# User Guide

## DeltaStream PON Management System

1910013088 REV1.0.0
JAN 2022

# 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.

| | |
|---|---|
| Note | 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:/ 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

## Manage Administrator Accounts of DPMS

# Overview

The chapter includes the following sections:



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

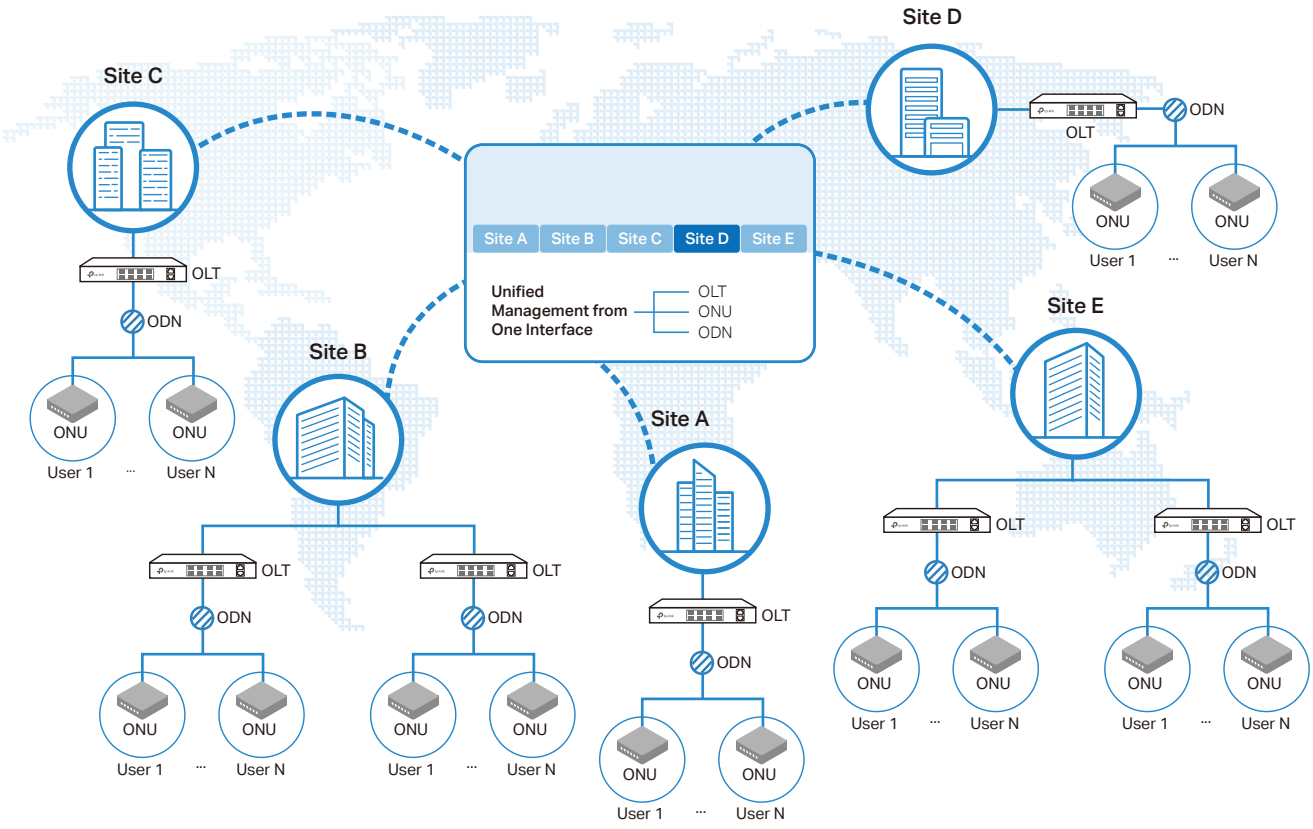
| Acronym | Full Name |
|---|---|
| **DPMS** | DeltaStream PON Management System |
| **GPON** | Gigabit-Capable Passive Optical Network |
| **ISP** | Internet Service Provider |
| **OLT** | Optical Line Terminal |
| **ONU** | Optical Network Unit |
| **ONT** | Optical Network Terminal |
| **FTTH** | 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.

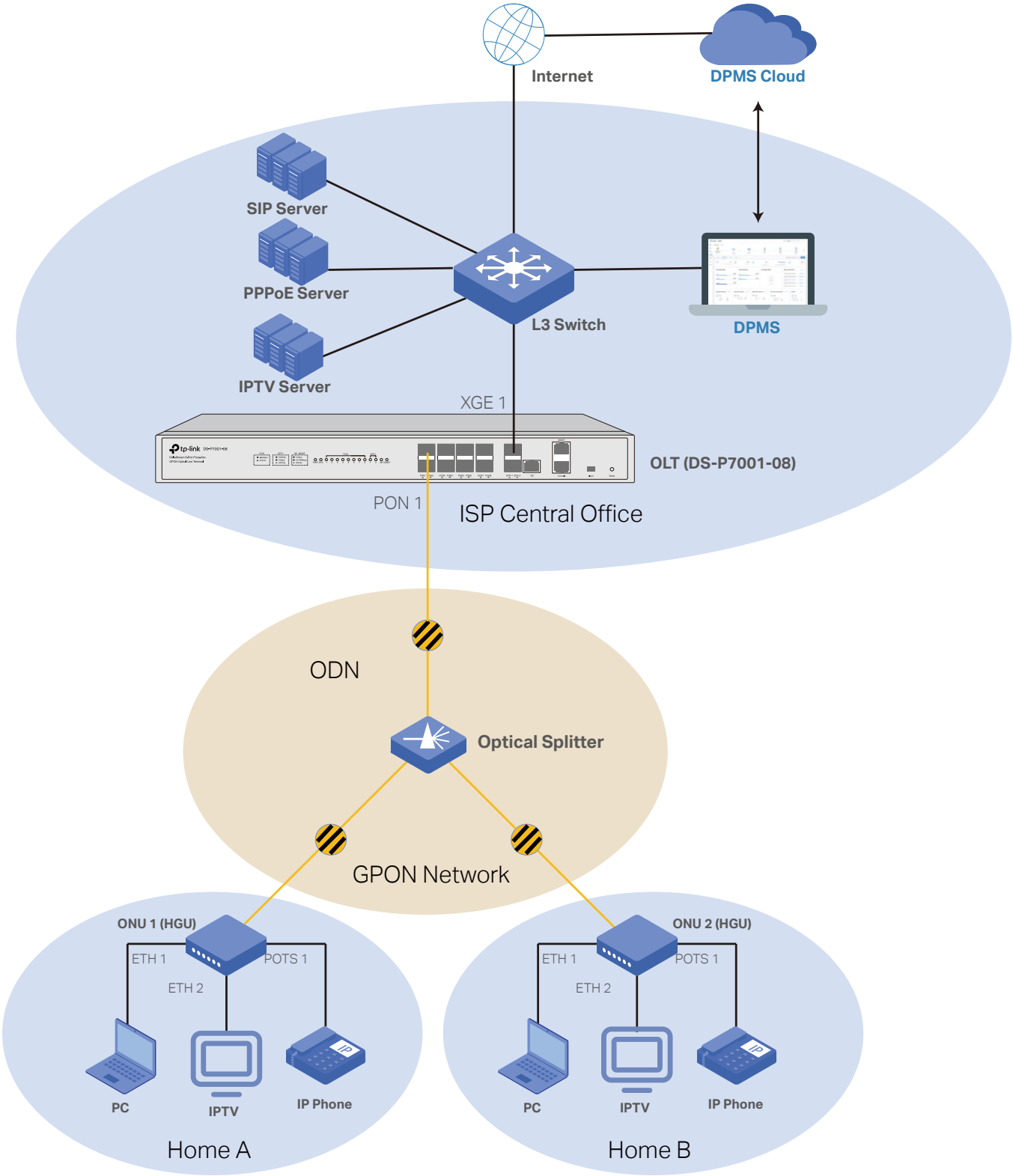
DPMS offers centralized management for configuring GPON of the ISP. DPMS simplifies deploying, configuring and monitoring the GPON networks by managing all the GPON-related devices at multiple sites from one central platform. This unleashes new levels of management to avoid complex and costly overprovisioning. 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 architeture 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 cetralized 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).<br><br>There are different types of ONUs, such as HGU (Home Gateway Unit) and SFU (Single Family Unit). |
| ODN | ODNis 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. |

# Get Started with DPMS

This chapter guides you on how to get started with DPMS to configure the GPON. including the initial setup steps, building your network topology, deploying your DPMS, and logging in to the DPMS.

# 2. 1 Install DPMS

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**

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

  **Web Browser:** Mozilla Firefox 83 (or above), Google Chrome 89 (or above), Safari, or Microsoft Internet Explorer 11 (or above).

- **Install DPMS**

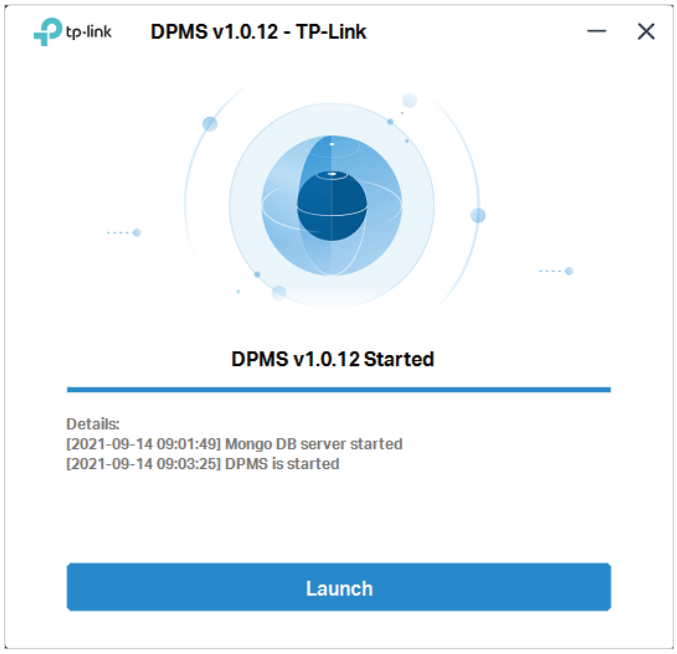
  Ensure that the Java Runtime Environment (JRE) have been installed in your system. The DPMS requires that the system have Java 8 installed. Download the installation file of DPMS from the website. Then follow the instructions to properly install DPMS. After a successful installation, a shortcut icon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

## 2. 1. 1 Start and Log In to the DPMS

Launch DPMS and follow the instructions to complete the basic configurations, and then you can log in to the management interface.

## Launch DPMS

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.



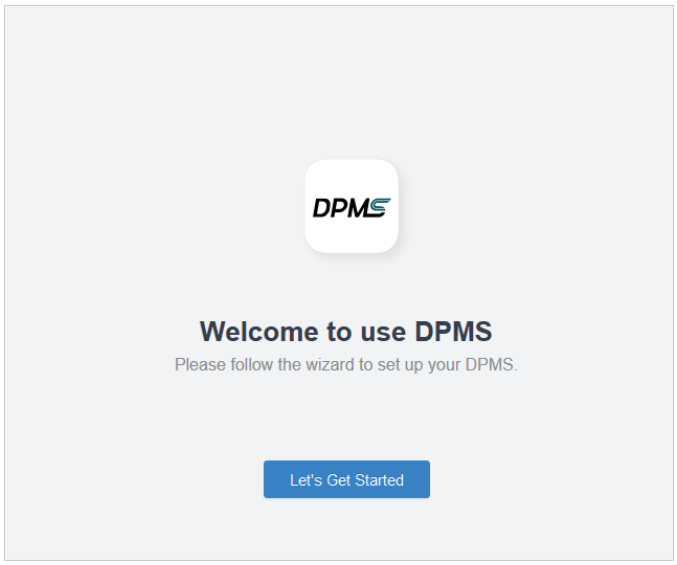

Note:

- 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.

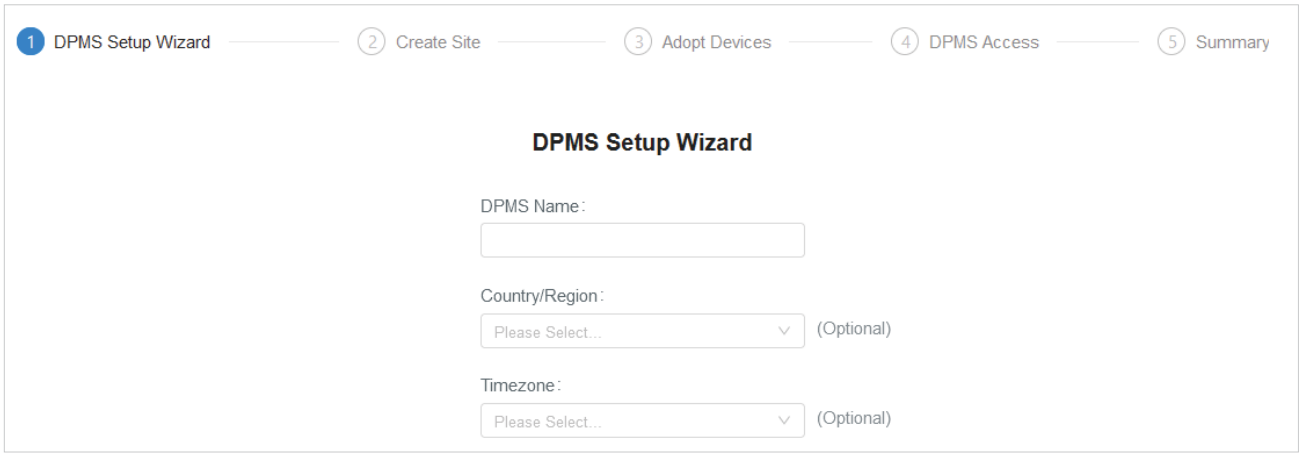
## Do the Basic Configurations

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

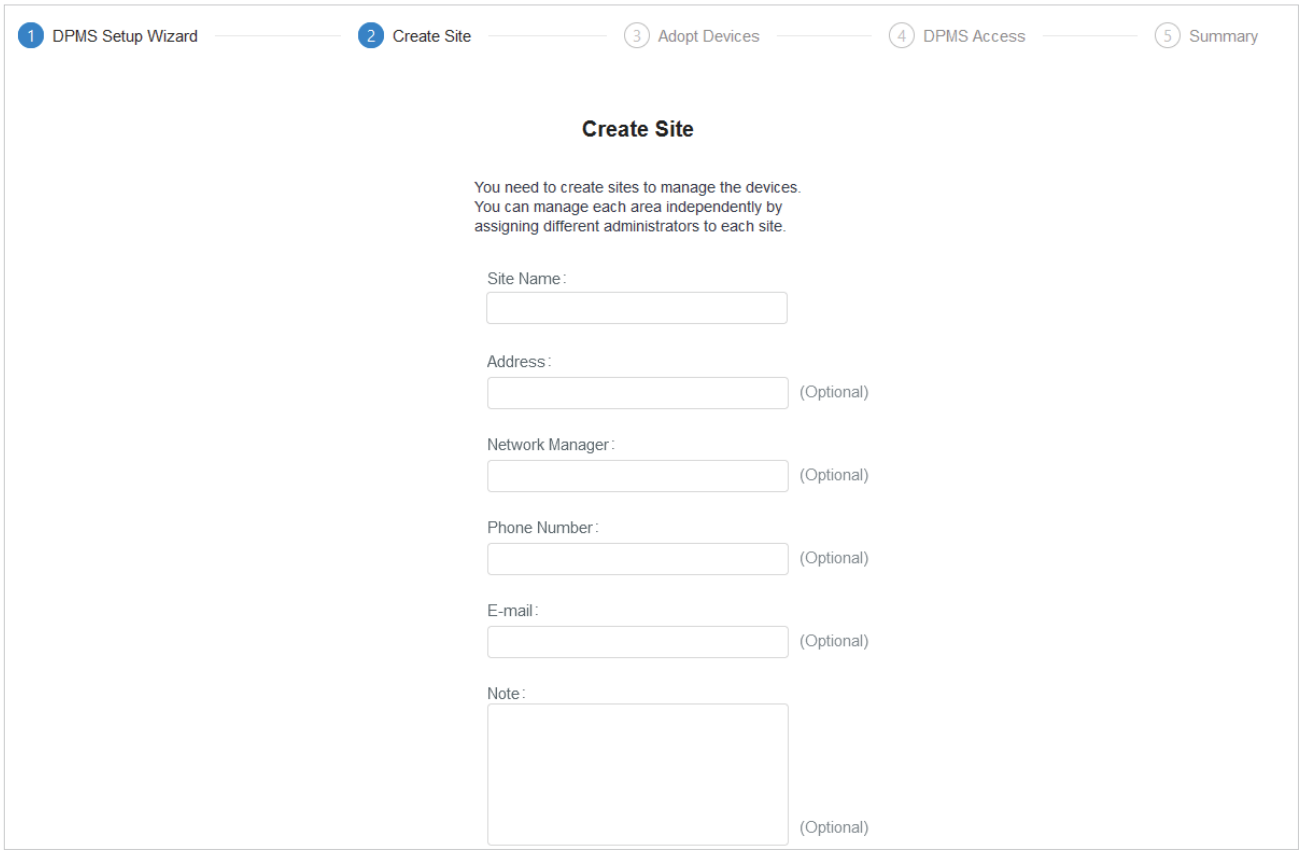
1. Click Let's Get Started.



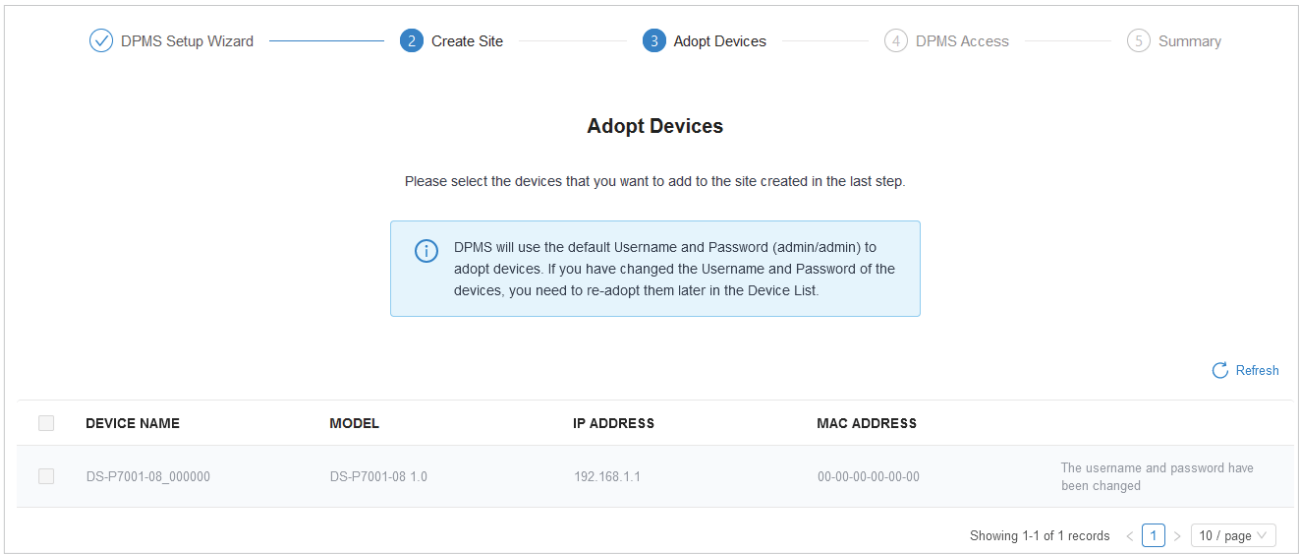
2. Specify a name for your DPMS, and set your region and timezone. Then click Next.




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



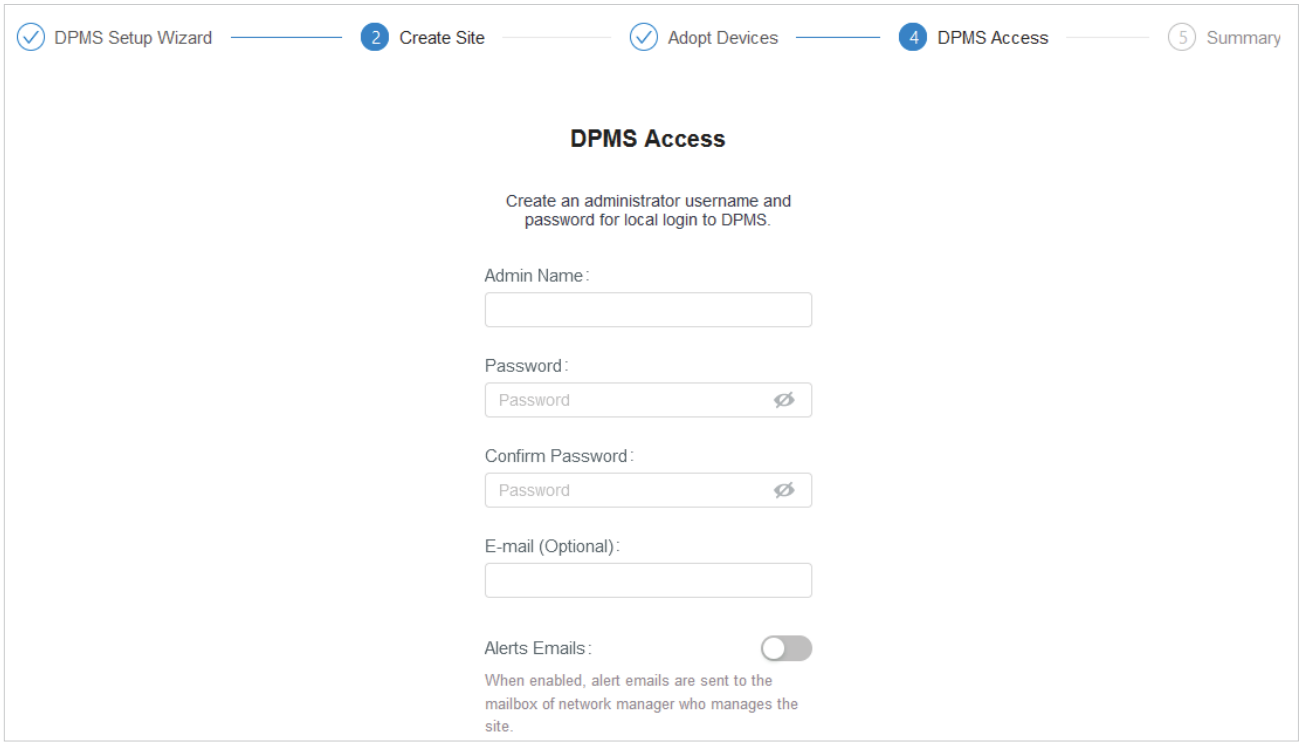
4. The setup page displays all the discovered devices in the network. Select one or more devices to adopt and add to the site. Click Next.



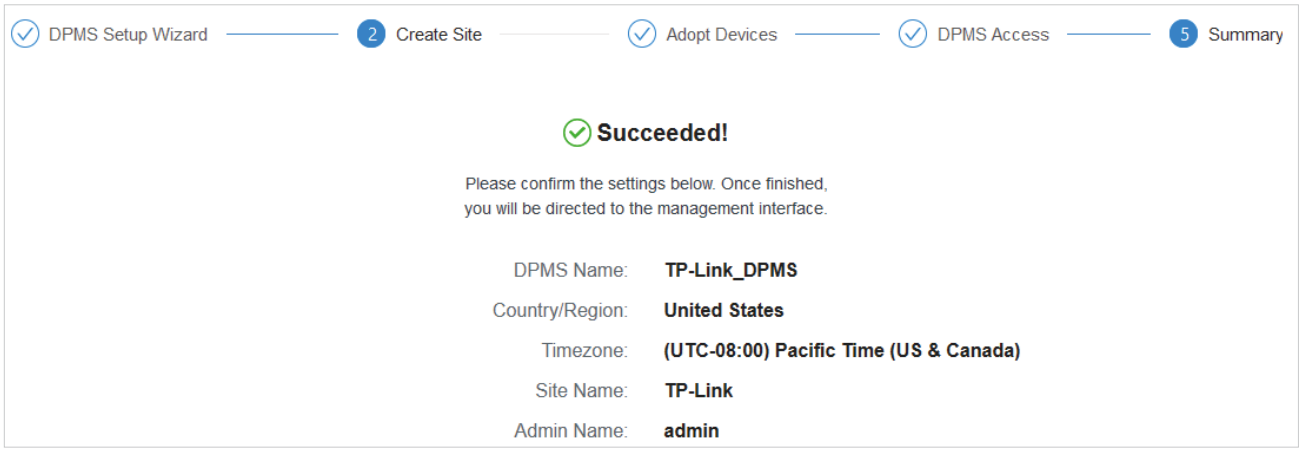

## Note:

- 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.



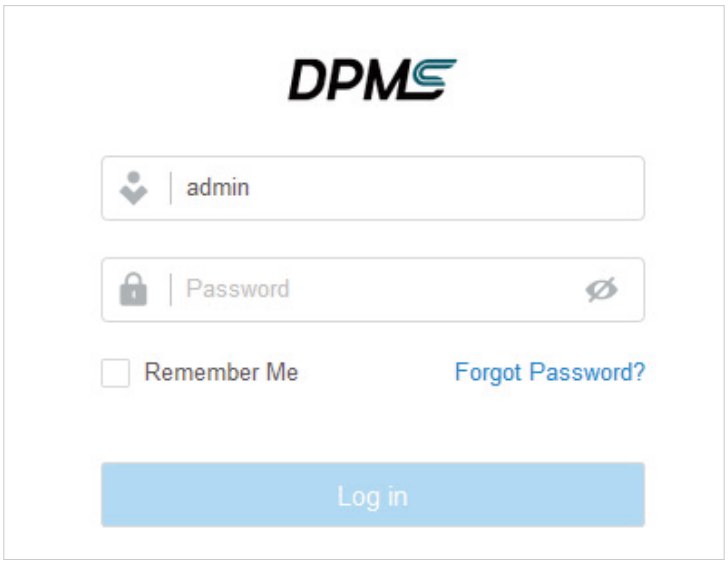
6. Review your settings and click Finish.




## 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.



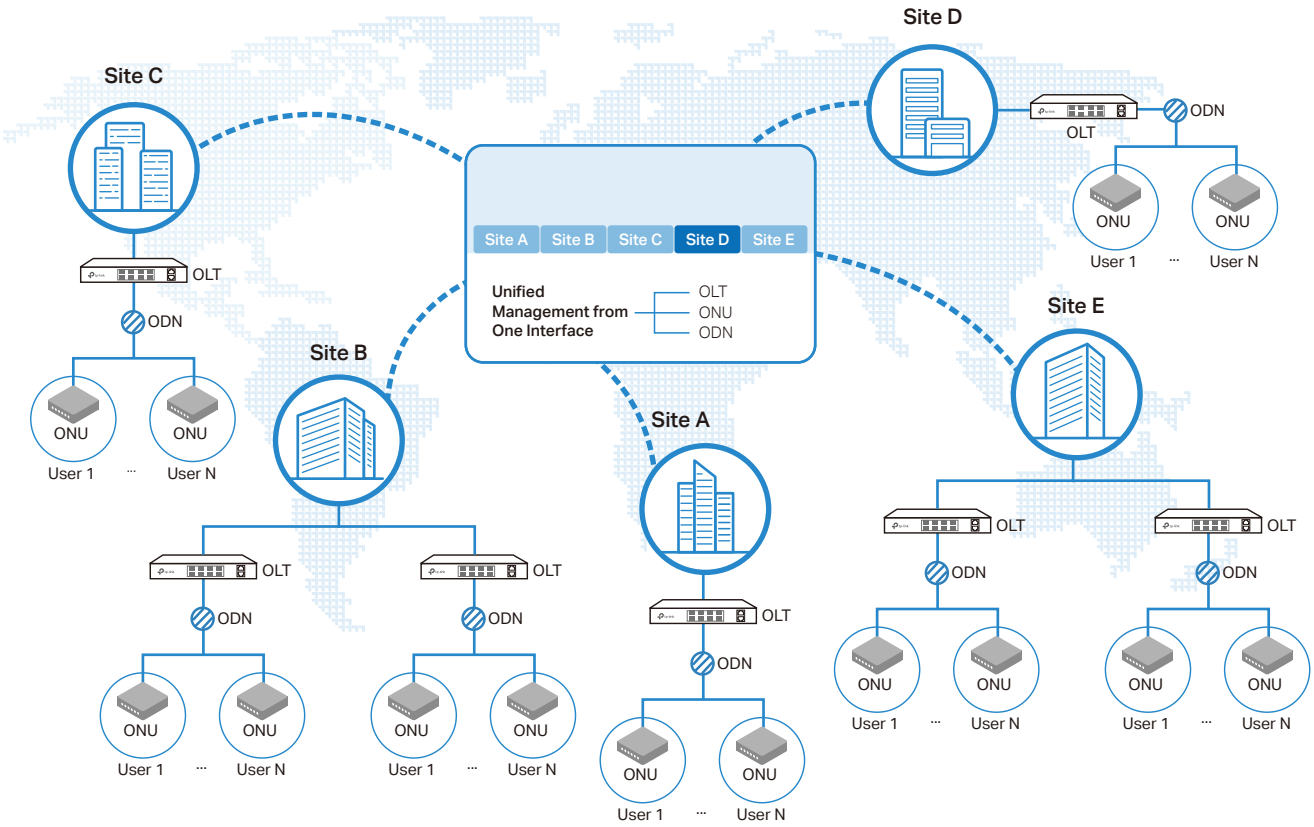
# Manage Devices and Sites

Start managing your network by creating sites and adopting devices so that you can configure and monitor your devices centrally while keeping things organized.

# 3. 1 Create Sites

## Overview

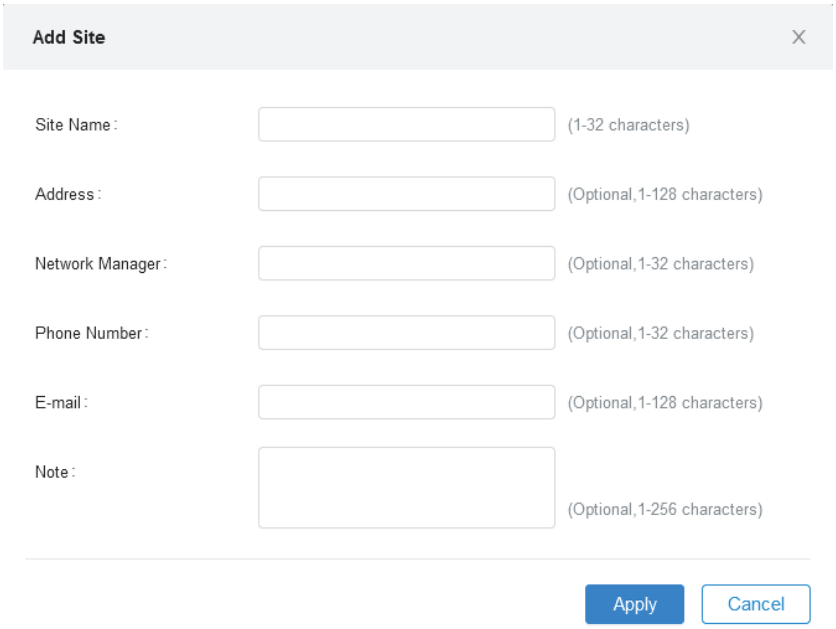
Different sites are logically separated network locations, like different subsidiaries or offices of the ISP. It's best practice to create one site for each location and add all the devices within the network to the site, including the OLTs and ONUs.



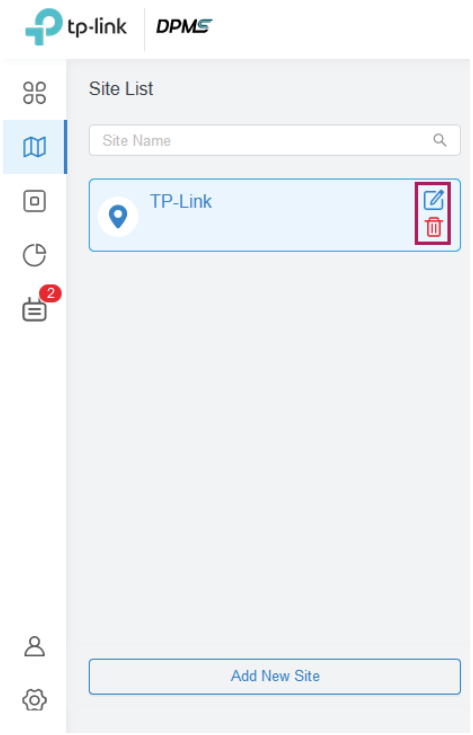
## Configuration

To create sites, follow these steps:

1. Go to Site. Click Add New Site. Configure the parameters and click Apply.

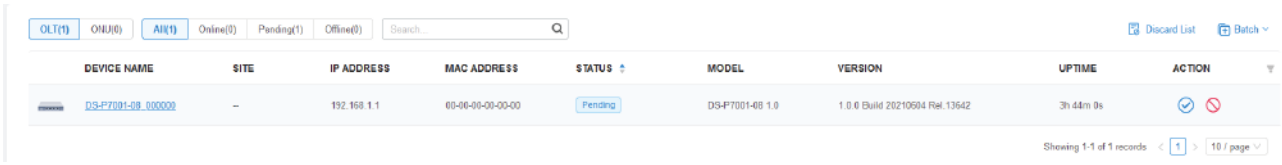



2. You can click in the site list to edit the site configuration. You can click to delete the site.

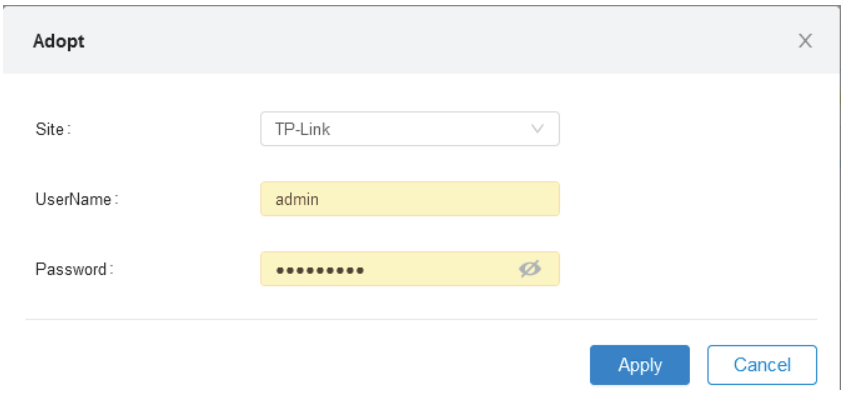


# 3. 2 Adopt Devices

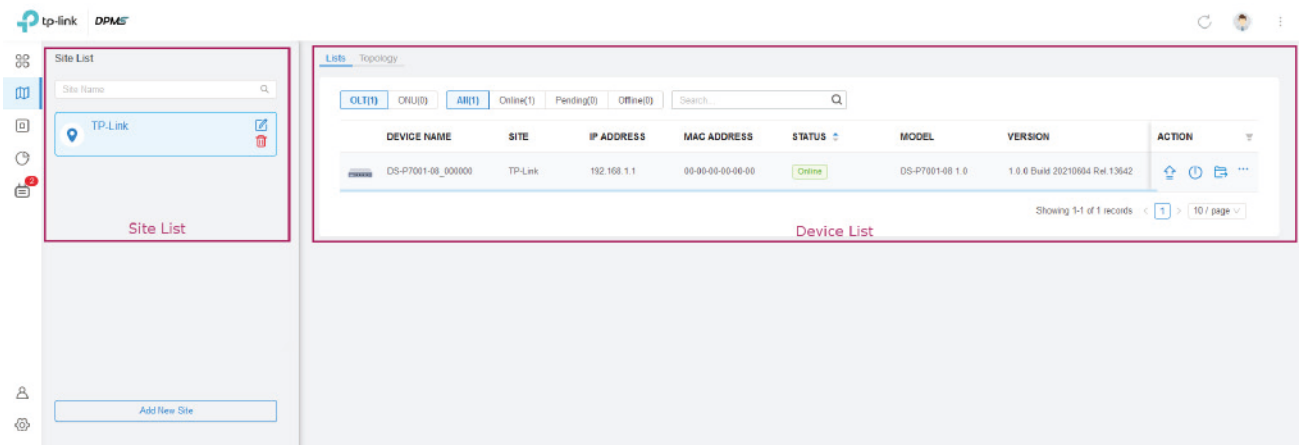
1. To add a device to the site, go to Devices. The devices which has been discovered by DPMS appear in the list and the status is Pending.



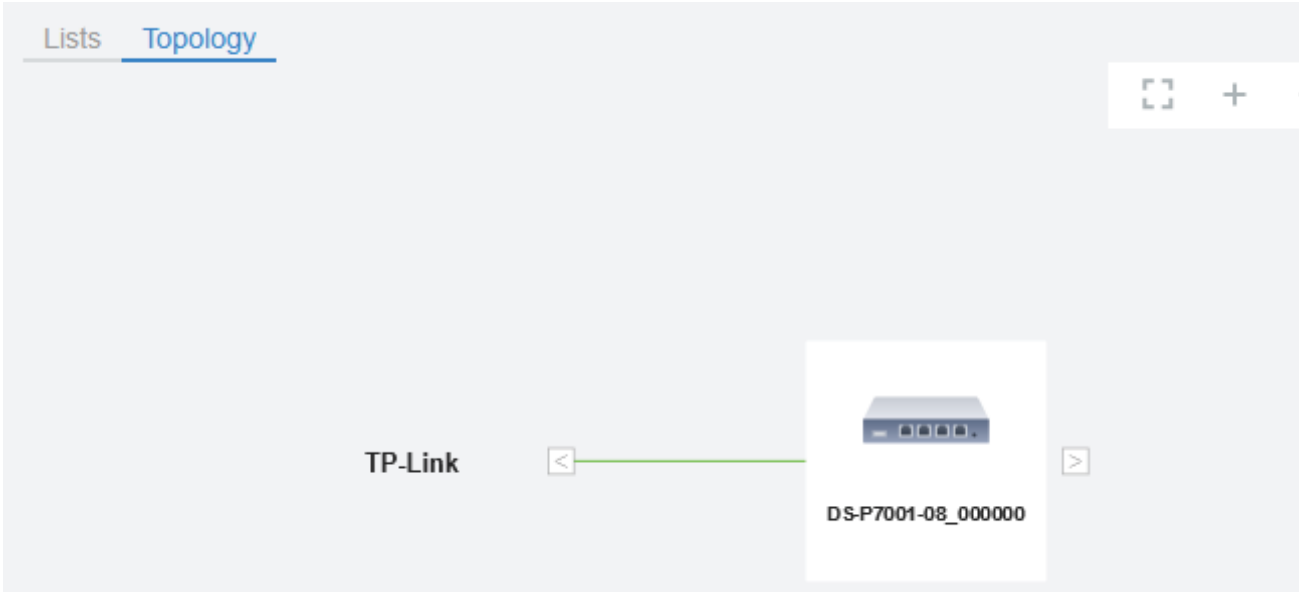

2. Select the device and click . Select the desired site and enter the username and password to adopt the device. Then click Apply.




3. Go to Site. Select the site from the site list and the devices of the site are displayed in the device list.



4. In the Topology tab, you can view the connections between all the OLTs and ONUs and get an intuitive overview of the whole network of the site.



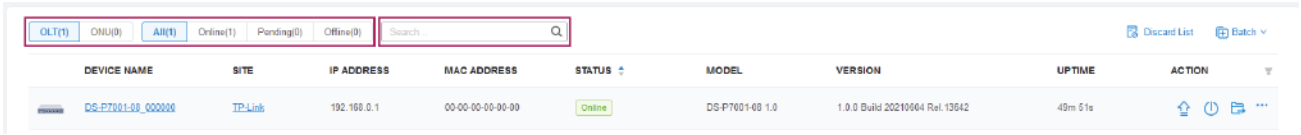
# 3. 3 Manage Devices

## Overview

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.

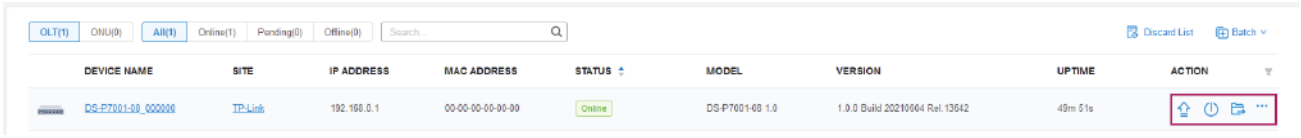
## Configuration

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.



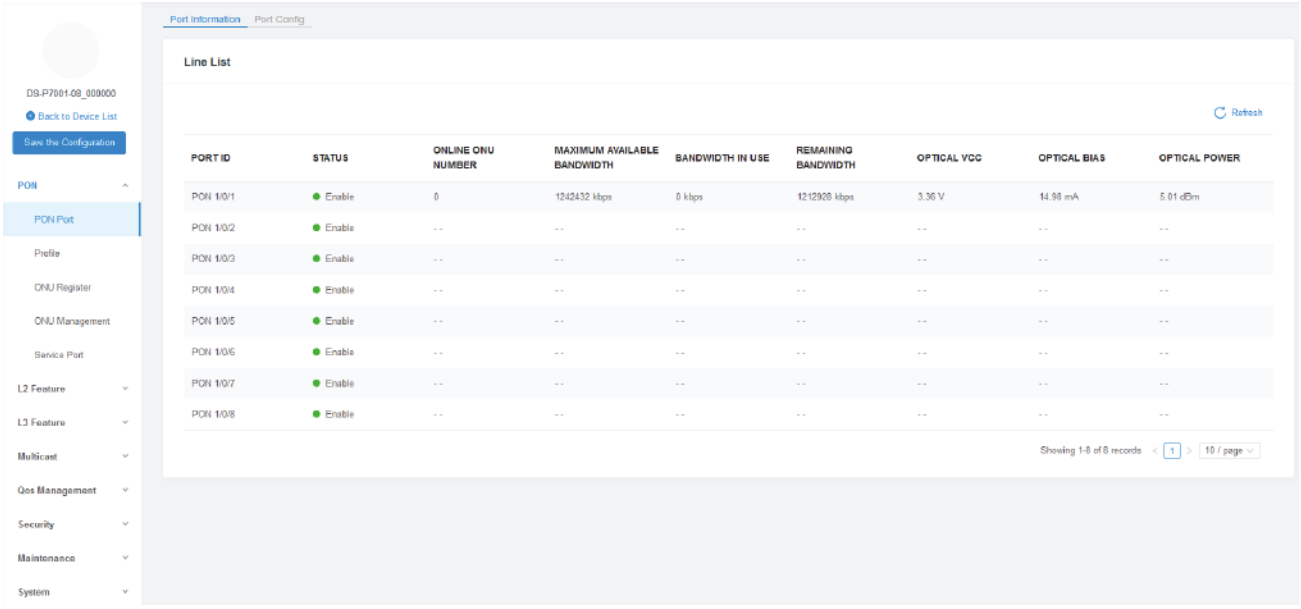

| | |
|---|---|
| Online | The device has been adopted by DPMS and it is powered on and connected to the network. |
| Pending | The device has been discovered by DPMS and has not been adopted. |
| Offline | The device has been adopted by DPMS but it is powered off or disconnected from the network. |

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 deivce. Alternatively, you can click Batch and select the operations to perform on devices in batches.




| | |
|---|---|
| | To manaully 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. |

3. 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.



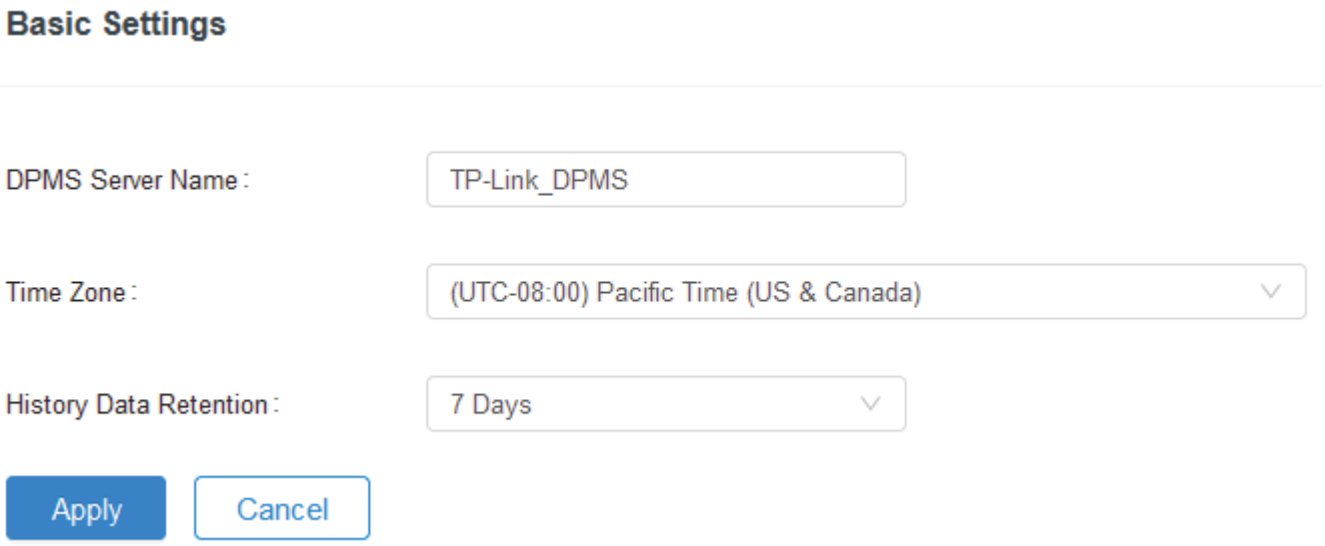
# Configure DPMS

DPMS Settings control the appearance and behavior of DPMS and provide methods of data backup, restore:

# 4. 1 General Settings

## 4. 1. 1 Basic Settings

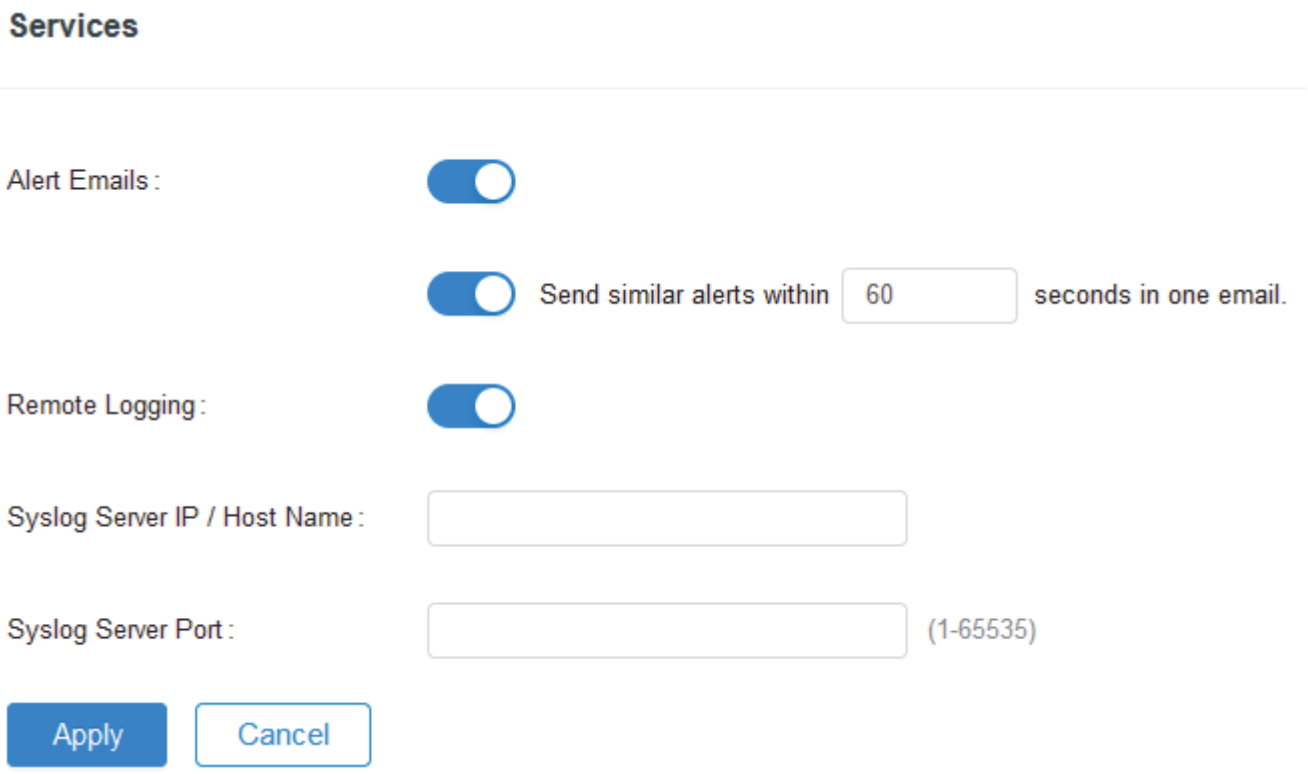
Go to Settings > General Settings. In Basic Settings, configure the parameters and click Apply.




| | |
|---|---|
| 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.




| | |
|---|---|
| Alert Emails | Enable alert emails: When enabled, DMPS can send emails to notify the administrators, operators and viewers of the alert logs once generated.<br><br>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.<br><br>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:<br><br>Syslog Server IP/Hostname: Enter the IP address or hostname of the log server.<br><br>Syslog Server Port: Enter the port of the server. |

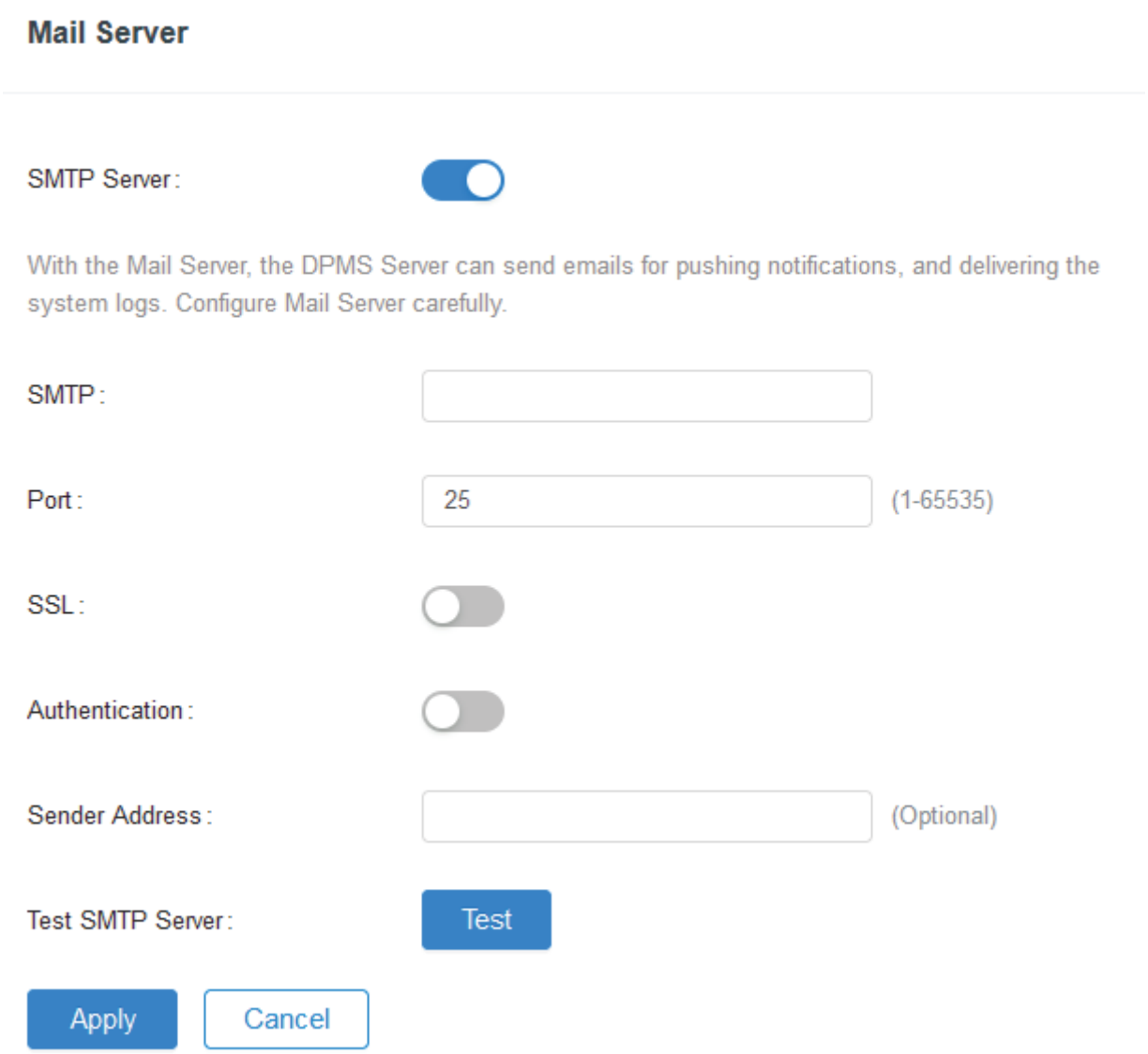
### 4. 1. 3 Mail Server

#### Overview

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.

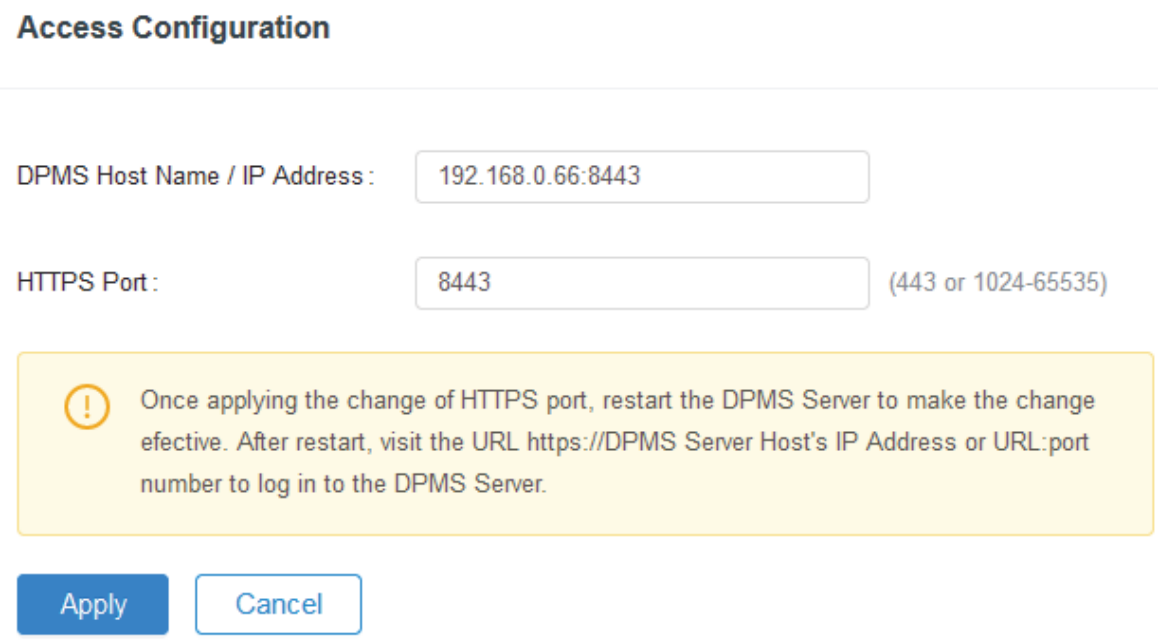



| | |
|---|---|
| SMTP | Enter the URL or IP address of the SMTP server according to the instructions of the email service provider. |
| Port | Configure the port used by the SMTP server according to the instructions of the email service provider. |
| SSL | Enable or disable SSL according to the instructions 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.




| | |
|---|---|
| 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

### Overview

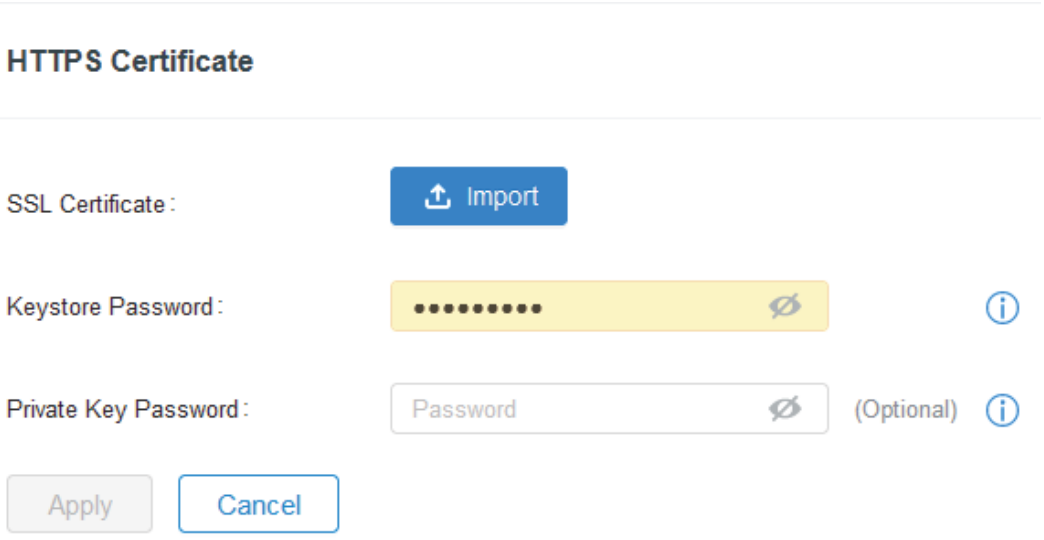
If you have assigned a domain name to the controller for login, to eliminate the "untrusted certificate" error message that will appear in the login process, you can import the corresponding SSL certificate and private key here. The certificate and private key are issued by the certificate authority.

Note:

- You need to restart you 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. Then click Save.




| | |
|---|---|
| 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

## Overview

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

## Configuration

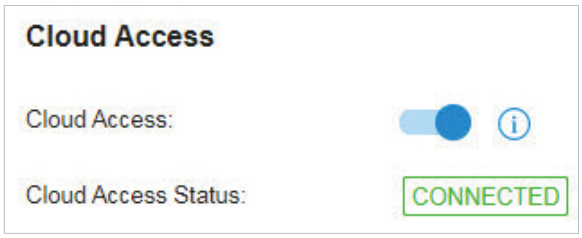
To manage your DPMS from anywhere, follow these steps:

1. Prepare your DPMS for Cloud Access

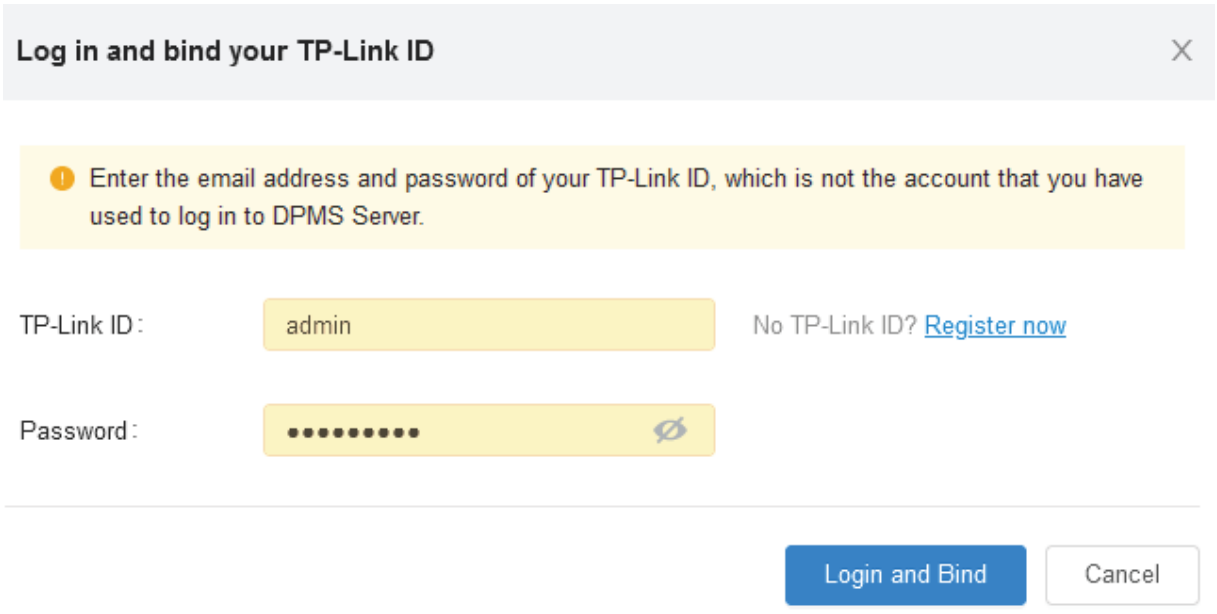
Note:

- 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.

**1)** Go to Settings > Cloud Access. Enable Cloud Access.




**2)** Enter your TP-Link ID and password. Then click Log In and Bind.




**3)** 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

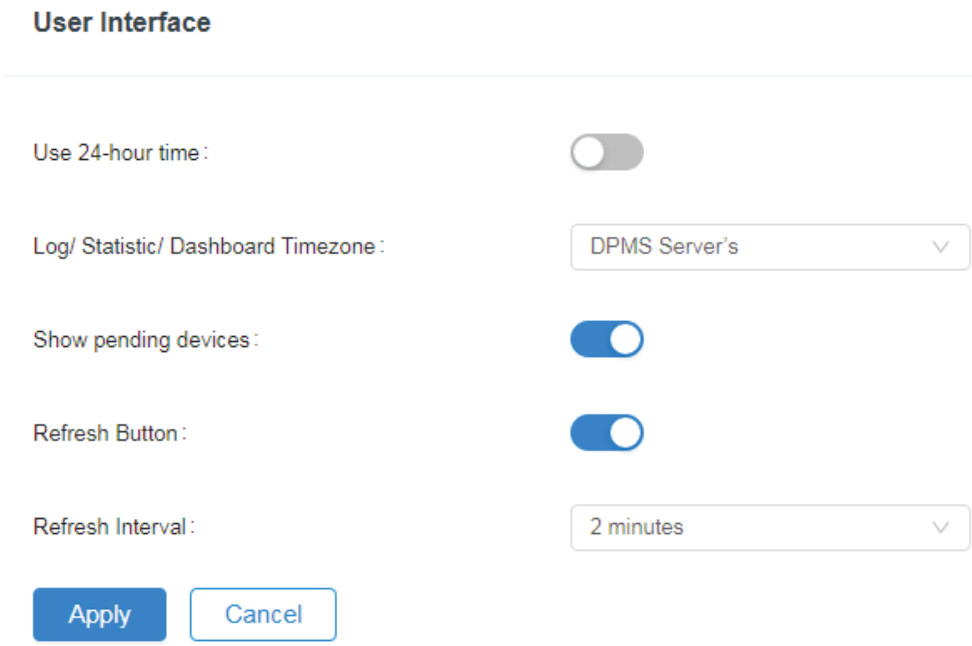
## 4. 3. 1 User Interface

### Overview

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.




| | |
|---|---|
| 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.<br>Browser's (PC): Browser's Timezone is synchronized with the browser configuration.<br>DPMS Server's: DPMS Server's Timezone is set in General Settings of DPMS.<br>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

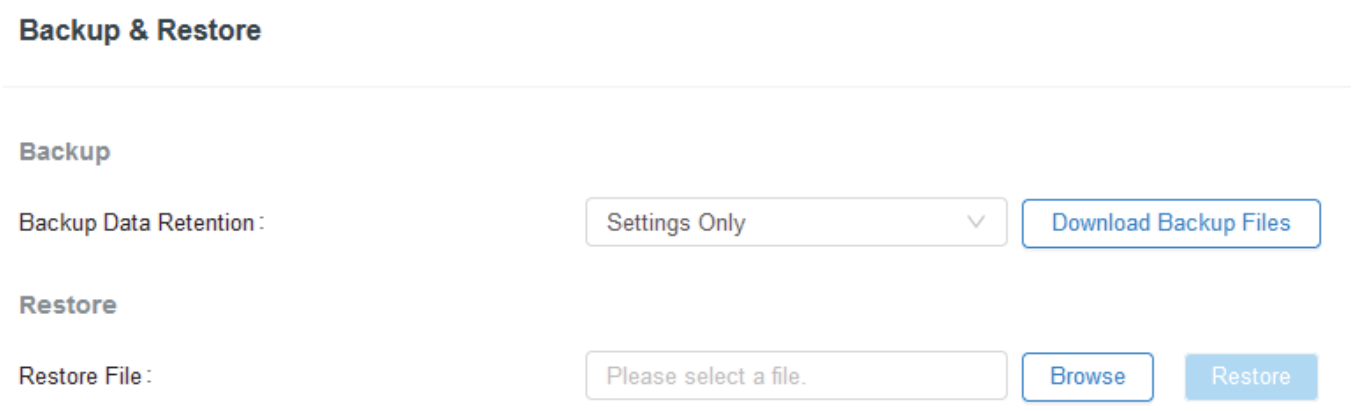
### Overview

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

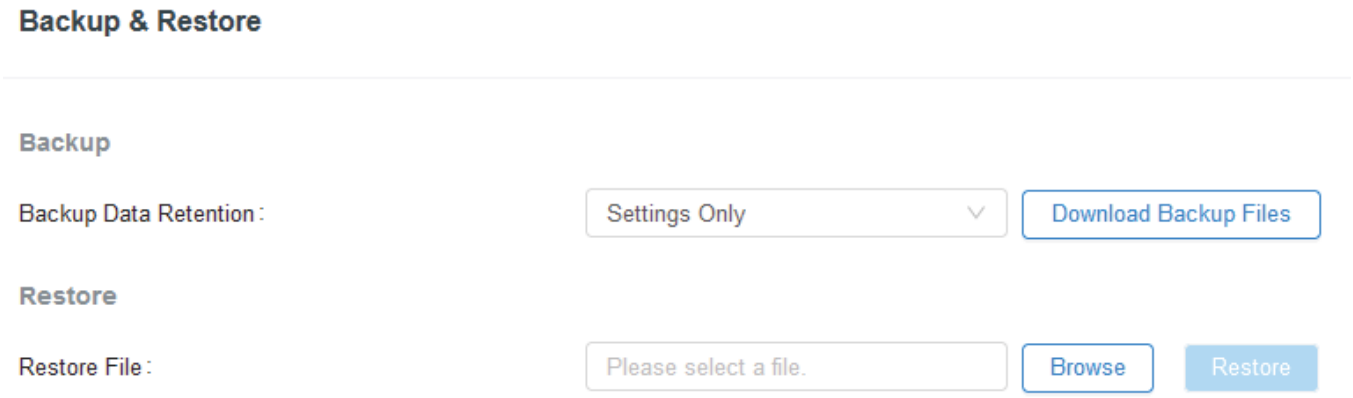
- **Backup**

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.



- **Restore**

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



# 4. 4 Auto Backup

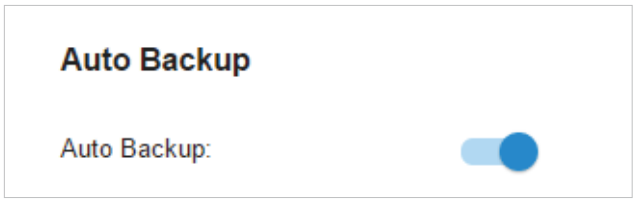
## Overview

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.

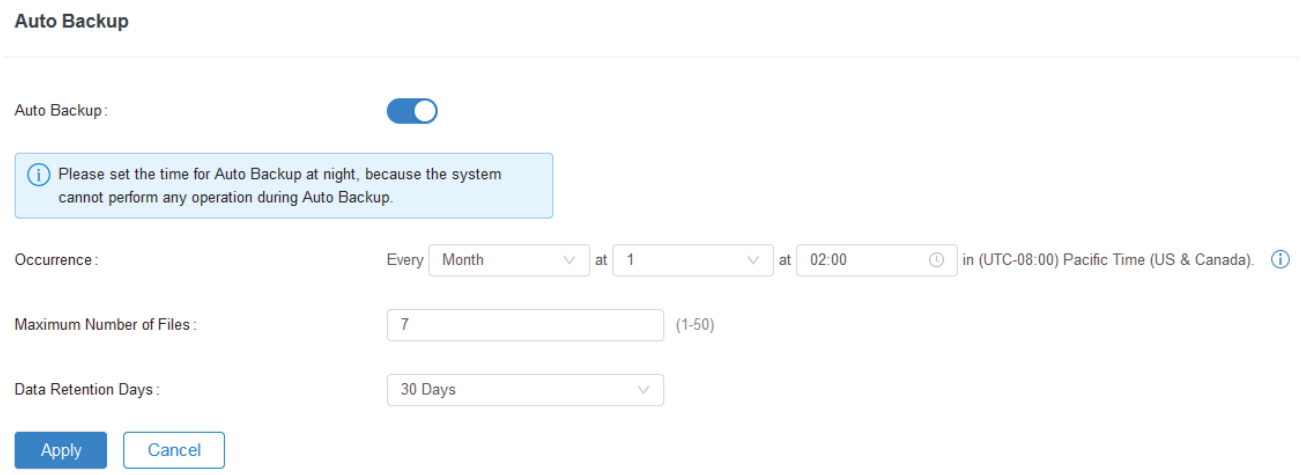
## Configuration

To configure Auto Backup, follow these steps:

1. Go to Settings > Auto Backup. Click to enable Auto Backup.



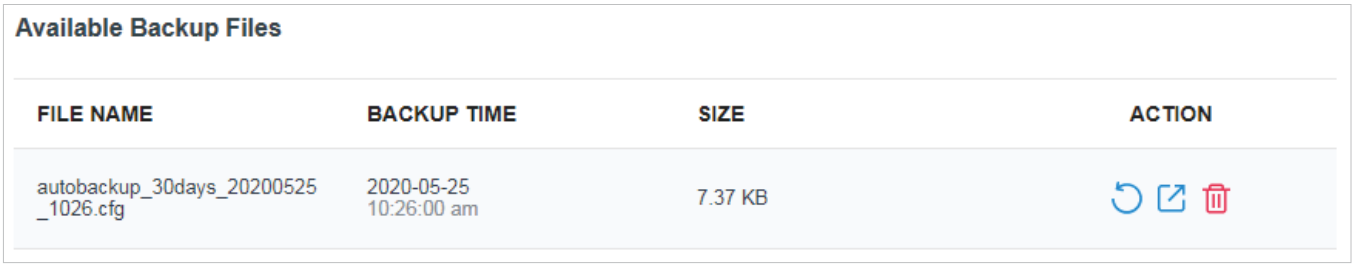

2. Configure the following parameters to specify the rules of Auto Backup. Click Apply.




| | |
|---|---|
| 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.<br><br>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. |

| | |
|---|---|
| Data Retention Days | Select the length of time in days that data will be backed up.<br><br>Settings Only: Back up DPMS settings only.<br><br>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.<br><br>All Time: Back up all data in DPMS. |

You can view the name, backup time and size of backup files in Available Backup Files.




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.<br><br>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. |

# 5

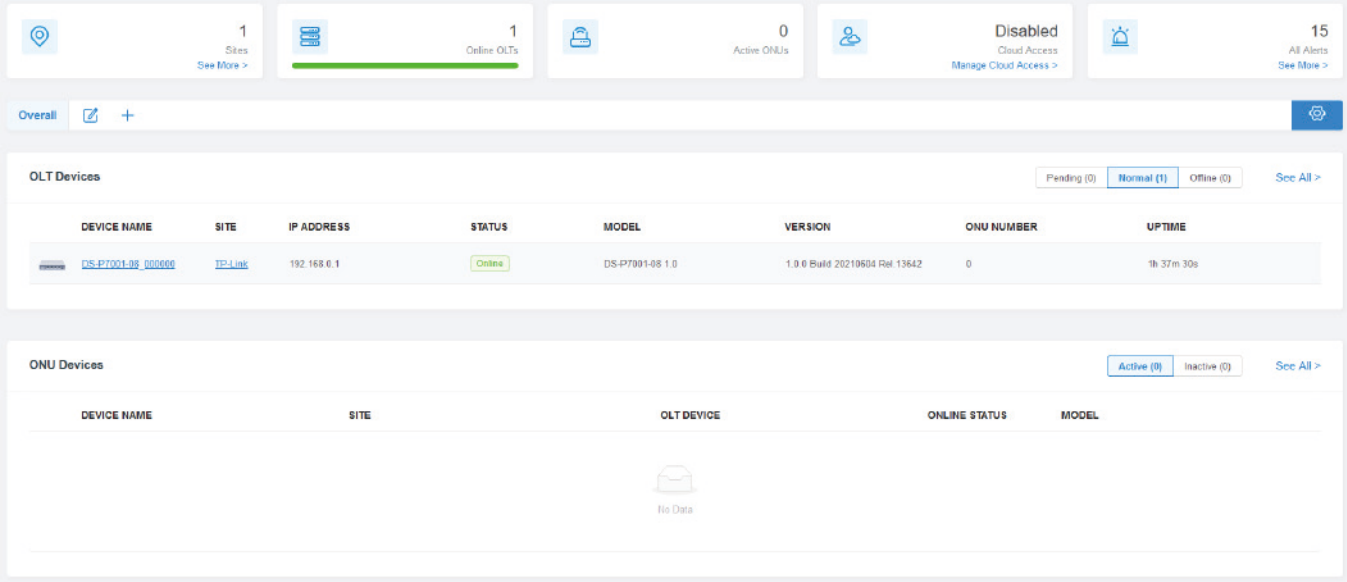
# *Monitor the Network*

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. This chapter includes the following sections:

# 5. 1 View the Status of Network with Dashboard

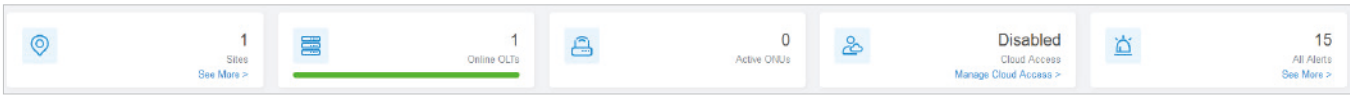
## 5. 1. 1 Page Layout of Dashboard

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.



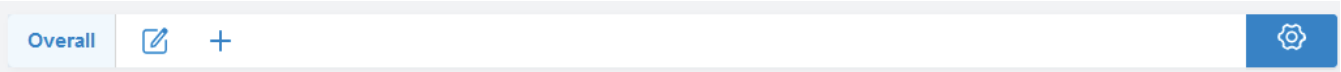

### Network Overview

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. |

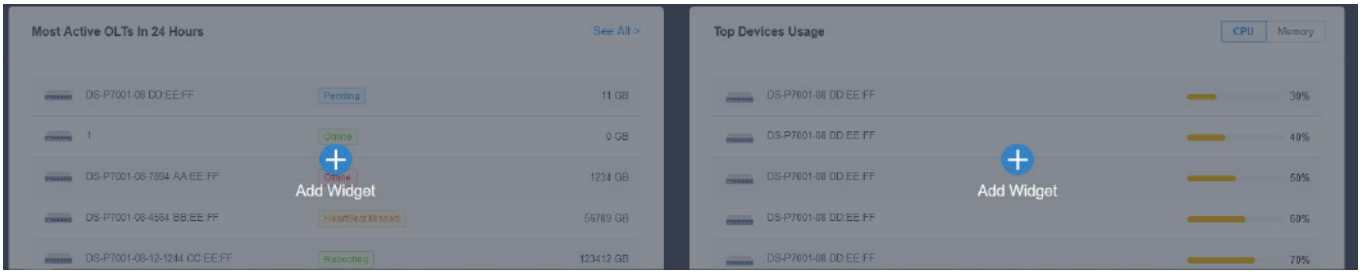
In the tab bar, you can take the following action to edit the tabs and customize the widget to be displayed.

| | |
|---|---|
|  | 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. |

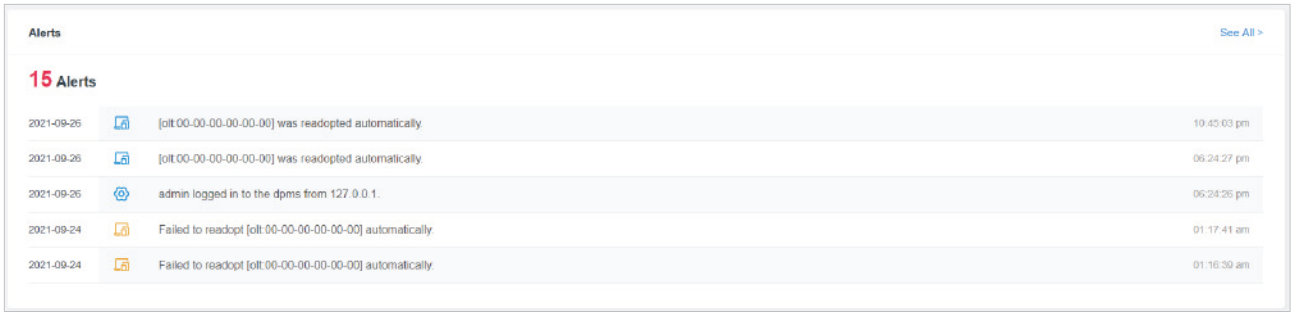
## 5. 1. 2 Explanation of Widgets

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



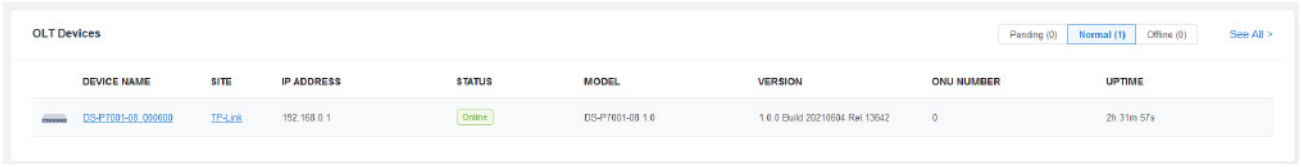

- **Alerts**

  The Alerts widget displays the total number of unarchived alerts happened in the network and details of the latest ten. 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.



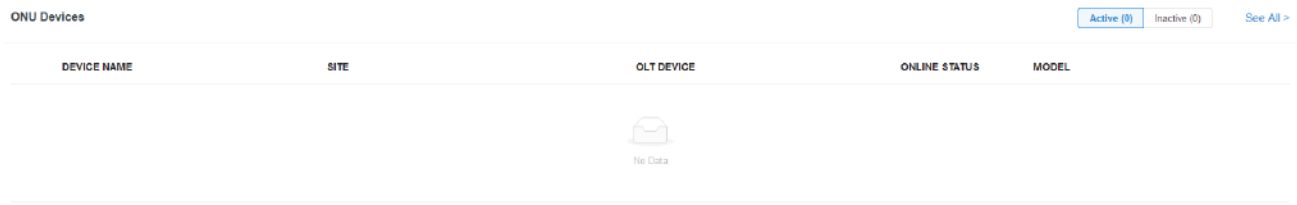

- **OLT Devices**

  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.



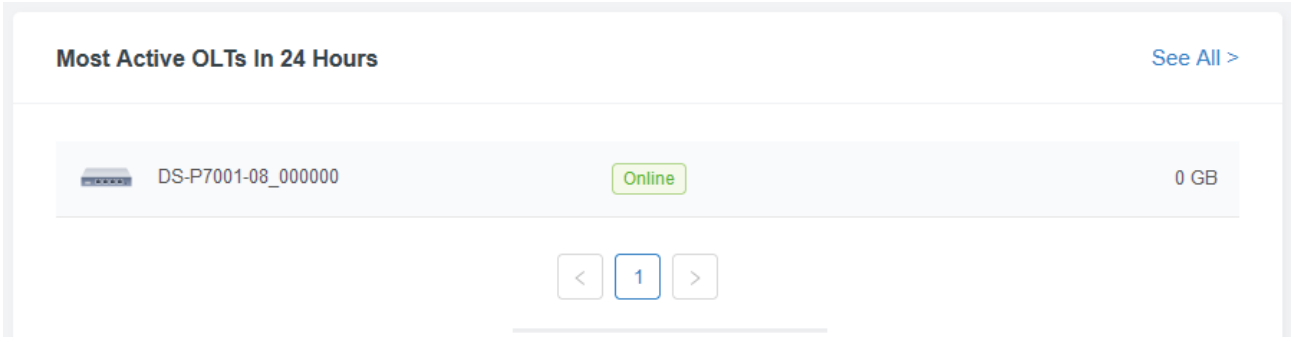
- **ONU Devices**

  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.



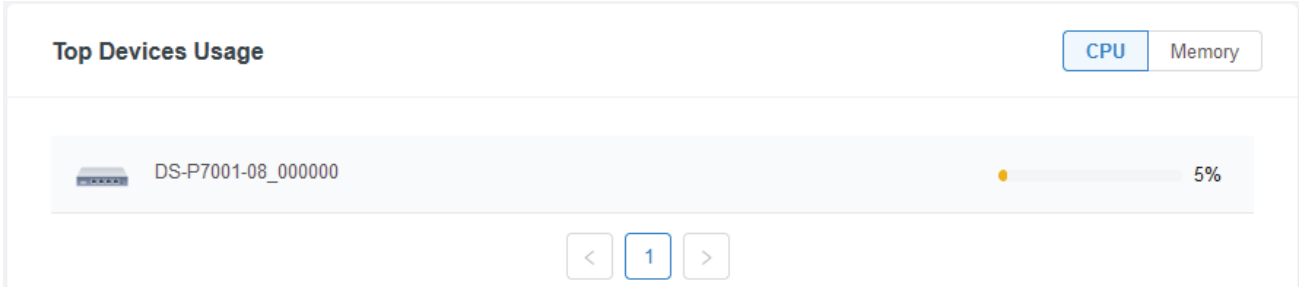

- **Most Active OLTs In 24 Hours**

  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.




- **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.



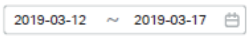
# 5. 2 View the Statistics of the Network

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.

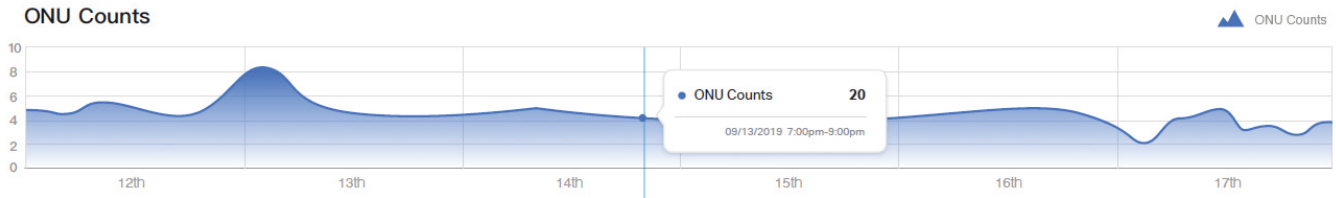
### Tab Bar


| | |
|---|---|
|  | 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.<br><br>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

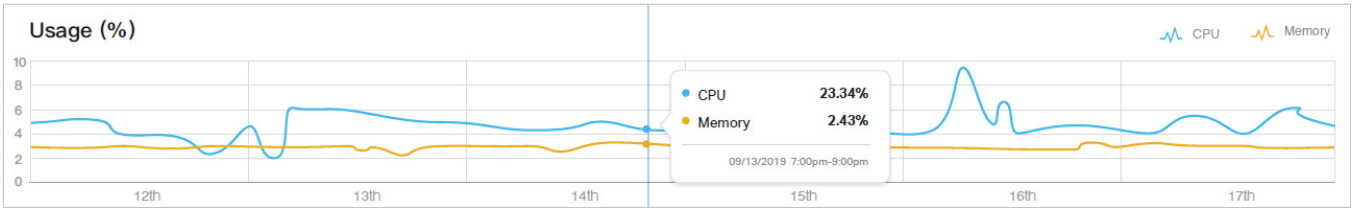
- **ONU Counts**

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.



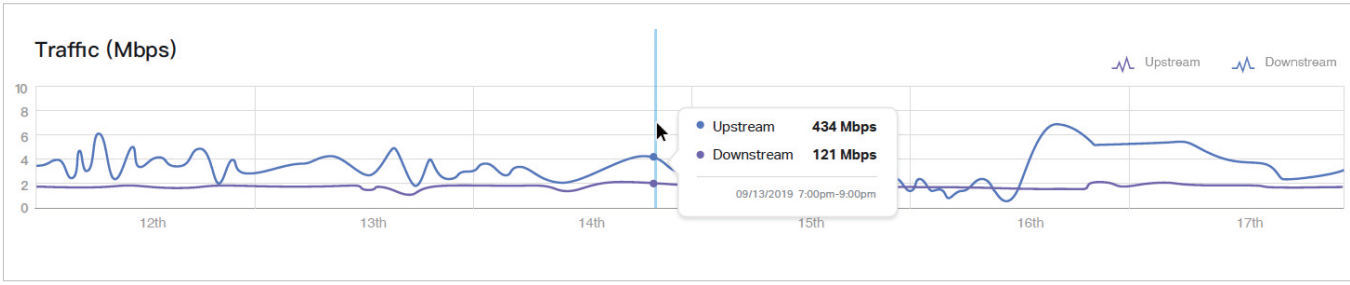
- **Usage**

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.

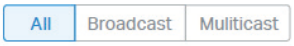



## 5. 2. 2 Traffic/DDM Statistics

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

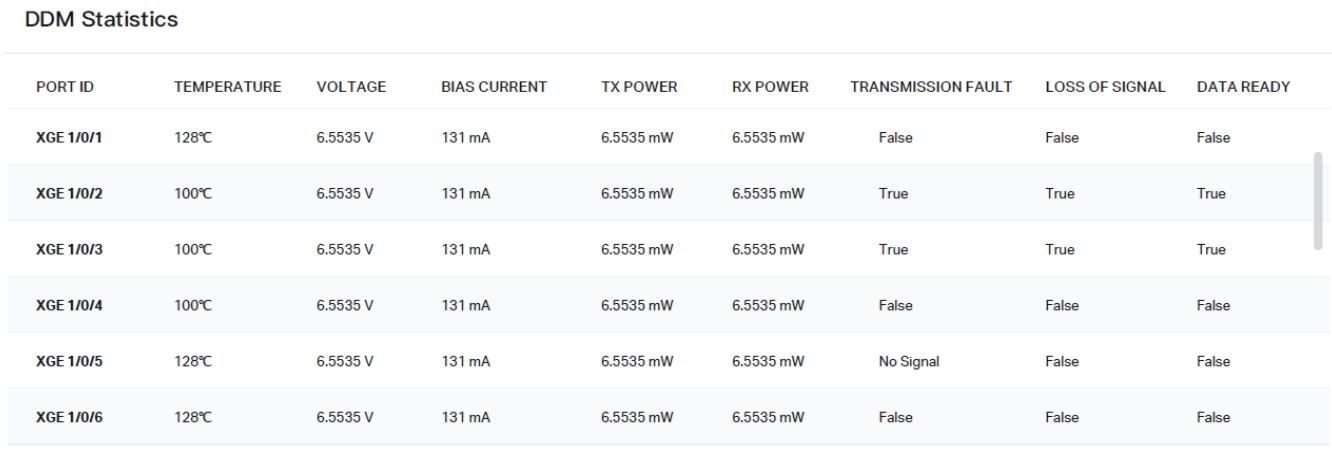

| | |
|---|---|
|  | Click to select a device from the drop-down list to view its statistics. |
|  | Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right.<br><br>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. |

| | |
|---|---|
|  | Select Natural, Transmitted, Received, or Total to specify the graph order of ports.<br><br>Natural: Displays the line graphs in ascending order of the port number.<br><br>Transmitted: Displays the line graphs in descending order based on the traffic volume of transmitted packets.<br><br>Received: Displays the line graphs in descending order based on the traffic volume of received packets.<br><br>Total: Displays the line graphs in descending order based on the total traffic volume of transmitted and received packets. |
|  | Select bps, Bytes or Packets to specify the data type and measuring unit.<br><br>Mbps: Displays the traffic rate in Mbps.<br><br>MB: Displays the traffic statistics in MB.<br><br>Packets: Displays the total number of packets. |
|  | If you select Packet, click the tab to specify which type of packet statistics to be displayed.<br><br>All: Displays statistics of all packets, including broadcast and multicast packets.<br><br>Broadcast: Displays statistics of broadcast packets only.<br><br>Multicast: Displays statistics of multicast packets only. |

## Statistical Tables/Graphs

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

### ■ DDM Statistics (GE Port Excluded)

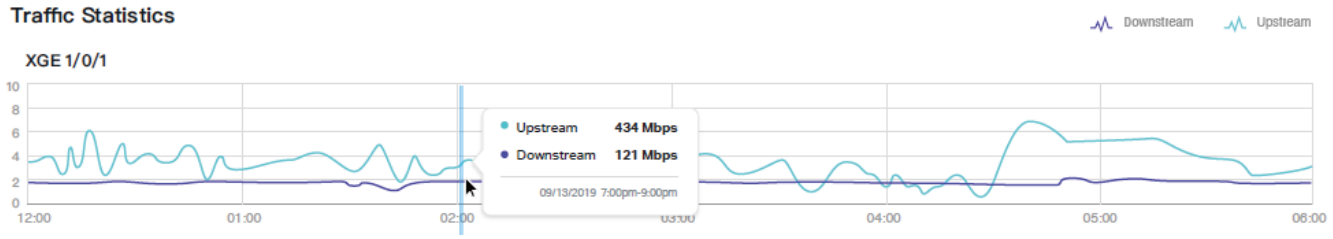



| | |
|---|---|
| Temperature | Displays the temperature of the port. |
| Voltage | Displays the voltage of the port. |

| | |
|---|---|
| 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.



## 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**

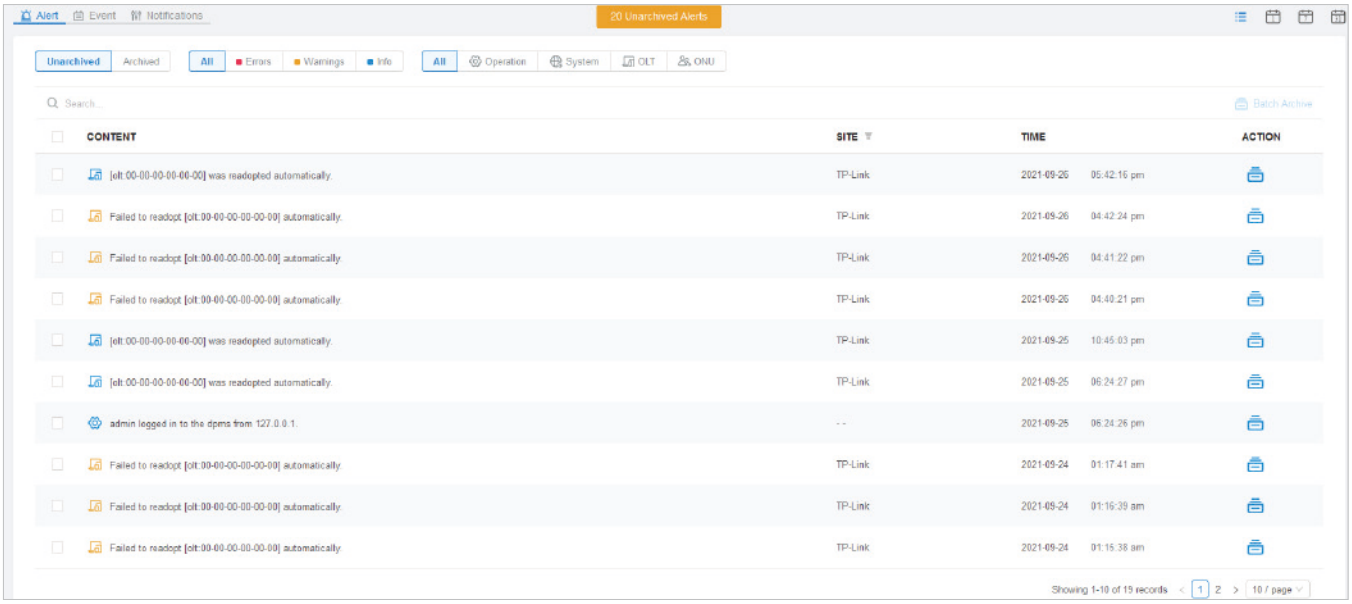
  Three levels in severities are Error, Warning, and Info, whose influences are ranked from high to low.

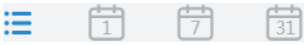
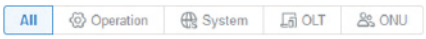
- **Contents**

  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.

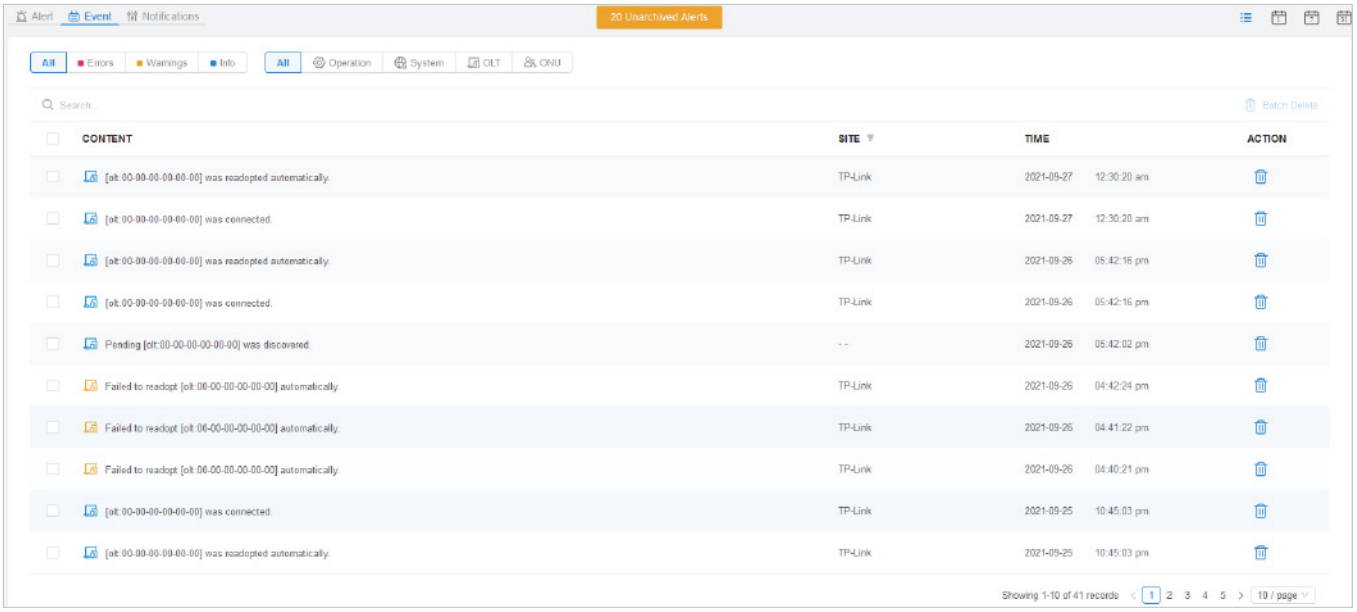


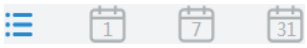
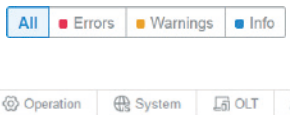

| | |
|---|---|
|  | Click to change the view mode for a better overview.<br><br>: Displays the logs in a table.<br><br>/ / : Displays the logs in a day/week/month. To change the time, click or . To jump back to the current one, click Today/This Week/This Month. |
|  <br>  <br>  | Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously.<br><br>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.<br><br>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.<br><br>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. |
|  | 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 Archive | Select the log entries and click Batch Archive to archive them in batches. |
| | Click to archive the log entry. |

## 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.

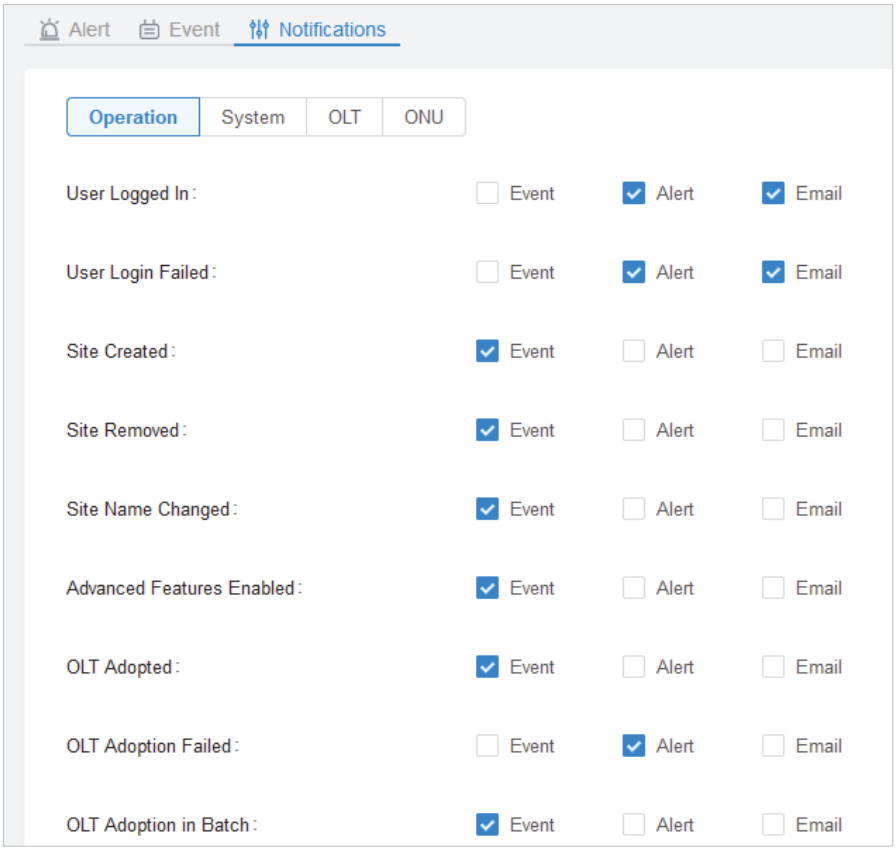



| | |
|---|---|
|  | Click to change the view mode.<br><br>: Displays the logs in a table.<br><br>/ / : Displays the logs in a day/week/month. To change the time, click or . To jump back to the current one, click Today/This Week/This Month. |
|  | Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously.<br><br>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.<br><br>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. |
|  | Enter the content types, severity levels, or key words to search the logs. |
| Content | Displays the log types and detailed message. |

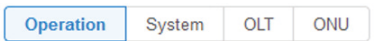
| | |
|---|---|
| Site | Displays the site where the activity happened. |
| Time | Displays when the activity happened. |
| Batch Delete | Select the log entries and click Batch Delete to delete them in batches. |
|  | Click to delete the log entry. |

### 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 for the logs. With proper configurations, DPMS will send emails 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. |
|  | Click the tabs to display the configurations of corresponding log types. |
|  | 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 checkboxes 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 checkboxes are 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

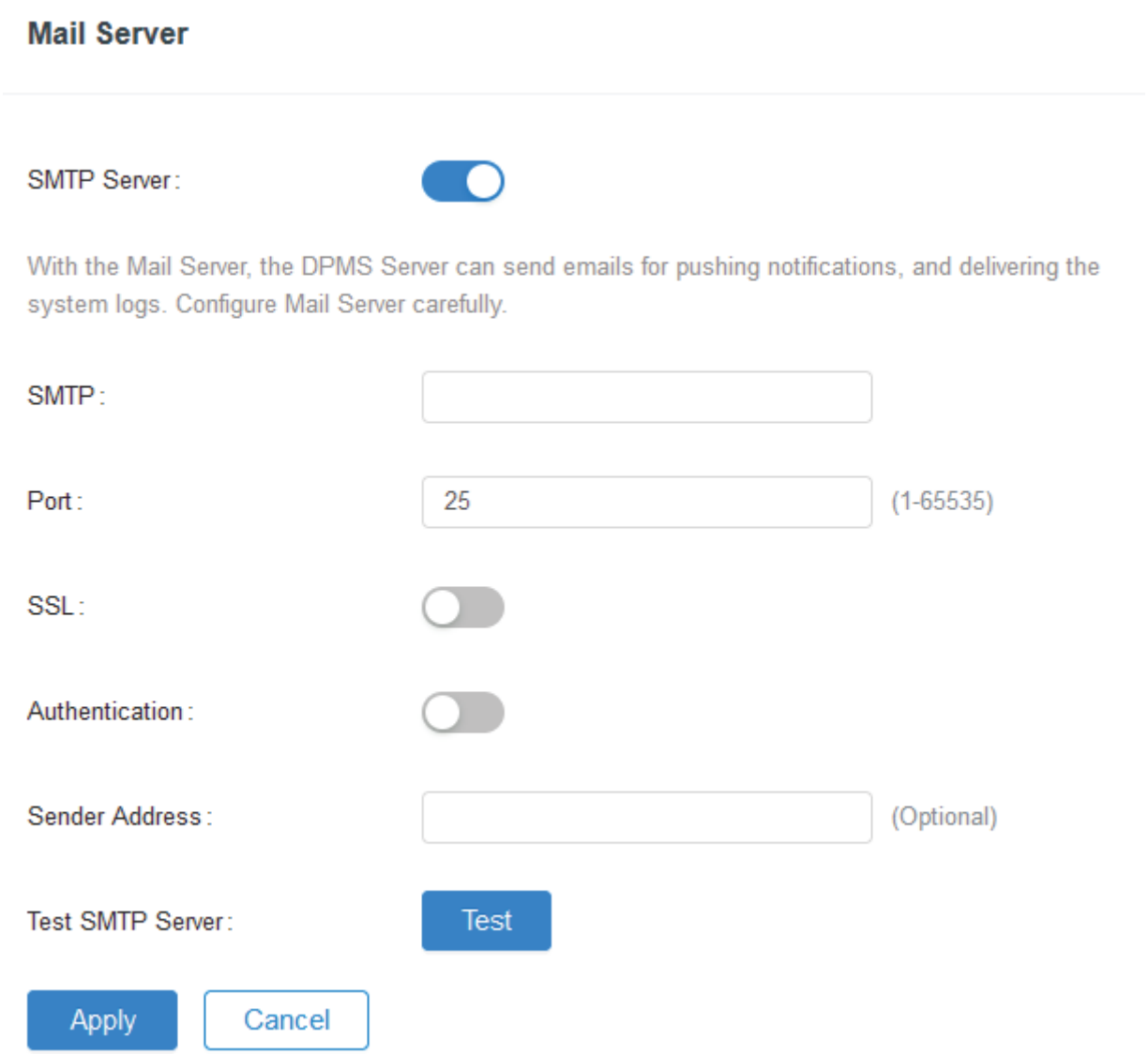
**2 )** Enable Alert Emails in General Settings

**3 )** Enable Alert Emails in Account Settings

**4 )** Enable Alert Emails in Logs

Enable Mail Server > Enable Alert Emails in General Settings > Enable Alert Emails in Account Settings

Go to Settings > General Settings. In the Mail Server section, enable SMTP Server and configure the parameters. Then click Apply.

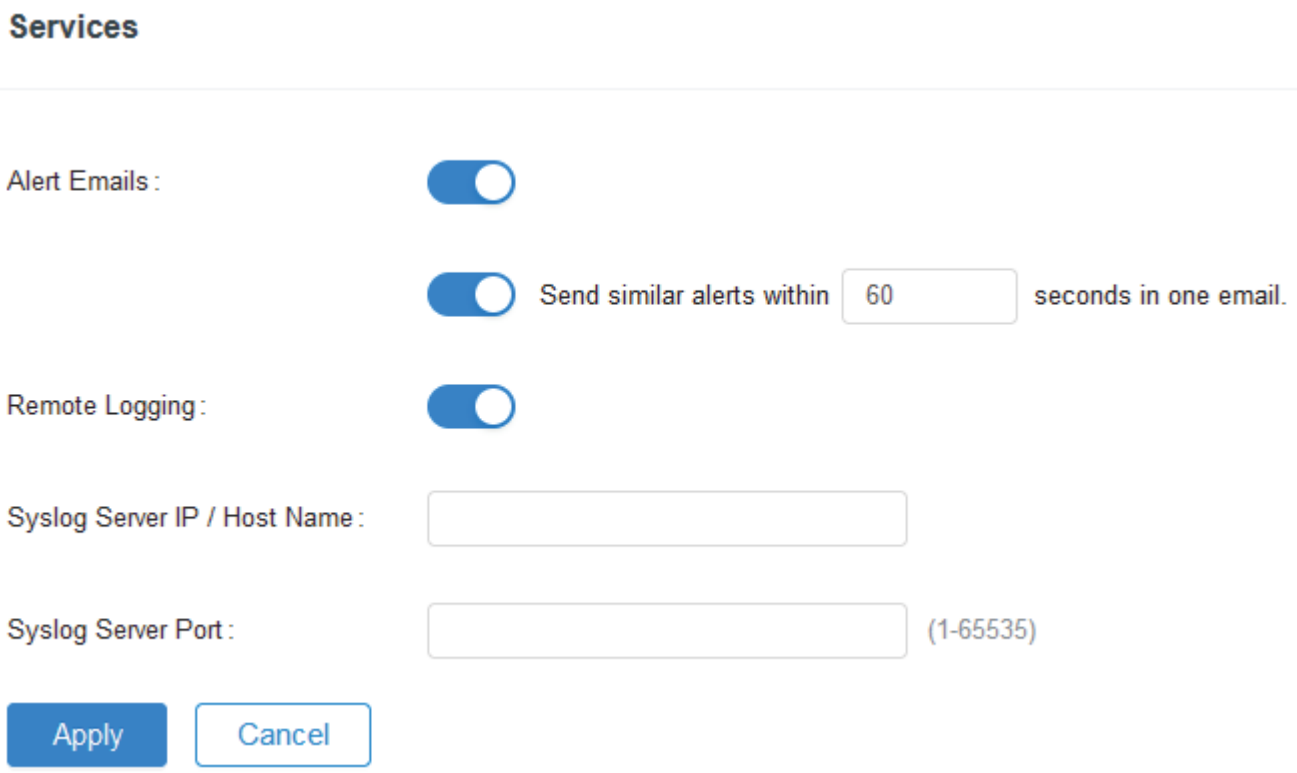



| | |
|---|---|
| SMTP | Enter the URL or IP address of the SMTP server according to the instructions of the email service provider. |
| Port | Configure the port used by the SMTP server according to the instructions of the email service provider. |
| SSL | Enable or disable SSL according to the instructions 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. |

Enable Mail Server > Enable Alert Emails in General Settings > Enable Alert Emails in Account Settings

Go to Settings > General Settings and enable Alert Emails in the Services section. Then click Apply.

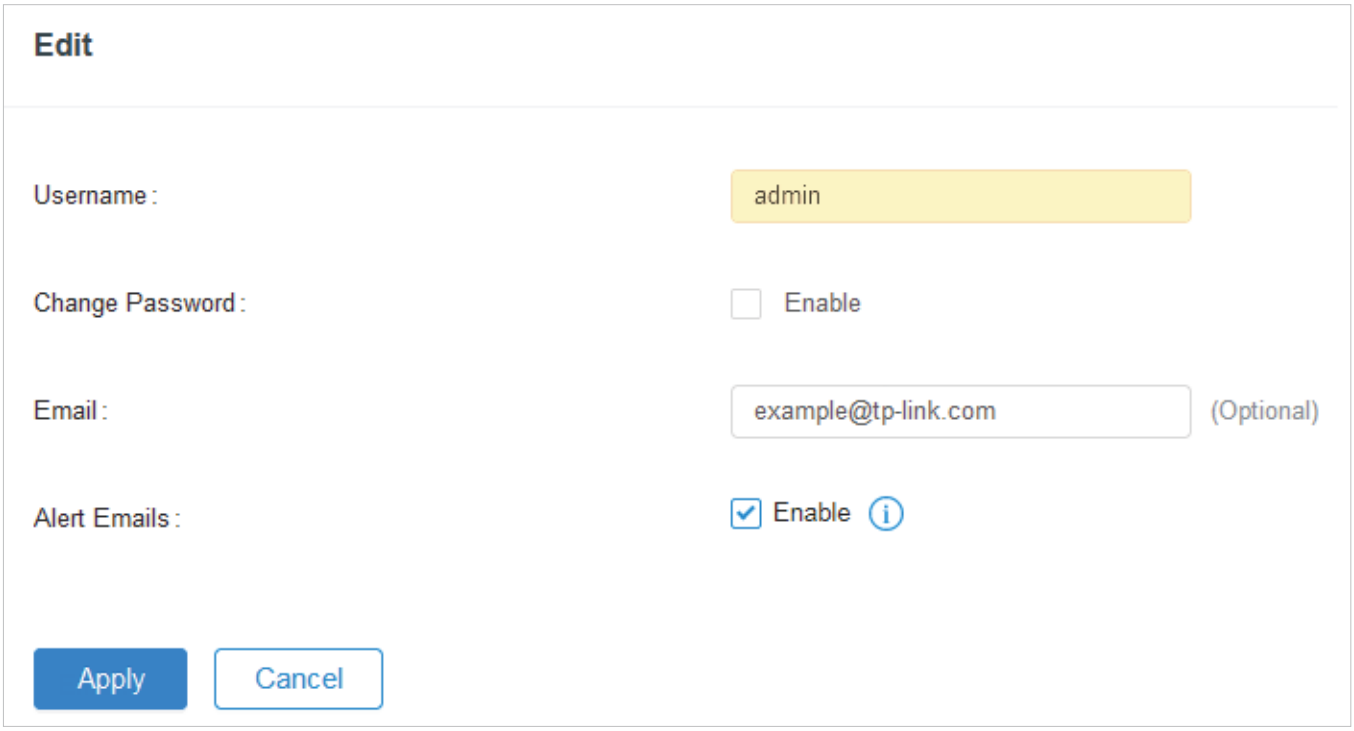



| | |
|---|---|
| Alert Emails | Enable alert emails: When enabled, DMPS can send emails to notify the administrators and viewers of the site's alert logs once generated.<br><br>Send similar alerts within seconds in one email: When enabled, the similar alerts generated in each time period are collected and sent to administrators and viewers in one email.<br><br>To configure alert-level logs and enable email notifications on the controller, refer to 5. 3. 3 Notifications. |

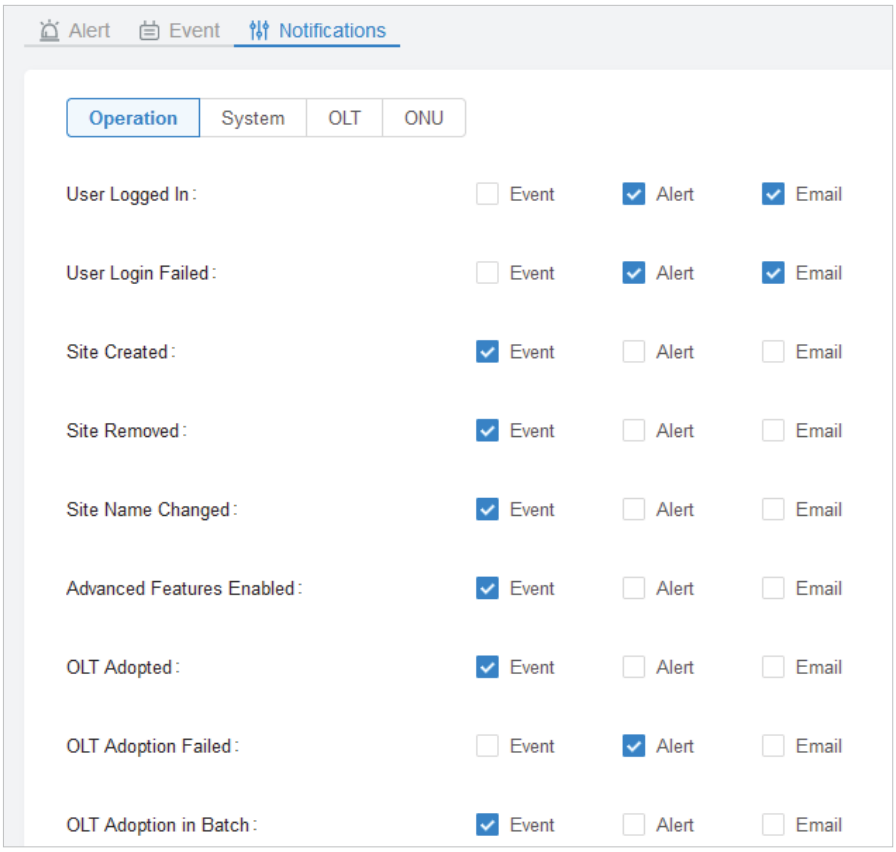
| | |
|---|---|
| Remote Logging | With this feature configured, DPMS will send generated site logs to the log server. When enabled, the following items are required:<br><br>Syslog Server IP/Hostname: Enter the IP address or hostname of the log server.<br><br>Syslog Server Port: Enter the port of the server. |

Enable Alert Emails in General Settings | **Enable Alert Emails in Account Settings** | Enable Alert Emails in Logs

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.



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.



# 6

# *Manage Administrator Accounts of DPMS*

This chapter gives an introduction to different user levels of administrator accounts and guides you on how to create and manage them in the Admin page. The chapter includes the following sections:

# 6. 1 Introduction to User Accounts

DPMS offers three levels of access available for users: administrator, system operator, and viewer. Because DPMS can be accessed both locally and via cloud access, users can be further grouped into local users and cloud users. Multi-level administrative account presents a hierarchy of permissions for different levels of access to DPMS as required. This approach ensures security and gives convenience for management.

- **Administrator**

There is only one administrator who has access to all features. The account who first launches DPMS will be the administrator and cannot be changed and deleted.

- **System Operator**

System Operators can create and delete viewers in the Admin page, but they can be created and deleted only by administrator. In the Settings page, administrators have no permission to some modules, including cloud access, and auto-backup, etc.

- **Viewer**

Viewers can only view the status and settings of the network, and they cannot change the settings. The entrance to Admin page is hidden for viewers, and they can be created or deleted by the administrator and system operator.

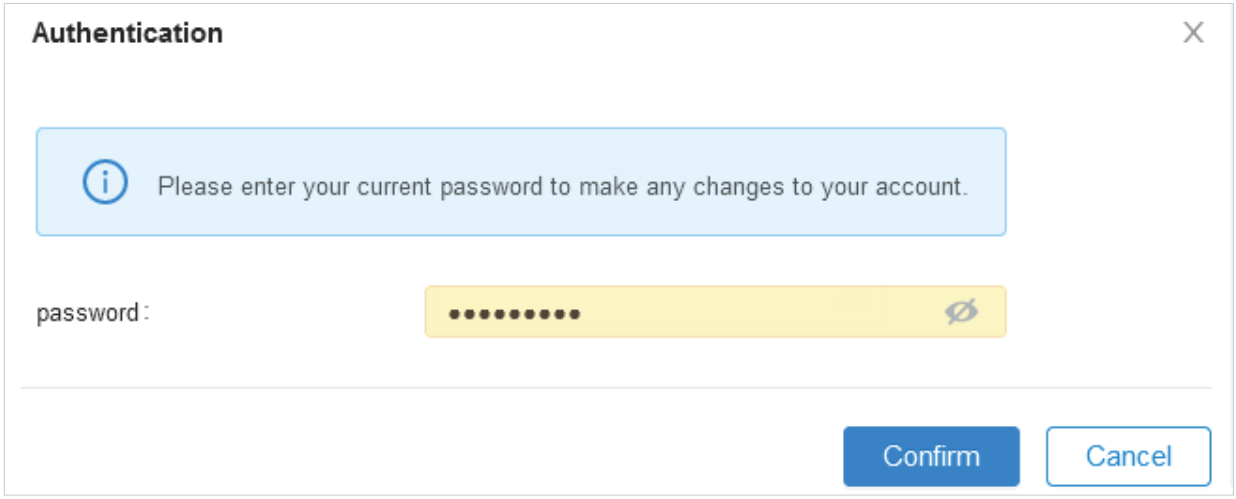
# 6. 2 Manage and Create Local User Accounts

By default, DPMS automatically sets up a local user as the administrator. The username and password of the administrator are the same as that of DPMS account by default. The administrator cannot be deleted, and it can create, edit, and delete other levels of user accounts.

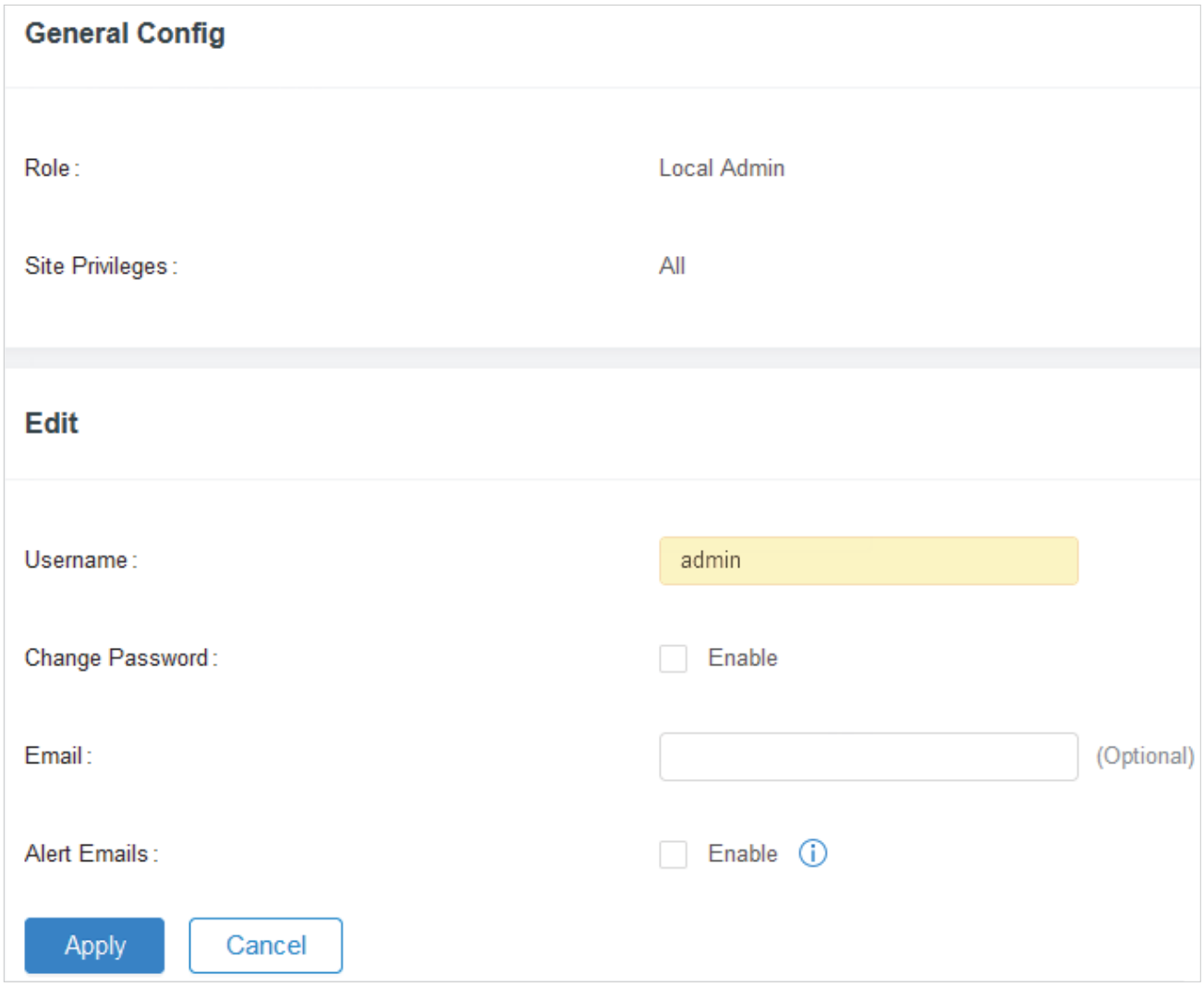
## 6. 2. 1 Edit the Administrator Account

To view basic information and edit the administrator account, follow these steps:

1. Go to Account, click in the Action column. Enter the password and click Confirm (by default, the password of the administrator is the same as the DPMS account).



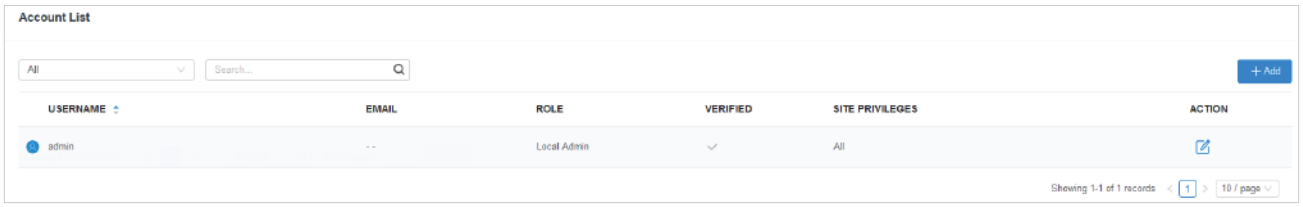
2. Basic information including role and device permissions is shown. You can change the password and enable alert emails by checking the box. Click Apply.



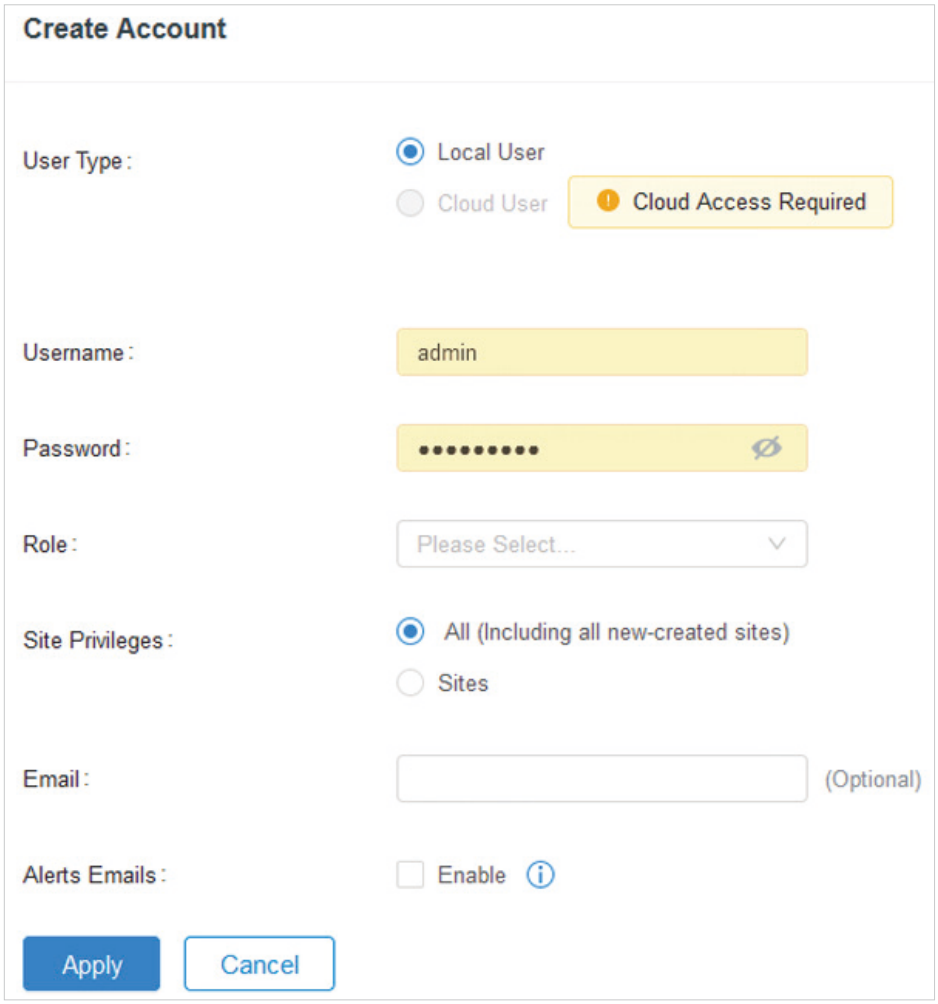

## 6. 2. 2 Create and Manage Local User

To create and manage local user account, follow these steps:

1. Go to Account. In the account list, Click + Add.



2. Select Local User for the user type and specify other parameters. Then click Apply.




| | |
|---|---|
| Username | Specify the username. The username should be different from the existing ones. |
| Password | Specify the password. |
| Role | Select a role for the created user account.<br><br>Local System Operator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete the administrator account.<br><br>Local Viewer: This role can view the information of the sites chosen in the site privileges. It can only edit itself. |
| Site Privileges | Assign the site permissions to the created local user.<br><br>All: The created user has device permissions in all sites, including all new-created sites.<br><br>Sites: The created user has device permission in the sites that are selected. Select the sites from the drop-down list. |

| | |
|---|---|
| Email (optional) | Enter an email address for receiving alert emails. |
| Alert Emails | Check the box if you want the created user to receive emails about alerts of the privileged sites. |

To edit and delete the accounts, click icons in the Action Column.

| | |
|---|---|
|  | To edit the parameters for the user.<br><br>Administrator can edit all user accounts, System Operators can edit itself and viewer accounts of its privileged sites, and viewer can only edit itself. |
|  | To delete the account.<br><br>Administrator can delete all user accounts apart from itself, System Operators can delete viewer accounts of its privileged sites, and viewer cannot delete any accounts. |

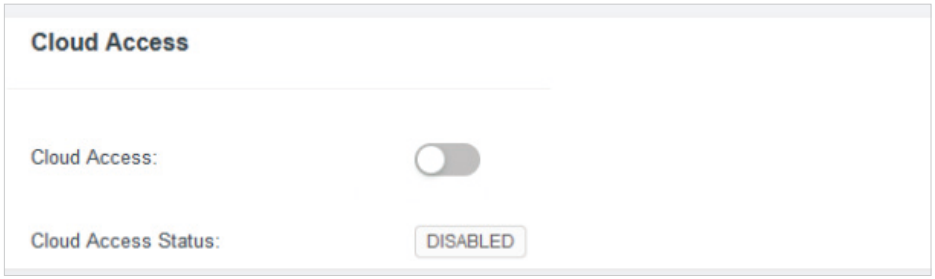
# 6. 3 Manage and Create Cloud User Accounts

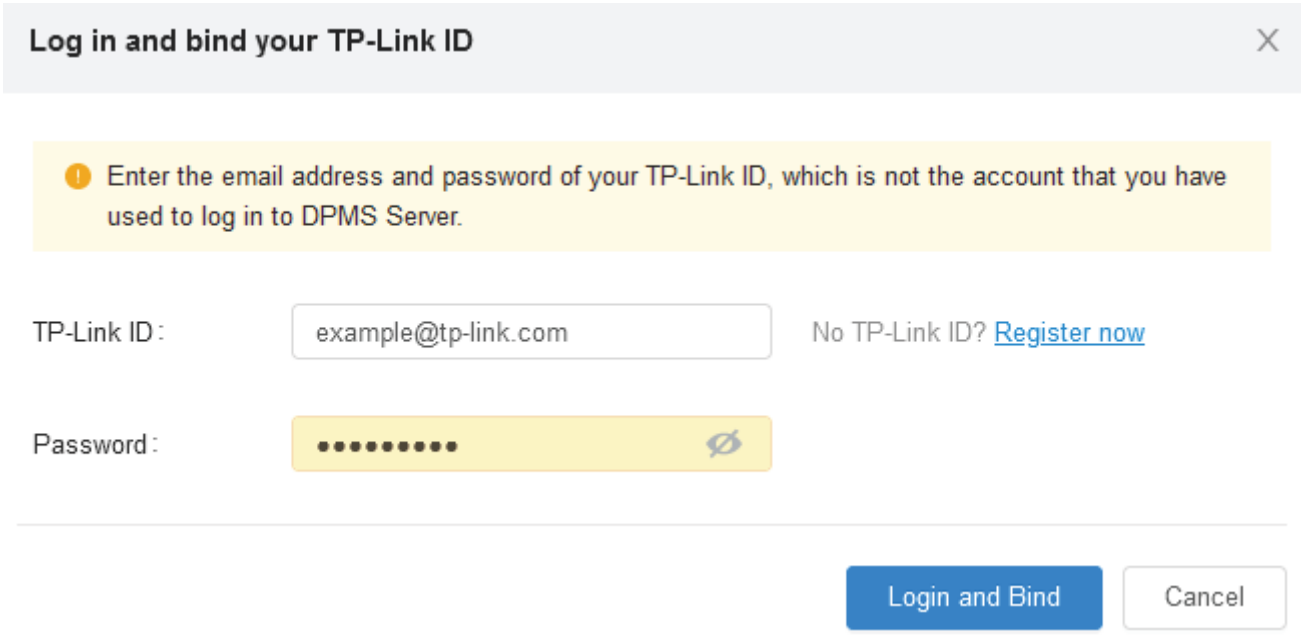
DPMS automatically sets up the cloud administrator if you have enabled cloud access and bound the DPMS account with a TP-Link ID in the quick setup. The username and password is the same as that of the TP-Link ID. The cloud administrator cannot be deleted, and it can create, edit, and delete other levels of user accounts.

## 6. 3. 1 Set Up the Cloud Administrator

If you have not enabled the cloud access and bound DPMS with a TP-Link ID in quick setup, to set up the cloud administrator, follow these steps:

1. Go to Settings > Cloud Access to enable Cloud Access and bind your TP-Link ID.



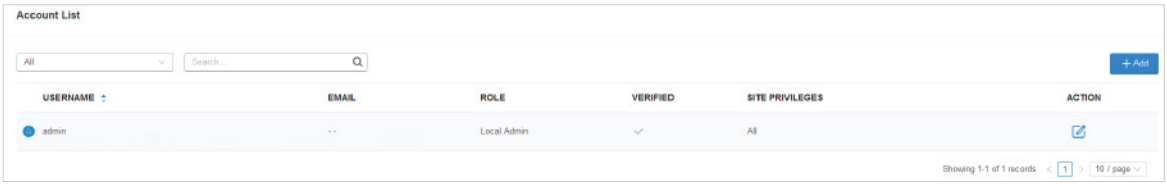




2. Enable Mail Server and set up the parameters. For details, refer to 4. 1. 3 Mail Server.
3. In Admin, a Cloud Administrator with the same username as the TP-Link ID will be automatically created. The Cloud Administrator cannot be deleted. You can log in with the cloud administrator when the cloud access is enabled.

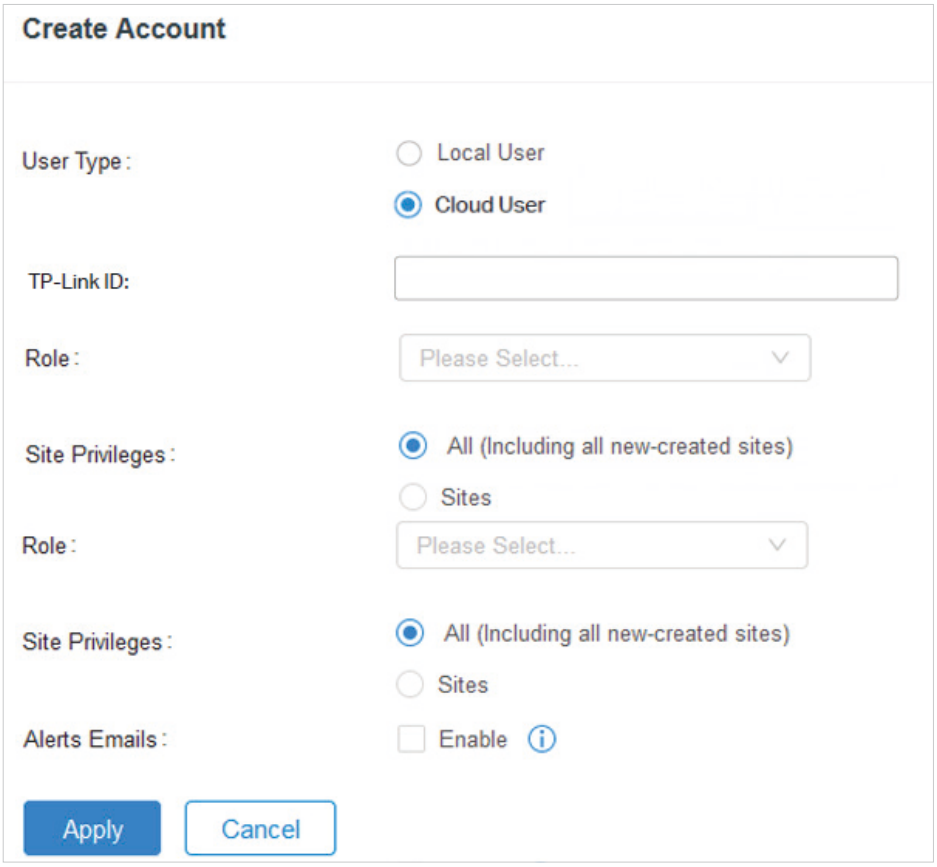
## 6. 3. 2 Create and Manage Cloud Administrator and Cloud Viewer

To create and manage cloud user account, follow these steps:

1. Go to Admin. In the account list, Click + Add.




2. Select Cloud User for the administrator type in the pop-out window. Specify the parameters and click Apply.




| | |
|---|---|
| TP-Link ID | Enter an email address of the created cloud user, and then an invitation email will be sent to the email address.<br><br>If the email address has already been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation.<br><br>If the email address has not been registered, it will receive an invitation email for registration. After finishing registration, it will automatically becomes a valid cloud user. |
| Role | Select a role for the created cloud user.<br><br>System Operator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete the administrator account.<br><br>System Viewer: This role can view the information of the sites chosen in the site privileges. It can only edit itself. |

| | |
|---|---|
| Site Privileges | Assign the site permission to the created cloud user.<br><br>All: The created user has permission in all sites, including all new-created sites.<br><br>Sites: The created user has permission in the sites that are selected. Select the sites from the drop-down list. |
| Alert Emails | Check the box if you want the created user to receive emails about alerts of the privileged sites. |

To edit and delete the accounts, click icons in the Action Column.

| | |
|---|---|
|  | To edit the parameters for the user.<br><br>Cloud Administrator can edit all user accounts, System Operator can edit itself and viewer accounts of its privileged sites, viewer can only edit itself. |
|  | To delete the account.<br><br>Administrator can delete all user accounts apart from itself, System Operators can delete viewer accounts of its privileged sites, and viewer cannot delete any accounts. |