshes the data displayed on the page.

4.3.2 Backup & Restore

You can backup the configuration and data of your DPMS to prevent any loss of important information. If necessary, restore DPMS to a previous status using the backup file.

➤ Configuration

■ Backup

Go to [Settings](#) > [Maintenance](#). In [Backup & Restore](#), select the time range in the drop-down menu of [Data Backup Retention](#). Only configuration and data within the time range is backed up. If you select [Settings Only](#), only configuration (no data) is backed up. Click [Download Backup Files](#) to download the backup file to your computer.

Backup & Restore

Backup

Backup Data Retention :

Settings Only



[Download Backup Files](#)

Restore

Restore File :

Please select a file.

[Browse](#)

[Restore](#)

■ Restore

Go to [Settings](#) > [Maintenance](#). In [Backup & Restore](#) section, Click [Browse](#) and select a backup file from your computer. Click [Restore](#).

Backup & Restore

Backup

Backup Data Retention :

Settings Only



[Download Backup Files](#)

Restore

Restore File :

Please select a file.

[Browse](#)

[Restore](#)

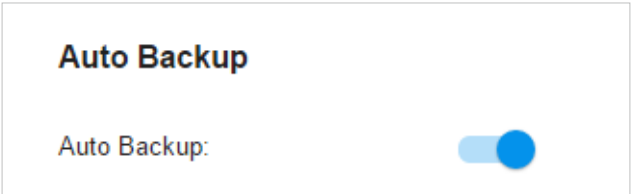
♥ 4.4 Auto Backup

With Auto Backup enabled, DPMS will be scheduled to back up the configurations and data automatically at the specified time. You can easily restore the configurations and data when needed.

➤ Configuration

To configure [Auto Backup](#), follow these steps:

1. Go to [Settings > Auto Backup](#). Click  to enable [Auto Backup](#).



2. Configure the following parameters to specify the rules of [Auto Backup](#). Click [Apply](#).

Auto Backup

Auto Backup:



 Please set the time for Auto Backup at night, because the system cannot perform any operation during Auto Backup.

Occurrence :

Every

Month

at

1

at

02:00

in (UTC-08:00) Pacific Time (US & Canada)

Maximum Number of Files :

7

(1-50)

Data Retention Days :

30 Days

Apply

Cancel

Occurrence

Specify when to perform Auto Backup regularly. Select [Every Day](#), [Week](#), [Month](#), or [Year](#) first and then set a time to back up files. Note the time availability when you choose [Every Month](#). For example, if you choose to automatically backup the data on the 31st of every month, Auto Backup will take effect on the last day of the month when it comes to the month with no 31st, such as February, April, and June.

Maximum Number of Files

Specify the maximum number of backup files to save.

Select the length of time in days that data will be backed up.

Data Retention Days

[Settings Only](#): Back up DPMS settings only.

[7 Days/30 Days/60 Days/90 Days/180 Days/365 Days](#): Back up the data in the recent 7 Days/30 Days/60 Days/90 Days/180 Days/365 Days.

[All Time](#): Back up all data in DPMS.

3. You can view the name, backup time and size of backup files in [Available Backup Files](#).

Available Backup Files			
FILE NAME	BACKUP TIME	SIZE	ACTION
autobackup_30days_20200525_1026.cfg	2020-05-25 10:26:00 am	7.37 KB	  

4. To restore, export, or delete the backup file, click the icon in the [Action](#) column.



Restore the configurations and data in the backup file. All current configurations will be replaced after the restoration.

To keep the backup data safe, please wait until the operation is finished. This will take several minutes.



Export the backup file. The exported file will be saved in the saving path of your web browser.



Delete the backup file.

▼ 4.5 Task

In the DPMS Tasks module, you can create task templates, configure the required parameters, filter devices that meet specific criteria, and schedule bulk device upgrades or bulk configuration backup operations to run at a specified time.

4.5.1 Create Task

General Settings

Go to [Task](#) page, click the [add](#) button to create a new task, and fill in the [Task Profile](#) information.

<

Add New Task

Task Profile

Profile Name :

Sites:

Please Select...

Device Type:

▼

Model:

▼

When the model meets all these conditions:

No matching conditions added.

Add Condition

Then do the following:

Firmware Upgrade

▼

Deployed Devices:

Get Details

Profile Name	The name of the Task Profile.
Site	Select the Site where the target devices are located. You can choose All to include devices across all sites. If a specific site is selected, its sub-sites are not included.
Device Type	The device type. Options: OLT, ONU.
Model	The device model. This field becomes configurable after selecting Site and Device Type . The drop-down list shows all model categories for the selected device type within the selected site.

 Create a Bulk OLT Upgrade / Config Backup Task

1. Configure the **Create Task** parameters, and set **Device Type** to **OLT**.

- 2. Filter and select the applicable model. The drop-down list will display all model information under the selected site.
- 3. Add Condition: Introduce filter criteria so that only devices meeting the conditions are included in the TASK device list. Click [Add Condition](#) to select a condition from the drop-down list, choose an operator, and specify the condition value.

When the model meets all these conditions:

Firmware Version

=

×

Then

Firmware Version

MAC Address List

IP Address

Firmware Version	Device firmware version.
Mac Address List	Device MAC address list (required format: .xlsx file)
IP Address	Device IP address.

- 4. Then do the following:

Then do the following:

Firmware Upgrade

Firmware Upgrade

Scheduled Config Backup

- 1) **To create a bulk OLT firmware upgrade task:** select Firmware Upgrade, then click [Please click to upload a file](#) to upload the firmware image you want to deploy.

You can click [Get Details](#) of **Deployed Devices** to view how many devices match the current filter conditions before creating/running the task.

Please click to upload a file

- 2) **To create a bulk OLT Config Backup task:** select [Schedule Config Backup](#), then select the target export path.

Export to:

☐ Local Path
(/data/olt_config_auto_backup)

☒ Remote Server

File Path:

Type:

FTP

▼

Server Hostname/IP:

Port:

(1-65535)

FTP Username:

FTP Password:

Local Path

Local path. By default set to `/data/olt_config_auto_backup`.

Remote Server

Type:

TFTP

^

Server Hostname/IP:

FTP

TFTP

Optional. Configure a remote FTP/TFTP server and specify the required FTP/TFTP server parameters.

5. Set the [Upgrade Schedule](#) / [Backup Schedule](#) and specify the execution time for the upgrade/ backup task.

Upgrade:

Upgrade Schedule

Timezone:

(UTC+08:00) China Standard Time

▼

Current Time:

2025-09-01 16:39:31

Start Date:

End Date:

Daily Update Time:

Start Time

🕒

→

End Time

🕒

Backup:

Backup Schedule

Timezone:

(UTC+08:00) China Standard Time

▼

Current Time:

2025-09-04 15:41:29

Start Date:

End Date:

Repeat:

Every

Month

▼

On

1

▼

At

17:30:00

🕒

Save

Cancel

Time Zone	Select and specify the time zone.
Current	The current time in the selected time zone.
Start Date	The start date of the schedule window.
End Date	The end date of the schedule window.
Daily Update Time / Repeat	For a Firmware Upgrade task, configure Daily Update Time to define the daily upgrade time window. Daily Update Time : Start Time ⌚ → End Time ⌚ For a Config Backup task, configure Repeat to define the backup recurrence interval. Repeat : Every Month ▾ On 1 ▾ At Select time ⌚

6. Click [Save](#).

➤ **Create a Bulk ONU Firmware Upgrade Task**

1. Configure the [Create Task](#) parameters, and set [Device Type](#) to [ONU](#).
2. Filter and select the applicable model. The drop-down list will display all model information under the selected site.
3. Add Condition: Introduce filter criteria so that only devices meeting the conditions are included in the TASK device list. Click [Add Condition](#) to select a condition from the drop-down list, choose an operator, and specify the condition value.

When the model meets all these conditions:

Firmware Version ^

= ▾

▾

×

Then

Firmware Version

MAC Address List

OLT MAC Address List

Firmware Version	Device firmware version.
Mac Address List	Device MAC address list (required format: .xlsx file) If you want to target ONU devices under specific OLT(s), configure this option to limit the ONU selection scope to ONUs associated with the specified OLT(s).

4. Create a bulk ONU firmware upgrade task: select [Firmware Upgrade](#), then click [Please click to upload a file](#) to upload the firmware image you want to deploy.

Please click to upload a file

5. Configure the **FTP server** that hosts the ONU upgrade firmware file (FTP server address and related access parameters as required)

Then do the following:

Firmware Upgrade

FTP Server :

Username :

(1-32 characters)

Password :

Password

(1-32 characters)

File Name :

(1-64 characters)

Deployed Devices :

[Get Details](#)

You can click **Get Details** of **Deployed Devices** to view how many devices match the current filter conditions before creating/running the task.

6. Configure the **Upgrade Schedule** and specify the planned upgrade execution time window.

Upgrade Schedule

Timezone :

(UTC+08:00) China Standard Time

Current Time :

2025-09-01 16:39:31

Start Date :

2025-09-16

End Date :

2025-09-24

Daily Update Time :

Start Time

→

End Time

Time Zone	Select and specify the time zone.
Current	The current time in the selected time zone.
Start Date	The start date of the schedule window.
End Date	The end date of the schedule window.
Daily Update Time	For a Firmware Upgrade task, configure Daily Update Time to define the daily upgrade time window. Daily Update Time : Start Time → End Time

7. Click **Save**.

4. 5. 2 Manage Task

In the [Task](#) page, you can manage tasks, view each task’s execution status, and edit or delete the task.

Tasks

Filter Name, Model

Filter

Firmware Upgrade(2)

Scheduled Config Backup(0)

Task Data

+ Add

☐	PROFILE NAME	TASK TYPE	SITES	DEVICE TYPE	MODEL	PROGRESS (COMPLETED / IN PROGRESS / FAILED)	EXECUTION TIME PERIOD	ACTION
☐	TASK-OLT-UPGRADE	Firmware Upgrade	TP-Link, TP-Link-1.1, TP-Link-1	OLT	DS-P7881-04 1.0	0 / 1 / 0	2025/09/11 - 2025/09/30 06:15 pm - 09:30 pm	...
☐	TASK-ONU	Firmware Upgrade	TP-Link, TP-Link-1.1, TP-Link-1	ONU	X2005-07	0 / 1 / 0	2025/09/10 - 2025/09/26 07:05 pm - 11:35 pm	...

Showing 1-2 of 2 records

1

>

<

10 / page

All

All tasks.

Firmware Upgrade

Firmware upgrade tasks.

Schedule Config Backup

Scheduled configuration backup tasks.

Task Progress icon. Click to view the execution progress, including number of devices completed, number of devices pending, number of devices in progress, and number of devices failed.

Click [Export](#) to export the device list and execution status.

Click to open the drop-down menu. In the pop-up dialog, click [Edit](#) to modify the task, or click [Remove](#) to delete the task.

...

Edit

Remove

54

♥ 4.6 Notification Strategy

In this section, you can configure Email Notifications, Remote Logging, SNMP Traps, and Webhooks. After the configuration is complete, enable the required feature(s) to push system logs to the specified remote destination(s).

4.6.1 Enable Notification

In the configured Email Notifications, Remote Logging, SNMP Traps, and Webhooks profiles, you can enable log forwarding for specific log modules as needed.

Enable Notifications

Email: ☒ Remote Logging: ☐ SNMP Trap: ☐ Webhook: ☐

☐ Operation ☐ System ☐ OLT ☐ ONU

4.6.2 Email

You can select [Immediate](#), [30 Minutes](#), [1 Hour](#), [1 Day](#), or set a [Custom](#) interval for notification interval.

Notification Interval: Immediate

SMTP:

Port:

SSL:

Immediate
30 Minutes
1 Hour
1 Day
Custom

4.6.3 Remote Logging

Click and complete the following settings:

Add Entry

Syslog Server IP / Host Name :

Syslog Server Port:

(1-65535)

TLS:

Apply

Cancel

Syslog Server IP / Host Name	The address of the configured remote logging (syslog) server (IP address or hostname).
Syslog Server Port	The port used by the configured remote logging (syslog) server.
TLS	Toggle to enable or disable TLS encryption for log transport.

4.6.4 SNMP

- Click [+ Add User](#) to add an SNMP user configuration. You can click [Export MIB](#) to download the DPMS SNMP MIB file for use.

Add User

Security Model :

v3

▼

Username :

Receiving Server IP :

(Format: 192.168.0.1)

Receiving Port :

(1-65535)

Security Level :

NoAuthNoPriv

AuthNoPriv

☒ AuthPriv

Authentication Mode :

☒ MD5

SHA

Authentication Password :

Password

(16 characters maximum)

Privacy Mode :

☒ DES

Privacy Password :

Password

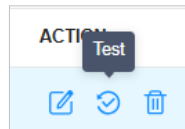
(16 characters maximum)

Apply

Cancel

Security Model	The SNMP security model. Options: v1, v2c, v3.
Username	SNMP username.
Receiving Server IP	SNMP server IP address.
Receiving Port	SNMP server port.
Security Level	SNMP security level. Options: NoAuthNoPriv, AuthNoPriv, AuthPriv.
Authentication Mode	Authentication algorithm. Required when Security Model = v3 and Security Level = AuthNoPriv or AuthPriv.
Authentication Password	Authentication password. Required when Security Model = v3 and Security Level = AuthNoPriv or AuthPriv.
Privacy Mode	Privacy (encryption) algorithm. Required when Security Model = v3 and Security Level = AuthPriv.
Privacy Password	Privacy (encryption) password. Required when Security Model = v3 and Security Level = AuthPriv.

2. After the configuration is complete, you can click  to send a test SNMP Trap message.



3. On the configured SNMP server (trap receiver), you should see SNMP trap output similar to the following.

```
receive snmp trap message...
snmp trap message oid[1.3.6.1.2.1.1.3.0], variable[124940]
snmp trap message oid[1.3.6.1.6.3.1.1.4.1], variable[1.3.6.1.4.1.11863.1]
snmp trap message oid[1.3.6.1.4.1.11863], variable[This is test snmp trap]
```

4. 6. 5 Webhook

1. Click  to configure.

Create Webhook

Name :

Shared Secret :

(Optional) 

URL :

+ Add URL

Payload Template :

DPMS

Retry Policy :

☒ None

☐ Important (Up to 5 retries over 60 minutes)

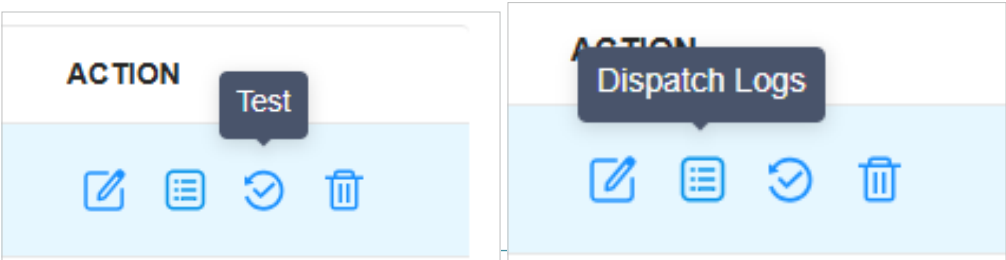
☐ Critical (Up to 5 retries over 24 hours)

Apply

Cancel

Name	Webhook configuration name. Must be unique.
Shared Secret	Optional pre-shared authentication/verification secret. If not specified, the system auto-generates one. The receiver can use the shared secret to validate webhook requests (for example, via HMAC signature verification, depending on implementation).
URL	The destination URL to which webhook messages are sent. You can configure multiple URLs. In general, use an HTTPS (TLS-enabled) endpoint.
Payload Template	Select the payload template/format used to construct the webhook message body (for example, predefined JSON schemas).
Retry Policy	Defines the retry behavior when delivery fails (for example, retry attempts and backoff/interval).

2. After the configuration is complete, click  to send a test webhook message, or click  to view the delivery result.



5

Monitor the Network

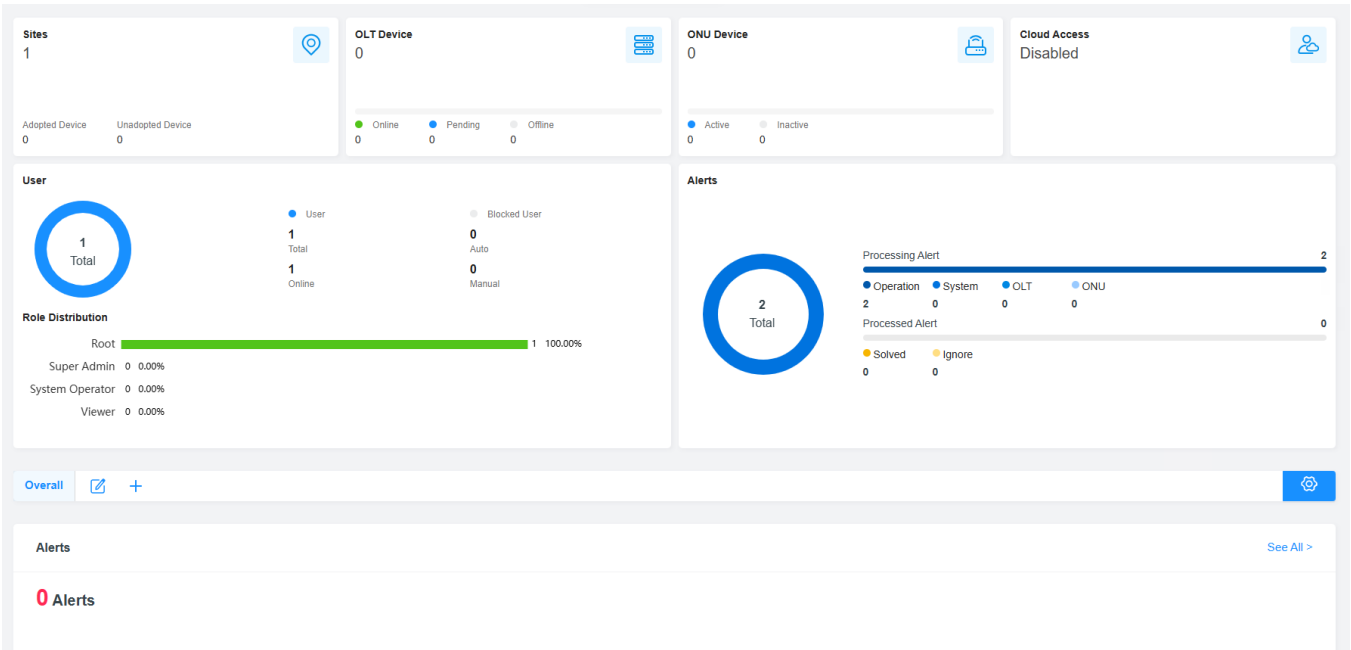
This chapter guides you on how to monitor the network devices and their statistics. Through visual and real-time presentations, DPMS keeps you informed about the accurate status of the managed network. The chapter includes the following sections:

- [5. 1 View the Status of Network with Dashboard](#)
- [5. 2 View the Statistics of the Network](#)
- [5. 3 View and Manage Logs](#)

♥ 5.1 View the Status of Network with Dashboard

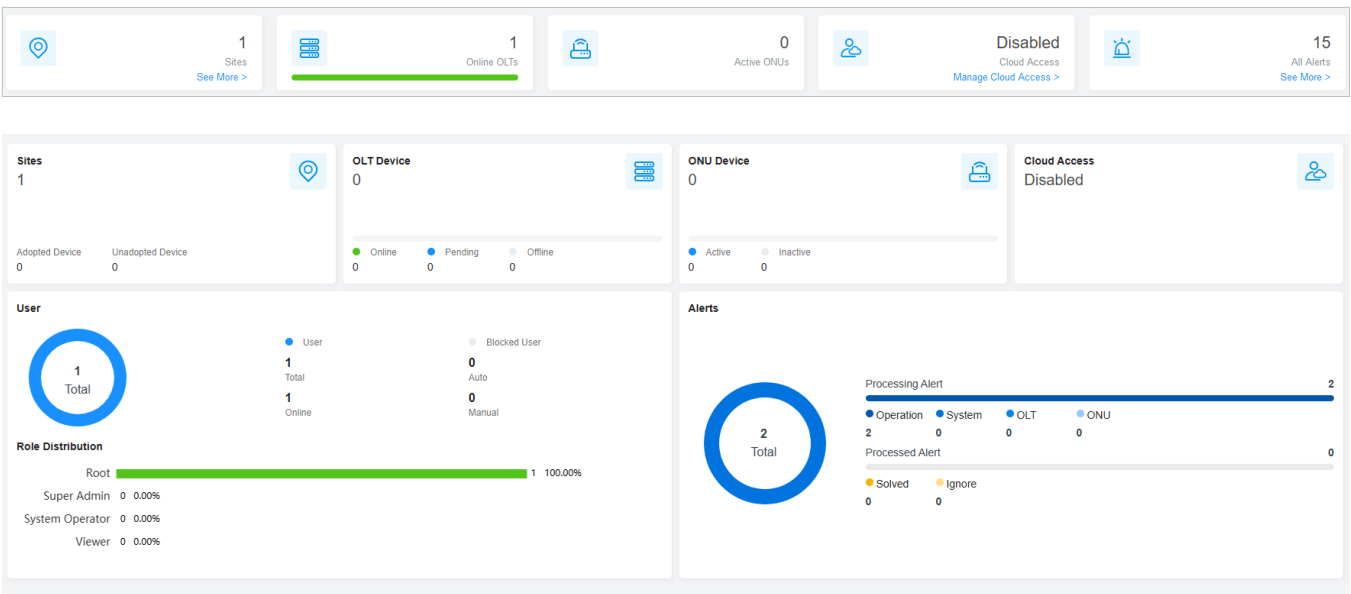
5.1.1 Page Layout of Dashboard

Dashboard is designed for a quick real-time monitor of the network. An overview of network is at the top of Dashboard, and the below is a tab bar followed with customized widgets.



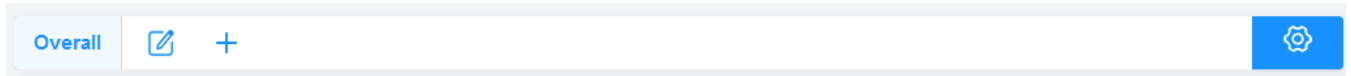
Network Overview

Network Overview on the top shows the numbers of sites, devices, and alerts, and the status of Cloud Access.



Tab Bar

You can customize the widgets displayed on the tab for Dashboard page. The Overall tab is created by default and cannot be deleted.



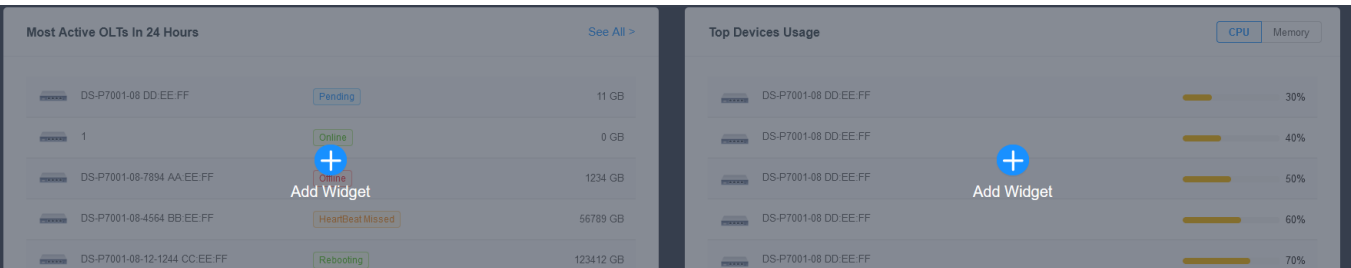
Overall	Displays OLT Devices, ONU Devices, Alerts, Top Device Usage, and Most Active OLTs in 24 hours by default.
---------	---

In the tab bar, you can take the following action to edit the tabs and customize the widget to be displayed.

	Click the icon to edit the tabs. For the default tabs, you can reset them to the default settings. For a created tab, you can edit its name or delete it.
	Click the icon and enter the name in the pop-up window to create a new tab.
	Click a tab and then click the widget in the pop-up page to add it to this tab or remove it. After you finish, click DONE .

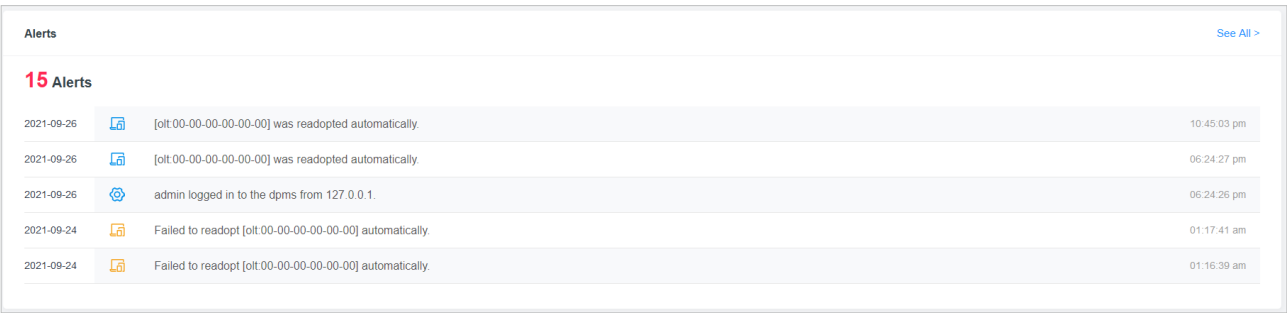
5. 1. 2 Explanation of Widgets

You can click the  icon to add or remove the widgets.



■ Alerts

The Alerts widget displays the total number of alerts which are processing and error level. To view all the alerts and archive them, click [See All](#) to jump to [Log > Alert](#). To specify events appeared in Alerts, go to [Log > Notifications](#) and configure the events as the Alert level. For details, refer to [5.3 View and Manage Logs](#).



■ OLT Devices

The OLT Devices widget displays the number of OLT devices in different status. To view all the device, click [See All](#) to jump to [Devices](#).

OLT Devices

Pending (0) Normal (1) Offline (0) [See All >](#)

DEVICE NAME	SITE	IP ADDRESS	STATUS	MODEL	VERSION	ONU NUMBER	UPTIME
 DS-P7001-08_000000	TP-Link	192.168.0.1	Online	DS-P7001-08 1.0	1.0.0 Build 20210604 Rel.13642	0	2h 31m 57s

■ ONU Devices

The ONU Devices widget displays the number of ONU devices in different status. To view all the device, click [See All](#) to jump to [Devices](#).

ONU Devices

Active (0) Inactive (0) [See All >](#)

DEVICE NAME	SITE	OLT DEVICE	ONLINE STATUS	MODEL
 No Data				

■ Most Active OLTs In 24 Hours

The widget displays the most active OLTs in the network based on the total number of traffic within the time range. Only the devices that has been adopted by DPMS will be displayed. To view all the devices discovered by DPMS, click [See All](#) to jump to [Devices](#).

Most Active OLTs In 24 Hours

[See All >](#)

 DS-P7001-08_000000	Online	0 GB
--	--------	------

< 1 >

■ Top Devices Usage

The widget displays the CPU utilization and memory utilization of devices at present. Click the tab to select the CPU or memory for display.

Top Devices Usage

CPU Memory

 DS-P7001-08_000000	5%
--	---------------------------

< 1 >

♥ 5.2 View the Statistics of the Network

Statistics provides a visual representation of device data in DPMS. You can easily monitor the network traffic and performance under the following tabs, Performance and Traffic/DDM Statistics.

5.2.1 Performance

In Performance, you can view the device performance in a specified period by graphs, such as ONU counts, CPU and memory usage, and upstream and downstream traffic.

Tab Bar

AA:BB:CC:DD:EE:FF
▼

2019-03-12
~
2019-03-17
📅

Hourly
▼

AA:BB:CC:DD:EE:FF
▼

2019-03-12
~
2019-03-17
📅

Hourly
▼

Click to select a device from the drop-down list to view its statistics.

Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right.

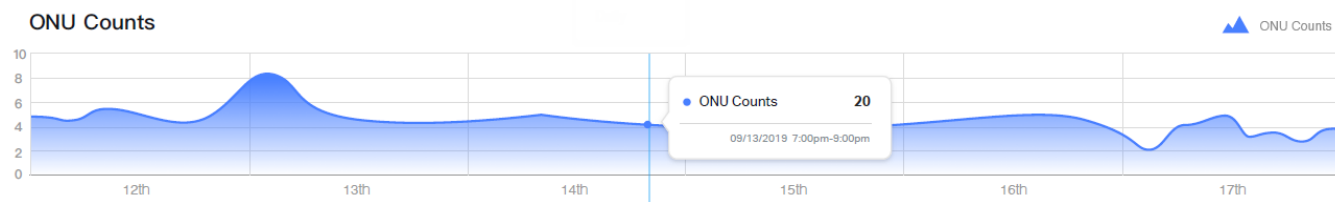
The available time range is restricted by the time interval. Before selecting a long time range, select Hourly or Daily as the time interval.

Select [5 minutes](#), [Hourly](#), or [Daily](#) to specify the time interval of the data. When selecting a long time range, a longer time interval is recommended for a better view.

Statistical Tables/Graphs

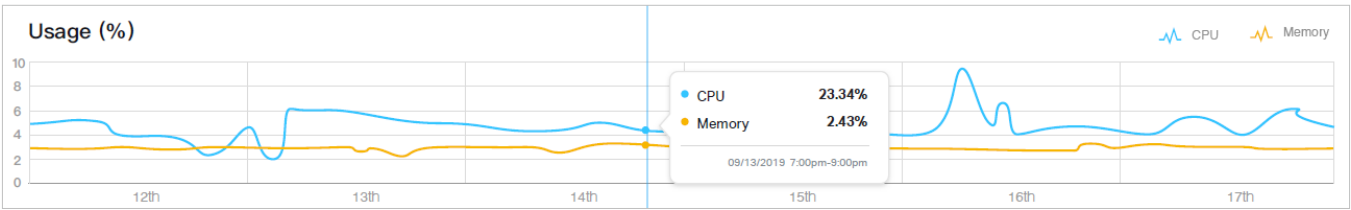
■ ONU Counts

The ONU Counts graph displays the number of ONUs connected to the OLT during the selected time range. Hover the cursor over the line to display the specific values.



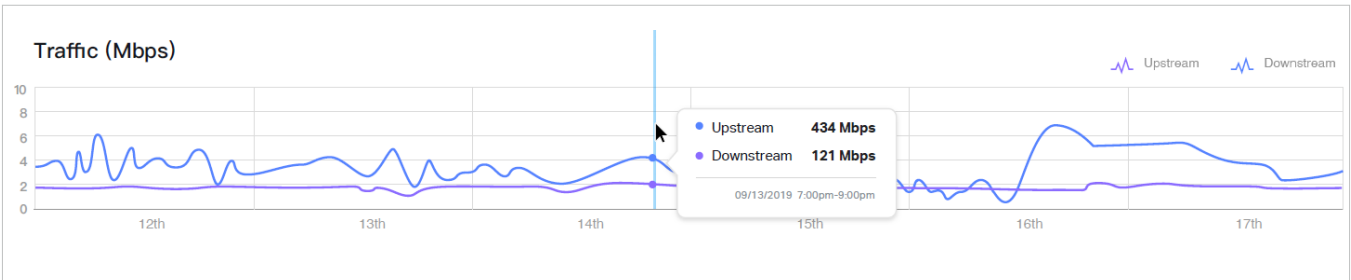
■ Usage

The Usage graph uses lines of different colors to display the percentage of CPU usage and used memory during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



■ Traffic

The Traffic graph uses lines of different colors to display the traffic rate of upstream and downstream traffic during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



5. 2. 2 Traffic/DDM Statistics

In Traffic/DDM Statistics, you can view the current status of ports and their traffic/DDM statistics of the selected OLT in the specified time range via a monitor panel and graphs.

Tab Bar

AA:BB:CC:DD:EE:FF

2019-03-12 ~ 2019-03-17

Hourly

Sort:Natural

Mbps

MB

Packets

All

Broadcast

Multicast

AA:BB:CC:DD:EE:FF

Click to select a device from the drop-down list to view its statistics.

2019-03-12 ~ 2019-03-17

Click the date to display a calendar.

Click a specific date twice in the calendar for the widgets to display its statistics.

To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right.

The available time range is restricted by the time interval. Before selecting a long time range, select Hourly or Daily as the time interval.

Hourly

Select 5 minutes, Hourly, or Daily to specify the time interval of the data. When selecting a long time range, a longer time interval is recommended for a better view.

Select Natural, Transmitted, Received, or Total to specify the graph order of ports.

Natural: Displays the line graphs in ascending order of the port number.

Transmitted: Displays the line graphs in descending order based on the traffic volume of transmitted packets.

Received: Displays the line graphs in descending order based on the traffic volume of received packets.

Total: Displays the line graphs in descending order based on the total traffic volume of transmitted and received packets.

Sort:Natural ▾

Select bps, Bytes or Packets to specify the data type and measuring unit.

Mbps: Displays the traffic rate in Mbps.

MB: Displays the traffic statistics in MB.

Packets: Displays the total number of packets.

MbpsMBPackets

If you select **Packet**, click the tab to specify which type of packet statistics to be displayed.

All: Displays statistics of all packets, including broadcast and multicast packets.

Broadcast: Displays statistics of broadcast packets only.

Multicast: Displays statistics of multicast packets only.

AllBroadcastMulticast

Statistical Tables/Graphs

Select ports to display the DDM/traffic statistics of the ports.

■ DDM Statistics (GE Port Excluded)

DDM Statistics

PORT ID	TEMPERATURE	VOLTAGE	BIAS CURRENT	TX POWER	RX POWER	TRANSMISSION FAULT	LOSS OF SIGNAL	DATA READY
XGE 1/0/1	128°C	6.5535 V	131 mA	6.5535 mW	6.5535 mW	False	False	False
XGE 1/0/2	100°C	6.5535 V	131 mA	6.5535 mW	6.5535 mW	True	True	True
XGE 1/0/3	100°C	6.5535 V	131 mA	6.5535 mW	6.5535 mW	True	True	True
XGE 1/0/4	100°C	6.5535 V	131 mA	6.5535 mW	6.5535 mW	False	False	False
XGE 1/0/5	128°C	6.5535 V	131 mA	6.5535 mW	6.5535 mW	No Signal	False	False
XGE 1/0/6	128°C	6.5535 V	131 mA	6.5535 mW	6.5535 mW	False	False	False

Temperature

Displays the temperature of the port.

Voltage

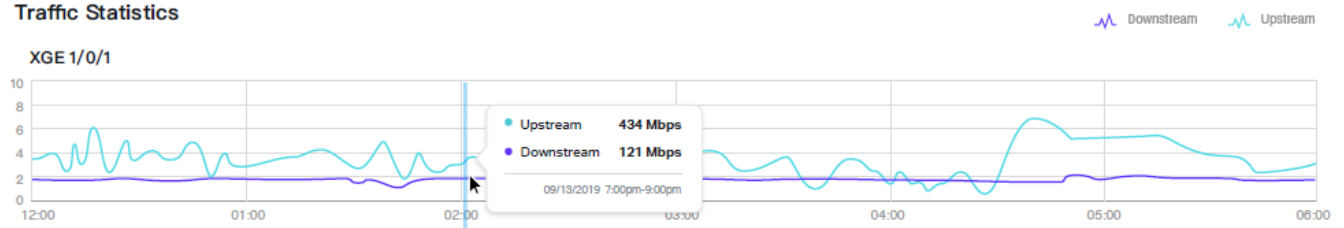
Displays the voltage of the port.

Bias Current	Displays the bias current of the port.
TX Power (dBm)	Displays the TX power of the port.
RX Power (dBm)	Displays the RX power of the port.
Transmit Fault	Displays whether the remote optical module works abnormally.
Loss of Signal	Displays whether the local optical module works abnormally.
Data Ready	Displays whether the optical module of the port is ready to transmit data.

■ Traffic

The Traffic graph uses lines of different colors to display the traffic rate of upstream and downstream traffic during the selected time range, respectively. Hover the cursor over the lines to display the specific values.

Traffic Statistics



♥ 5.3 View and Manage Logs

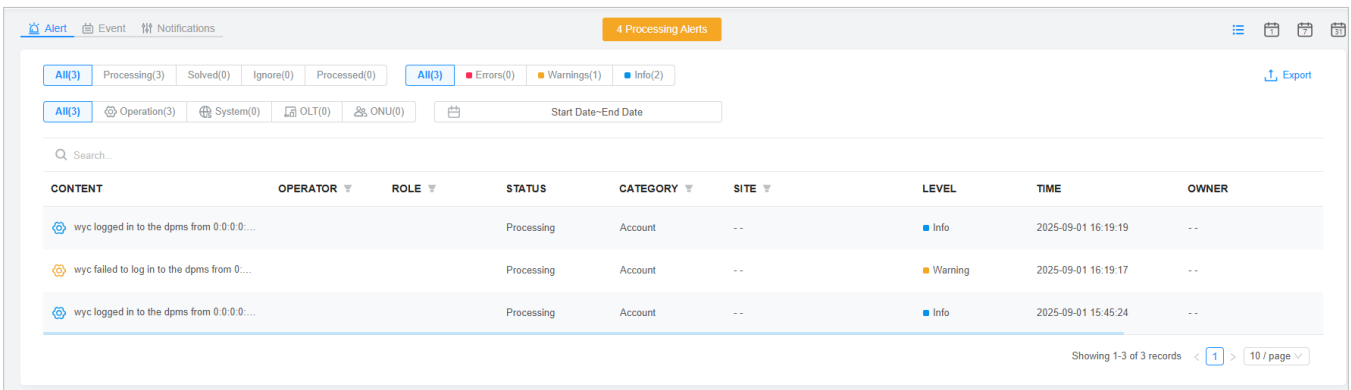
DPMS uses logs to record the activities of the system, devices, users and administrators, which provides powerful supports to monitor operations and diagnose anomalies. In the Logs page, you can conveniently monitor the logs in [5.3.1 Alerts](#) and [5.3.2 Events](#), and configure their notification levels in [5.3.3 Notifications](#).

All logs can be classified from the following four aspects.

- **Occurred Hierarchies**
Two categories in occurred hierarchies are DPMS level and device level (including OLTs and ONUs). Only Administrators can view the logs happened at the DPMS level.
- **Notifications**
Two categories in notifications are Event and Alert, and you can classify the logs into them by yourself.
- **Severities**
Three levels in severities are Error, Warning, and Info, whose influences are ranked from high to low.
- **Contents**
Four types in contents are Operation, System, OLT, and ONU, which indicate the log contents relating to.

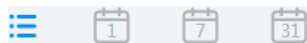
5.3.1 Alerts

Alerts are the logs that need to be noticed and archived specially. You can configure the logs as Alerts in Notifications, and all the logs configured as Alerts are listed under the Alerts tab for you to search, filter, and archive.



CONTENT	OPERATOR	ROLE	STATUS	CATEGORY	SITE	LEVEL	TIME	OWNER
wyc logged in to the dpms from 0.0.0.0...			Processing	Account	--	Info	2025-09-01 16:19:19	--
wyc failed to log in to the dpms from 0...			Processing	Account	--	Warning	2025-09-01 16:19:17	--
wyc logged in to the dpms from 0.0.0.0...			Processing	Account	--	Info	2025-09-01 15:45:24	--

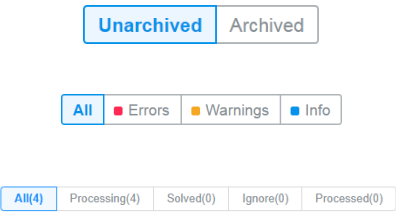
Click to change the view mode for a better overview.



: Displays the logs in a table.

: Displays the logs in a day/week/month. To change the time, click  or . To jump back to the current one, click [Today/This Week/This Month](#).

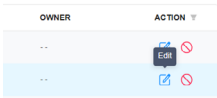
Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously.



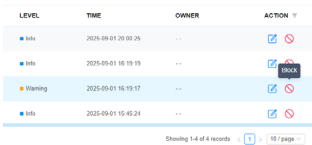
Unarchived/Archived: Click the tab to filter the unarchived and archived logs. You can click  and **Archive All** to archive a single log and all, respectively.

All/Errors/Warnings/Info: Click **All** to display all the logs in Error, Warning, and Info levels. Click **Errors**, **Warnings** or **Info** to display logs in the corresponding level only.

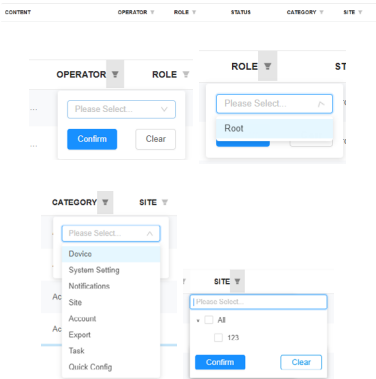
All/Processing/Solved/Ignored/Processed: Click **All** to display all types of logs. Click **Processing** or **Solved** or **Ignored** or **Processed** to display the corresponding type of logs only.



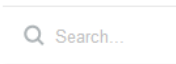
Click **Edit** icon in the **ACTION** column to change **Status** to **Solved** or **Ignore**, adjust the **Level**, and select an **Assignee**. The assignee list is limited to sub-sites under the current site.



Click **Block** icon in the **ACTION** column to navigate to Notifications. You can select the current log category to block this type of log.



You can filter logs by **Operator**, **Role**, **Category**, and **Site**. After filtering, only logs that match the criteria are displayed.



Enter the content types, severity levels, or key words to search the logs.

Content

Displays the log types and detailed message.

Site

Displays the site where the activity happened.

Time

Displays when the activity happened.

5.3.2 Events

Events are the logs that can be viewed but have no notifications. You can configure the logs as Events in Notifications, and all the logs configured as Events are listed under the Events tab for you to search and filter.

AlertEventNotifications

20 Unarchived Alerts

AllErrorsWarningsInfo

AllOperationSystemOLTONU

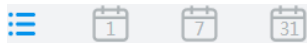
Search...

Batch Delete

CONTENT	SITE	TIME	ACTION
[olt:00-00-00-00-00-00] was readopted automatically.	TP-Link	2021-09-27 12:30:20 am	
[olt:00-00-00-00-00-00] was connected.	TP-Link	2021-09-27 12:30:20 am	
[olt:00-00-00-00-00-00] was readopted automatically.	TP-Link	2021-09-26 05:42:16 pm	
[olt:00-00-00-00-00-00] was connected.	TP-Link	2021-09-26 05:42:16 pm	
Pending [olt:00-00-00-00-00-00] was discovered.	--	2021-09-26 05:42:02 pm	
Failed to readopt [olt:00-00-00-00-00-00] automatically.	TP-Link	2021-09-26 04:42:24 pm	
Failed to readopt [olt:00-00-00-00-00-00] automatically.	TP-Link	2021-09-26 04:41:22 pm	
Failed to readopt [olt:00-00-00-00-00-00] automatically.	TP-Link	2021-09-26 04:40:21 pm	
[olt:00-00-00-00-00-00] was connected.	TP-Link	2021-09-25 10:45:03 pm	
[olt:00-00-00-00-00-00] was readopted automatically.	TP-Link	2021-09-25 10:45:03 pm	

Showing 1-10 of 41 records < 1 2 3 4 5 > 10 / page

Click to change the view mode.



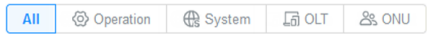
Displays the logs in a table.

: Displays the logs in a day/week/month. To change the time, click or . To jump back to the current one, click [Today/This Week/This Month](#).

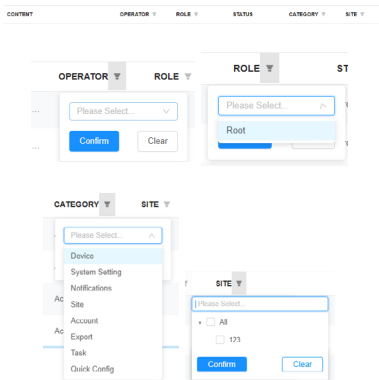
Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously.



All/Errors/Warnings/Info: Click [All](#) to display all the logs in Error, Warning, and Info levels. Click [Errors](#), [Warnings](#) or [Info](#) to display logs in the corresponding level only.



All/Operation/System/OLT/ONU: Click [All](#) to display all types of logs. Click [Operation](#) or [System](#) or [OLT](#) or [ONU](#) to display the corresponding type of logs only.



You can filter logs by [Operator](#), [Role](#), [Category](#), and [Site](#). After filtering, only logs that match the criteria are displayed.



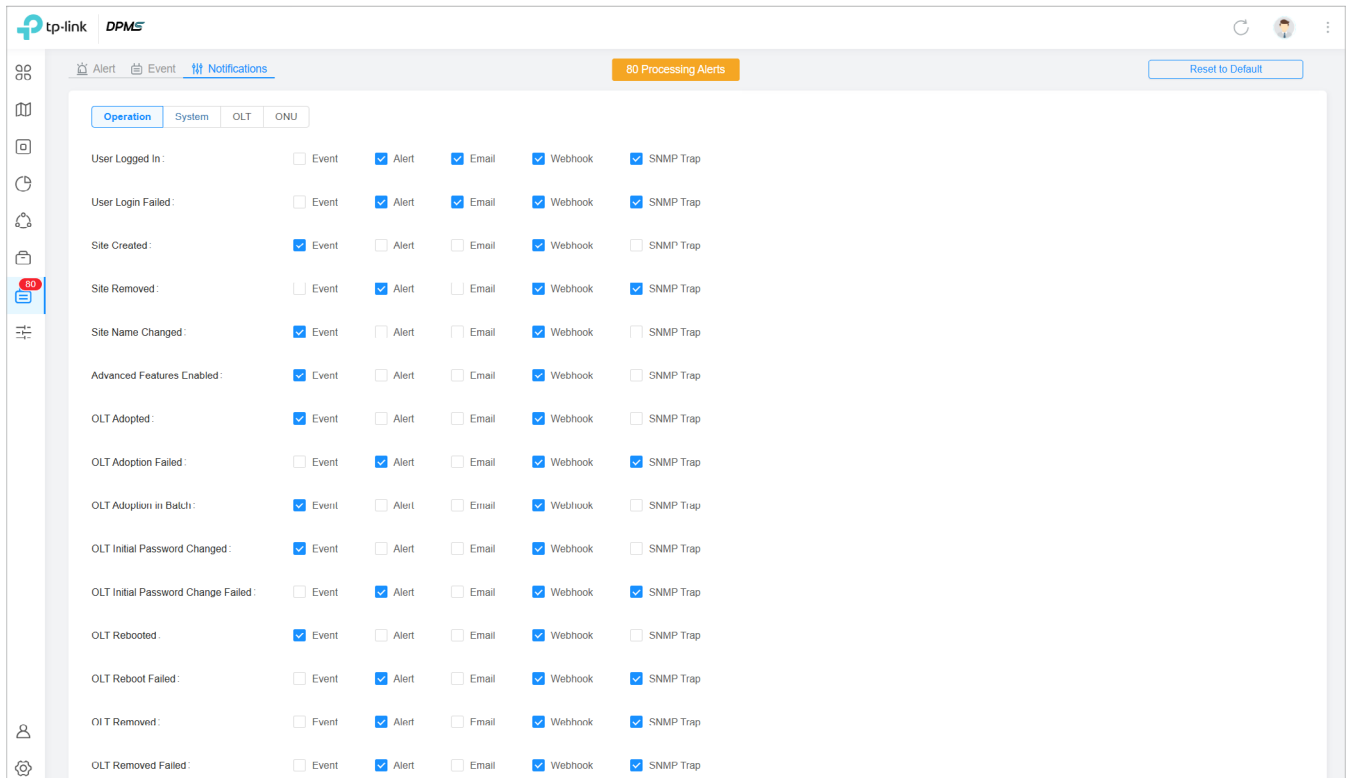
Enter the content types, severity levels, or key words to search the logs.

Content	Displays the log types and detailed message.
Site	Displays the site where the activity happened.
Time	Displays when the activity happened.
Batch Delete	Select the log entries and click Batch Delete to delete them in batches.
Action	Click  to delete the log entry.

5.3.3 Notifications

In Notifications, you can find all kinds of activity logs classified by the content and specify their notification categories as Event and Alert. Also, you can enable Email, Webhook or SNMP Trap for the logs. With proper configurations, DPMS will send emails, webhook message or SNMP trap message to the administrators when it records the logs.

☒ Webhook	With proper configurations, DPMS will send webhook message to the administrators when it records the logs
☒ SNMP Trap	With proper configurations, DPMS will send SNMP trap message to the administrators when it records the logs



To specify the logs as Alert/Event, click the corresponding checkboxes of logs and click [Apply](#). The following icons and tab are provided as auxiliaries.

[Reset to Default](#)

Click to reset all notification configurations to the default.

Operation

System

OLT

ONU

Click the tabs to display the configurations of corresponding log types.

☐ Event ☐ Alert

Enable the checkboxes to specify the activity logs as Events/Alerts, and then the recorded logs will be displayed under the Events/Alerts tab. If both of them are disabled, DPMS will not record the activity logs.

☐ Email

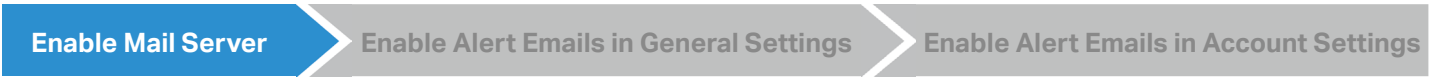
Enable the checkbox to specify the activity logs as alert logs. With proper configurations, DPMS will send emails to the administrators when it records the logs.



This icon appears when the configuration of a log is changed but has not been applied. Click it to reset the configuration of the log to the previous state.

The Email checkbox is used to enable [Alert Emails](#) for the logs. To make sure the administrators and viewers can receive alert emails, follow the following steps:

- 1) Enable [Mail Server](#).
- 2) Enable [Alert Emails](#) in [General Settings](#).
- 3) Enable [Alert Emails](#) in [Account Settings](#).
- 4) Enable [Alert Emails](#) in [Logs](#).



Go to [Settings](#) > [General Settings](#). In the [Mail Server](#) section, enable SMTP Server and configure the parameters. Click [Apply](#).

Mail Server

SMTP Server :

☒

With the Mail Server, the DPMS Server can send emails for pushing notifications, and delivering the system logs. Configure Mail Server carefully.

SMTP :

Port :

(1-65535)

SSL :

☐

Authentication :

☐

Sender Address :

(Optional)

Test SMTP Server :

Test

Apply

Cancel

SMTP	Enter the URL or IP address of the SMTP server according to the instructions of the email service provider.
Port	Configure the port used by the SMTP server according to the instructions of the email service provider.
SSL	Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between DPMS and the SMTP server.
Authentication	Enable or disable Authentication according to the instructions of the email service provider. If Authentication is enabled, the SMTP server requires the username and password for authentication.
Username	When Authentication is enabled, enter your email address as the username.
Password	When Authentication is enabled, enter the authentication code as the password, which is provided by the email service provider when you enable the SMTP service.
Sender Address	(Optional) Specify the sender address of the email. If you leave it blank, DPMS uses your email address as the Sender Address.
Test SMTP Server	Test the Mail Server configuration by sending a test email to an email address that you specify.



Go to [Settings](#) > [General Settings](#) and enable [Alert Emails](#) in the [Services](#) section. Then click [Apply](#).

Services

Alert Emails : ☒

☒ Send similar alerts within seconds in one email.

Remote Logging : ☒

Syslog Server IP / Host Name :

Syslog Server Port : (1-65535)

	Enable alert emails: When enabled, DPMS can send emails to notify the administrators and viewers of the site's alert logs once generated.
Alert Emails	Send similar alerts within seconds in one email: When enabled, the similar alerts generated in each time period are collected and sent to administrators and viewers in one email. To configure alert-level logs and enable email notifications on the controller, refer to 5.3.3 Notifications.
Remote Logging	With this feature configured, DPMS will send generated site logs to the log server. When enabled, the following items are required: Syslog Server IP/Hostname: Enter the IP address or hostname of the log server. Syslog Server Port: Enter the port of the server.



Go to [Admin](#) and configure Alert Emails for the administrators and viewers to receive the emails. Click [+ Add](#) to create an account or click [✎](#) to edit an account. Enter the email address in [Email](#) and enable [Alert Emails](#). Click [Create](#) or [Apply](#).

Edit

Username :

admin

Change Password :

☐ Enable

Email :

example@tp-link.com

(Optional)

Alert Emails :

☒ Enable

i

Apply

Cancel

Enable Alert Emails in General Settings

Enable Alert Emails in Account Settings

Enable Alert Emails in Logs

Go to [Logs](#) and click [Notifications](#). Click a tab of content types and enable [Email](#) for the activity logs that DPMS emails administrators. Click [Save](#).

	Alert	Event	Notifications
Operation			
System			
OLT			
ONU			
User Logged In :	☒	☐	☒
User Login Failed :	☒	☐	☒
Site Created :	☐	☒	☐
Site Removed :	☐	☒	☐
Site Name Changed :	☐	☒	☐
Advanced Features Enabled :	☐	☒	☐
OLT Adopted :	☐	☒	☐
OLT Adoption Failed :	☒	☐	☐
OLT Adoption in Batch :	☐	☒	☐

6

Manage User Accounts of DPMS

This chapter provides a comprehensive guide to managing user accounts within the system. It outlines the essential procedures for creating new users, assigning roles and permissions and modifying existing profiles. The chapter includes the following sections:

- [6. 1 Introduction to User Accounts](#)
- [6. 2 Manage Roles](#)
- [6. 3 Manage Local User Accounts](#)
- [6. 4 Manage Cloud User Accounts](#)

♥ 6.1 Introduction to User Accounts

DPMS utilizes a comprehensive role-based access control architecture to ensure security and operational efficiency. Users are categorized into two primary types: Local Users and Cloud Users (who connect via the Cloud Access feature).

Access to system features is determined by the specific Role assigned to a user account. These roles are organized hierarchically and define the level of permission granted to the user.

■ Default Local Roles

The system comes pre-configured with four standard roles. The permission levels for these roles are fixed by default to ensure the system stability and cannot be modified.

Root: The supreme administrator

Super Admin: Full administrative access

System Operator: Operational access to day-to-day tasks

Viewer: Read-only access for monitoring

■ The Root Account

The Root user is a unique, permanent Local User created explicitly during the initial system setup wizard.

Unrestricted Access: The Root user possesses absolute authority over the entire system.

Permanence: There is only one Root account. It cannot be deleted, disabled or recreated.

Local Only: The Root user must always be a Local User.

■ Custom Roles & Administrative Privileges

For specific operation needs, the system supports Custom Roles. You may create these roles, freely edit their permission sets and assign them to old and new users (Local Users only). However, please note critical administrative functions and high-level system features are exclusively reserved for the Root and Super Admin roles and cannot be assigned to Custom Roles.

■ Cloud User Roles

Users accessing the system via Cloud Access are subject to specific role restrictions. Cloud Users are limited to the following three pre-defined roles:

Cloud Super Admin (Maximum of one account allowed)

Cloud Operator

Cloud Viewer

These roles mirror the functionality of their local counterparts, serving to clearly distinguish this user type from standard Local Users.

To view the complete list of default roles and inspect their specific configurations:

1. Navigate to the [Account](#) page using the left sidebar menu.
2. Click the [Role Management](#) icon located at the top-right corner of the [Account List](#).

[Account List](#) [Block List](#)

Account List

All [Export](#) [+ Add](#) [Role Management](#)

USERNAME	EMAIL	ROLE	VERIFIED	SITE PRIVILEGES	DESCRIPTION	STATUS	ACTION
 Dpms_Root	--	Root	✓	All	--	● Online	

Showing 1-1 of 1 records < 1 > 10 / page

Role List

[+ New Role](#)

- Root
- Cloud Super Admin
- Super Admin
- System Operator 
- Viewer 
- Cloud System Operator
- Cloud Viewer

♥ 6.2 Manage Roles

This section outlines the structure of system privileges and provides detailed instructions on how to configure access control. By effectively managing roles, administrators can ensure that users have the appropriate level of access required to perform their duties without compromising system security.

ⓘ **Note:**

- The ability to manage (create, modify, disable or delete) roles is strictly reserved for administrators (Root, Super Admin, Cloud Super Admin).

6.2.1 Understanding Permissions

Permissions in this system are granular and organized by functional modules(e.g., Dashboard, Site Management, User management). Within each module, permissions are generally categorized into two types:

- **Read Access:** Grants the user the ability to view specific pages, dashboards, or retrieve data via GET APIs. Users with only Read Access cannot alter configurations.
- **Write Access:** Grants the user the ability to modify settings, execute control commands, or perform actions via POST/PUT/DELETE APIs.

➤ Viewing the Full System Permission List

To view a comprehensive inventory of every permission item available in the system:

1. On the [Role List](#), click the [Root](#) role entry. (Since Root holds all privileges by default)
2. Navigate to [Feature Permissions](#) section.

Feature Permissions		
DASHBOARD		
Tab :	☒ Read	☒ Write
Alert :	☒ Read	
Device :	☒ Read	
Overall :	☒ Read	
SITE		
Site management :	☒ Read	☒ Write
DEVICE		
OLT config :	☒ Read	☒ Write
OLT management :	☒ Read	☒ Write

6. 2. 2 Role-Based Security Policies

Beyond functional module permissions (Read/Write), security constraints such as access time control and account (auto) logout are also defined at the Role level. This means these policies apply to all users assigned to a specific role, rather than being configured individually for each user.

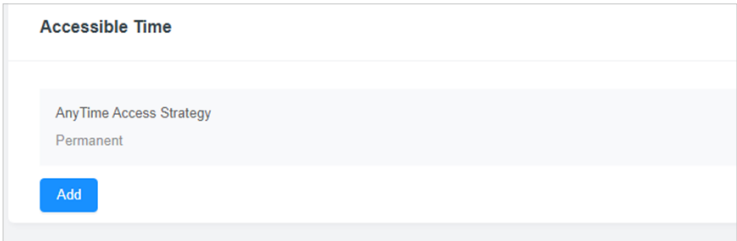
➤ Accessible Time Strategy

The feature restricts system access to specific time windows. Users assigned to a role with time restrictions will be unable to log in or perform operations outside the permitted time.

Default Configuration: By default, all default roles apply the [AnyTime Access Strategy](#), granting 24/7 access.

How to configure:

1. Define your schedule: Go to [Setting](#) > [Auto Lock Strategy](#) > [Accessible Time](#). All the time policies in the system are displayed here. Click [Add](#) to create a new one.



2. Configure the parameters and click [Confirm](#).

A screenshot of the 'Add' modal form. The form has a title bar 'Add' with a close button. It contains several input fields: 'Strategy Name' (text input), 'Effective Period' (range from 'Start date' to 'End date'), 'Accessible Time' (checkboxes for 'Select All' and days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday), 'Start Time' (time picker), and 'End Time' (time picker). At the bottom right, there are 'Cancel' and 'Confirm' buttons.

Strategy Name	Specify the strategy name. It must not duplicate any existing one.
Effective Period	Set the start date and end date for when this strategy takes effect.
Accessible Time	Specify the days of week (Monday through Sunday) on which users are permitted to access the system.

Start Time	Defines the start time of the allowed access period for each selected day.
End Time	Defines the end time of the allowed access period for each selected day.

3. Assign to Role: When creating or editing a Custom Role, locate the following [Accessible Time Strategy](#) dropdown menu. Select your pre-defined strategy from the list.

Accessible Time Strategy :

Please Select... ▾

➤ **Auto Lock Strategy**

The Auto Lock Strategy is a security measure designed to prevent brute-force attacks. If a user consecutively enters an incorrect password, their account will be temporarily locked.

Global Rules vs. Role Toggle

- **Global Configuration:** The specific rules—number of allow attempts (e.g., 5 failures), time window (e.g., 30 minutes) and lockout duration (e.g., 30 minutes)—are set globally. To configure these parameters, go to [Setting](#) > [Auto Lock Strategy](#) > [Auto Lock Strategy](#).
- **Role configuration:** In the Role settings, Auto Lock is controlled by a simple On/Off toggle. Enable this switch ensures that global lockout rules apply to all users holding this role.

Auto Lock :

☐ Enable

6. 2. 3 Default System Roles

The system includes pre-defined roles: Root, Super Admin, System Operator, and Viewer (and their Cloud counterparts).

These roles are designed to cover standard operational scenarios. Please note the following restrictions regarding Default Roles:

- [Immutable Configuration](#): The role settings (include Basic and Feature Permissions) for these roles are fixed and cannot be edited.
- [Permanent Status](#): These roles cannot be renamed, disabled, or deleted from the system.

6. 2. 4 Managing Custom Roles

For scenarios where default roles do not fit specific operational workflows, administrators can create Custom Roles with tailored role settings.

➤ **Create a Custom Role**

1. Go to [Account](#) > [Role Management](#), click [+New Role](#).

Role Management

Role List

+ New Role

Root

Cloud Super Admin

Super Admin

System Operator

Viewer

Cloud System Operator

Cloud Viewer

(Unsaved) New Role

Role Settings

Basic

Role Name:

Default User Name: (Optional)

Default Password: (Optional)

Email: (Optional)

Description: (Optional)

Accessible Time Strategy:

Please Select...

Alert Email:

☐ Enable

Auto Lock:

☐ Enable

Feature Permissions

2. Configure basic settings and feature permissions

Role Name	Specify the role name. It must not duplicate any existing one.
Default User Name	Optional. If specified, this value is automatically populated in the User Name field when creating a user with this role (editable later).
Default Password	Optional. If specified, this value is automatically populated in the Password field when creating a user with this role (editable later).
Email	Optional. If specified, this value is automatically populated in the Email field when creating a user with this role (editable later).
Description	Provides a description of the role for reference and management purposes.
Accessible Time Strategy	Select an accessible time strategy to apply access control. For details, refer to 6.2.2 Role-Based Security Policies.
Alert Email	Indicates whether log notification emails are enabled. A mail server must be configured in advance for this feature to take effect.
Auto Lock	Indicates whether the global auto lock strategy is applied to users of this role. For details, refer to 6.2.2 Role-Based Security Policies.

ⓘ Note:

- Some critical permissions(e.g., role management: write) are reserved for administrator-level roles and therefore do not appear in the permission list for custom roles.
- Permissions for certain modules may depend on other modules. You can hover your mouse over a disabled module to view the dependency details.

4. Click **Save**.

ACCOUNT

User management :

☒ Read
 ☒ Write

Role management :

☐ Read

Blacklist management :

☒ Read
 ☐ Write

SETTINGS

General settings :

☒ Read

Save

Cancel

➤ Modify, Disable, and Delete Custom Roles

Administrators can edit role settings, toggle the Enable/Disable status and delete custom roles.

- **Modify:** Click the [Custom Role](#) item in the role list and modify its settings. Changes to permissions and security policies take effect immediately. Users currently logged in with this role may need to re-login to view the changes.
- **Disable:** To disable a custom role, click [Disable Role](#) in the drop-down menu at the end of the entry. Disabling a role prevents it from being assigned to users and also disables all the users of that role. On the settings page of a disabled role, a light yellow notification banner will appear with the message "This role has been disabled." Click [Enable Role](#) in the banner to re-enable the role.

Role List

+ New Role

Root

Cloud Super Admin

Super Admin

System Operator

Viewer

Cloud System Operator

Cloud Viewer

Custom_Role0

⋮

⋮

⋮

Role Settings

Basic

Role Name :

Default User Name :

Default Password :

Email :

Description :

Duplicate Role

Disable Role

Delete Role

Role Settings

ⓘ

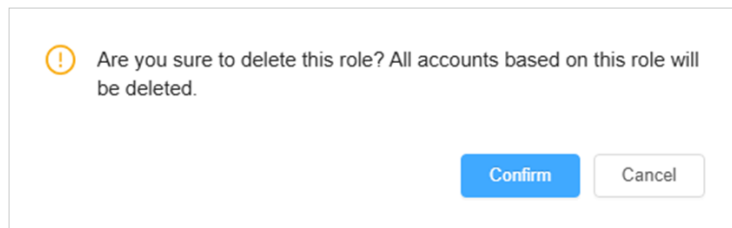
This role has been disabled.

Enable Role

- **Delete:** [Custom Roles](#) that are no longer needed can be permanently removed from the system. Click [Delete Role](#) in the menu to remove the role. Please be aware that when a role is removed, all users with the role will also be removed.

➤ **Warn: Critical Operation**

Modifying, disabling, or deleting a custom role impacts all users currently assigned to that role. These actions may result in access restrictions or service disruption for those users. Before execution, DPMS will trigger a pop-up confirmation dialog. Review the prompt and click [Confirm](#) to authorize the action. Please proceed with caution and ensure you fully understand the impact before making any changes.



♥ 6.3 Manage Local User Accounts

This section guides you through the lifecycle of Local User Management. Local Users are accounts that are fully managed by locally deployed DPMS. These users are intended for use within local environment only. Unlike Cloud Users, they do not support the Cloud Access feature that enables remote system access through the cloud.

6.3.1 Create a New Local User

The first local user is the Root user created in DPMS initialization. To create more local users, follow these steps:

1. Go to [Account List](#) and click **+ Add** above the account list.

Account List

All Search... Export

+ Add Role Management

USERNAME	EMAIL	ROLE	VERIFIED	SITE PRIVILEGES	DESCRIPTION	STATUS	ACTION
Dpms_Root	--	Root	✓	All	--	Online	

2. Select [Local User](#) for User Type and specify other parameters. Click [Apply](#) to create the account.

Create Account

User Type: ☒ Local User ☐ Cloud User Cloud Access Required Mail Server Required

Username:

Password:

Role:

Site Privileges: ☒ All (Including all new-created sites) ☐ Sites

Email: (Optional)

Alerts Emails: ☐ Enable Mail Server Required

Description: (Optional)

Auto Lock Strategy: ☐ Enable

Access Time Control:

Apply **Cancel**

Username	Specify the username. It must not duplicate any existing one.
Password	Enter a password. It should be at least 8 characters.
Role	Select a role for the user from the dropdown list. This list shows all the (local) roles that the current user (who performs the creation) is allowed to assign. Note: the selected role dictates not only the user’s functional permissions (Read/Write) but also accessible time and whether auto lockout is enabled.
Site Privileges	Assign site permissions to the user. All means the created user has device permissions in all sites, including possible new ones created later. Sites means the created user has device permission in certain sites. If Sites is selected, you must specify the sites from a dropdown list.
Email	Optional. Enter an email address for receiving alert emails.
Alerts Emails	Whether to send alert emails to the user. The user’s email address and the system mail server configuration are required to enable this feature.
Description	Optional. Write something that describes the user for reference.
Auto Lock Strategy	Whether global lockout rules apply to the user. Determined by the user’s role and displayed for reference only. Cannot be modified manually. Ensure the appropriate user role is selected.
Access Time Control	Accessible Time Strategy for the user. Determined by the user’s role and displayed for reference only. Cannot be modified manually. Ensure the appropriate user role is selected.

6.3.2 Edit, Block, and Delete Local Users

Local Users can be managed using the buttons in the Action column of the account list. Available operations include editing, blocking and deleting users.

USERNAME	EMAIL	ROLE	VERIFIED	SITE PRIVILEGES	DESCRIPTION	STATUS	ACTION
 Dpms_Root	--	Root	✓	All	--	● Online	
admin_1	--	Super Admin	✓	All	--	● Offline	   

	Edit. Click to edit the account settings for the target entry.
	Delete. Click to delete the target entry.
	Copy. It is a shortcut to creating a new user with the same account settings of the selected user. Further confirmation is required to finalize creation. Settings can still be modified before that.
	Block. Blocked users are not able to log in or perform any operations.
	Unblock (for blocked users). Remove an account from the block list so that it works properly.

➤ Edit

- **Edit current user:** Click the edit icon and enter the password. Modify account settings and click [Apply](#). Leaving the Password field empty means the password will not be changed, rather than being removed.

Authentication ✕

 Please enter your current password to make any changes to your account.

password:

Confirm

Cancel

Edit Account

Username:

Password:

Role:

Root

Site Privileges:

All (Including all new-created sites)

Sites

Email: (Optional)

Alerts Emails:

☐ Enable

 Mail Server Required

Description: (Optional)

Auto Lock Strategy:

☐ Enable

Access Time Control:

AnyTime Access Strategy

Apply

Cancel

 Note:

- Role and site privileges cannot be changed in self-editing.
-
- **Edit other users:** Click the edit icon in the target entry. You can change role and site privileges of the user here.

Edit Account

Username :

m1

Password :

Password 

Role :

Custom_Role0 

Site Privileges :

☒ All (Including all new-created sites)

☐ Sites

 Block/Unblock

A blocked status indicates that the user account is suspended. Blocked users are prohibited from logging in or performing any operations within the system. Unblocking an account restores full access rights.

A user account may be locked under the following three specific conditions:

- 1) **Auto-Lockout:** This occurs when a user (auto lock is enabled for the user’s role) exceeds the maximum allowed number of failed login attempts
- 2) **Role Deactivation:** If an administrator manually disables a custom role (for more details, please refer to [6. 2. 4 Managing Custom Roles](#)), all users assigned to that role are automatically disabled.
- 3) **Manual User Suspension:** Manually block a user by clicking the block icon in the account list.

Blocked users will appear in the block list that is next to account list.

p-link DPMS

Account List

Block List

All Auto Manual

Search:

+ Add

 Batch Unblock

☒	USERNAME	ROLE	BLOCK TYPE	BLOCK TIME	UNBLOCK TIME	Unblock User 
☒	c2	System Operator	Manual	2026-06-01 11:02:04	--	

Select 1 of 1 items

Showing 1-1 of 1 records < 1 > 10 / page

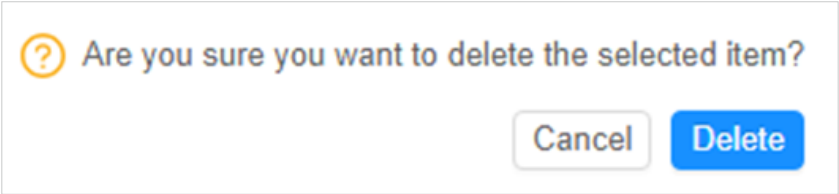
Username	Username of the blocked account.
Role	Role type of the blocked account.

Block Type	Auto or Manual. Only auto-lockout (condition 1) is classified as Auto.
Block Time	The time when the user was blocked, including Manual and Auto Block.
Unblock Time	Only available when the block type is Auto. Indicates when the user will be unblocked automatically.
Action	Click  to unblock the user.

-  **Note:**
- The Root account cannot be blocked.
 - If the user's assigned role is disabled, you cannot simply unblock the user. You need to enable the role first.

 Delete

To permanently remove an account from the system, click the **Delete** icon for the corresponding entry. To prevent accidental deletion, you will be prompted to confirm the action.



-  **Note:**
- The Root account is integral to the system and cannot be deleted.

♥ 6.4 Manage Cloud User Accounts

This section guides you through the lifecycle of Cloud User Management. Cloud user accounts are certain TP-Link accounts that are granted access to the local DPMS. With cloud access enabled, cloud users can be added to the system and access the system through cloud.

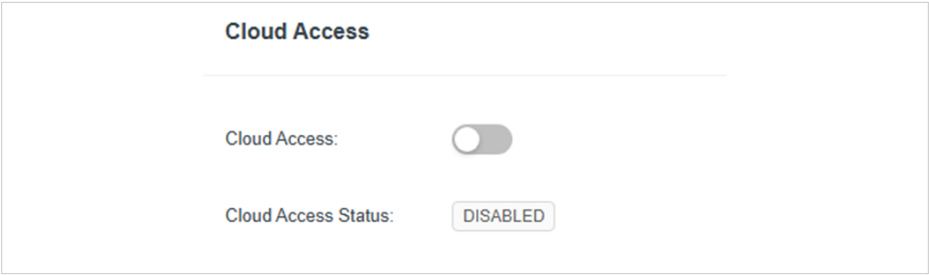
6.4.1 Adding A Cloud User

DPMS does not create any cloud user out of thin air. Cloud user accounts are valid TP-Link accounts that are added to the local system.

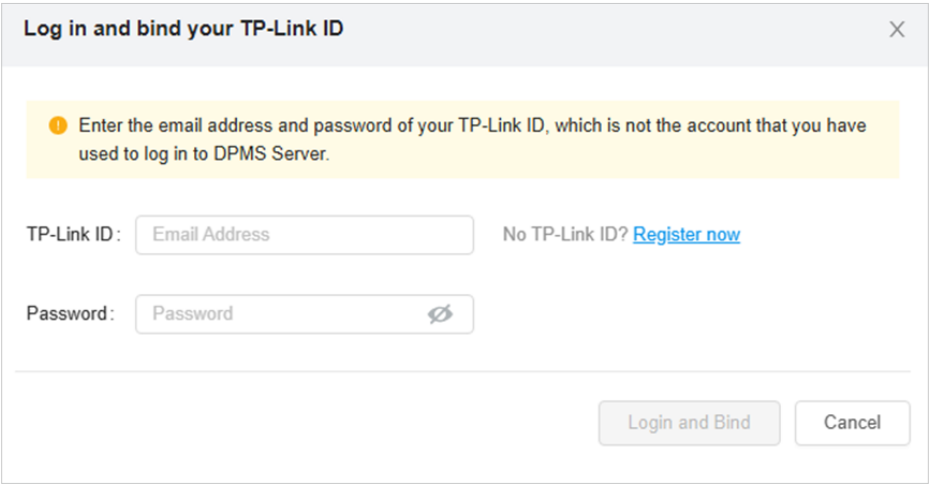
➤ Set up the Cloud Administrator

To enable cloud access, a cloud administrator (role: Cloud Super Admin) is required.

1. Go to [Setting](#) > [Cloud Access](#).



2. Toggle the switch on and bind your TP-Link ID.



3. If the action is successful, a cloud user with the [Cloud Super Admin](#) role will be automatically added to the system. You can view it in the account list.

USERNAME	EMAIL	ROLE	VERIFIED	SITE PRIVILEGES	DESCRIPTION	STATUS	ACTION
Dpms_Root	--	Root	✓	All	--	Online	Edit
admin_1	--	Super Admin	✓	All	--	Offline	Edit Delete Reset Lock
m1	--	Custom_Role0	✓	All	--	Account Ban	Edit Delete Reset Lock
zyf3da4@yzm.de	zyf3da4@yzm.de	Cloud Super Admin	✓	All	--	Offline	Edit Delete

Like the Root user, cloud administrator is unique in DPMS. If there is a cloud administrator in the system, it cannot be added again.

Note:

- The Root account is integral to the system and cannot be deleted.

➤ Add other cloud users

After setting up the cloud administrator, you can add other cloud users. Cloud access and mail server are required during the process. If mail server is not available, please configure it first (refer to [4. 1. 3 Mail Server](#)).

1. Go to [Account](#) and click [+ Add](#) above the account list.
2. Select [Cloud User](#) for [User Type](#).
3. Specify other parameters and click [Apply](#).

Create Account

User Type :

☐ Local User

☒ Cloud User

TP-Link ID :

Role :

Please Select...

Site Privileges :

☒ All (Including all new-created sites)

☐ Sites

Alerts Emails :

☐ Enable

Description :

(Optional)

Auto Lock Strategy :

☐ Enable

Access Time Control :

AnyTime Access Strategy

Apply

Cancel

TP-Link ID	Enter an email address of the new cloud user; an invitation email will be sent to this address. If the email address is already registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation. If not, register a TP-Link ID with the email address first, then accept the invitation.
Role	Select a role for the cloud user. There are only 3 roles for cloud users: Cloud Super Admin , Cloud System Operator , Cloud Viewer . Since a cloud administrator cannot be added again, the available role options are Cloud System Operator and Cloud Viewer.
Other parameters	Please refer to 6. 3. 1 Create a New Local User .

If the cloud user has not accepted the invitation, the verified field of the account will be displayed as empty, which means the account is not valid and cannot access the system.

In the unverified state, there are two actions to perform.

	Reinvite, send the invitation email again.
	Delete, remove the cloud user from the system. It also invalidates the invitation.

If the cloud user accepts the invitation, the account will become verified and ready to use.

USERNAME	EMAIL	ROLE	VERIFIED	SITE PRIVILEGES	DESCRIPTION	STATUS	ACTION
Dpms_Root	--	Root	✓	All	--	Online	
admin_1	--	Super Admin	✓	All	--	Offline	  
m1	--	Custom_Role0	✓	All	--	Account Ban	  
ccmgg992@uof.me	ccmgg992@uof.me	Cloud System Operator	✓	All	--	Offline	  
zvj63de4@yzm.de	zvj63de4@yzm.de	Cloud Super Admin	✓	All	--	Online	

6. 4. 2 Edit, Block, and Delete Cloud Users

Cloud user management is largely the same as local user management and can be accessed from the [Account List](#) page.

➤ Edit

- Edit current user:** Click the edit icon, modify the setting, and click [Apply](#).

Edit Account

TP-Link ID :

zvj63de4@yzm.de

Role :

Cloud Super Admin

Site Privileges :

All (Including all new-created sites)

Sites

Alerts Emails :

Enable

Description :

(Optional)

Auto Lock Strategy :

Enable

Access Time Control :

AnyTime Access Strategy

Apply

Cancel

- **Edit other cloud users:** Click the edit icon in the target entry. You can change role and site privileges of the cloud user here.

Edit Account

TP-Link ID :

Role :

Site Privileges :
☒ All (Including all new-created sites)
☐ Sites

Alerts Emails :
☐ Enable ⓘ

Description :
 (Optional)

Auto Lock Strategy :
☐ Enable

Access Time Control :

ⓘ Note:

- Cloud administrator cannot be edited by another user.

➤ Block/Unblock

Cloud users use the same block/unblock mechanism as local users. For more details, please refer to [6.3.2 Edit, Block, and Delete Local Users](#).

➤ Delete

- **Cloud System Operator and Cloud Viewer**

Delete a cloud non-administrator user is similar to deleting a local user. For more details, please refer to [6.3.2 Edit, Block, and Delete Local Users](#).

- **Cloud Super Admin**

The cloud administrator cannot be removed through normal deletion operations, as the Cloud Access feature depends on the existence of a cloud administrator. To remove a cloud administrator, please go to [Setting > Cloud Access](#) and unbind the TP-Link ID that is called [Owner ID](#).

Cloud Access

Cloud Access:



Cloud Access Status:

CONNECTED

Cloud Service:

<https://dpms.tplinkcloud.com/>

Owner ID:

zvj63de4@yzm.de

You can also log in locally using the TP-Link ID.

Unbind TP-Link ID

Note:

- Unbind TP-Link ID will disable the Cloud Access feature and delete all other cloud users. Please proceed with caution.



Quick Config

This chapter introduces two methods for configuring OLT equipment. It outlines single and batch operations for OLT equipment configuration. The chapter includes the following sections:

- [7.1 Overview](#)
- [7.2 Quick Config Create](#)
- [7.3 Quick Config Apply](#)
- [7.4 Quick Config History](#)

♥ 7.1 Overview

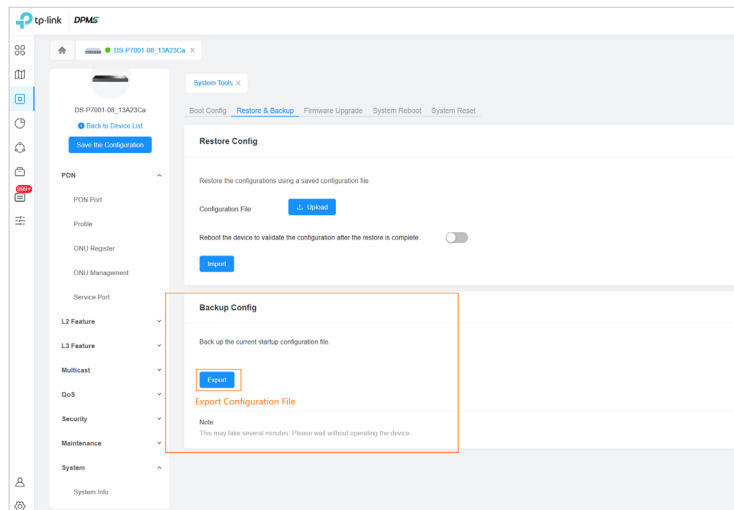
When facing inefficient configuration management for multiple OLT devices with identical/similar setups, the optimal approach is to implement unified configuration for such devices. This chapter provides two methods for configuring OLT equipment:

- Based on device system configuration files ([Quick Config File](#))
- User-defined configurations ([Quick Config Profile](#))

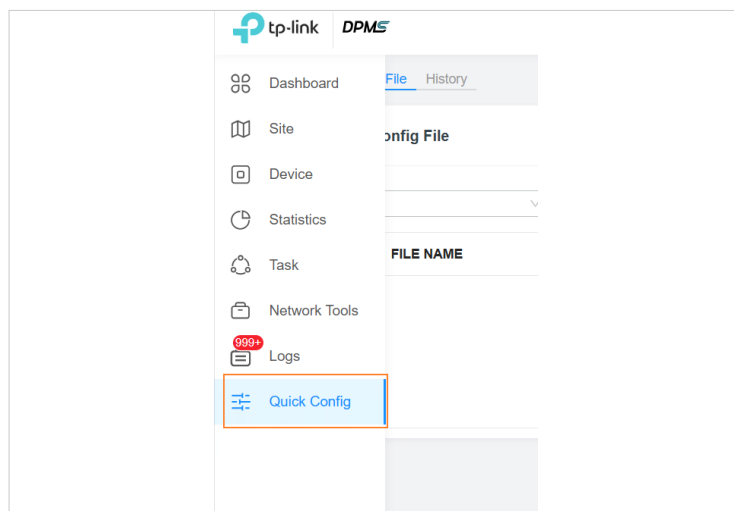
♥ 7.2 Quick Config Create

7.2.1 Quick Config File Create

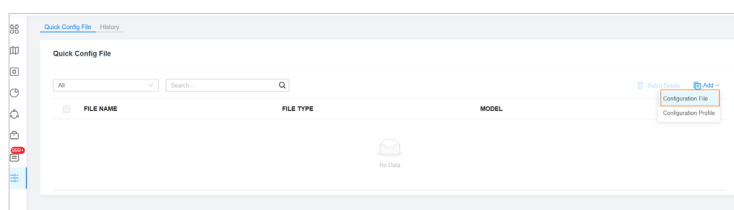
1. Download OLT configuration file: Go to [Device](#), you can view the basic information of the devices in a list. Select the OLT whose configuration you need to extract, click on the OLT device name to access the device. Then use the path [System](#) > [System Tools](#) > [Restore & Backup](#) > [Backup Config](#), click [Export](#) to export the configuration items of the current device.



2. Go to the sidebar manual, and click [Quick Config](#).



3. Click the [Add](#) button and select a [Configuration File](#).



4. Upload the configuration file, and name the configuration using the corresponding model + scenario convention (e.g., DS-7001-08_TEST_CONFIG_FILE) as the connection name.

Create Configuration File

Configuration File

File Name:

DS-7001-08_TEST_CONFIG_FILE

OLT Configuration File:

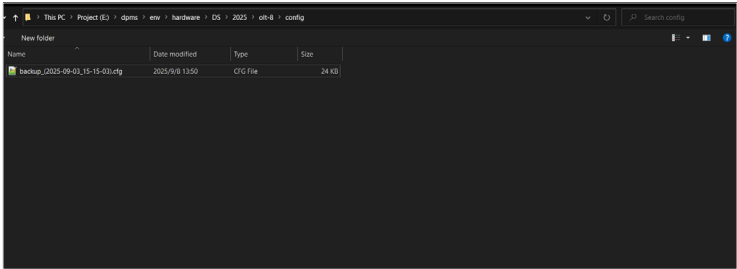
Upload

Import the configuration file to quickly config the same model in batch

Apply

Cancel

5. Click **Upload** to select the required configuration file, and then click **Open** to upload it.



6. After the Configuration File is uploaded successfully, click the **Apply** button.

Quick Config File

History

< Back

Create Configuration File

Configuration File

File Name:

DS-7001-08_TEST_CONFIG_FILE

OLT Configuration File:

backup_(2025-09-03_15-15-03).cfg

Change

Import the configuration file to quickly config the same model in batch

Apply

Cancel

7. The new configuration can be seen in configuration list.

Quick Config File

All

Search

Search Config

Refresh

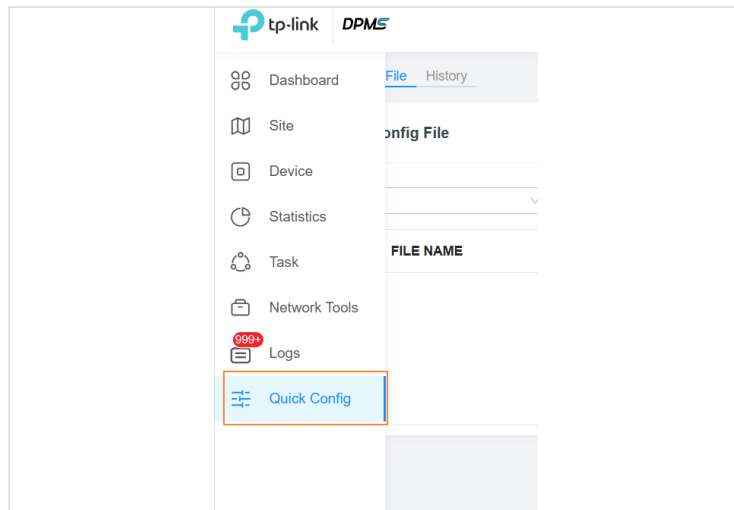
FILE NAME	FILE TYPE	MODEL	ACTION
DS-7001-08_TEST_CONFIG_FILE	Configuration File	DS-77001-08	

Showing 1 of 1 records

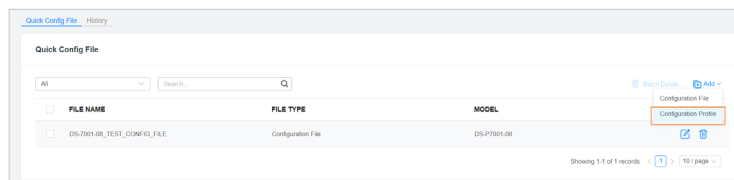
File Name	quick config user defined file name
File Type	Quick Config file type. E.g. configuration file, configuration profile
Model	OLT Device Type.
Action	Edit or delete the quick config file.

7.2.2 Quick Config Profile Create

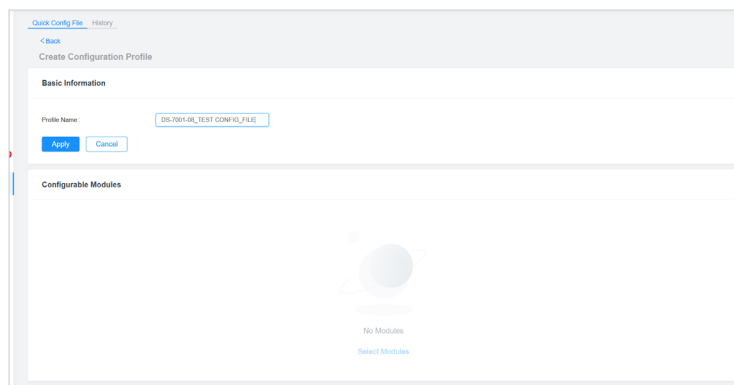
1. Go to sidebar manual, and then click **Quick Config**.



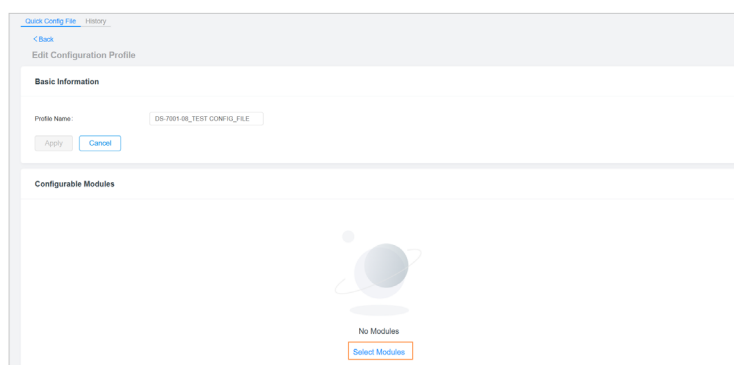
2. Click the **Add** button and select a **Configuration Profile**.



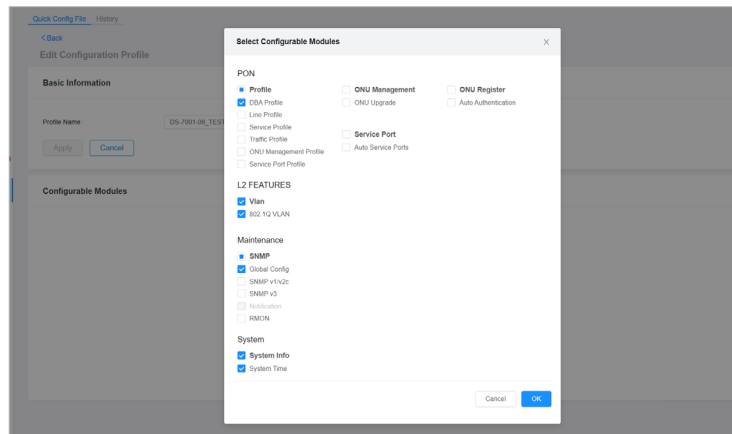
3. Enter the **Profile Name**, typically following the format as the connection name: model + scenario (e.g., DS-7001-08_TEST_CONFIG_FILE). Then click **Apply** button.



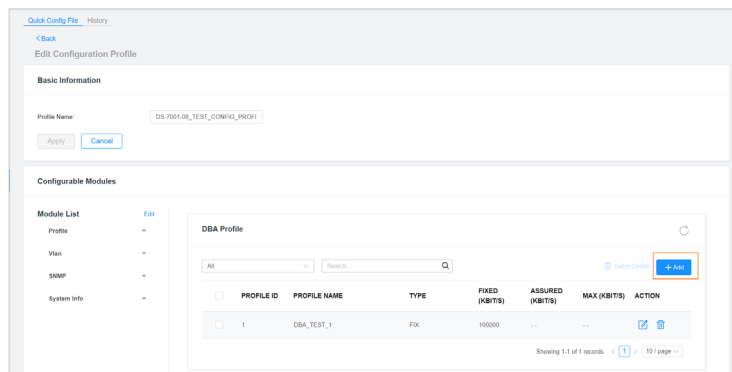
4. Click **Select Modules**, and select configurable modules as needed.



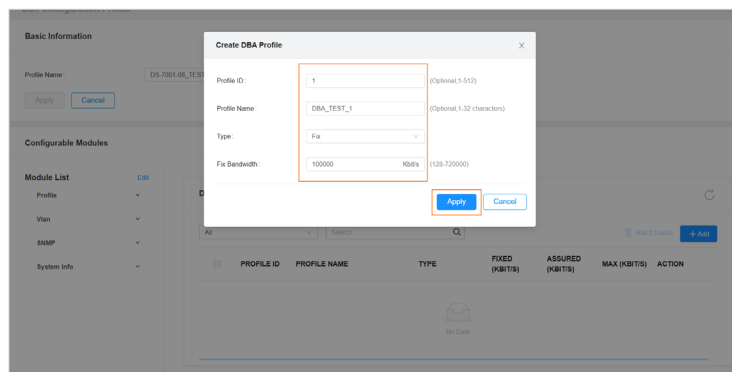
5. Select feature templates for OLT configurations. Check the target modules, and click **OK** to confirm.



6. Adjust configurations within the corresponding feature template as needed. The configuration is similar to the operation on the device's management page. For example, click **Add** in the **DBA Profile** section to create a new entry.



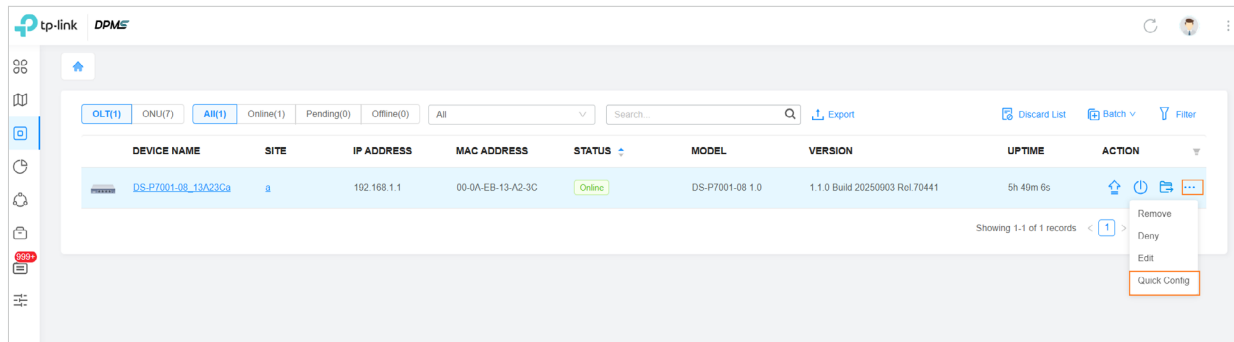
7. Fill in the configuration parameters and click **Apply** to save.



♥ 7.3 Quick Config Apply

7.3.1 Single OLT Device Apply Quick Config

1. Navigate to the [Device List](#) homepage, select the target OLT device, click [...](#) and proceed with [Quick Config](#) to execute configuration.



2. Pick up configuration type (1.Configuration File; 2. Configuration profile) from config type list, select the item from file list, and then click [Apply](#). The device will restart after applied successfully.

Config Type

Config Type :

Configuration File

File Name :

DS-7001-08_TEST_CONFIG_FILE ^

DS-7001-08_TEST_CONFIG_FILE

Apply

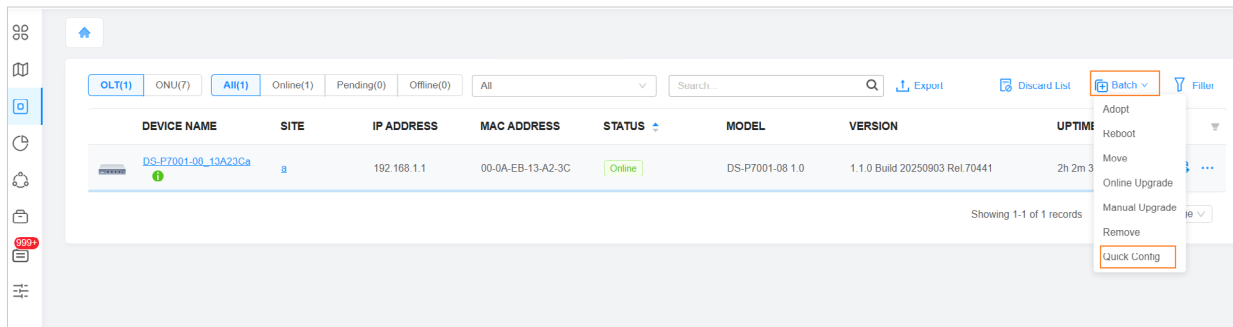
Cancel

ⓘ Note:

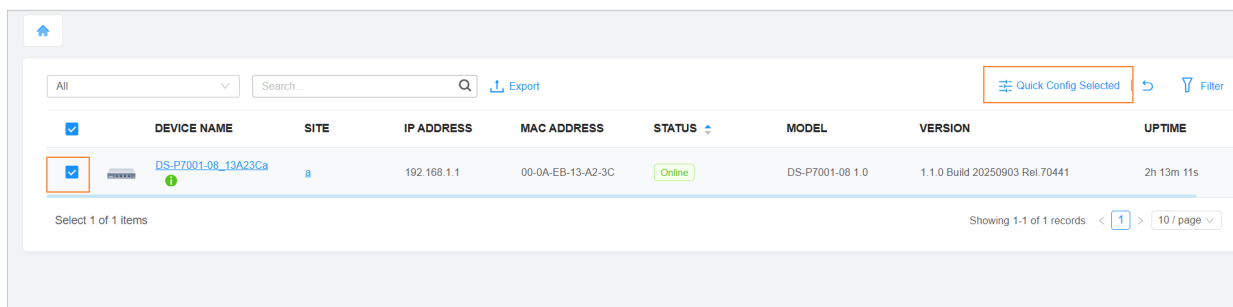
- If select [Configuration File](#) for [Config Type](#), the device will reboot, and the configuration takes effect after device reboot.

7.3.2 Batch Configuration Provisioning for OLT Devices

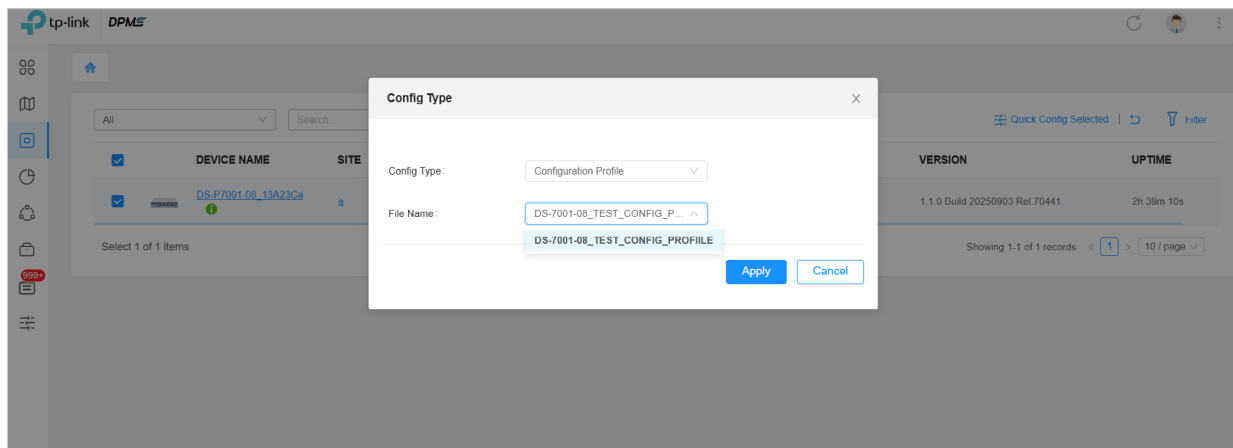
1. Navigate to the [Device List](#) homepage, click the [Batch](#) button, and then click [Quick Config](#).



2. Check the box(es) for device of the same model in the device list, and click [Quick Config Selected](#).



3. Select the [Config type](#), choose the corresponding configuration file under that type.



! Note:

- If select [Configuration File](#) for [Config Type](#), the device will reboot, and the configuration takes effect after device reboot.

♥ 7.4 Quick Config History

To view OLT configuration deployment operations records, please go to [Quick Config > History](#) page.

7.4.1 Quick Config File History

Take DS-7001-08_TEST CONFIG_FILE record as a successful deployment example:

Quick Config File [History](#)

History

All

Search...

Q

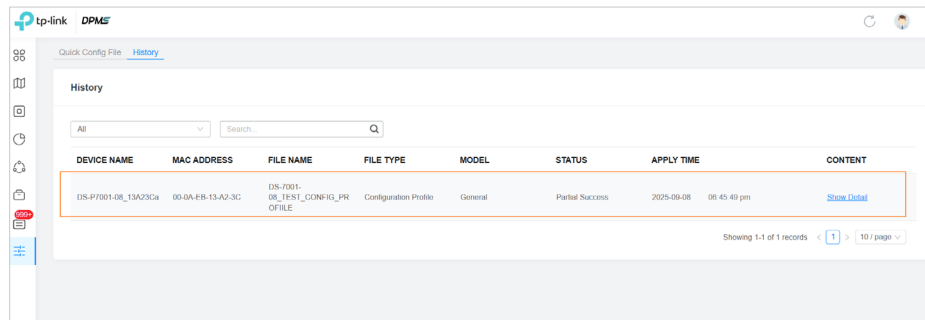
DEVICE NAME	MAC ADDRESS	FILE NAME	FILE TYPE	MODEL	STATUS	APPLY TIME		CONTENT
DS-P7001-08_13A23Ca	00-0A-EB-13-A2-3C	DS-7001-08_TEST_CONFIG_FILE	Configuration File	DS-P7001-08	Success	2025-09-08	04:04:09 pm	Operation succeeded.

Showing 1-1 of 1 records < 1 > 10 / page

Device Name	Quick Config-provisioned OLT device name
MAC Address	Quick Config-provisioned OLT device MAC address
File Name	Quick Config-provisioned file name
File Type	Quick Config-provisioned file type
Model	Quick Config-provisioned OLT device model
Status	Quick Config file provisioning status
Apply Time	Quick Config file provisioning apply time
Content	Quick Config file provisioning result content

7.4.2 Quick Config Profile History

1. Take DS-7001-08_TEST_CONFIG_PROFILE record as a successful deployment example:



2. During Quick Config Profile deployment, specific configuration parameters are displayed. Click the [Show Detail](#) button reveals the deployment status of sub-functions for each functional template within the configuration entries.

