User Guide

Omada SDN Controller

1910012850 REV4.0.0
July 2020

About this Guide

This User Guide provides information for centrally managing TP-Link devices via Omada SDN Controller. 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 Omada SDN Controller may vary due to your region, controller 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 controller.
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://www.tp-link.com/support.
- 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.



Omada SDN Controller Solution Overview

Omada SDN Controller Solution offers centralized and efficient management for configuring enterprise networks comprised of security gateways, switches, and wireless access points.

With a reliable network management platform powered by TP-Link Omada SDN Controller, you can develop comprehensive, software-defined networking across demanding, high-traffic environments with robust wired and wireless solutions.

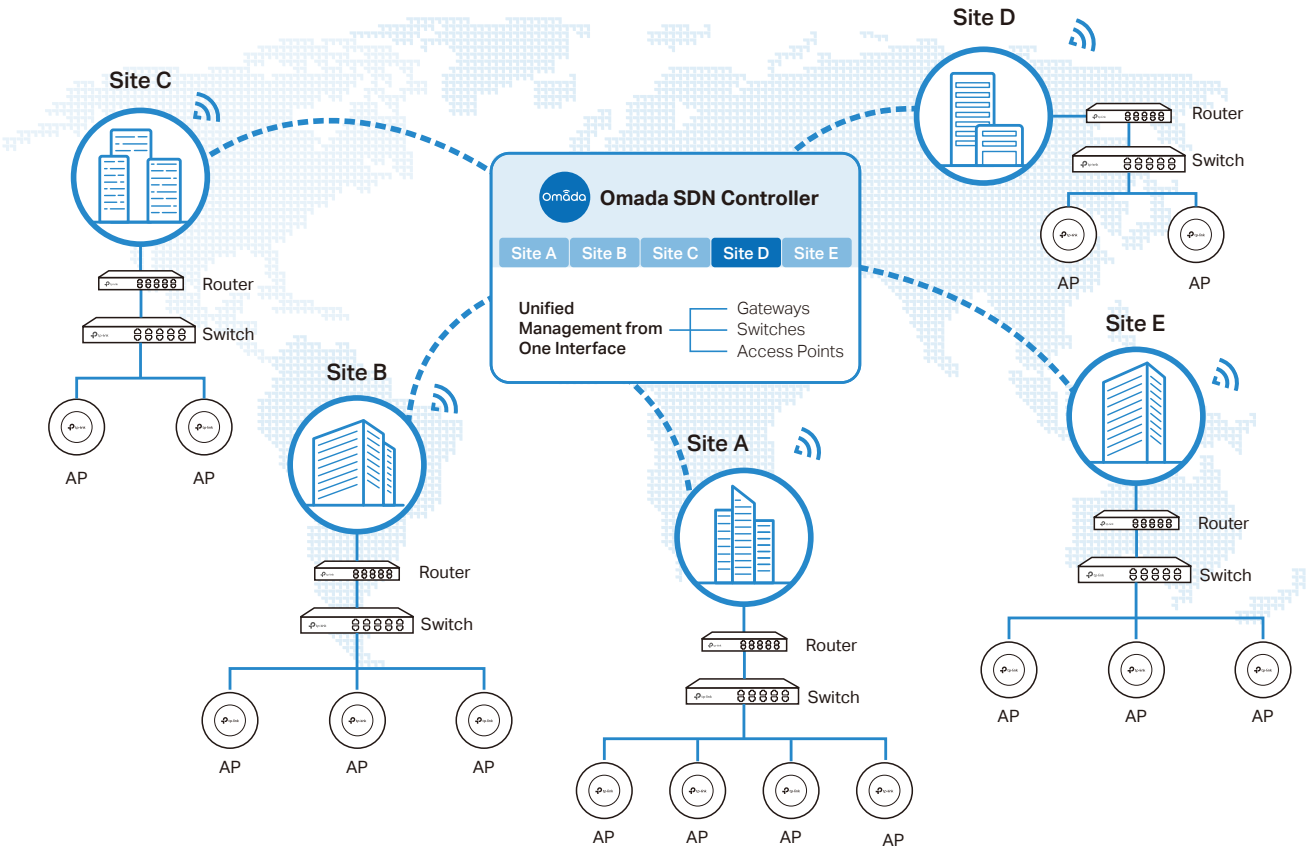
The chapter includes the following sections:

- Overview of Omada SDN Controller Solution
- Core Components

1. 1 Overview of Omada SDN Controller Solution

Omada SDN Controller Solution is designed to provide business-class networking solutions for demanding, high-traffic environments such as campuses, hotels, malls, and offices. Omada SDN Controller Solution simplifies deploying and managing large-scale enterprise networks and offers easy maintenance, ongoing monitoring, and flexible scalability.

This figure shows a sample architeture of an Omada SDN enterprise network:



The interconnected elements that work together to deliver a unified enterprise network include: Omada SDN Controller, gateways, switches, access points, and client devices. Beginning with a base of client devices, each element adds functionality and complexity as the network is developing, interconnecting with the elements above and below it to create a comprehensive, secure wired and wireless solution.

Omada SDN Controller is a command center and management platform at the heart of the Omada network. With a single platform, the network administrators configure and manage enterprise networks comprised of routers, switches, and wireless access points in batches. This unleashes new levels of management to avoid complex and costly overprovisioning.

1. 2 Core Components

An Omada SDN network consists of the following core components:

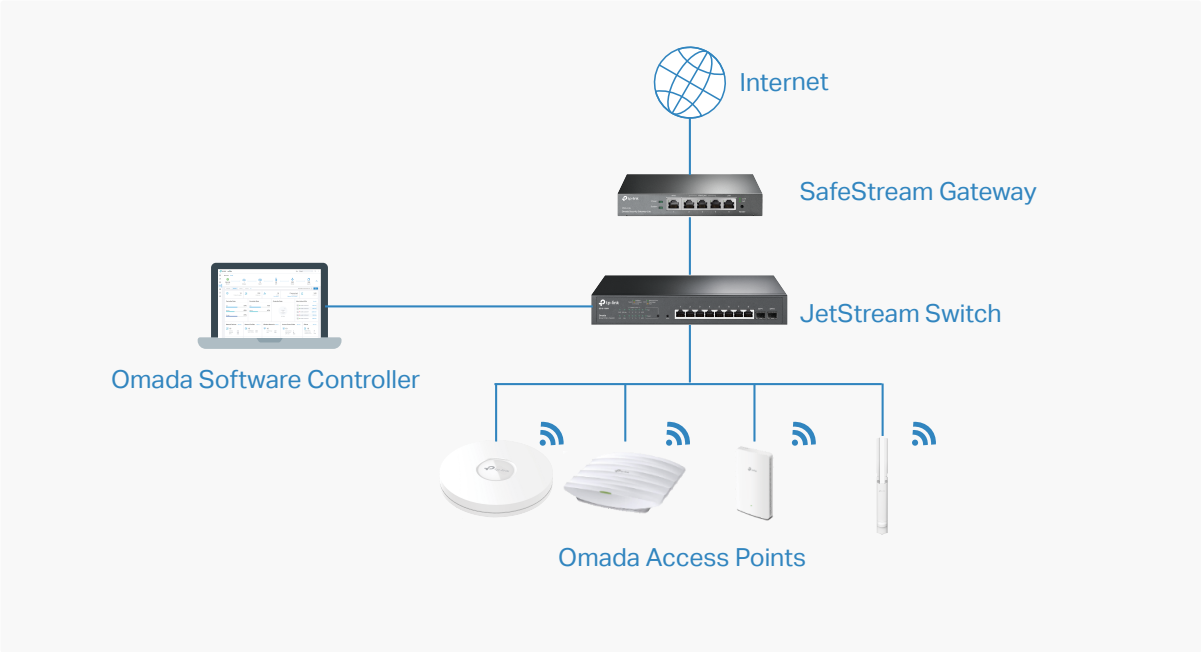
- Omada SDN Controller—a command center and management platform at the heart of Omada network solution for the enterprise. With a single platform, the network administrators configure and manage all Omada products which have all your needs covered in terms of routing, switching and Wi-Fi.
- Gateways—boast excellent data processing capabilities and an array of powerful functions, including IPsec/OpenVPN/PPTP/L2TP VPN, Load Balance, and Bandwidth Control, which are ideal for the business network where a large number of users require a stable, secure connection.
- Switches—offer flexible and cost-effective network solution with powerful Layer 2 features and PoE options. Advanced features such as Access Control, QoS, LAG and Spanning Tree will satisfy advanced business networks.
- Access Points (Omada EAPs)—satisfy the mainstream Wi-Fi Standard and address your high-density access needs with TP-Link's innovation to help you build the versatile and reliable wireless network for all business applications.

Omada SDN Controller

Tailored to different needs and budgets, Omada SDN Controller offers diverse deployment solutions. Omada Software Controller, Omada Hardware Controller, and Omada Cloud-Based Controller, each have their own set of advantages and applications.

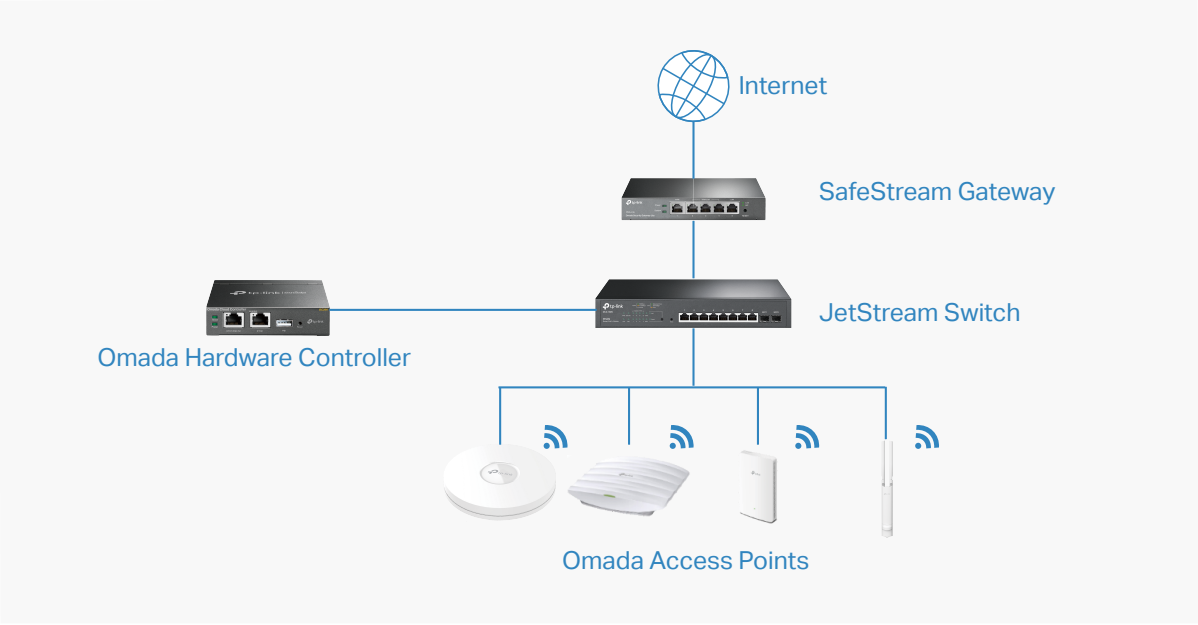
- Omada Software Controller

  Omada Software Controller is totally free, as well as all upgrades. The controller can be hosted on any computers with Windows or Linux systems on your network.



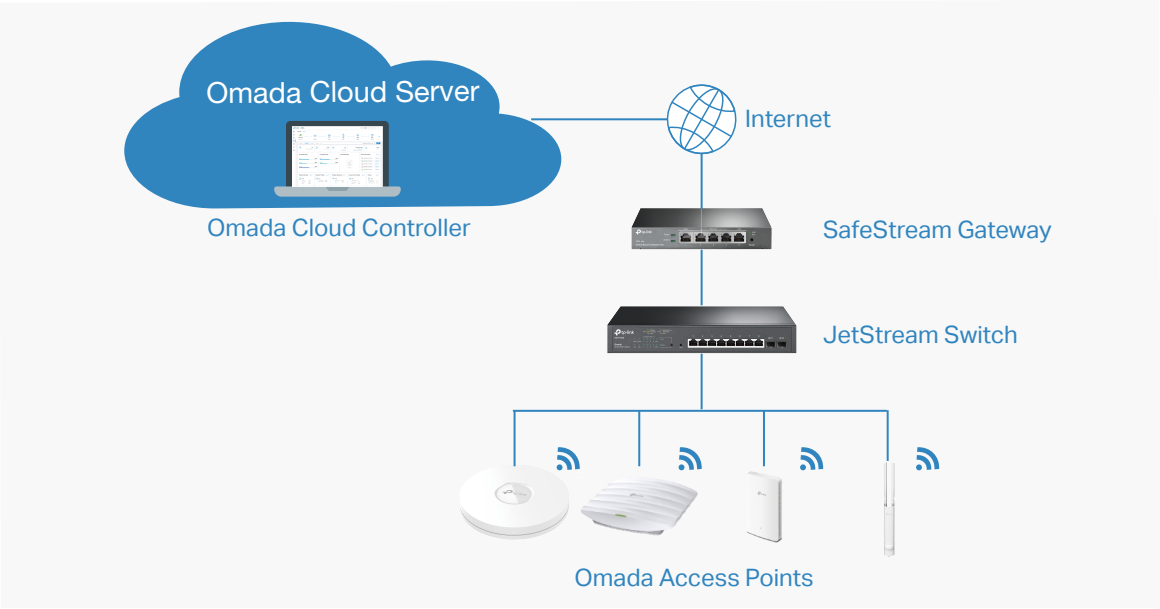
- Omada Hardware Controller

  Omada Hardware Controller is the management device which is pre-installed with Omada Software Controller. You just need to pay for the device, then the built-in Omada Controller software is free to use, no license fee or extra cost required. About the size of a mobile phone, the device is easy to deploy and install on your network.



- Omada Cloud-Based Controller

  Omada Cloud controller is deployed on the Omada Cloud server, providing paid service with tiered pricing. With a paid subscription to the Omada Cloud Service, you need not purchase an additional hardware device or install the software on the host.



The controllers differ in forms, but they have almost the same browser–based management interface and serve the same functions of network management. In this guide, Omada Software Controller, Omada Hardware Controller, and Omada Cloud-Based Controller are referred to as the controller, unless we mention otherwise.

Omada Managed Gateways

TP-Link's SafeStream VPN Router supports Gigabit Ethernet connections on both WAN and LAN ports which keep the data moving at top speed. Including all the routing and network segmentation functions that a business router must have, SafeStream VPN Router will be the backbone of the Omada SDN network. Moreover, the router provides a both secure and easy approach to deploy site-to-site VPN tunnels and access for remote clients.

Managing the gateway centrally through Omada SDN Controller is available on certain models only. The following table provides specific information of the router which can be managed by the controller.

Omada Supported Gateways	TL-R605(UN) V1 (default factory version or above)
	TL-ER7206(UN) V1 (default factory version or above)

Omada Managed Switches

TP-Link's JetStream Switch provides high-performance and enterprise-level security strategies and a numble of advanced features, which is ideal access-edge for the Omada SDN network.

Managing the switch centrally through Omada SDN Controller is available on certain models only. The following table provides specific information of the switch which can be managed by the controller.

Omada Supported Switches	TL-SG2210MP V1 (default factory version or above)
	TL-SG2428P V1 (default factory version or above)
	TL-SG2008P V1 (default factory version or above)
	TL-SG2008 V3 (version 3.0.0 or above)
	TL-SG2210P V3.20 (version 3.2.0 or above)
	TL-SG3428 V1 (default factory version or above)
	TL-SG3428MP V1 (default factory version or above)
	TL-SG3452 V1 (default factory version or above)
	TL-SG3452P V1 (default factory version or above)
	TL-SG3428X V1 (default factory version or above)
	TL-SG3428XMP V1 (default factory version or above)
	TL-SG3210XHP-M2 V1 (default factory version or above)

Omada Access Points

TP-Link's Omada Access Point provides business-class Wi-Fi with superior performance and range which guarantees reliable wireless connectivity for the Omada SDN network.

Managing the access points centrally through Omada SDN Controller is available on certain models only. The following table provides specific information of the access points which can be managed by the controller.

Omada Supported APs	EAP660 HD V1 (default factory version or above)
	EAP620 HD V1 (default factory version or above)
	EAP265HD V1 (1.0.0 Build 20200424 or above)
	EAP245 V3 (2.20.0 Build 20200423 or above)
	EAP235-Wall (1.0.1 Build 20200618 or above)
	EAP230-Wall (1.0.0 Build 20200618 or above)
	EAP225 V3 (2.20.0 Build 20200630 or above)
	EAP225-Wall V2 (1.20.0 Build 20200422 or above)
	EAP225-Outdoor V1 (1.20.0 Build 20200422 or above)
	EAP115 V4 (3.20.0 Build 20200525 or above)
	EAP115-Wall V1 (1.20.0 Build 20200619 or above)
	EAP110 V4 (3.20.0 Build 20200525 or above)
	EAP110-Outdoor V3 (3.20.0 Build 20200511 or above)

2

Get Started with Omada SDN Controller

This chapter guides you on how to get started with Omada SDN Controller to configure the network. Omada Software Controller, Omada Hardware Controller, and Omada Cloud-Based Controller differ in forms, but they have almost the same browser–based management interface for network management. Therefore, they have almost the same initial setup steps, including building your network topology, deploying your controller, and logging in to the controller. The chapter includes the following sections:

- Set Up Your Software Controller
- Set Up Your Hardware Controller
- Set up Your Cloud-Based Controller

2. 1 Set Up Your Software Controller

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up Omada Software Controller:

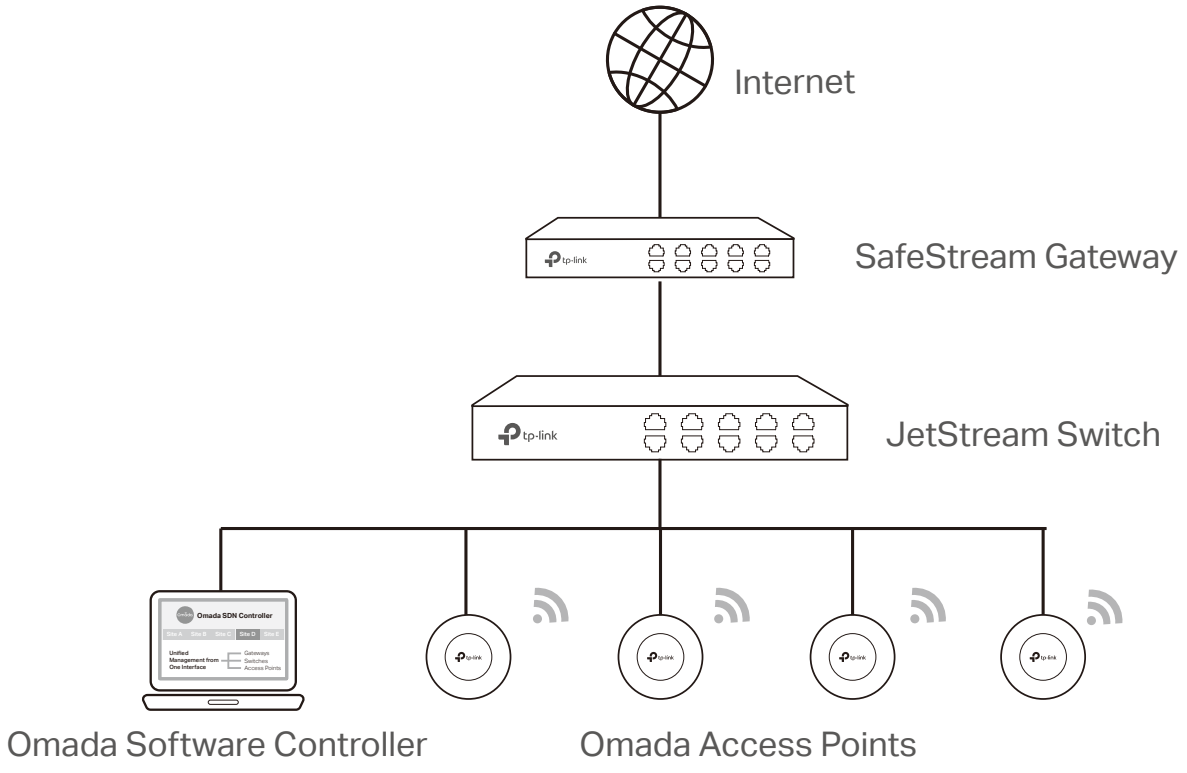
1) Determine the network topology.

2) Install Omada Software Controller.

3) Start and log in to the controller.

2. 1. 1 Determine the Network Topology

The network topology that you create for Omada SDN Controller varies depending on your business requirements. The following figure shows a typical topology for a high-availability use case.



Note:

When using Omada SDN Controller, we recommend that you deploy the full Omada topology with supported TP-Link devices. If you use third-party devices, Omada SDN Controller cannot discover and manage them.

2. 1. 2 Install Omada Software Controller

Omada Software Controller is provided for both Windows and Linux operating systems. Determine your operating system and follow the introductions below to install Omada Software Controller.

Installation on Windows Host

Omada Software Controller 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 Omada Software Controller.

- **Hardware Requirements**

  Omada Software Controller can manage up to 1500 EAPs if the Controller Host has enough hardware resources. To guarantee operational stability for managing 1500 EAPs, 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 the controller 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).

- **Install Omada Software Controller**

  Download the installation file of Omada Software Controller from the website. Then follow the instructions to properly install the Omada Software Controller. After a successful installation, a shortcut icon  of the Omada Software Controller will be created on your desktop.

Installation on Linux Host

Two versions of installation package are provided: **.tar.gz** file and **.deb** file. Both of them can be used in multiple versions of Linux operating system, including Ubuntu, CentOS, Fedora, and Debian.

Make sure your PC's hardware and system meet the following requirements, then choose the proper installation files to install the Omada Software Controller.

- **Hardware Requirements**

  Omada Software Controller can manage up to 1500 EAPs if the Controller Host has enough hardware resources. To guarantee operational stability for managing 1500 EAPs, 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: 64-bit Linux operating system, including Ubuntu 14.04/16.04/17.04/18.04, CentOS 6.x/7.x, Fedora 20 (or above), and Debian 9.8.

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

- **Install Omada Software Controller**

  Download the installation file of Omada Software Controller from the website. Check the prerequisites and follow the steps based on your file version to install the controller.

  - Prerequisites for installing

    To successfully install Omada Software Controller, ensure that you have performed the following tasks before your installation:

  1. Ensure that the Java Runtime Environment (JRE) have been installed in your system. The controller requires that the system have Java 8 installed. Download the file according to your operating system from the website and follow the instructions to install the JRE.

     For Ubuntu16.04 or above, you can use the command: **apt-get install openjdk-8-jre-headless** to get the Java 8 installed.

  2. Ensure that MongoDB has been installed in your system. The controller works when the system runs MongoDB 3.0.15–3.6.18. Download the file according to your operating system from the website and follow the instructions to install the MongoDB.

  3. Ensure that you have **jsvc** and **curl** installed in your system before installation, which is vital to the smooth running of the system. If your system does not have **jsvc** or **curl** installed, you can install it manually with the command: **apt-get install** or **yum install**. For example, you can use the command: **apt-get install jsvc** or **yum install jsvc** to get **jsvc** installed. And if dependencies are missing, you can use the command: **apt-get -f install** to fix the problem.

  - Install the .tar.gz file

  1. Make sure your PC is running in the root mode. You can use this command to enter root mode: **sudo**

  2. Extract the tar.gz file using the command:
     tar zxvf Omada_Controller_v4.1.5_linux_x64_targz.tar.gz

  3. Install Omada Controller using the command:
     sudo bash ./install.sh

  - Install the .deb file

  1. Make sure your PC is running in the root mode. You can use this command to enter root mode: **sudo**

  2. Install the .deb file using the command:
     dpkg -i Omada_Controller_v4.1.5_linux_x64.deb

     If dependencies are missing during the installation, you can use the command: **apt-fix-broken install** to fix the problem.

After installing the controller, use the following commands to check and change the status of the controller.

1. **tpeap start** — start the controller, use the command.
2. **tpeap stop** — stop running the Omada Controller.
3. **tpeap status** — show the status of Controller.

Note:

- For installing the .tar.gz, if you want Omada Controller to run as a user (it runs as root by default) you should modify OMADA_USER value in bin/control.sh.
- To uninstall Omada Controller, go to the installation path: /opt/tplink/EAPController, and run the command: sudo bash ./uninstall.sh.
- During uninstallation, you can choose whether to back up the database. The backup folder is /opt/tplink/eap_db_backup.
- During installation, you will be asked whether to restore the database if there is any backup database in the folder /opt/tplink/eap_db_backup.

2. 1. 3 Start and Log In to the Omada Software Controller

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

Launch Omada Software Controller

Double click the icon and the following window will pop up. You can click Hide to hide this window but do not close it. After a while, your web browser will automatically open.



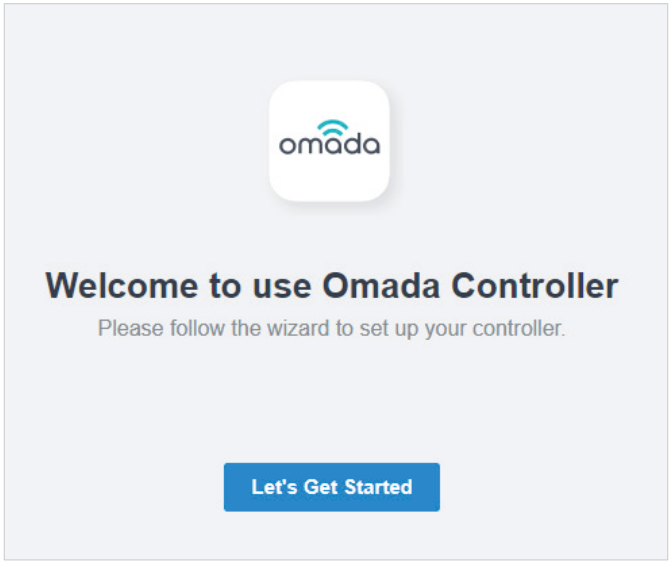
Note:

- If your browser does not open automatically, click Launch a Browser to Manage the Network. You can also launch a web browser and enter http://127.0.0.1:8088 in the address bar.
- If your web browser opens but prompts a problem with the website's security certificate, click Continue.
- Only one Omada Controller can run in a LAN. If an Omada Controller has already been running on a host that is in your LAN, you will be redirected to the Omada Controller interface on that host.

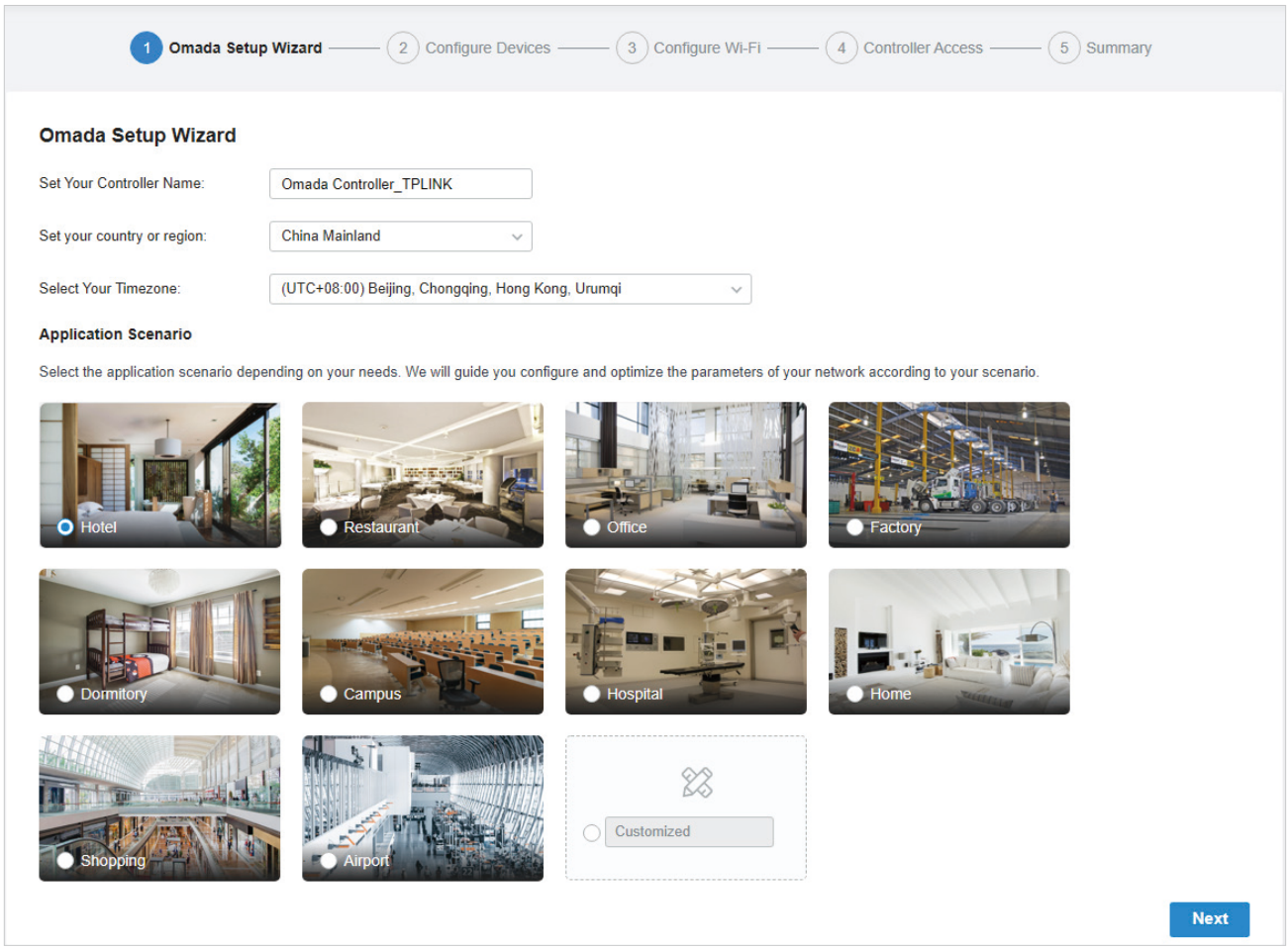
Do the Basic Configurations

In the web browser, you can see the configuration page. Follow the setup wizard to complete the basic settings for Omada Controller.

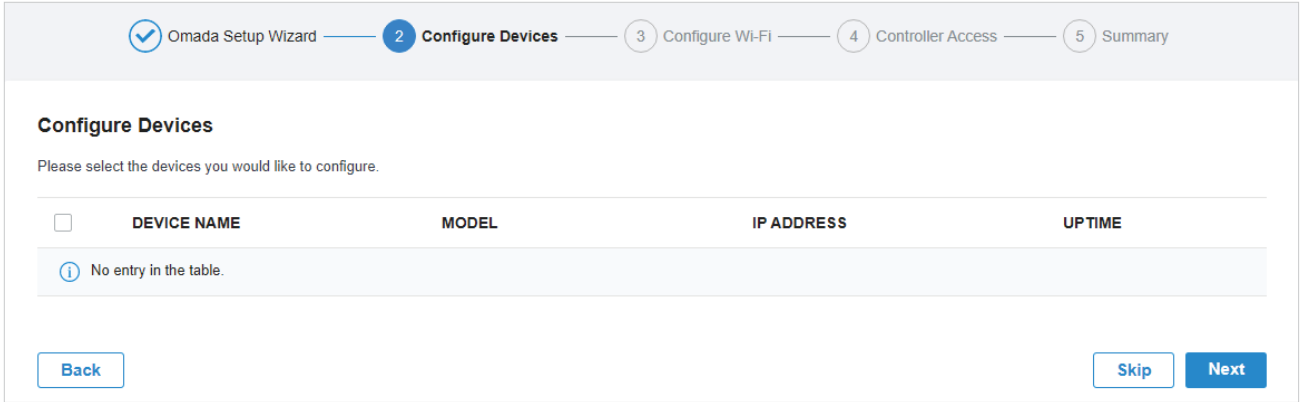
1. Click Let's Get Started.



2. Specify a name for Omada Controller, and set your region and timezone. Then select the application scenario depending on your needs. Click Next.

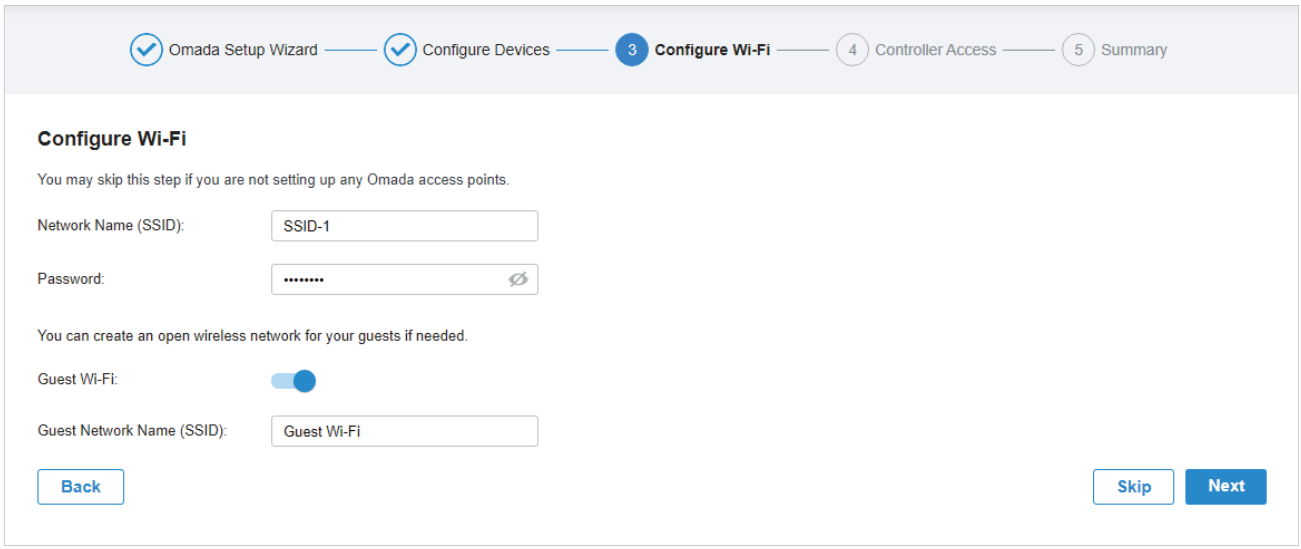


3. The setup page displays all the discovered devices in the network. Select one or more devices to be managed and click Next.

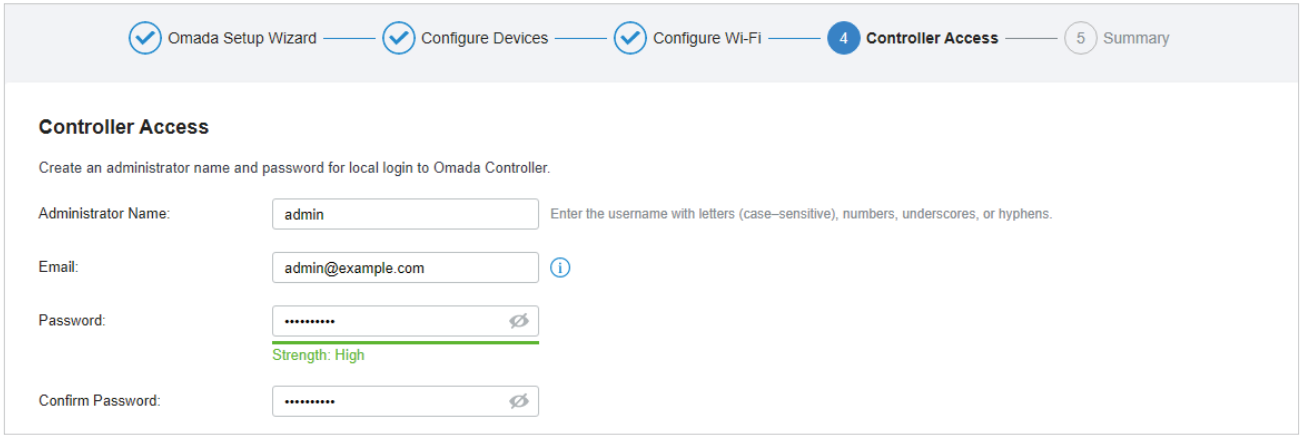


4. Set a wireless network name (SSID) and password for the EAPs to be managed. Omada Controller will create two wireless networks, a 2.4GHz one and a 5GHz one, both encrypted in WPA-Personal

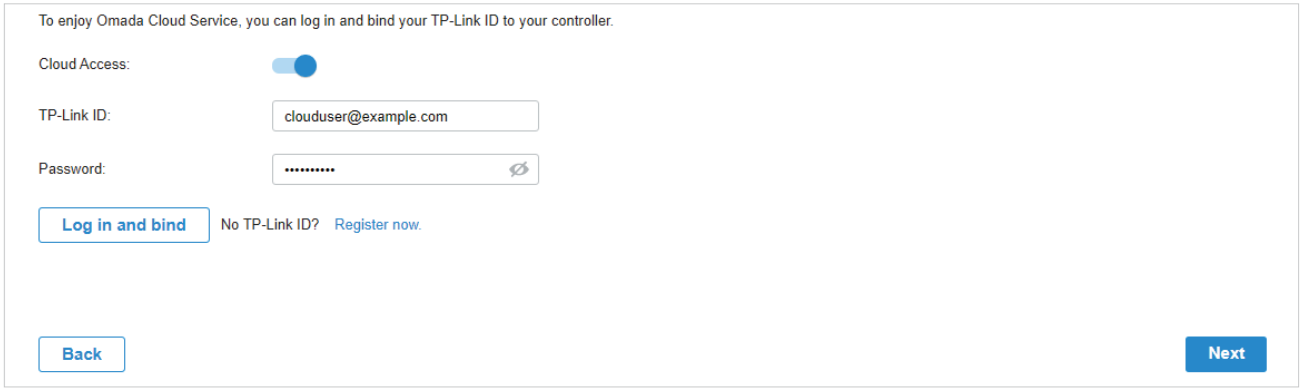
mode. You can set Guest Wi-Fi to provide open Wi-Fi access for guests without disclosing your main network if needed. Click Next.



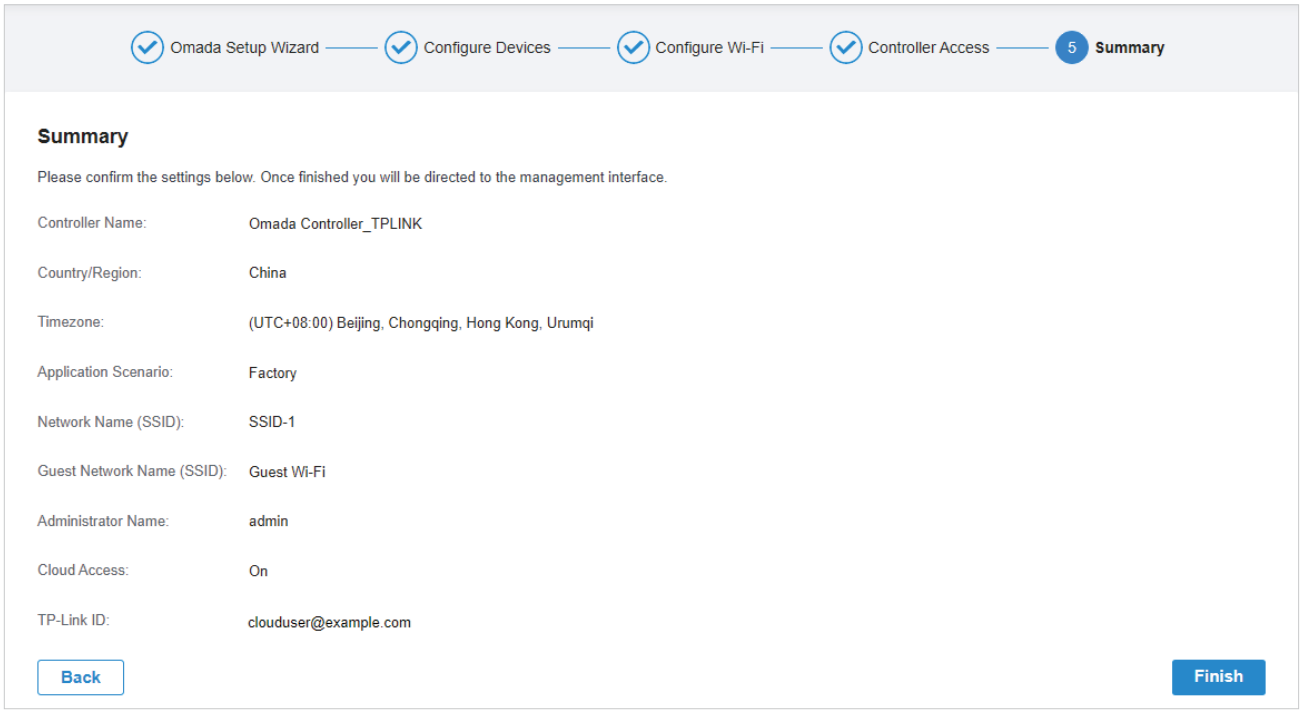
5. Set a username and password for the login account. Specify the email address for resetting your password in case that you forget the password. After logging in Omada Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to Notifications.



6. If you want to access the controller to manage networks remotely, enable the Cloud Access button, and bind your TP-Link ID to your Omada Controller, and then click Next. If not, click Next directly. For more details about Omada Cloud, please refer to Omada Cloud Service.

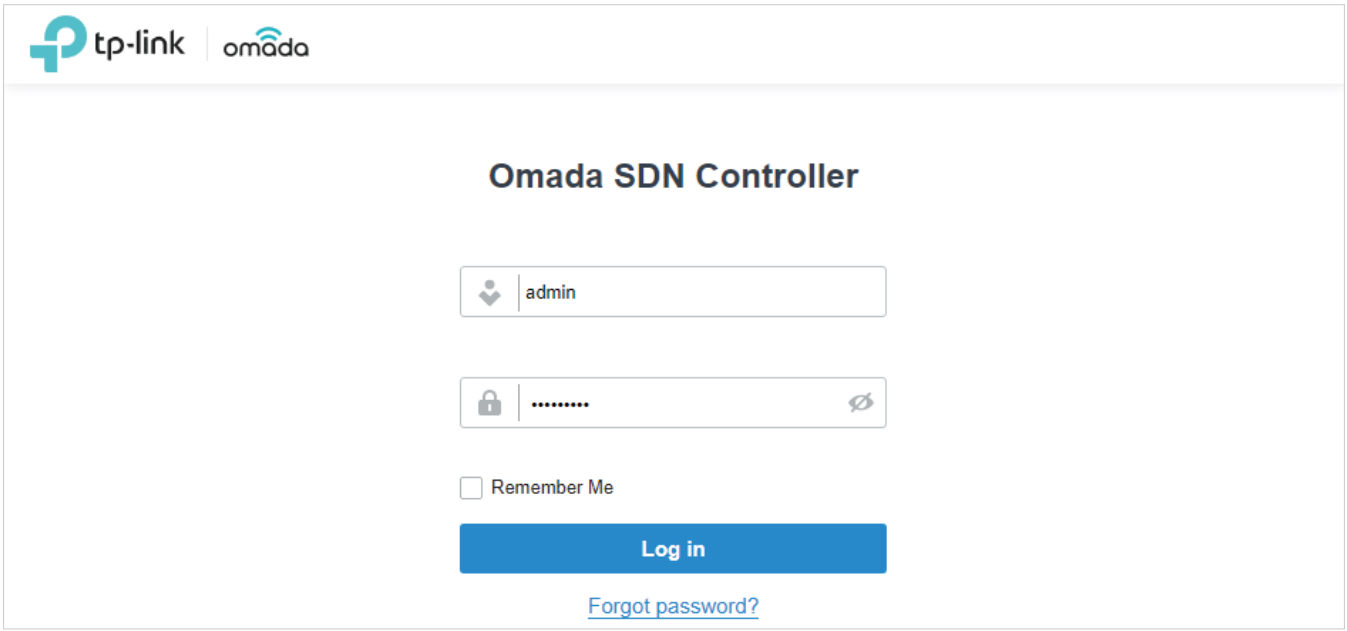


7. Review your settings and click Finish.



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.



Note:

In addition to the Controller Host, other hosts in the same LAN can also manage EAPs via remote access to the Controller Host. For example, if the IP address of the Controller Host is 192.168.0.100 and Omada Controller is running normally on this host, you can enter https://192.168.0.100:8043, or http://192.168.0.100:8088 in the web browser of other hosts in the same LAN to log in to the Omada Controller and manage EAPs. Or you can log in to Omada Controller using other management devices through Omada Cloud service.

2. 2 Set Up Your Hardware Controller

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up Omada Hardware Controller:

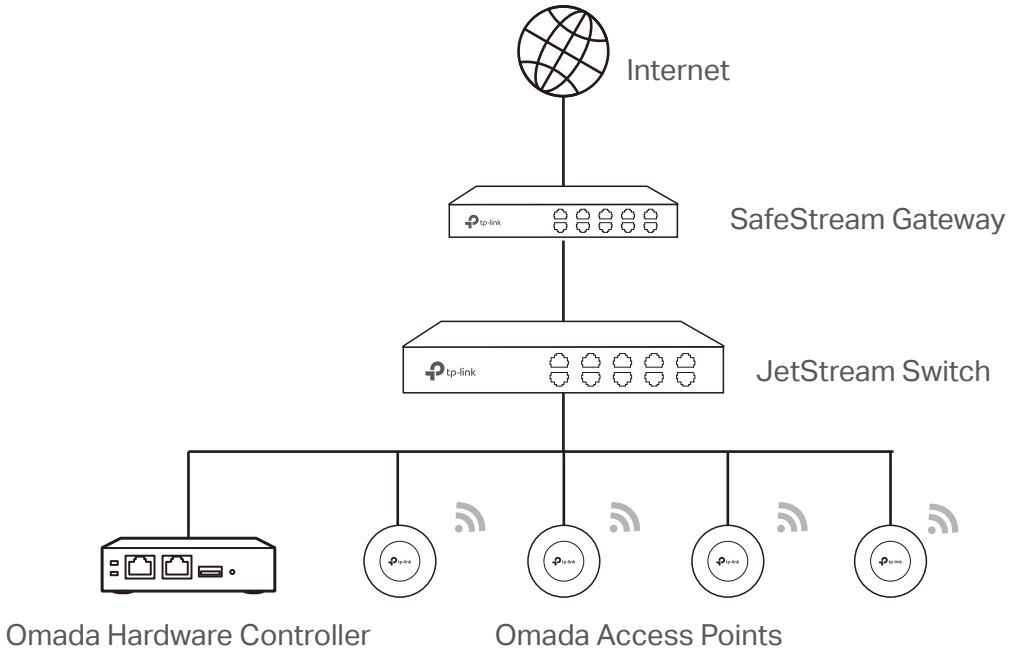
1) Determine the network topology.

2) Deploy Omada Hardware Controller.

3) Start and log in to the controller.

2. 2. 1 Determine the Network Topology

The network topology that you create for Omada SDN Controller varies depending on your business requirements. The following figure shows a typical topology for a high-availability use case.



Note:

When using Omada SDN Controller, we recommend that you deploy the full Omada topology with supported TP-Link devices. If you use third-party devices, Omada SDN Controller cannot discover and manage them.

2. 2. 2 Deploy Omada Hardware Controller

Omada Hardware Controller comes with the pre-installed controller software, so installation is not necessary. After deploying Omada Hardware Controller on your network infrastructure, proceed to configure the controller.

2. 2. 3 Start and Log in to the Controller

Log In to the Management Interface

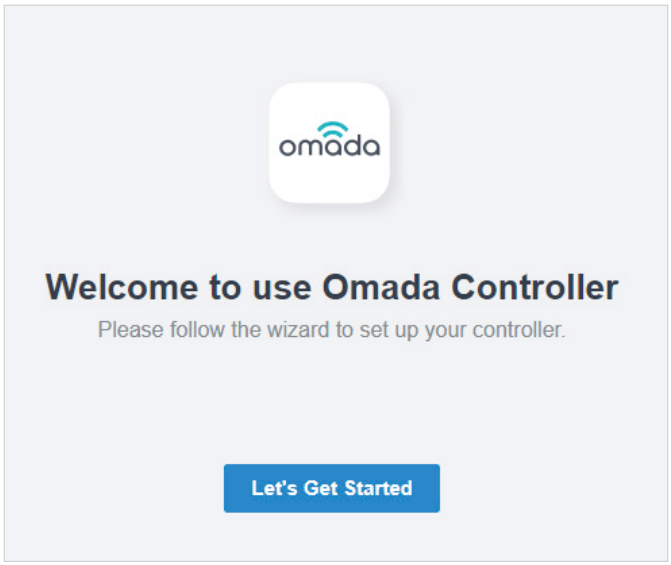
Follow the steps below to enter the management interface of Omada Hardware Controller:

1. Make sure that your management device has the route to access the controller.
2. Check the DHCP server (typically a router) for the IP Address of the controller. If the controller fails to get a dynamic IP address from the DHCP server, the default fallback IP address 192.168.0.253, is used.
3. Launch a web browser and type the IP address of the controller in the address bar, then press **Enter** (Windows) or **Return** (Mac).

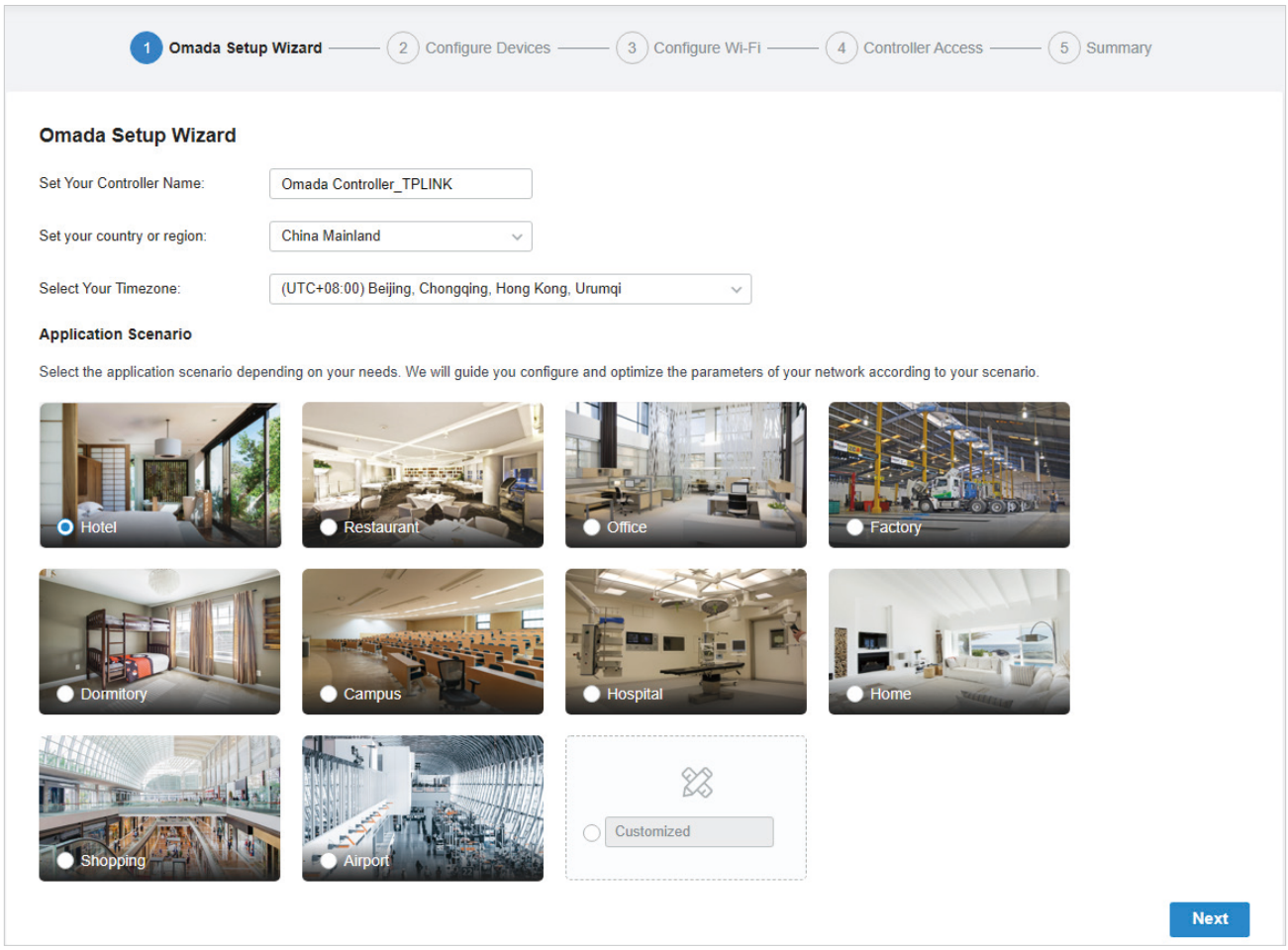
Do the Basic Configurations

In the web browser, you can see the configuration page. Follow the setup wizard to complete the basic settings for Omada Controller.

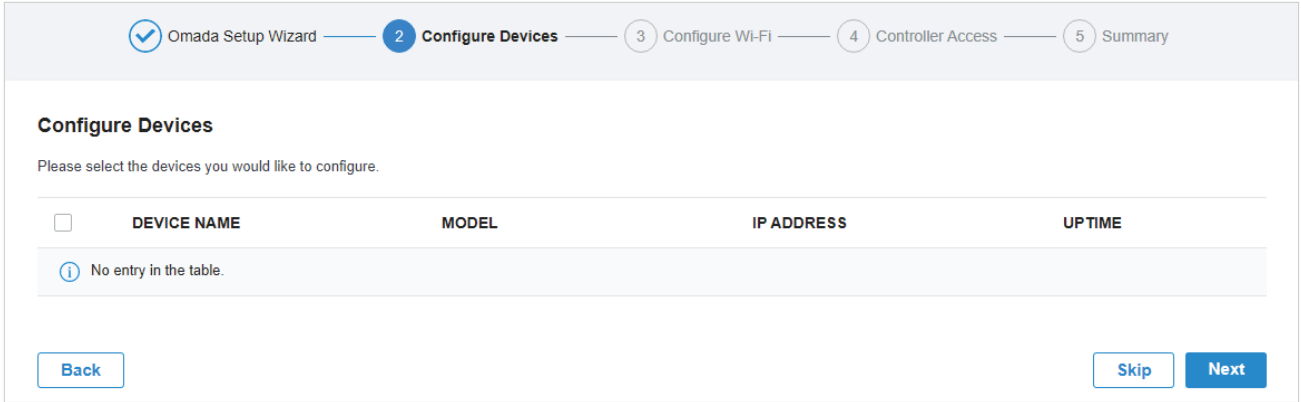
1. Click Let's Get Started.



2. Specify a name for Omada Controller, and set your region and timezone. Then select the application scenario depending on your needs. Click Next.

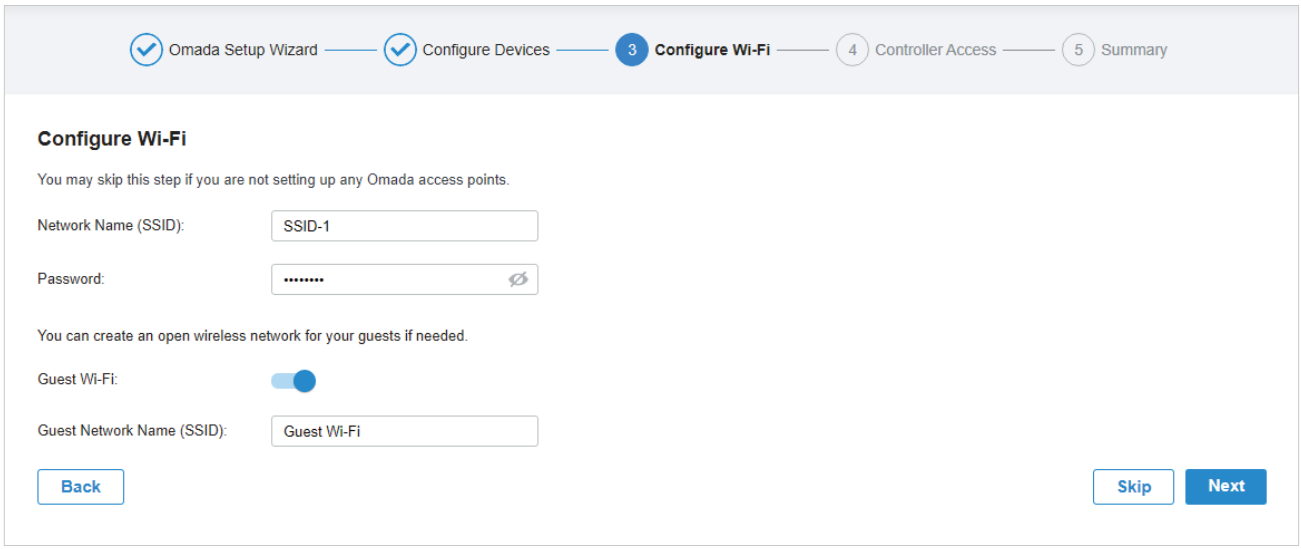


3. The setup page displays all the discovered devices in the network. Select one or more devices to be managed and click Next.

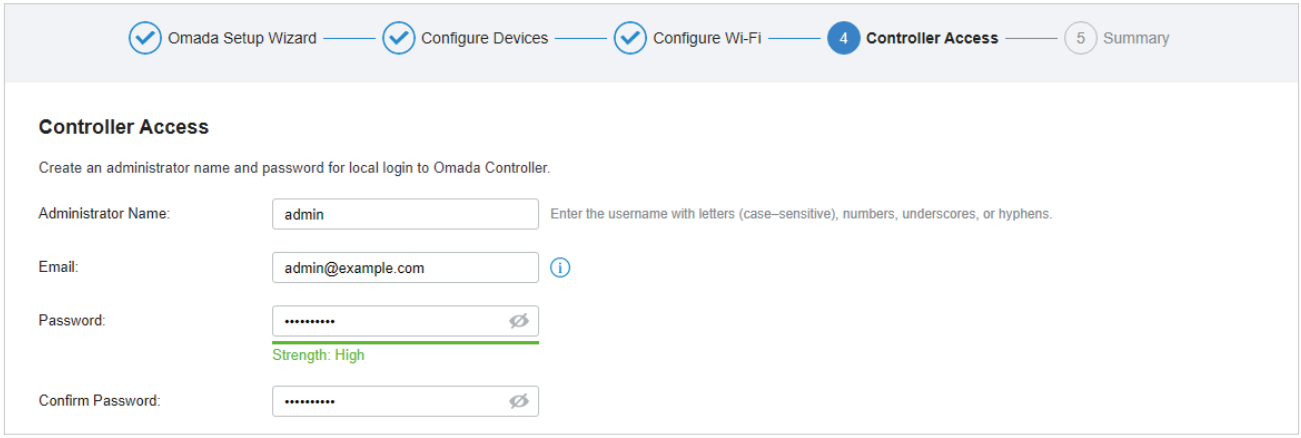


4. Set a wireless network name (SSID) and password for the EAPs to be managed. Omada Controller will create two wireless networks, a 2.4GHz one and a 5GHz one, both encrypted in WPA-Personal

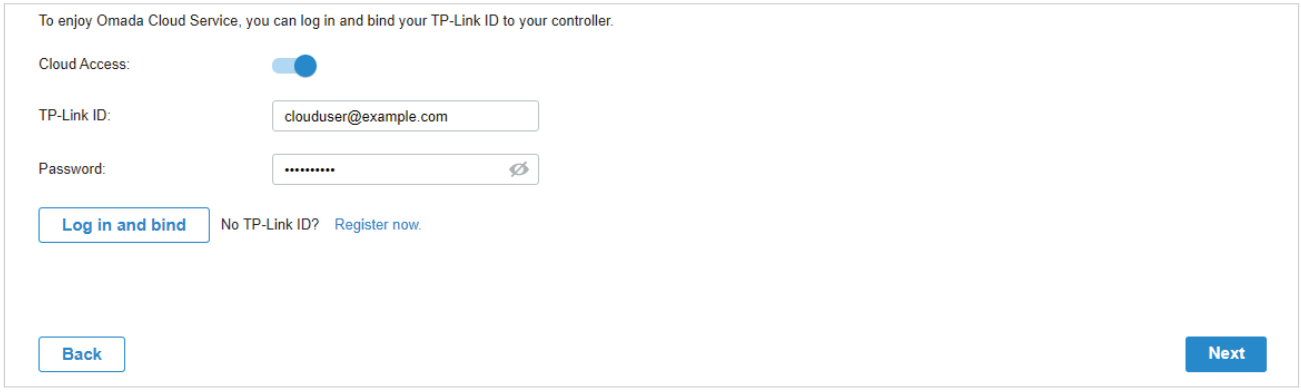
mode. You can set Guest Wi-Fi to provide open Wi-Fi access for guests without disclosing your main network if needed. Click Next.



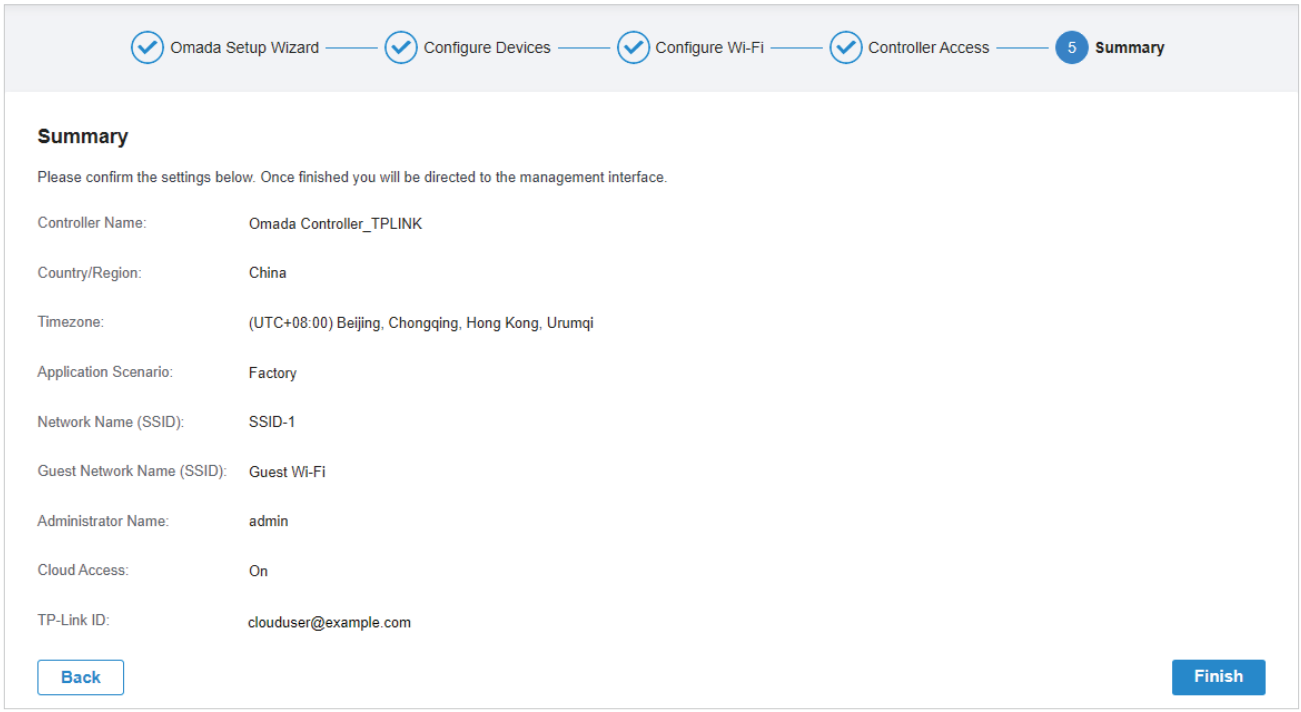
5. Set a username and password for the login account. Specify the email address for resetting your password in case that you forget the password. After logging in Omada Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to Notifications.



6. If you want to access the controller to manage networks remotely, enable the Cloud Access button, and bind your TP-Link ID to your Omada Controller, and then click Next. If not, click Next directly. For more details about Omada Cloud, please refer to Omada Cloud Service.

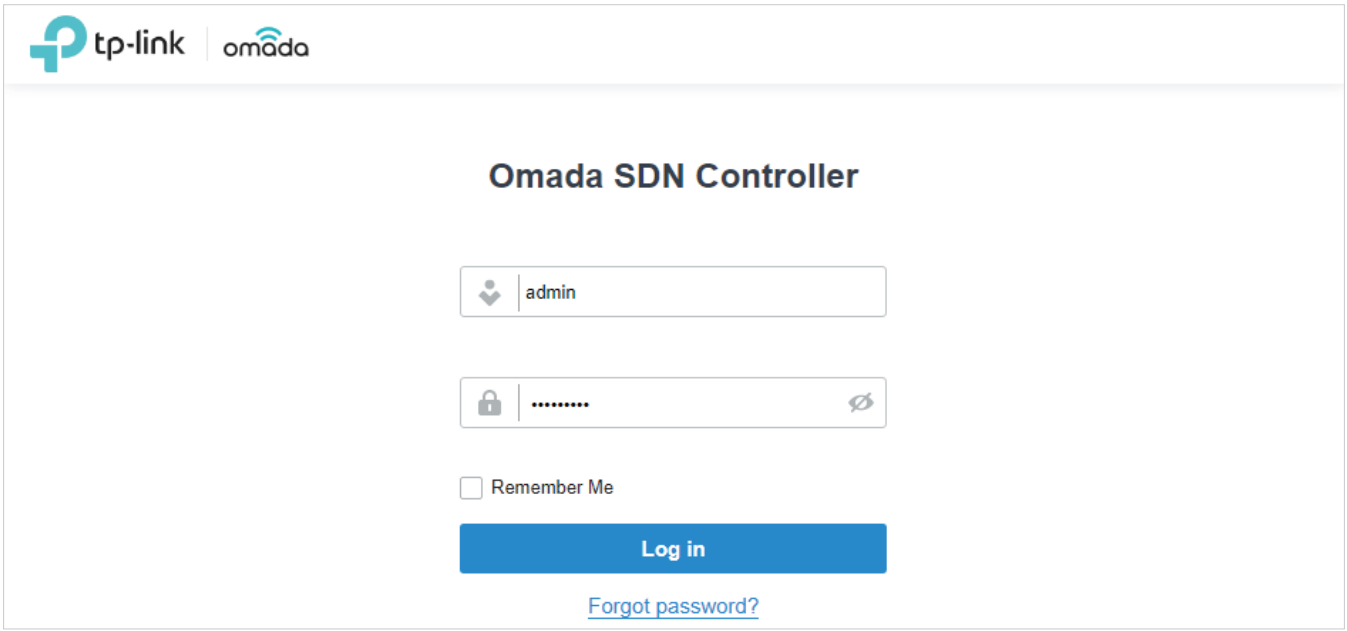


7. Review your settings and click Finish.



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.



Note:

In addition to the Controller Host, other hosts in the same LAN can also manage EAPs via remote access to the Controller Host. For example, if the IP address of the Controller Host is 192.168.0.100 and Omada Controller is running normally on this host, you can enter https://192.168.0.100:8043, or http://192.168.0.100:8088 in the web browser of other hosts in the same LAN to log in to the Omada Controller and manage EAPs. Or you can log in to Omada Controller using other management devices through Omada Cloud service.

2. 3 Set up Your Cloud-Based Controller

Omada SDN Controller Solution is designed for scalable networks. Deployments and configurations vary according to actual situations. Understanding your network requirements is the first step when planning to provision any project. After you have identified these requirements, follow the steps below to initially set up Omada Cloud-Based Controller:

1) Create a TP-Link ID.

2) Subscribe to Omada Cloud Service.

3) Start and log in to the controller.

The get-started configuration steps of Omada Cloud-Based Controller are similar to Omada Software Controller, refer to the Start and Log In to the Omada Software Controller to get detailed information.



Manage Omada Managed Devices and Sites

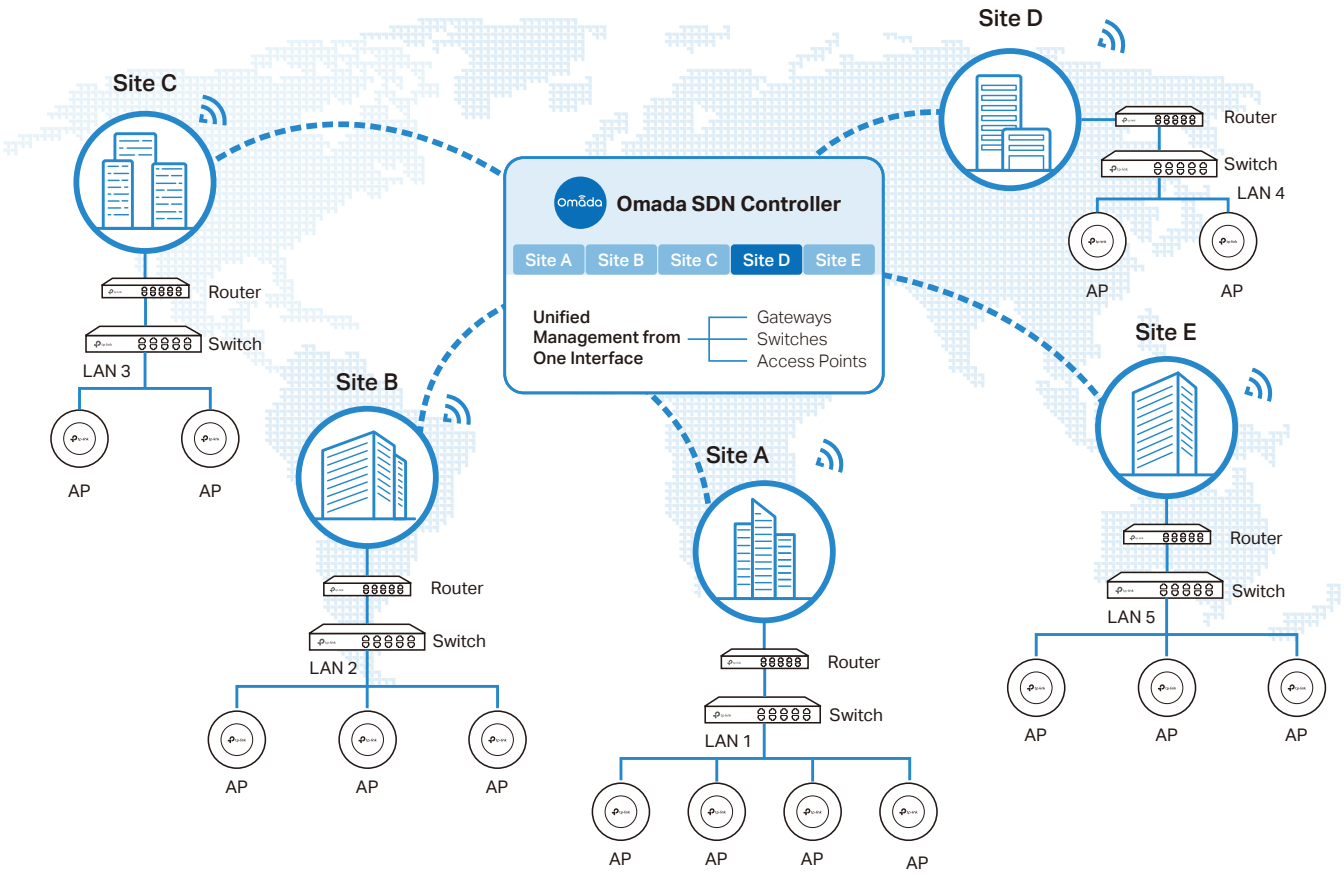
Start managing your network by creating sites and adopting devices so that you can configure and monitor your devices centrally while keeping things organized. The chapter includes the following sections:

- Create Sites
- Adopt Devices

3. 1 Create Sites

Overview

Different sites are logically separated network locations, like different subsidiary companies or departments. It's best practice to create one site for each LAN (Local Area Network) and add all the devices within the network to the site, including the router, switches and APs.



Devices at one site need unified configurations, whereas those at different sites are not relative. To make the best of a site, configure features simultaneously for multiple devices at the site, such as VLAN and PoE Schedule for switches, and SSID and WLAN Schedule for APs, rather than set them up one by one.

Configuration

To create and manage a site, follow these steps:

1) Create a site.

2) View and edit the site.

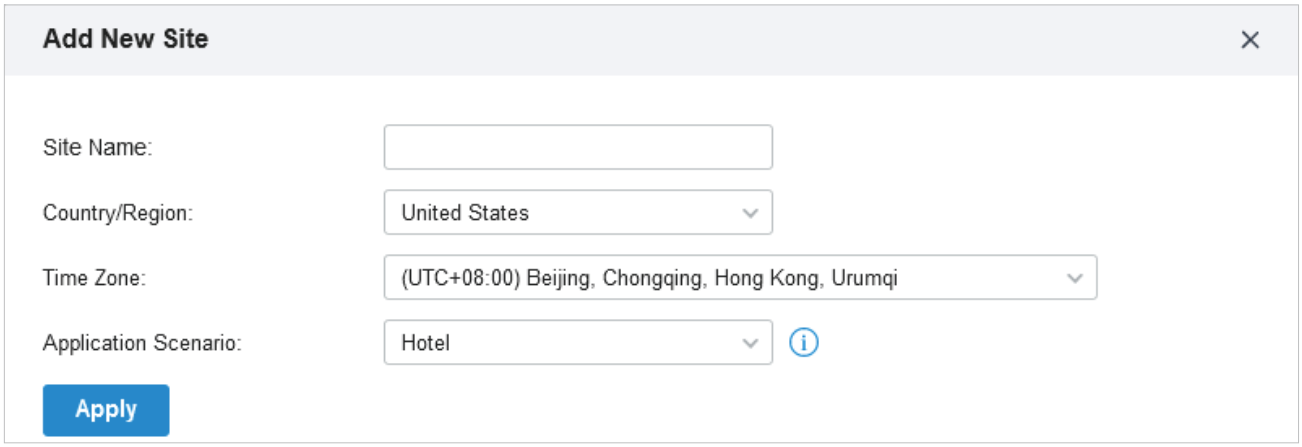
3) Go into the site.

Create a Site > View and Edit the Site > Go Into the Site

To create a site, choose one from the following methods according to your needs.

- **Create a site from scratch**

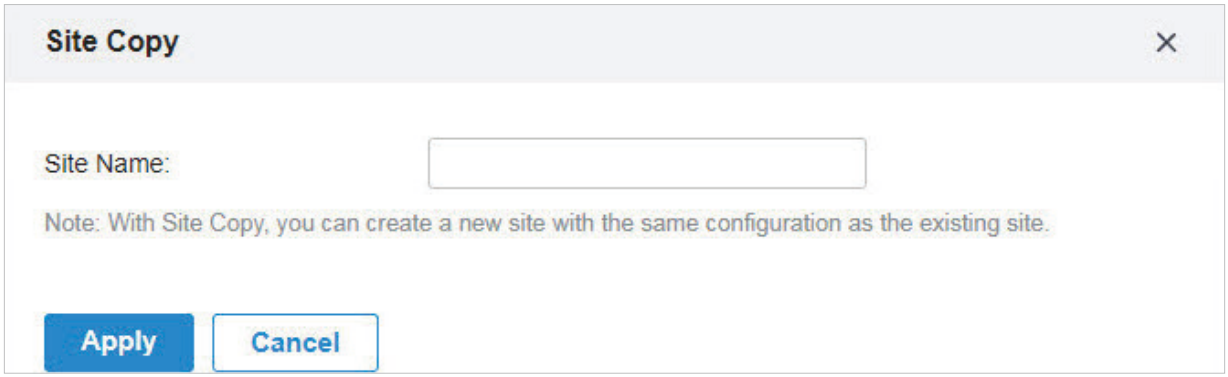
1. Click + Add New Site in the drop-down list of Sites. Alternatively, click Site Manager in the drop-down list of Sites and click ⊕ in the Site Management page.
2. Enter a Site Name to identify the site, and configure other parameters according to where the site is located. Then click Apply. The new site is added to the drop-down list of Sites, and the table in the Site Management page as well.



- **Copy an existing site**

You can quickly create a site based on an existing one by copying its site configuration, wired configuration, and wireless configuration among others. After that, you can flexibly modify the new site configuration to make it different from the old.

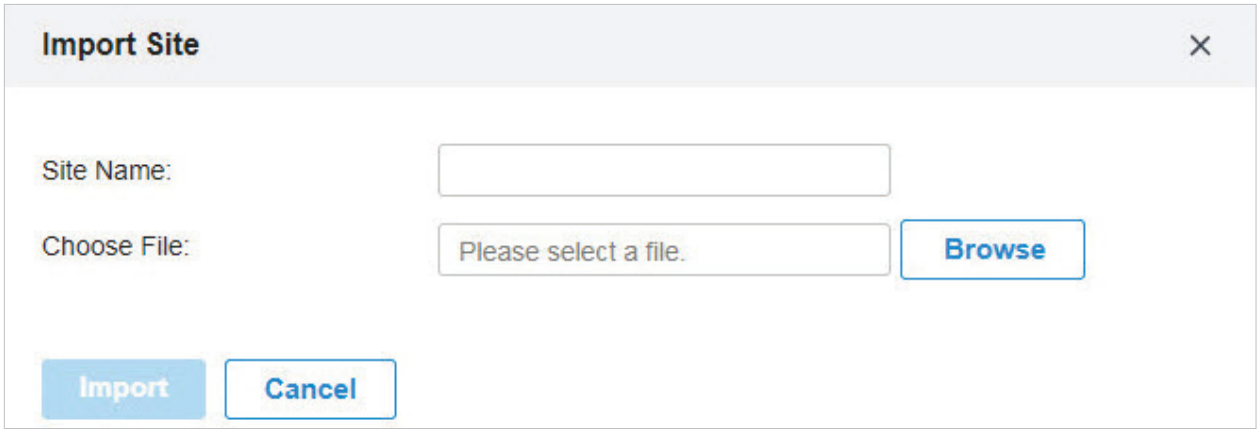
1. Click Site Manager in the drop-down list of Sites. In the Site Management page, click in the ACTION column of the site which you want to copy.
2. Enter a Site Name to identify the new site. Click Apply. The new site is added to the drop-down list of Sites, and the table in the Site Management page as well.



- **Import a site from another controller**

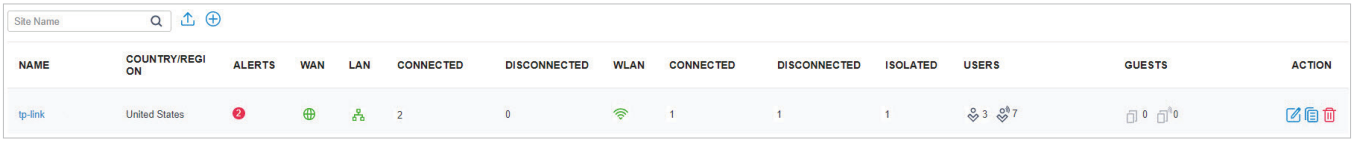
  If you want to migrate seamlessly from an old controller to a new one, import the site configuration file of the old controller into the new. Before that, you need to export the site configuration file from the old controller, which is covered in Site Migration.

  1. Click Import Site in the drop-down list of Sites. Alternatively, click Site Manager in the drop-down list of Sites and click in the Site Management page.
  2. Enter a Site Name to identify the site. Browse your file explorer and choose a site configuration file. Click Import. The new site is added to the drop-down list of Sites, and the table in the Site Management page as well.



Create a Site → View and Edit the Site → Go Into the Site

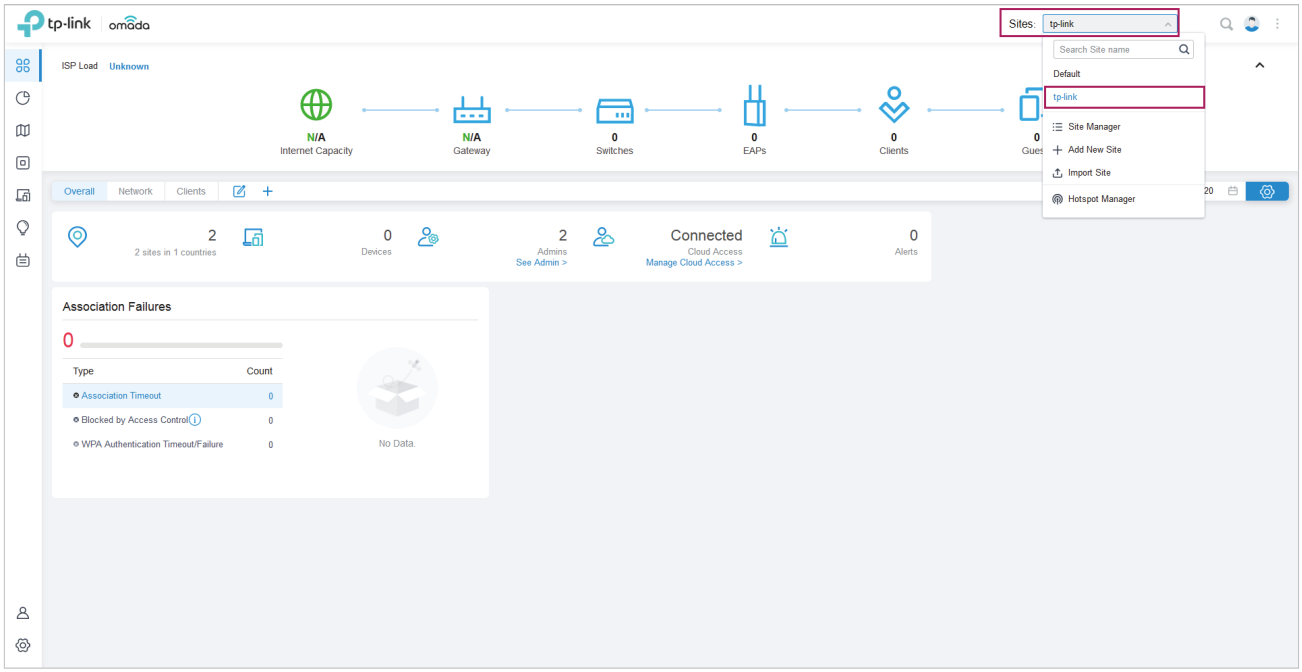
After you create the site, you can click Site Manager in the drop-down list of Sites, and view the site status in the Site Management page. You can click in the ACTION column to edit the site configuration. You can click in the ACTION column to delete the site.



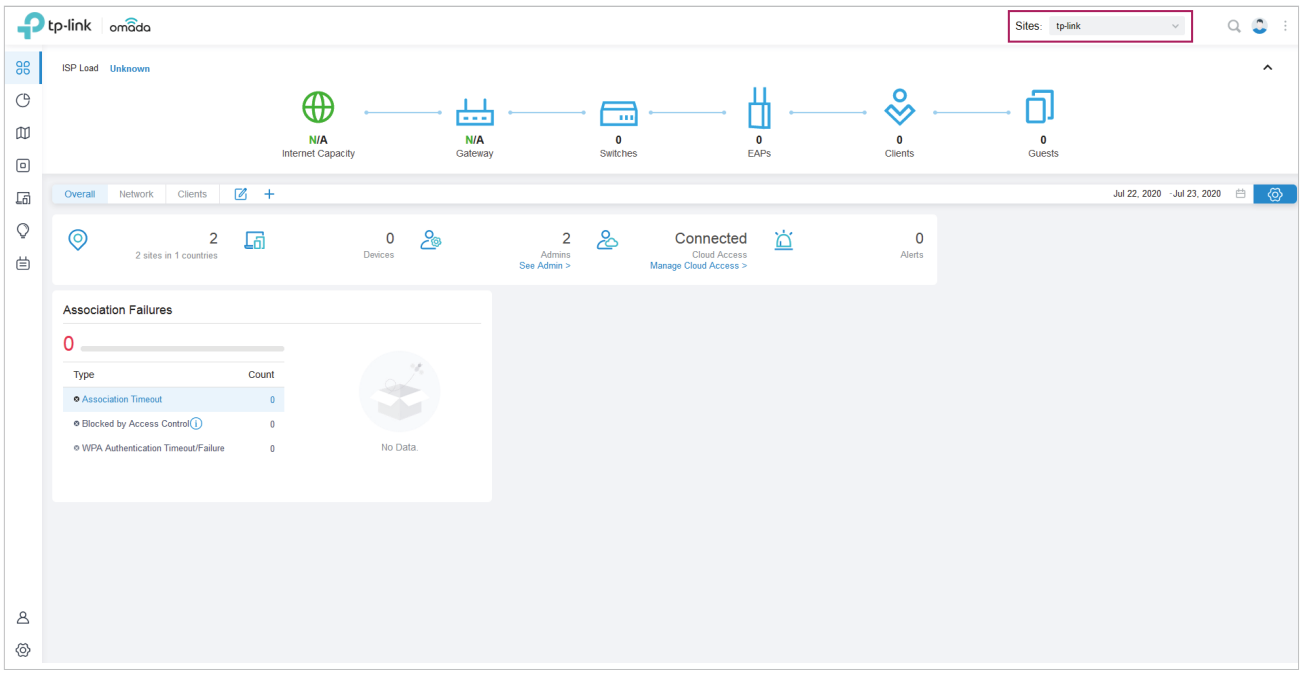
Create a Site → View and Edit the Site → Go Into the Site

To monitor and configure a site, you need first go into the site.

1. Select the site from the drop-down list of Sites to go into the site.



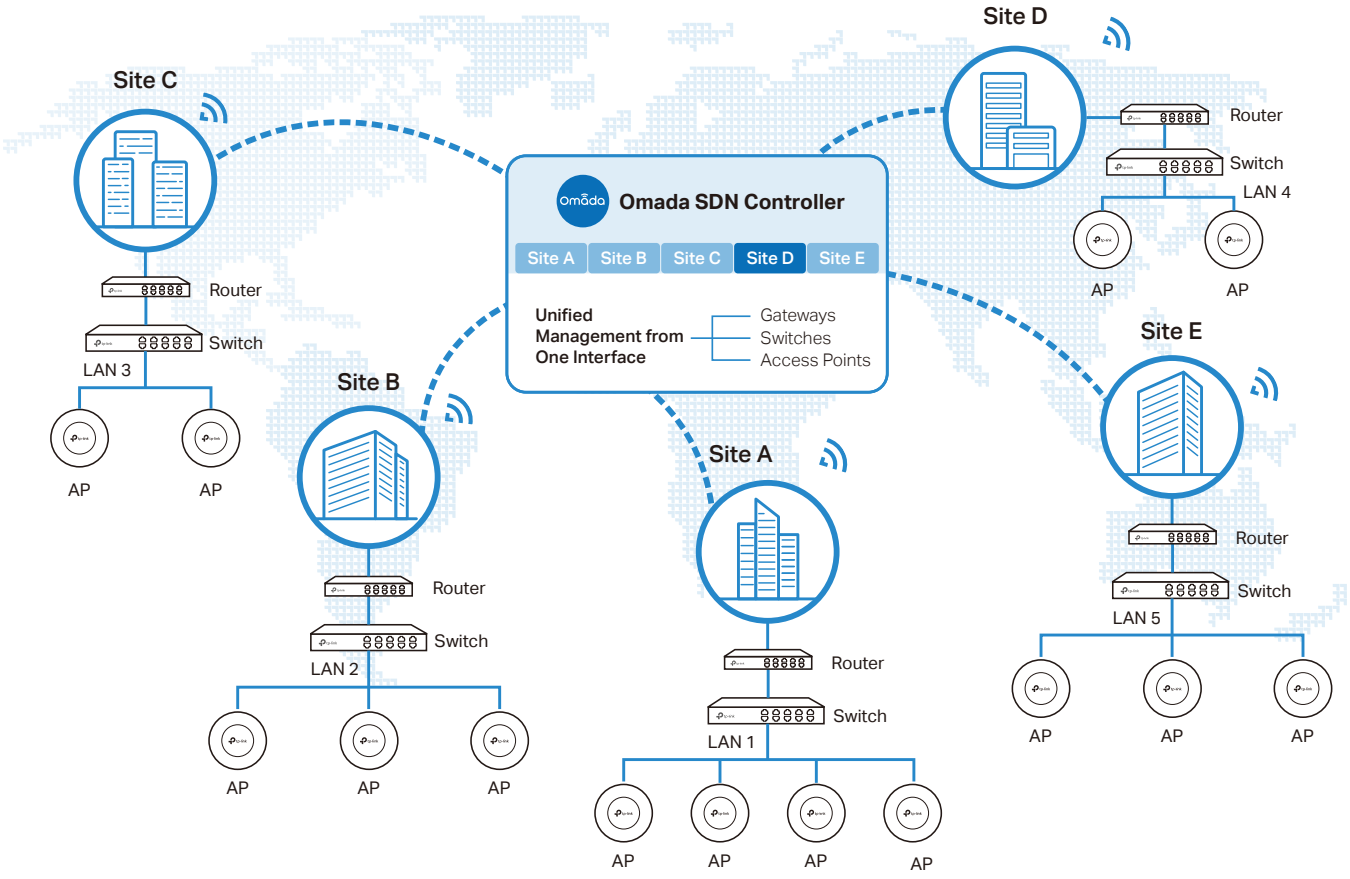
2. The Site field indicates the site which you are currently in. Some configuration items in the menu are applied to the site which you are currently in, whereas others are applied to the whole controller.



3. 2 Adopt Devices

Overview

After you create a site, add your devices to the site by making the controller adopt them. Make sure that your devices in each LAN are added to the corresponding site so that they can be managed centrally.



Configuration

Choose a procedure according to the type of your controller:

- For Omada Software Controller / Omada Hardware Controller
- For Omada Cloud-Based Controller

3. 3. 1 For Omada Software Controller / Omada Hardware Controller

To adopt the devices on the controller, follow these steps:

1) Prepare for communication between the controller and devices.

2) Prepare for device discovery.

3) Adopt the devices.

Note:

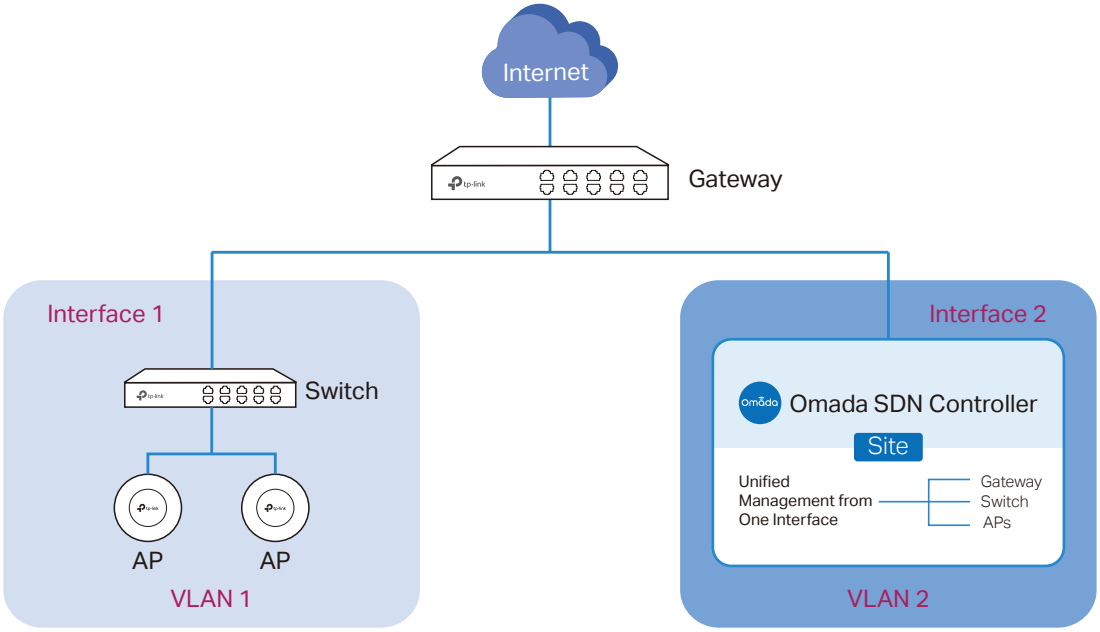
If the controller and devices are in the same LAN, subnet and VLAN, skip this step.

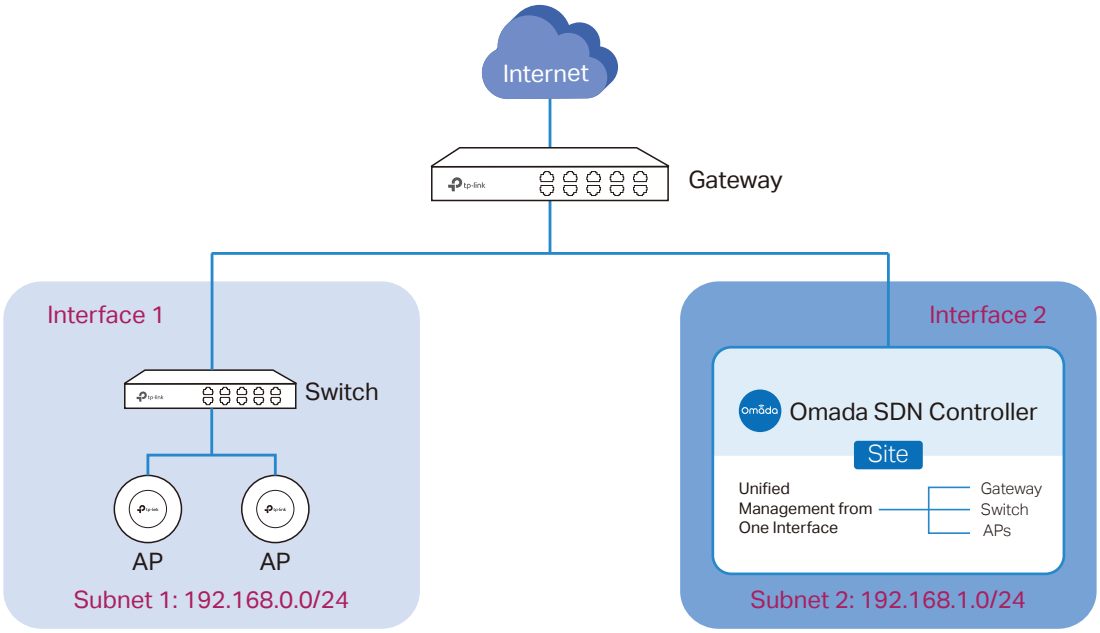
Make sure that the controller can communicate with the devices. Otherwise, the controller cannot discover or adopt the devices by any means. If the controller and devices are in different LANs, subnets or VLANs, use the following techniques to build up the connection according to your scenario.

1. Set up the Network

■ Scenario 1: Across VLANs or Subnets

As shown in the following figures, the controller and devices are in different VLANs or subnets. You need to set up a layer 3 interface for each VLAN or subnet, and make sure the interfaces can communicate with each other.





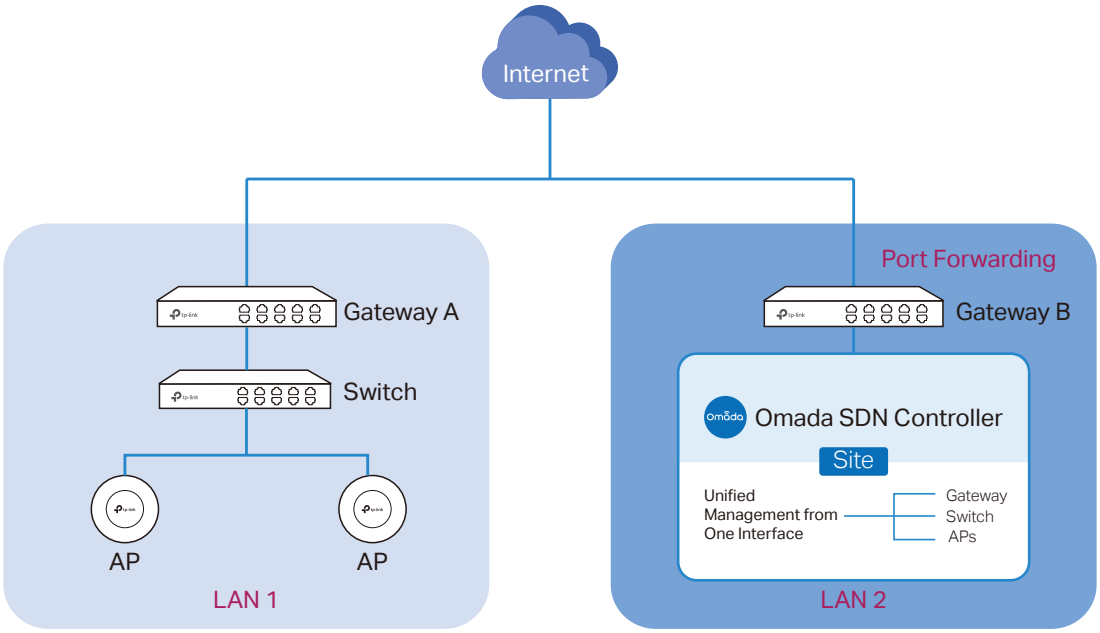
■ Scenario 2: Across LANs

As shown in the following figure, the controller and devices are in different LANs. You need to establish communication across the internet and the gateways.

By default, devices in LAN 1 cannot communicate with the controller in LAN 2, because Gateway B is in front of the controller and block access to it. To make the controller accessible to the devices, you can use Port Forwarding or VPN.

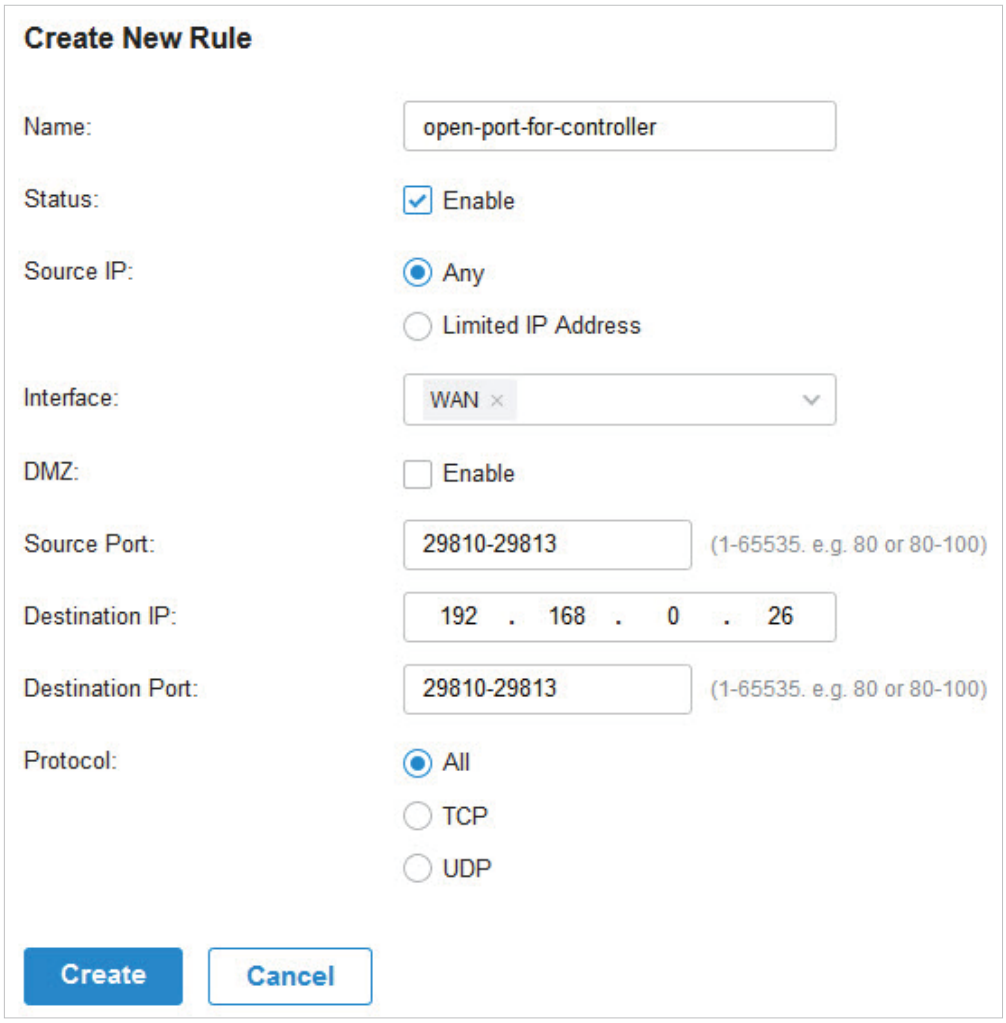
- Use Port Forwarding

Configure Port Forwarding on Gateway B and open port 29810-29813 for the controller, which are essential for discovering and adopting devices. If you are using firewalls in the networks, make sure that the firewalls don't block those ports.



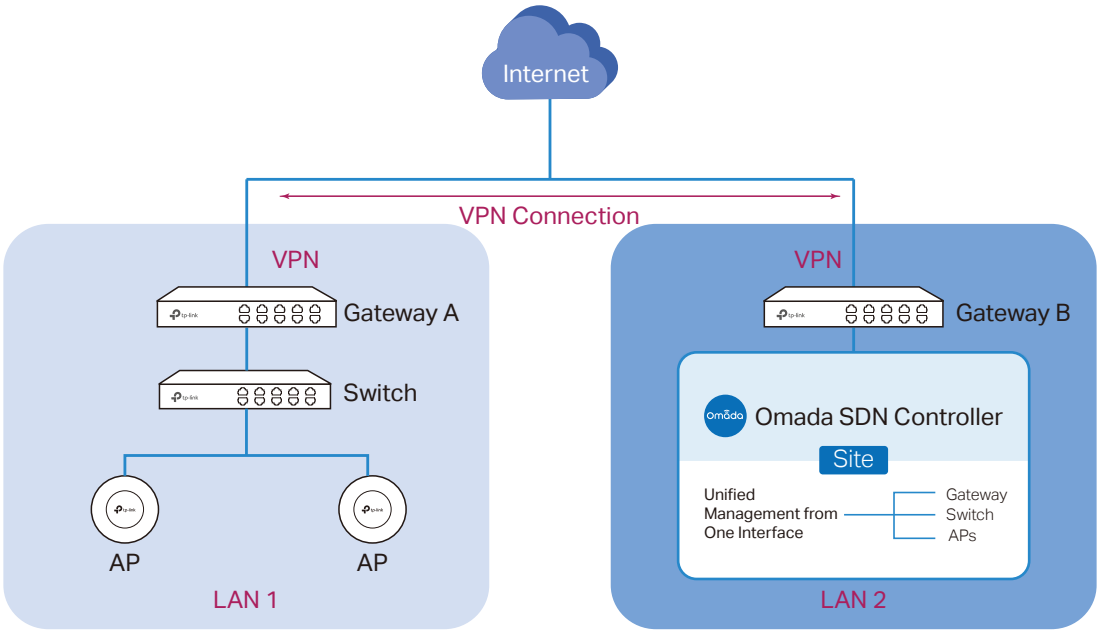
To configure Port Forwarding on Gateway B, you need first adopt Gateway B on the controller. For how to adopt Gateway B, refer to Adopt the Devices. Go to Settings > Transmission > NAT > Port Forwarding. Click + Create New Rule to load the following page. Specify a name to identify the Port Forwarding rule, check Enable for Status, select Any as Source IP, select the desired WAN port

as Interface, disable DMZ, specify 29810-29813 as Source Port and Destination Port, specify the controller's IP address as Destination IP, and select All as Protocol. Then click Create.



- Use VPN

Set up a VPN connection between Gateway A and Gateway B in Standalone Mode. For details about VPN configuration, refer to the User Guide of the gateways.

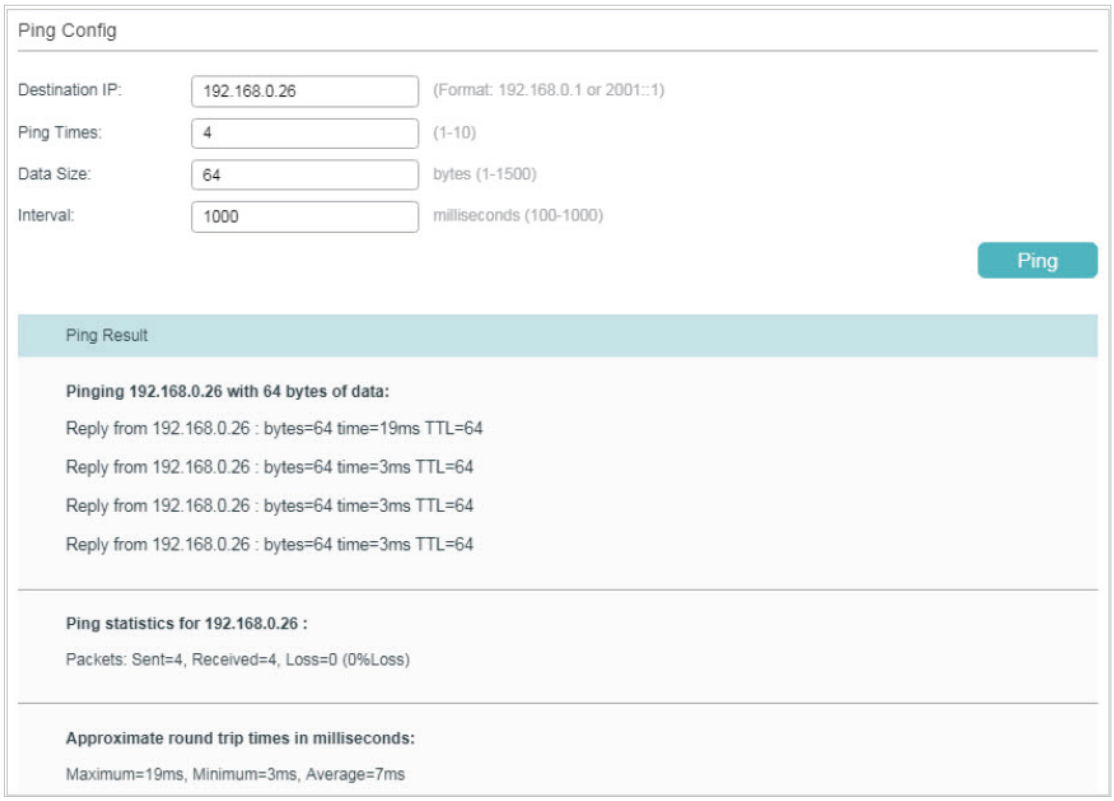


2. (Optional) Test the network

If you are not sure whether the controller and devices can establish communication, it's recommended to do the ping test from the devices to the controller.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Then Go to MAINTENANCE > Network Diagnostics > Ping to load the following page, and specify Destination

IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click Ping.



If the ping result shows the packets are received, it implies that the controller can communicate with the devices. Otherwise, the controller cannot communicate with the devices, then you need to check your network.

Prepare for Communication > **Prepare for Device Discovery** > Adopt the Devices

Note:

If the controller and devices are in the same LAN, subnet and VLAN, skip this step. In this scenario, the controller can discover the devices directly, and no additional settings are required.

Make sure that the controller can discover the devices.

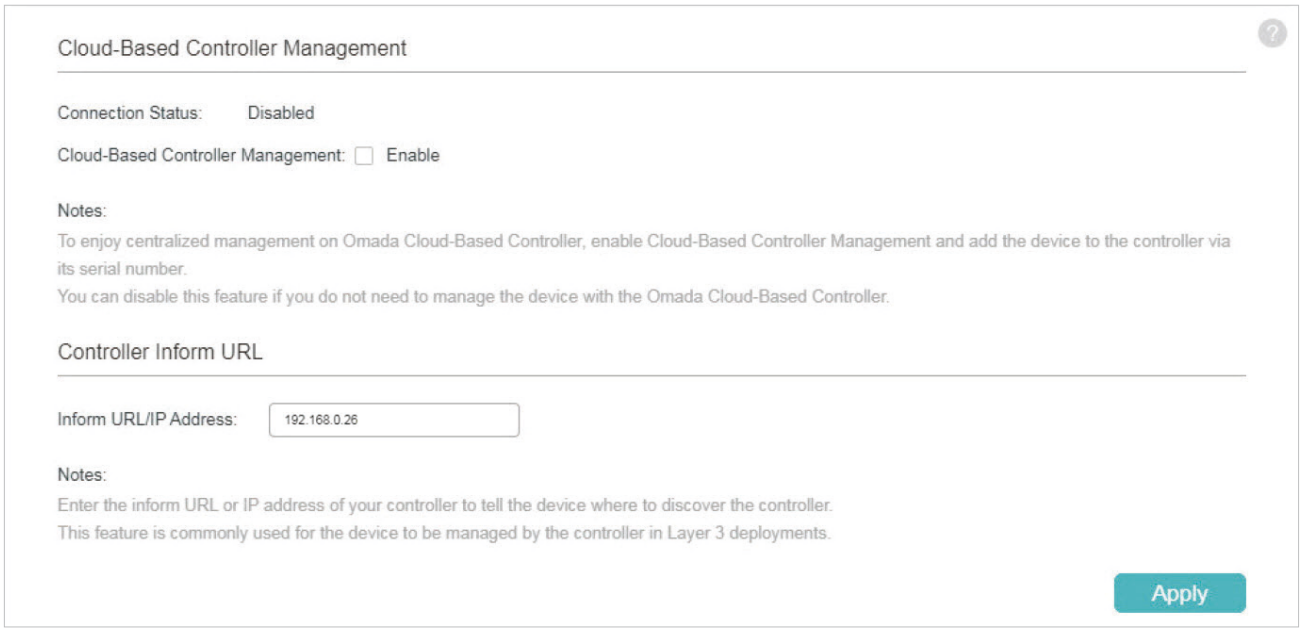
When the controller and devices are in different LANs, subnets or VLANs, the controller cannot discover the devices directly. You need to choose Controller Inform URL, Discovery Utility, or DHCP Option 138 as the method to help the controller discover the devices.

- **Controller Inform URL**

  Controller Inform URL informs the devices of the controller's URL or IP address. Then the devices make contact with the controller so that the controller can discover the devices.

  You can configure Controller Inform URL for devices in Standalone Mode. Let's take a switch for example. Log into the management page of the switch in Standalone Mode and go to SYSTEM > Controller Settings to load the following page. In Controller Inform URL, specify Inform URL/

IP Address as the controller's URL or IP address (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click Apply.

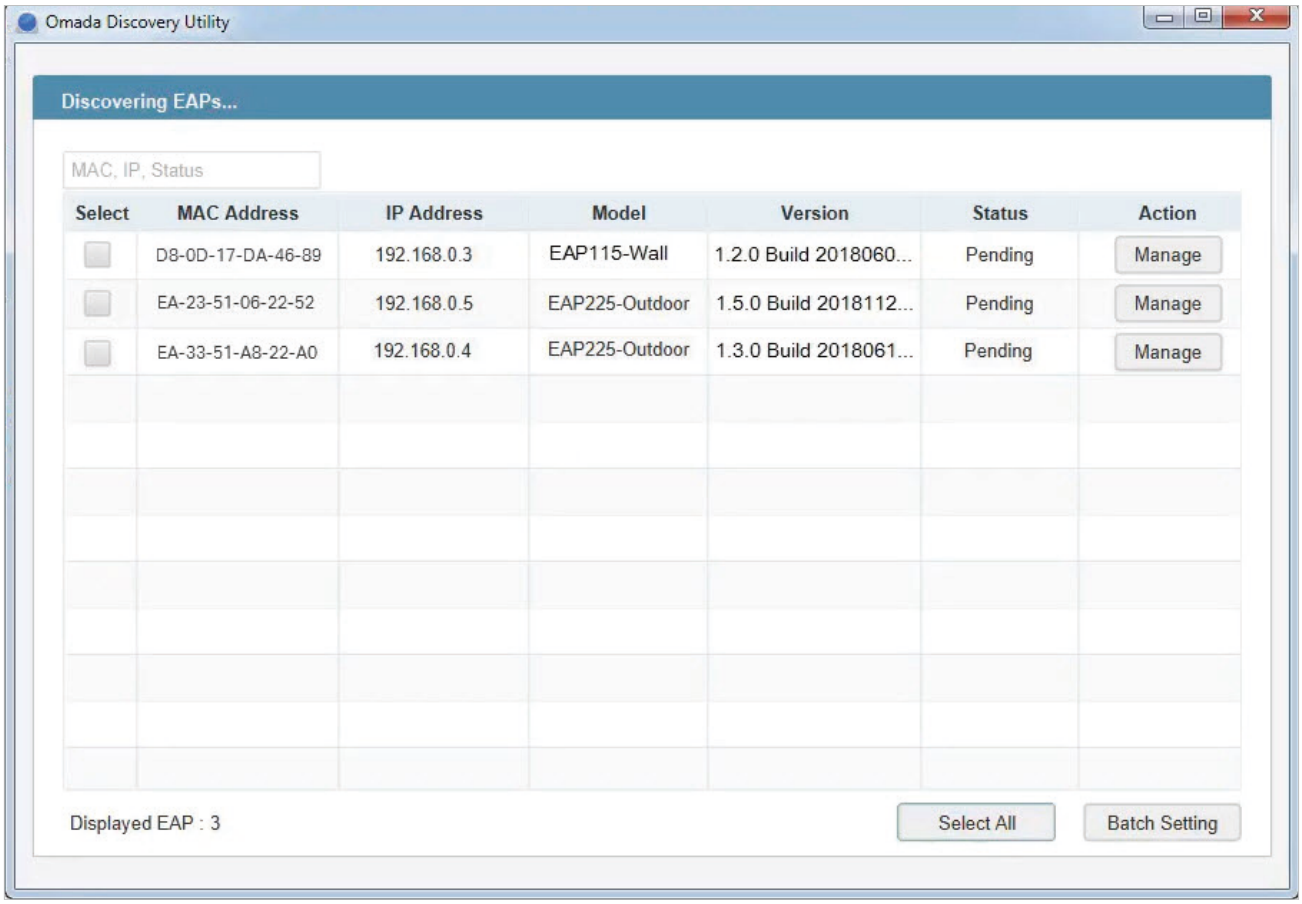


- **Discovery Utility**

  Discovery Utility can discover the devices in the same LAN, subnet and VLAN, and inform the devices of the controller's IP address. Then the devices make contact with the controller so that the controller can discover the devices.

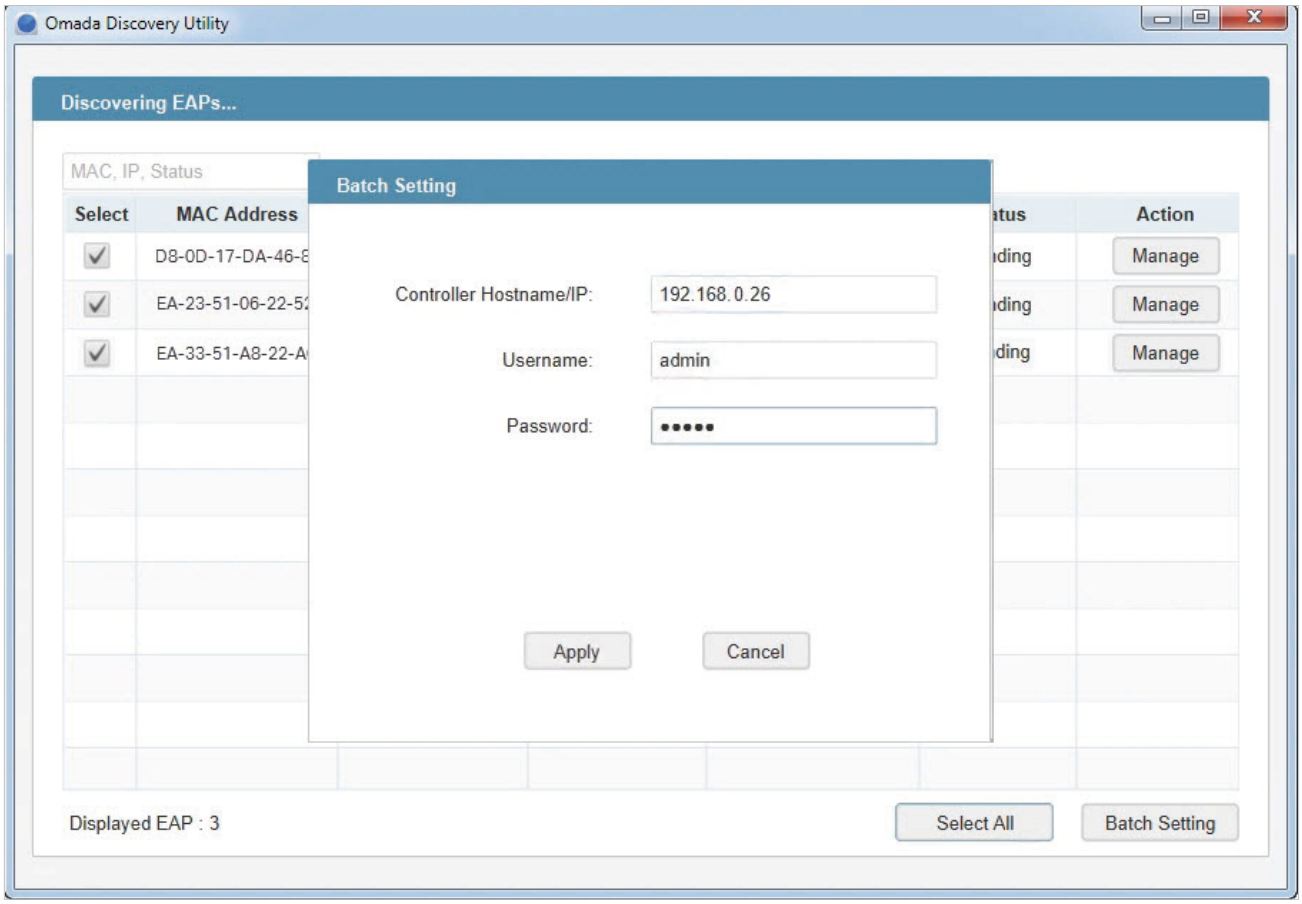
  1. Download Discovery Utility from the website and then install it on your PC which should be located in the same LAN, subnet and VLAN as your devices.

2. Open Discovery Utility and you can see a list of devices. Select the devices to be adopted and click Batch Setting.



3. Specify Controller Hostname/IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead), and

enter the username and password of the devices. By default, the username and password are both admin. Then click Apply. Wait until the setting succeeds.

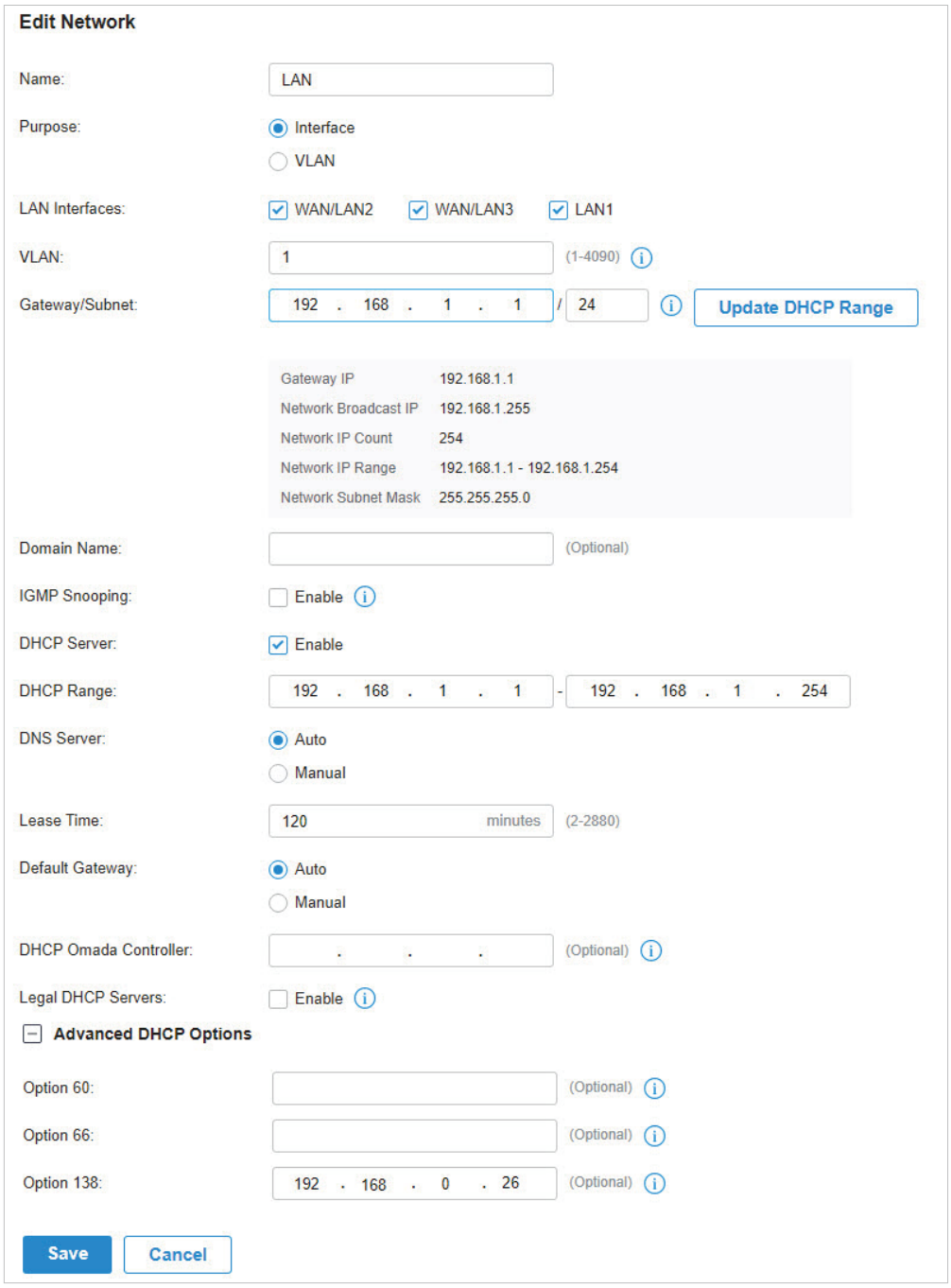


- **DHCP Option 138**

  DHCP Option 138 informs a DHCP client, such as a switch or an EAP, of the controller's IP address when the DHCP client sends DHCP requests to the DHCP server, which is typically a gateway.

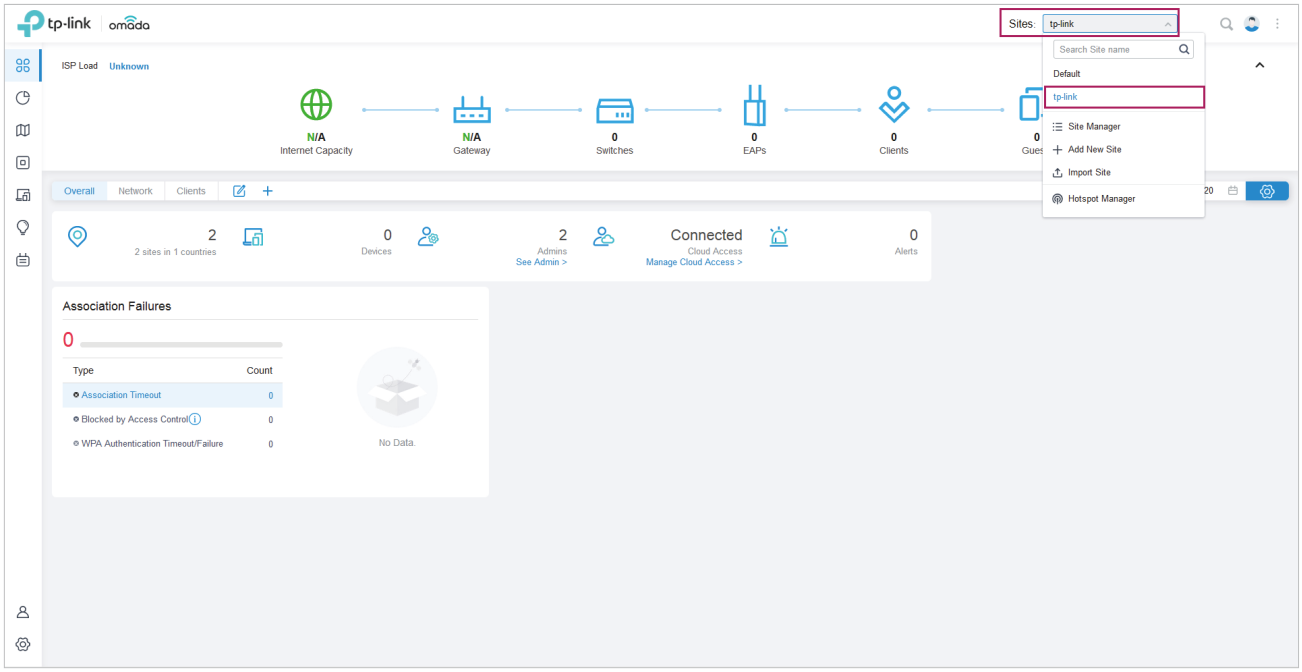
  1. To use DHCP Option 138, you need to adopt the gateway on the controller first, which may require other techniques like Controller Inform URL or Discovery Utility if necessary.
  2. After the gateway is adopted, go to Settings > Wired Networks > LAN > Networks, and click in the ACTION column of the LAN where the DHCP clients are located. Enable DHCP Server and configure common DHCP parameters. Then click Advanced DHCP Options and specify Option

138 as the controller's IP address (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Click Save.

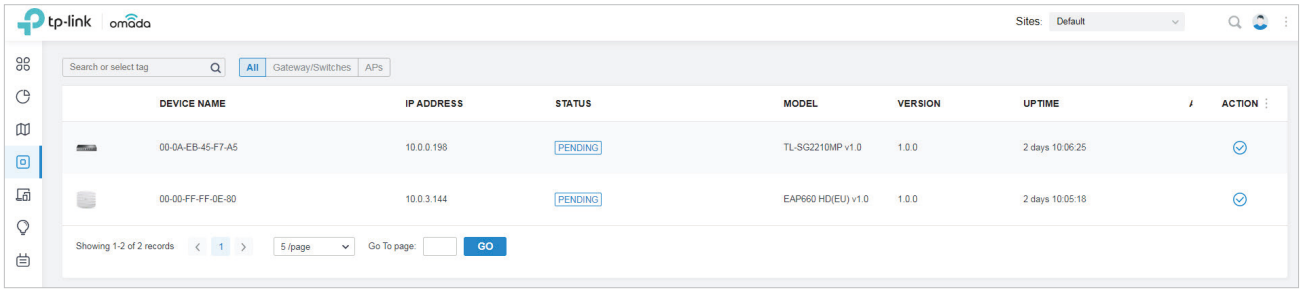


3. To make DHCP Option 138 take effect, you need to renew DHCP parameters for the DHCP clients. One possible way is to disconnect the DHCP clients and then reconnect them.

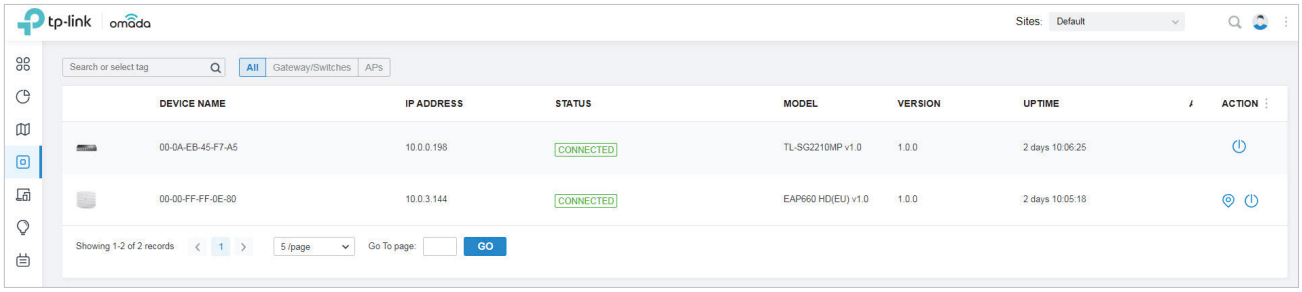
1. Decide which site you want to add the devices to. On the controller configuration page, select the site from the drop-down list of Sites.



2. Go to Devices, and devices which have been discovered by the controller are displayed. Click in the ACTION column of the devices which you want to add to the site.



3. Wait until the STATUS turns into Connected. Then the devices are adopted by the controller and added to the current site. Once the devices are adopted, they are subject to central management in the site.



3. 3. 2 For Omada Cloud-Based Controller

To adopt the devices on the controller, follow these steps:

1) Connect to the internet.

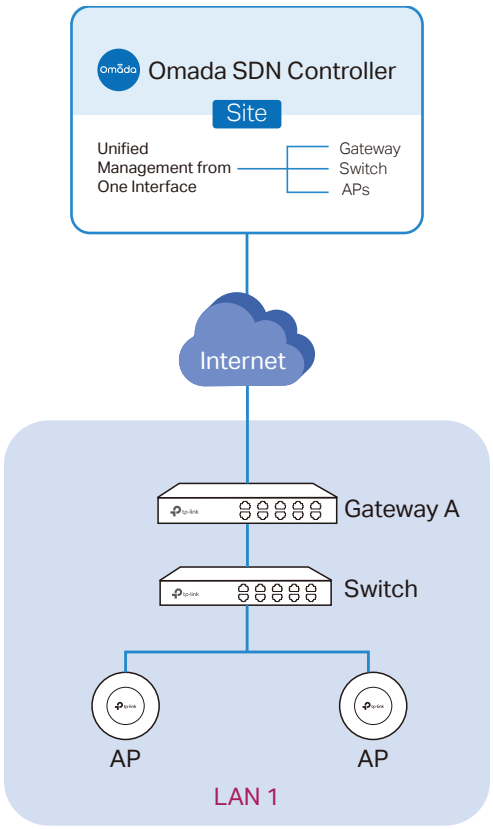
2) Prepare for controller management.

3) Adopt the devices.

Connect to the Internet > Prepare for Controller Management > Adopt the Devices

1. Set up the Network

   Make sure that your devices are connected to the internet.

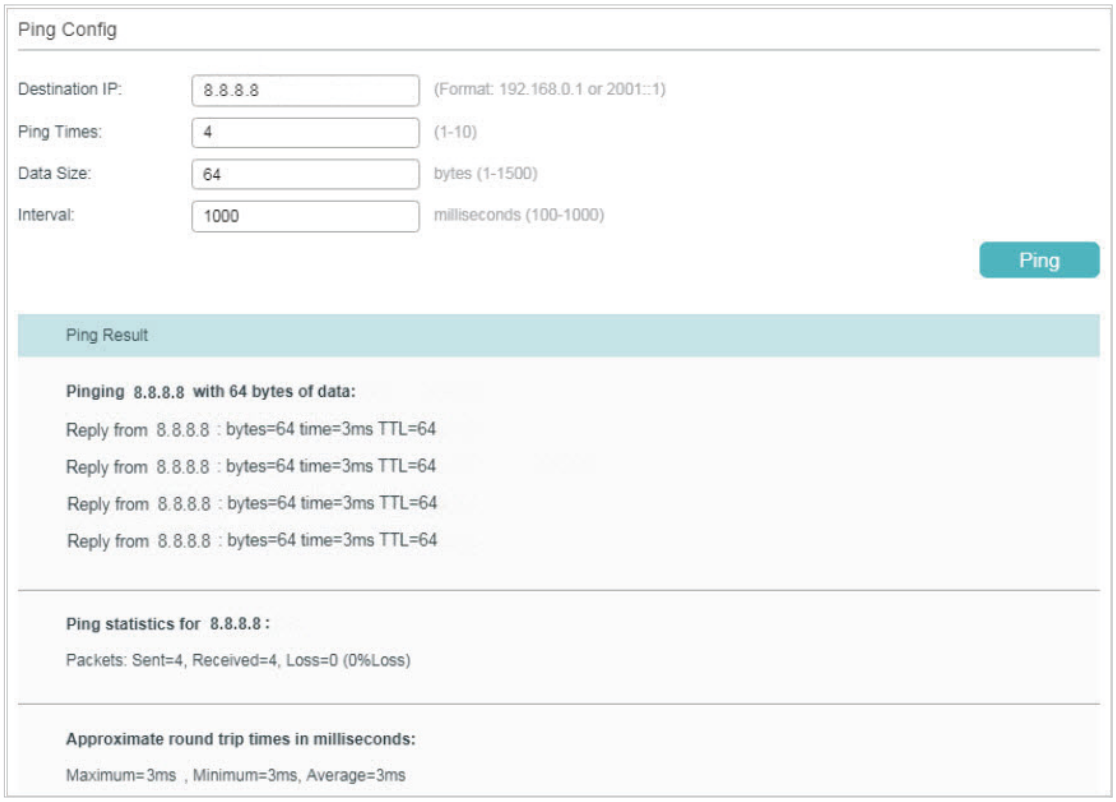


   If you are using firewalls in your network, make sure that the firewall doesn't block traffic from the controller. To configure your firewall policy, you may want to know the URL of the controller. After you open the web page of the controller, you can get the URL from the address bar of the browser.

2. (Optional) Test the network

   If you are not sure whether the devices are connected to the internet, it's recommended to do the ping test from the devices to a public IP address, such as 8.8.8.8.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Go to MAINTENANCE > Network Diagnostics > Ping to load the following page. Specify Destination IP as a public IP address, such as 8.8.8.8. Then click Ping.



If the ping result shows the packets are received, it implies that the devices are connected to the internet. Otherwise, the devices are not connected to the internet, then you need to check your network.

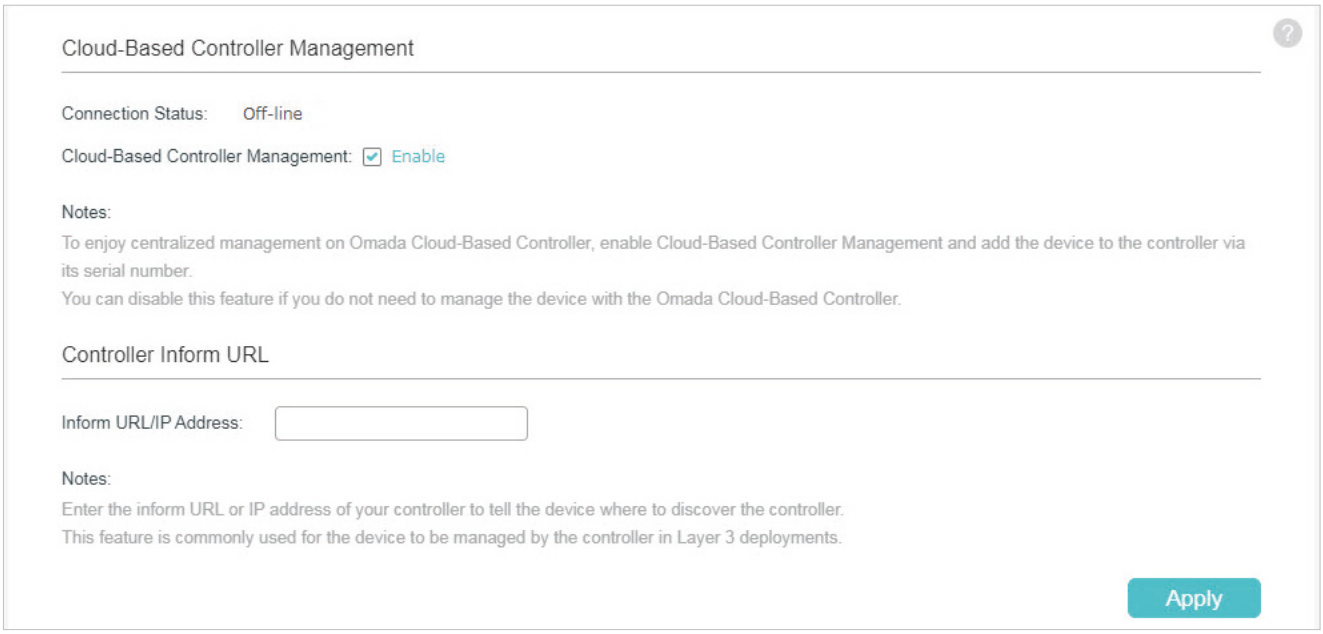
Connect to the Internet | **Prepare for Controller Management** | Adopt the Devices

Note:

If your devices are on the factory default setting, skip this step.

The Cloud-Based Controller Management feature allows the devices to be adopted by Omada Cloud-Based Controller. Make sure Cloud-Based Controller Management is enabled on the devices. For details, refer to the User Guide of your devices, which can be downloaded from the download center.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Go to SYSTEM > Controller Settings to load the following page. In Cloud-Based Controller Management, enable Cloud-Based Controller Management and click Apply.



Connect to the Internet > Prepare for Controller Management > **Adopt the Devices**

On the controller configuration page, go into the site where you want to add the devices. Go to Devices and click Add Devices. Then add your devices to the controller. Once the devices are adopted, they are subject to central management in the site.

4

Configure the Network with Omada SDN Controller

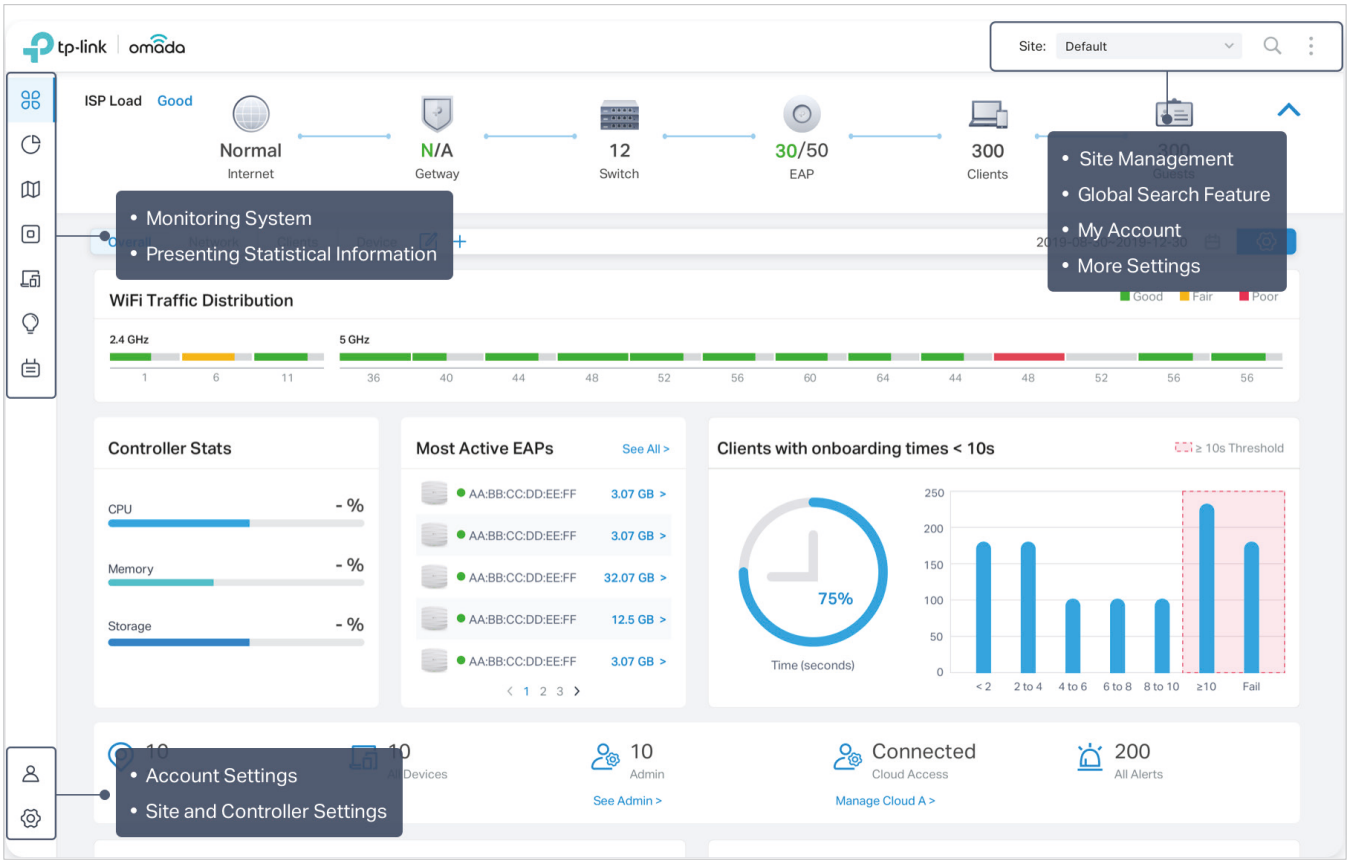
This chapter guides you on how to configure the network with Omada SDN Controller. As the command center and management platform at the heart of the Omada network, Omada SDN Controller provides a unified approach to configuring enterprise networks comprised of routers, switches, and wireless access points. The chapter includes the following sections:

- Navigate the UI
- Modify the Current Site Configuration
- Configure Wired Networks
- Configure Wireless Networks
- Network Security
- Transmission
- Configure VPN
- Create Profiles
- Authentication
- Services

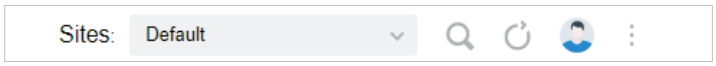
4. 1 Navigate the UI

As you start using the management interface of the controller (Controller UI) to configure and monitor your network, it is helpful to familiarize yourself with the most commonly-used elements of the Controller UI that are frequently referenced in this guide.

The Controller UI is grouped into task-oriented menus, which are located in the top right-hand corner and the left-hand navigation bar of the page. Note that the settings and features that appear in the UI depend on your user account permissions. The following image depicts the main elements of the Controller UI.



The elements in the top right corner of the screen give quick access to:



Site Management

Site, which means logically separated network location, is the largest unit for managing networks with Omada SDN Controller. You can simultaneously configure features for multiple devices at a site. The Site Management includes:

Site Manager — have a quick overview of sites, including the name, location, managed devices, and connected clients.

Add New Site — add a new site, which is the logically separated network location. The site is the largest unit for managing the network.

Import Site — import the site from another controller.

Global Search Feature

Click and enter the keywords to quickly look up the functions that you want to configure.

My Account

Click the account icon to display account information, Account Settings and Log Out. You can change your password on Account Settings.

More Settings

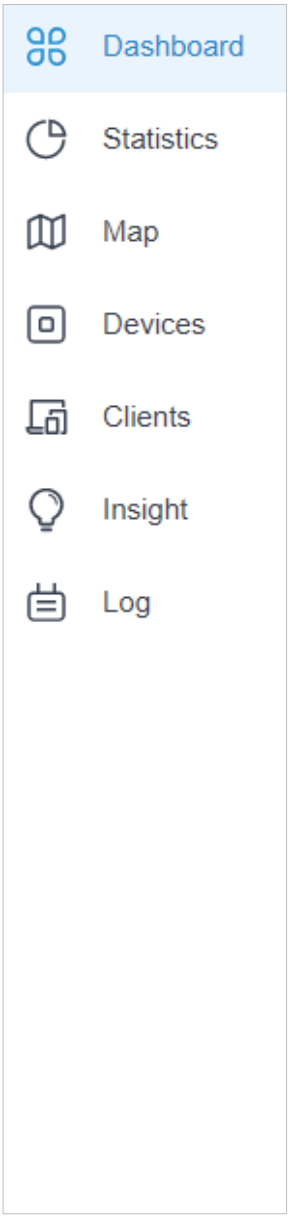
Click to display Preferences, About and Tutorial.

Preferences: Click to jump to Maintenance and customize the Controller UI depending on your needs. For details, refer to Maintenance

About: Click to display the controller version.

Tutorial: Click to view the quick Getting Started guide which demonstrates the navigation and tools available for the controller.

The left-hand navigation bar provides access to:



Dashboard displays a summarized view of the network status through different visualizations. The widget-driven dashboard is customizable depending on your needs.

Statistics provides a visual representation of the clients and network managed by the controller. The run charts show changes in device performances over time, including the status of switches and speed test results.

Map generates the system topology automatically and you can look over the provisioning status of devices. By clicking on each node, you can view the detailed information of each device. You can also upload images of your location for a visual representation of your network.

Devices displays all TP-Link devices discovered on the site and their general information. This list view can change depending on your monitoring needs through customizing the columns. You can click any device on the list to reveal the Properties window for more detailed information of each device and provisioning individual configurations to the device.

Clients displays a list view of wired and wireless clients that are connected to the network. This list view can change depending on your monitoring need through customizing the columns. You can click any clients on the list to reveal the Properties window for more detailed information of each client and provisioning individual configurations to the client.

Insight displays a list of statistics of your network device, clients and services during a specified period. You can change the range of date in one-day increments.

Log displays logs that record varied activities of users, devices, and systems events, such as administrative actions and abnormal device behaviors. You can also configure notifications to receive alert emails of certain activities.

Admin allows you to configure multi-level administrative accounts with a hierarchy of permissions that can be configured to provide finely grained levels of access to the controller as required by your enterprise.

Settings is divided to two parts: Site Settings and Controller Settings. In Site Settings, you can provision and configure all your network devices on the same site in minutes. In Controller Settings, you can maintain the controller system for best performance.

4. 2 Modify the Current Site Configuration

You can view and modify the configurations of the current site in Site, including the basic site information, centrally-managed device features, and the device account. The features and device account configured here are applied to all devices on the site, so you can easily manage the devices centrally.

4. 2. 1 Site Configuration

Overview

In Site Configuration, you can view and modify the site name, location, time zone, and application scenario of the current site.

Configuration

Select a site from the drop down list of Sites in the top-right corner, go to Settings > Site, and configure the following information of the site in Site Configuration. Click Save.



Site Name	Specify the name of the current site. It should be no more than 64 characters.
Country/Region	Select the location of the site.
Time Zone	Select the time zone of the site.
Application Scenario	Specify the application scenario of the site. To customize your scenario, click Create New Scenario in the drop-down list.

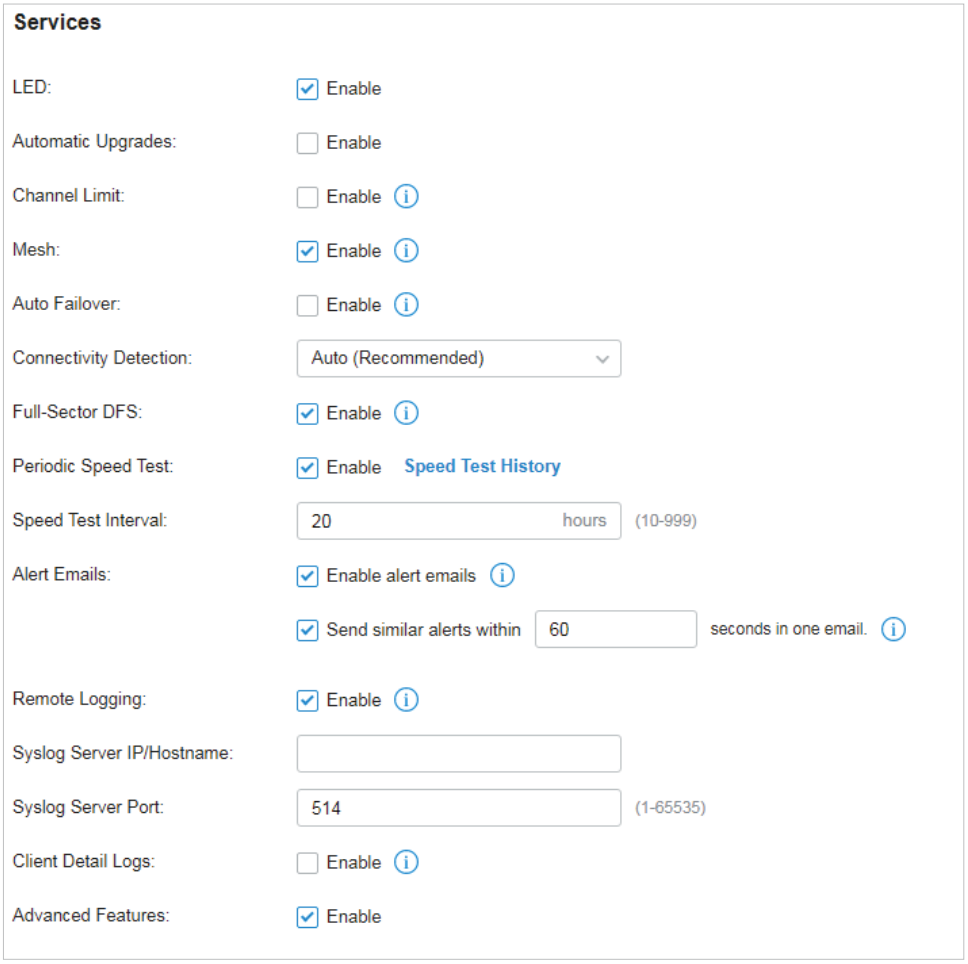
4. 2. 2 Services

Overview

In Services, you can view and modify the features applied to devices on the current site. Most features are applied to all devices, such as LED, Automatic Upgrades, and Alert Emails, while some are applied to EAPs only, such as Channel Limit and Mesh.

Configuration

Select a site from the drop down list of Sites in the top-right corner, go to Settings > Site, and configure the following features for the current site in Services. Click Save.



LED	Enable or disable LEDs of all devices in the site. By default, the device follows the LED setting of the site it belongs to. To change the LED setting for certain devices, refer to Configure and Monitor Omada Managed Devices.
Automatic Upgrades	When enabled, the controller will automatically upgrade devices in this site to the latest version.
Channel Limit	(For Outdoor APs) When enabled, outdoor EAPs do not use the channel with the frequency ranging from 5150 MHz to 5350 MHz to meet the local laws and regulations limit in EU countries.
Mesh	(For EAP225/EAP245/EAP225-Outdoor) When enabled, EAPs supporting Mesh can establish the mesh network at the site.
Auto Failover	(For APs in the mesh network) Auto Failover is used to automatically maintain the mesh network. When enabled, the controller will automatically select a new wireless uplink for the AP if the original uplink fails. To enable this feature, enable Mesh first.

Connectivity Detection	(For APs in the mesh network) Specify the method of Connection Detection when mesh is enabled. In a mesh network, the APs can send ARP request packets to a fixed IP address to test the connectivity. If the link fails, the status of these APs will change to Isolated. Auto (Recommended): Select this method and the mesh APs will send ARP request packets to the default gateway for the detection. Custom IP Address: Select this method and specify a desired IP address. The mesh APs will send ARP request packets to the custom IP address to test the connectivity. If the IP address of the AP is in different network segments from the custom IP address, the AP will use the default gateway IP address for the detection.
Full-Sector DFS	(For APs in the mesh network) With this feature enabled, when radar signals are detected on current channel by one EAP, the other EAPs in the mesh network will be also informed. Then all EAPs in the mesh network will switch to an alternate channel. To enable this feature, enable Mesh first.
Periodic Speed Test	When enabled, the controller tests and records the speed and latency of WAN ports periodically. Speed Test Interval: When enabled, specify the interval to decide how often to test the speed of devices. Speed Test History: Click it to view the history statistics of speed test in Speed Test Statistics.
Alert Emails	Enable alert emails: When enabled, the controller can send emails to notify the administrators and viewers of the site's 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 and viewers in one email. To configure alert-level logs and enable email notifications on the controller, refer to Notifications.
Remote Logging	With this feature configured, the controller will send generated system 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.
Advanced Features	(For APs) When enabled, you can configure more features for APs in Advanced Features. When disabled, these features keep the default settings. For detailed configuration, refer to Advanced Features.

4. 2. 3 Advanced Features

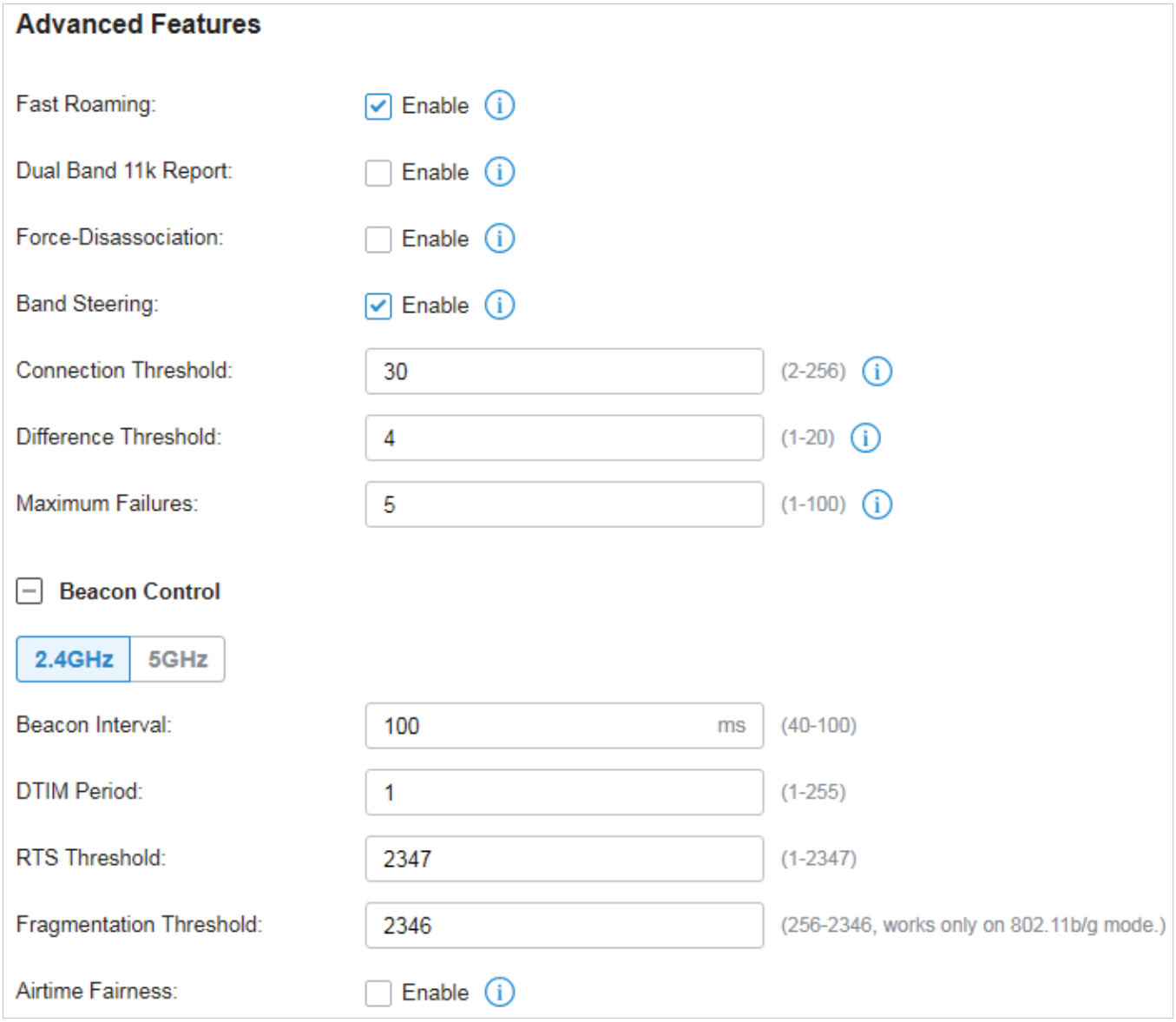
Overview

Advanced features include Fast Roaming, Band Steering, and Beacon Control, which are applicable to APs only. With these advanced features configured properly, you can improve the network's stability, reliability and communication efficiency.

Advanced features are recommended to be configured by network administrators with the WLAN knowledge. If you are not sure about your network conditions and the potential impact of all settings, keep Advanced Features disabled in Services to use their default configurations.

Configuration

Select a site from the drop down list of Sites in the top-right corner, go to Settings > Site, and enable Advanced Features in Services first. Then configure the following features in Advanced Features. Click Save.



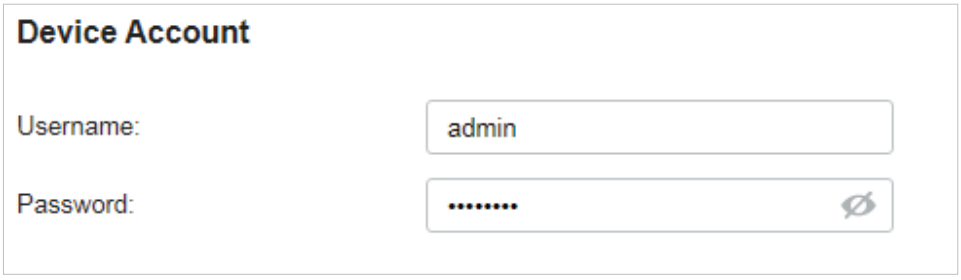
Fast Roaming	With this feature enabled, clients that support 802.11k/v can improve fast roaming experience when moving among different APs. By default, it is disabled.
Dual Bind 11k Report	When disabled, the controller provides neighbor list that contains only neighbor APs in the same band with which the client is associated. When enabled, the controller provides neighbor list that contains neighbor APs in both 2.4 GHz and 5 GHz bands. This feature is available only when Fast Roaming is enabled. By default, it is disabled.
Force-Disassociation	With this feature disabled, the AP only issues an 802.11v roaming suggestion when a client's link quality drops below the predefined threshold and there is a better option of AP, but whether to roam or not is determined by the client. With this feature enabled, the AP will force disassociate the client if it does not re-associate to another AP. This feature is available only when Fast Roaming is enabled. By default, it is disabled.
Band Steering	Band Steering can adjust the number of clients on 2.4 GHz and 5 GHz bands to provide better wireless experience. When enabled, dual-band clients will be steered to the 5 GHz band according to the configured parameters. With appropriate settings, Band Steering can improve the network performance because the 5 GHz band supports a larger number of non-overlapping channels and is less noisy. By default, it is disabled. Connection Threshold: Specify the maximum number of clients connected to the 5 GHz band. By default, the threshold is 30. Difference Threshold: Specify the maximum difference between the number of clients on the 5 GHz band and 2.4 GHz band. By default, the threshold is 4. When the connection number and difference of client number both exceed their configured threshold, the EAP will refuse the connection request on 5 GHz band and no longer steers other clients to the 5 GHz band. Maximum Failures: Specify the maximum number of the failed attempts when a client repeatedly tries to associate with an EAP on 5 GHz. When the number of rejections reaches Maximum Failures, the EAP will accept the client's request for connection. By default, it is 4.

Beacon Control	Beacons are transmitted periodically by the EAP to announce the presence of a wireless network for the clients. Click ⊞, select the band, and configure the following parameters of Beacon Control. Beacon Interval: Specify how often the APs send a beacon to clients. By default, it is 100. DTIM Period: Specify how often the clients check for buffered data that are still on the EAP awaiting pickup. By default, the clients check for them at every beacon. DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames indicating whether the EAP has buffered data for client devices. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend that you keep the default interval, 1. RTS Threshold: RTS (Request to Send) can ensure efficient data transmission by avoiding the conflict of packets. If a client wants to send a packet larger than the threshold, the RTS mechanism will be activated to delay packets of other clients in the same wireless network. We recommend that you keep the default threshold, which is 2347. If you specify a low threshold value, the RTS mechanism may be activated more frequently to recover the network from possible interference or collisions. However, it also consumes more bandwidth and reduces the throughput of the packet. Fragmentation Threshold: Fragmentation can limit the size of packets transmitted over the network. If a packet to be sent exceeds the Fragmentation threshold, the Fragmentation function will be activated, and the packet will be fragmented into several packets. By default, the threshold is 2346. Fragmentation helps improve network performance if properly configured. However, too low fragmentation threshold may result in poor wireless performance because of the increased message traffic and the extra work of dividing up and reassembling frames. Airtime Fairness: With this option enabled, each client connecting to the EAP can get the same amount of time to transmit data so that low-data-rate clients do not occupy too much network bandwidth and network performance improves as a whole. We recommend you enable this function under multi-rate wireless networks.

4. 2. 4 Device Account

You can specify a device account for all adopted devices on the site in batches. Once the devices are adopted by the controller, their username and password become the same as settings in Device Account to protect the communication between the controller and devices. By default, the username is admin and the password is generated randomly.

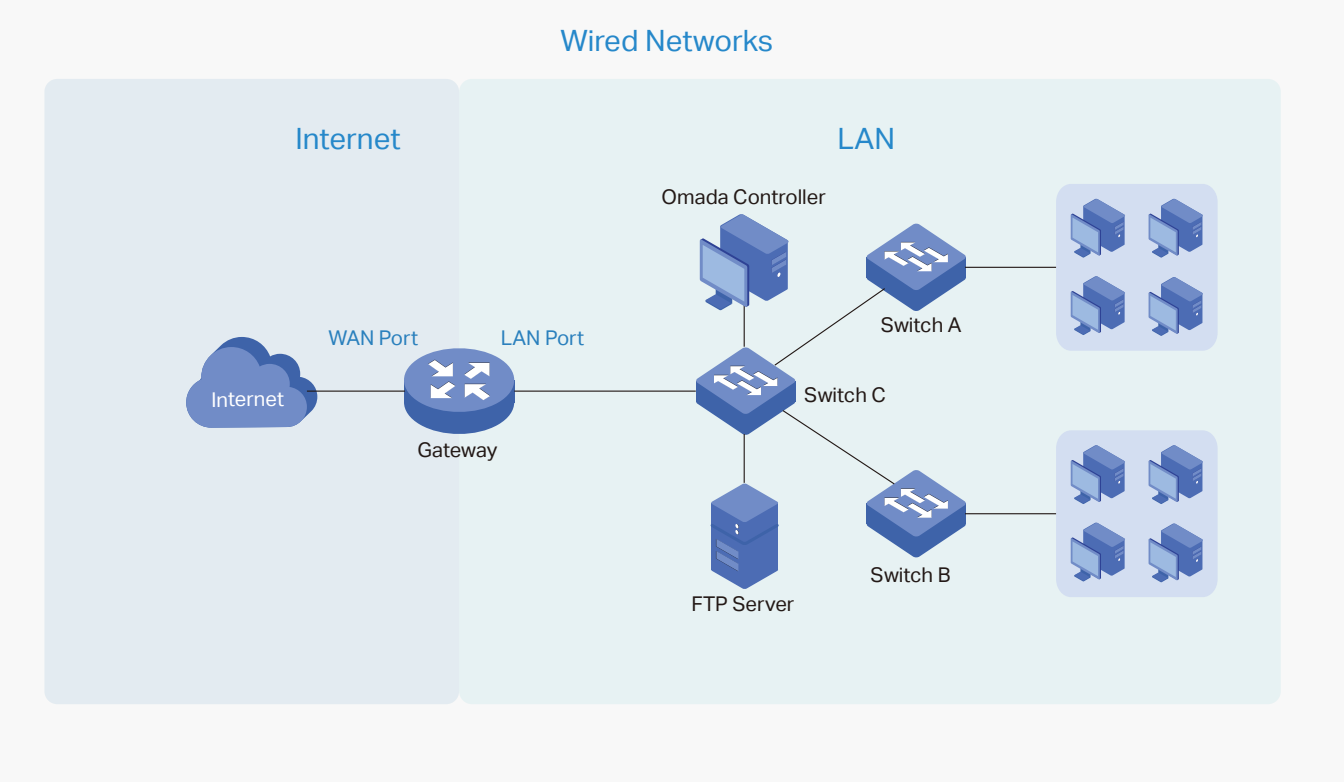
Go to Settings > Site and modify the username and password in Device Account. Click Save and the new username and password are applied to all devices on the site.



4. 3 Configure Wired Networks

Wired networks enable your wired devices and clients including the gateway, switches, EAPs and PCs to connect to each other and to the internet.

As shown in the following figure, Wired Networks consist of two parts: Internet and LAN.



For Internet, you determine the number of WAN ports deployed by the gateway and how they connect to the internet according to your needs. To connect to the internet, the gateway choose one from the following connection types: Dynamic IP, Static IP, PPPoE, L2TP, and PPTP.

For LAN, you configure the wired internal network and how your devices logically separate from or connect to each other by means of VLANs and interfaces. Advanced LAN features include IGMP Snooping, DHCP Server and DHCP Options, PoE, Voice Network, 802.1X Control, Port Isolation, Spanning Tree, LLDP-MED, and Bandwidth Control.

4. 3. 1 Set Up an Internet Connection

Configuration

To set up an internet connection, follow these steps:

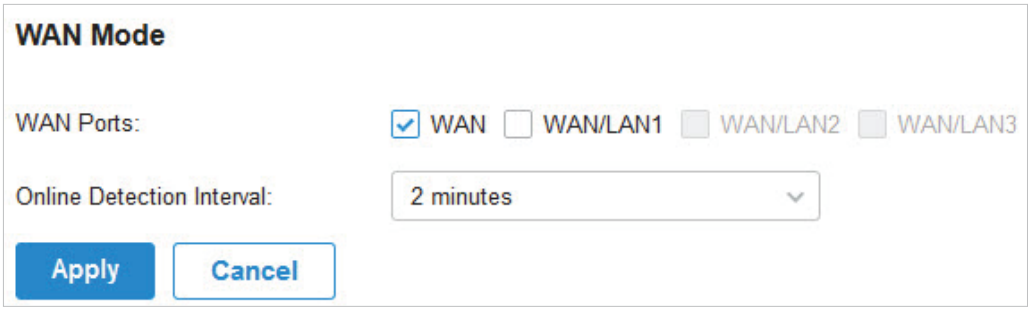
1) Select WAN Mode.

2) Configure WAN Connections.

3) (Optional) Configure Load Balancing.

Select WAN Mode > Configure WAN Connections > (Optional) Configure Load Balancing

Go to Settings > Wired Networks > Internet to load the following page. In WAN Mode, configure the number of WAN ports deployed by the gateway and other parameters. Then click Apply.



WAN Ports	Click the check box to enable the port as a WAN port. To configure multiple WAN ports, enable the ports one by one.
Online Detection Interval	Select how often the WAN ports detect WAN connection status. If you don't want to enable online detection, select Disable.

Select WAN Mode > **Configure WAN Connections** > (Optional) Configure Load Balancing

Note:

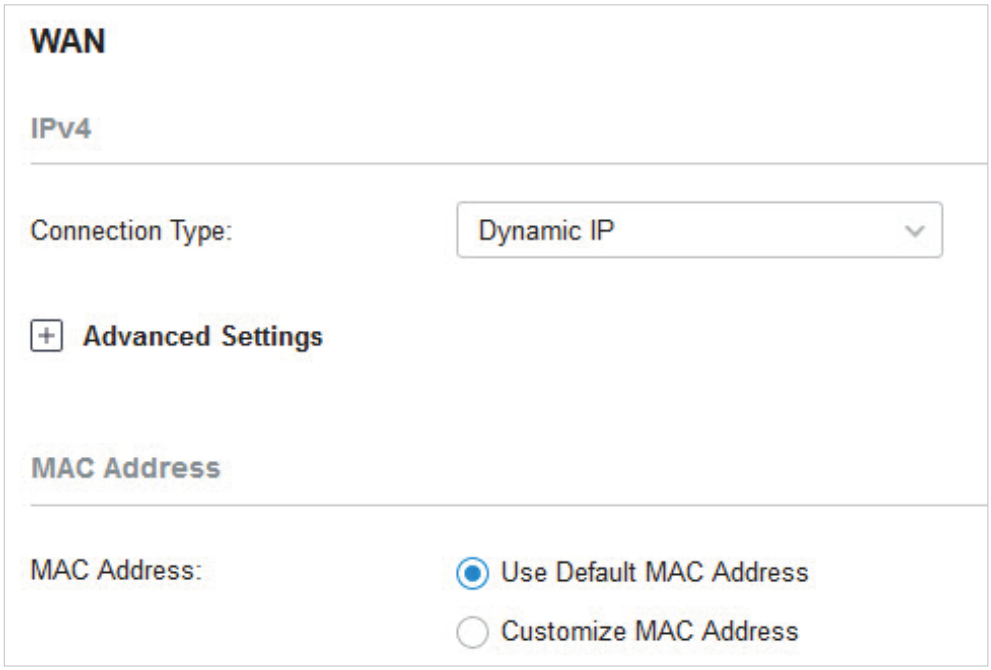
The number of configurable WAN ports is decided by WAN Mode.

Go to Settings > Wired Networks > Internet. For WAN connections, choose a Connection Type according to the service provided by your ISP.

Connection Type	Dynamic IP: If your ISP automatically assigns the IP address and the corresponding parameters, choose Dynamic IP. Static IP: If your ISP provides you with a fixed IP address and the corresponding parameters, choose Static IP. PPPoE: If your ISP provides you with a PPPoE account, choose PPPoE. L2TP: If your ISP provides you with an L2TP account, choose L2TP. PPTP: If your ISP provides you with a PPTP account, choose PPTP.

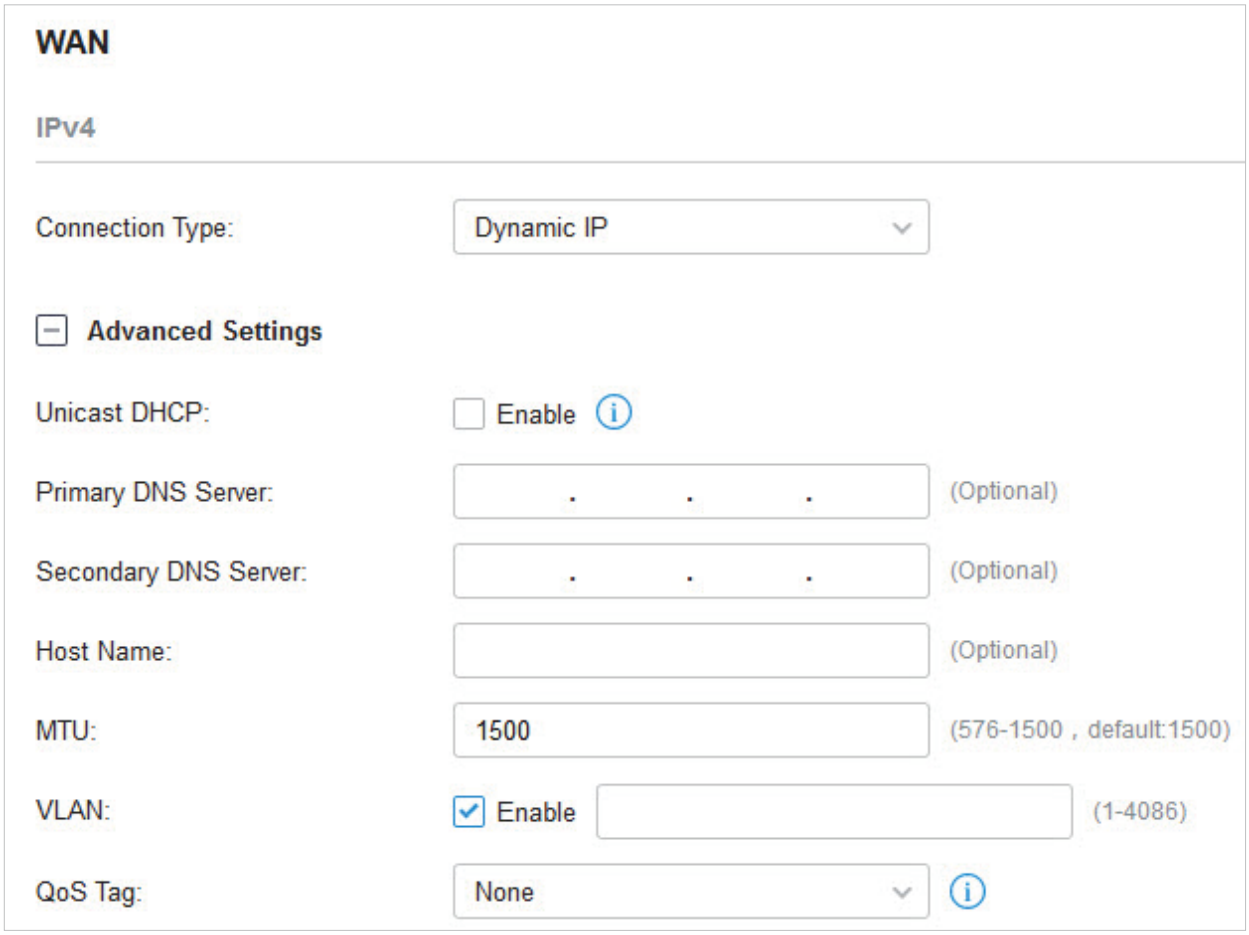
- **Dynamic IP**

1. Choose Connection Type as Dynamic IP and configure the following parameters.



MAC Address	Use Default MAC Address: The WAN port uses the default MAC address to set up the internet connection. It's recommended to use the default MAC address unless required otherwise. Customize MAC Address: The WAN port uses a customized MAC address to set up the internet connection and you need to specify the MAC address. Typically, this is required when your ISP bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

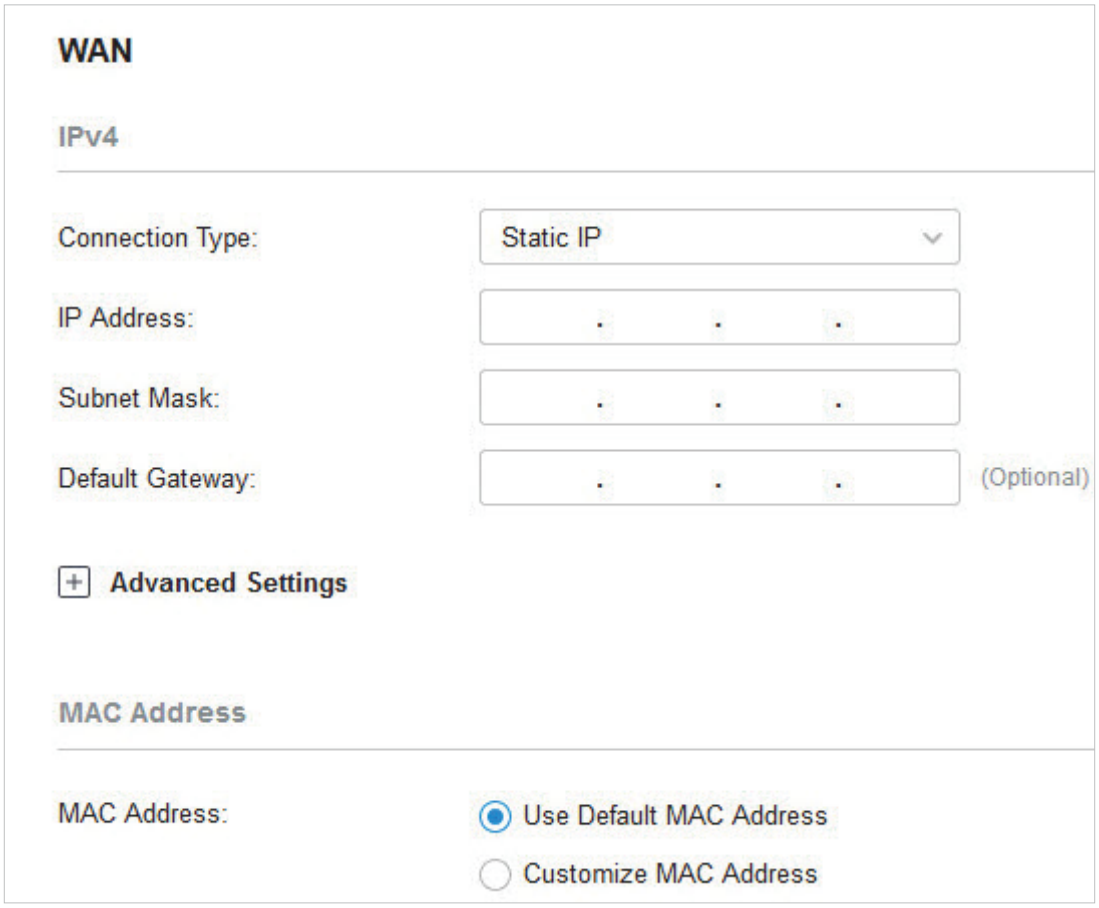
2. Click + Advanced Settings and configure the following parameters. Then click Apply.



Unicast DHCP	With this option enabled, the gateway will require the DHCP server to assign the IP address by sending unicast DHCP packets. Usually you need not to enable the option.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
Host Name	Enter a name for the gateway.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is Dynamic IP, MTU can be set in the range of 576-1500 bytes. The default value is 1500.
VLAN	Add the WAN port to a VLAN and you need to specify the VLAN. Generally, you don't need to manually configure it unless required by your ISP.
QoS Tag	The QoS (Quality of Service) function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 1 to 7. None means the packet will be forwarded without any operation. QoS Tag is only available when VLAN is enabled.

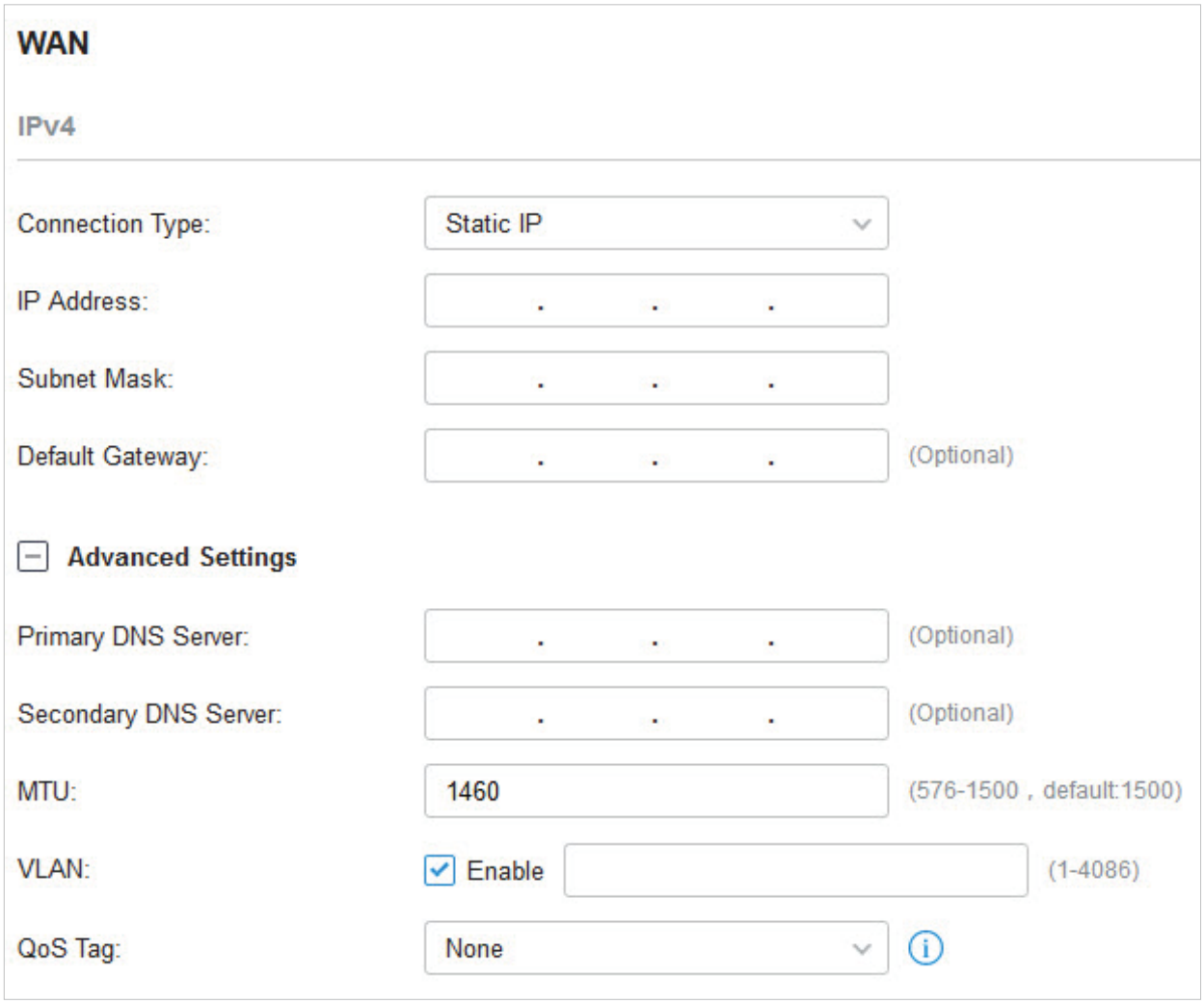
- **Static IP**

1. Choose Connection Type as Static IP and configure the following parameters.



IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Default Gateway	Enter the default gateway provided by your ISP.
MAC Address	Use Default MAC Address: The WAN port uses the default MAC address to set up the internet connection. It's recommended to use the default MAC address unless required otherwise. Customize MAC Address: The WAN port uses a customized MAC address to set up the internet connection and you need to specify the MAC address. Typically, this is required when your ISP bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

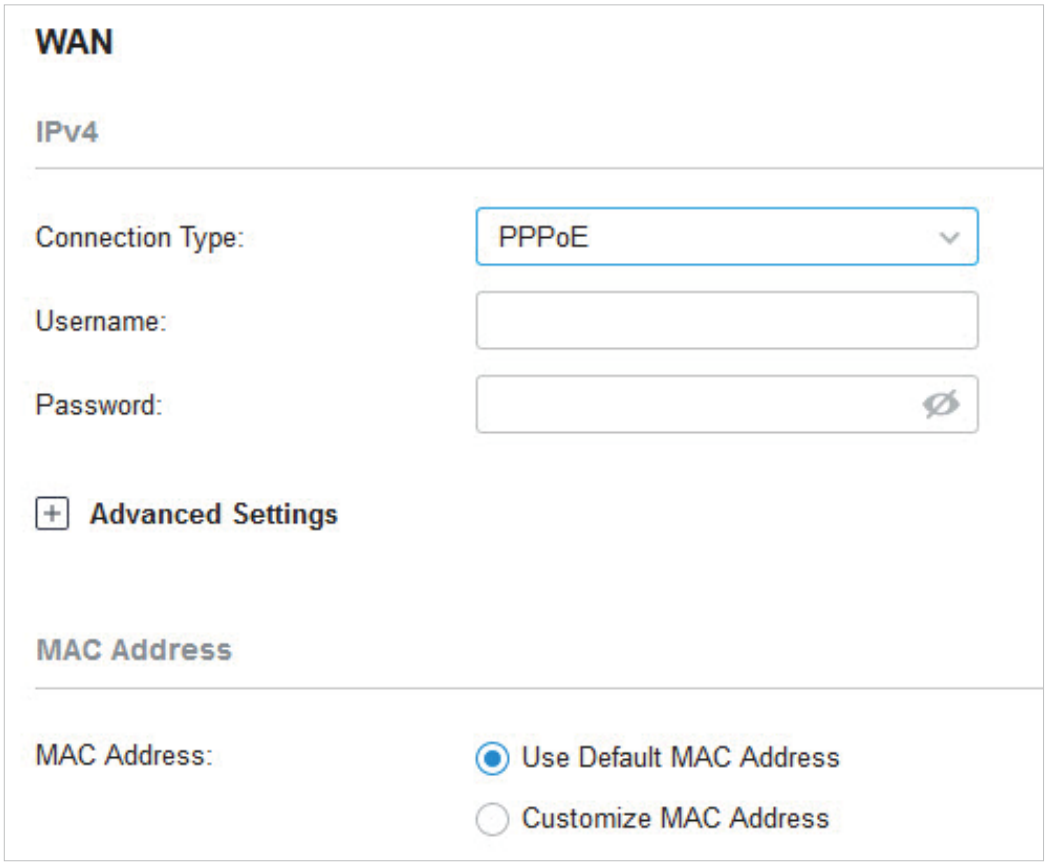
2. Click + Advanced Settings and configure the following parameters. Then click Apply.



Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is Static IP, MTU can be set in the range of 576-1500 bytes. The default value is 1500.
VLAN	Add the WAN port to a VLAN and you need to specify the VLAN. Generally, you don't need to manually configure it unless required by your ISP.
QoS Tag	The QoS (Quality of Service) function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 1 to 7. None means the packet will be forwarded without any operation. QoS Tag is only available when VLAN is enabled.

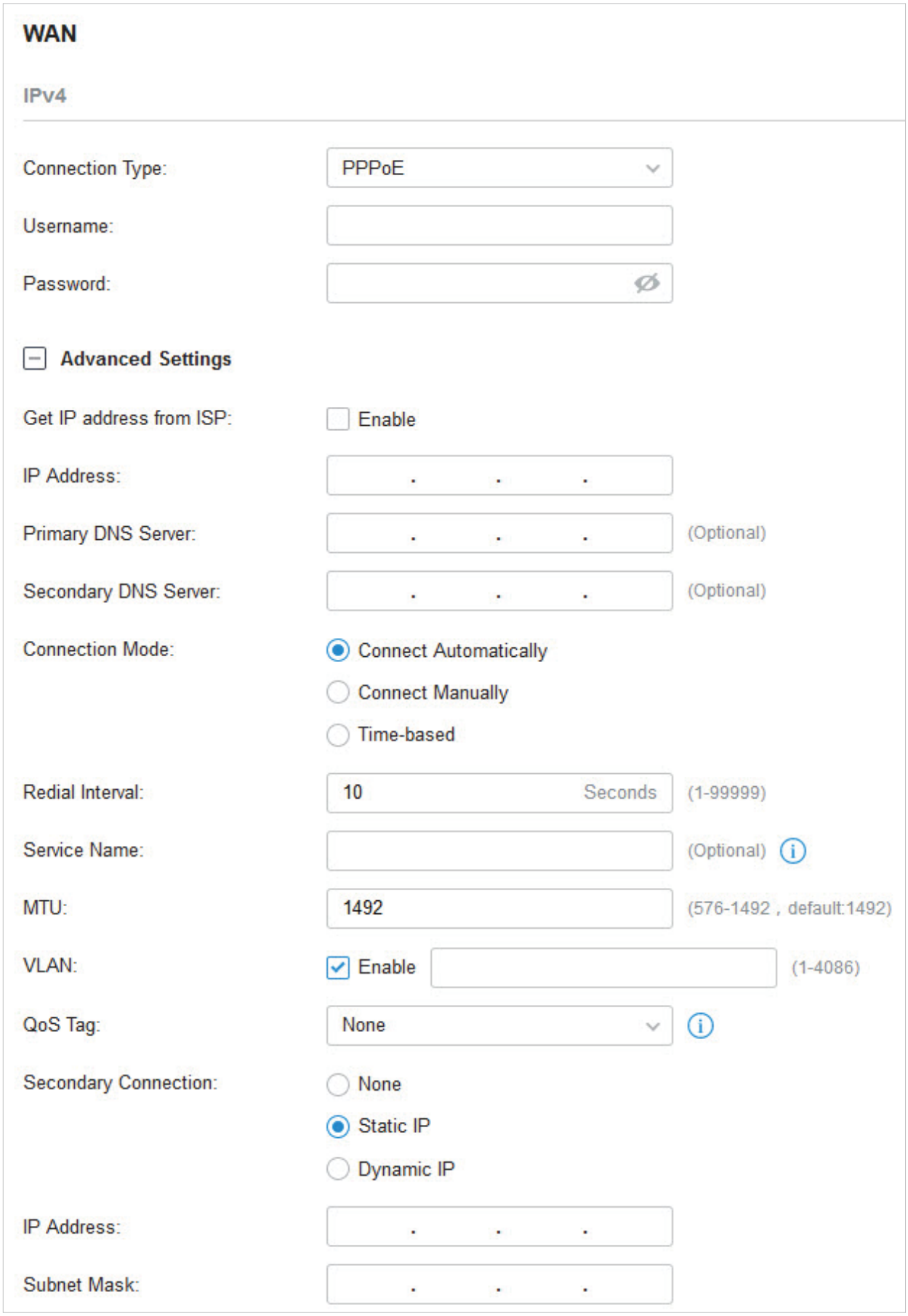
- **PPPoE**

1. Choose Connection Type as Static IP and configure the following parameters.



Username	Enter the PPPoE username provided by your ISP.
Password	Enter the PPPoE password provided by your ISP.
MAC Address	Use Default MAC Address: The WAN port uses the default MAC address to set up the internet connection. It's recommended to use the default MAC address unless required otherwise. Customize MAC Address: The WAN port uses a customized MAC address to set up the internet connection and you need to specify the MAC address. Typically, this is required when your ISP bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

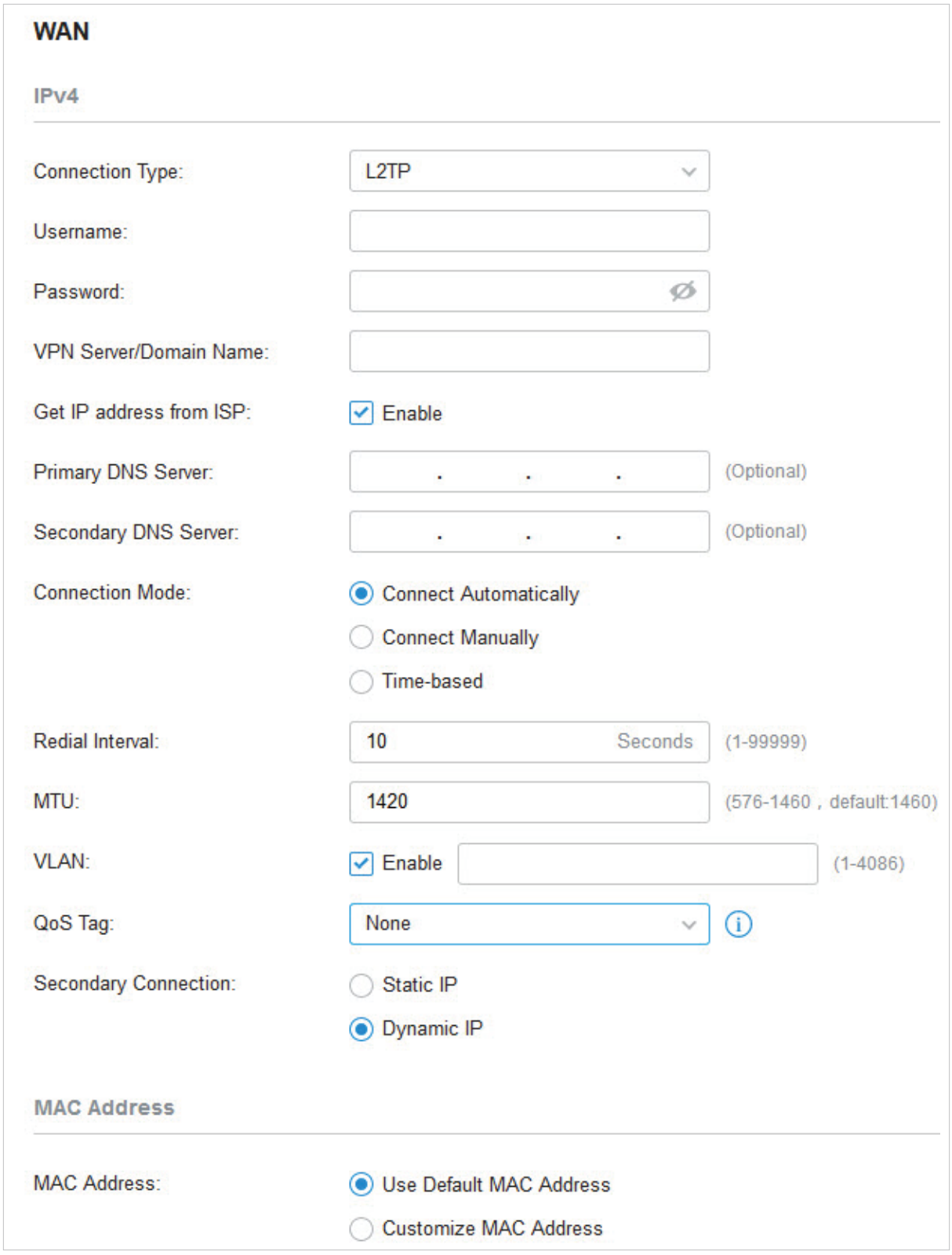
2. Click + Advanced Settings and configure the following parameters. Then click Apply.



Get IP address from ISP	With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection. With this option disabled, you need to specify the IP Address provided by your ISP.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
Connection Mode	Connect Automatically: The gateway activates the connection automatically when the connection is down. You need to specify the Redial Interval, which decides how often the gateway tries to redial after the connection is down. Connect Manually: You can manually activate or terminate the connection. Time-Based: During the specified period, the gateway will automatically activate the connection. You need to specify the Time Range when the connection is up.
Service Name	Keep it blank unless your ISP requires you to configure it.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is PPPoE, MTU can be set in the range of 576-1492 bytes. The default value is 1492.
VLAN	Add the WAN port to a VLAN and you need to specify the VLAN. Generally, you don't need to manually configure it unless required by your ISP.
QoS Tag	The QoS (Quality of Service) function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 1 to 7. None means the packet will be forwarded without any operation. QoS Tag is only available when VLAN is enabled.
Secondary Connection	Secondary connection is required by some ISPs. Select the connection type required by your ISP. None: Select this if the secondary connection is not required by your ISP. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection. You need to specify the IP Address and Subnet Mask provided by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.

- **L2TP**

Choose Connection Type as L2TP and configure the following parameters. Then click Apply.

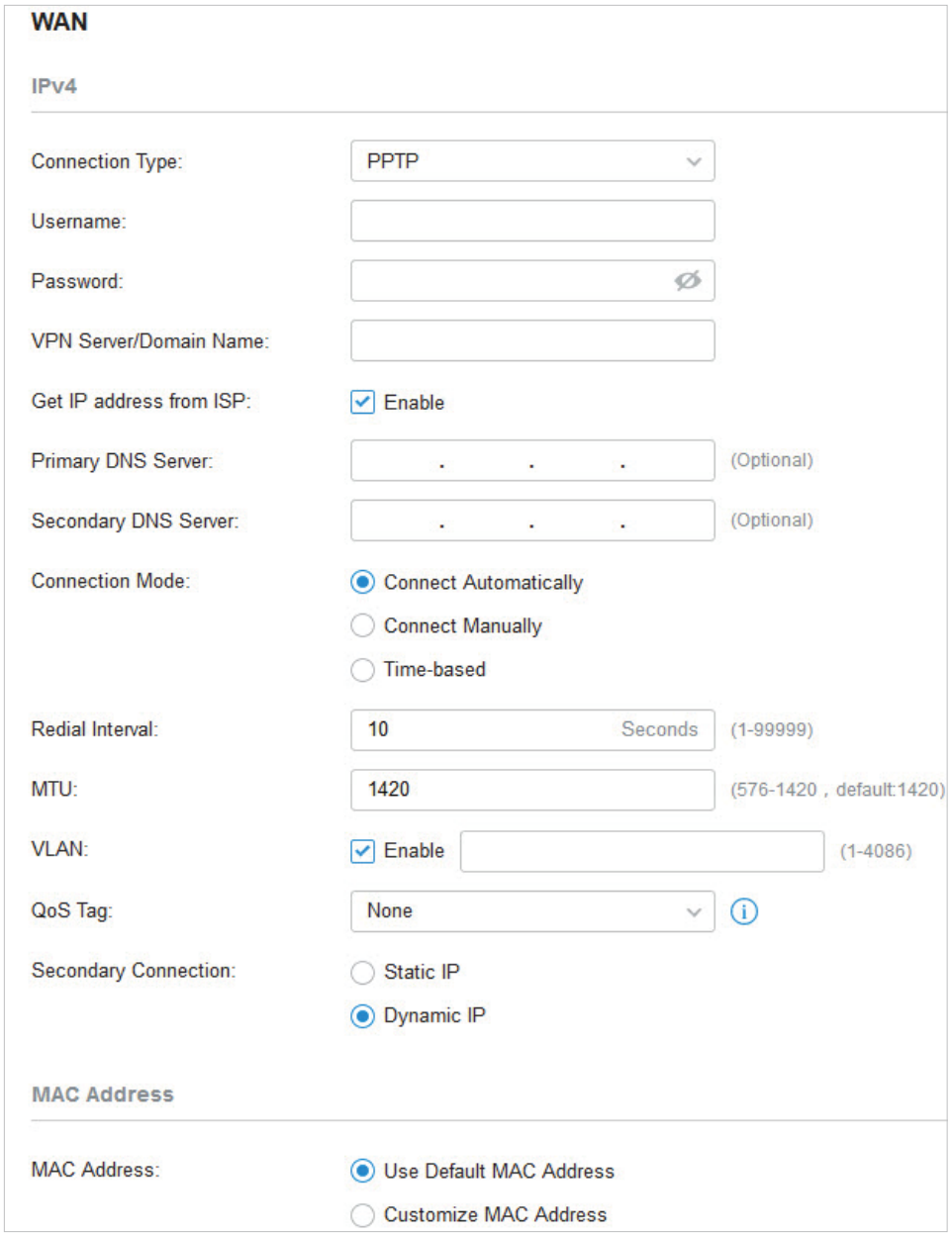


Username	Enter the L2TP username provided by your ISP.
Password	Enter the L2TP password provided by your ISP.

VPN Server / Domain Name	Enter the VPN Server/Domain Name provided by your ISP.
Get IP address from ISP	With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection. With this option disabled, you need to specify the IP address provided by your ISP.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
Connection Mode	Connect Automatically: The gateway activates the connection automatically when the connection is down. You need to specify the Redial Interval, which decides how often the gateway tries to redial after the connection is down. Connect Manually: You can manually activate or terminate the connection. Time-Based: During the specified period, the gateway will automatically activate the connection. You need to specify the Time Range when the connection is up.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is L2TP, MTU can be set in the range of 576-1460 bytes. The default value is 1460.
VLAN	Add the WAN port to a VLAN and you need to specify the VLAN. Generally, you don't need to manually configure it unless required by your ISP.
QoS Tag	The QoS (Quality of Service) function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 1 to 7. None means the packet will be forwarded without any operation. QoS Tag is only available when VLAN is enabled.
Secondary Connection	Select the connection type required by your ISP. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection. You need to specify the IP Address, Subnet Mask, Default Gateway (Optional), Primary DNS Server (Optional), and Secondary DNS Server (Optional) provided by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.
MAC Address	Use Default MAC Address: The WAN port uses the default MAC address to set up the internet connection. It's recommended to use the default MAC address unless required otherwise. Customize MAC Address: The WAN port uses a customized MAC address to set up the internet connection and you need to specify the MAC address. Typically, this is required when your ISP bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

PPTP

Choose Connection Type as PPTP and configure the following parameters. Then click Apply.



Username	Enter the PPTP username provided by your ISP.
Password	Enter the PPTP password provided by your ISP.
VPN Server / Domain Name	Enter the VPN Server/Domain Name provided by your ISP.
Get IP address from ISP	With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection. With this option disabled, you need to specify the IP address provided by your ISP.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.

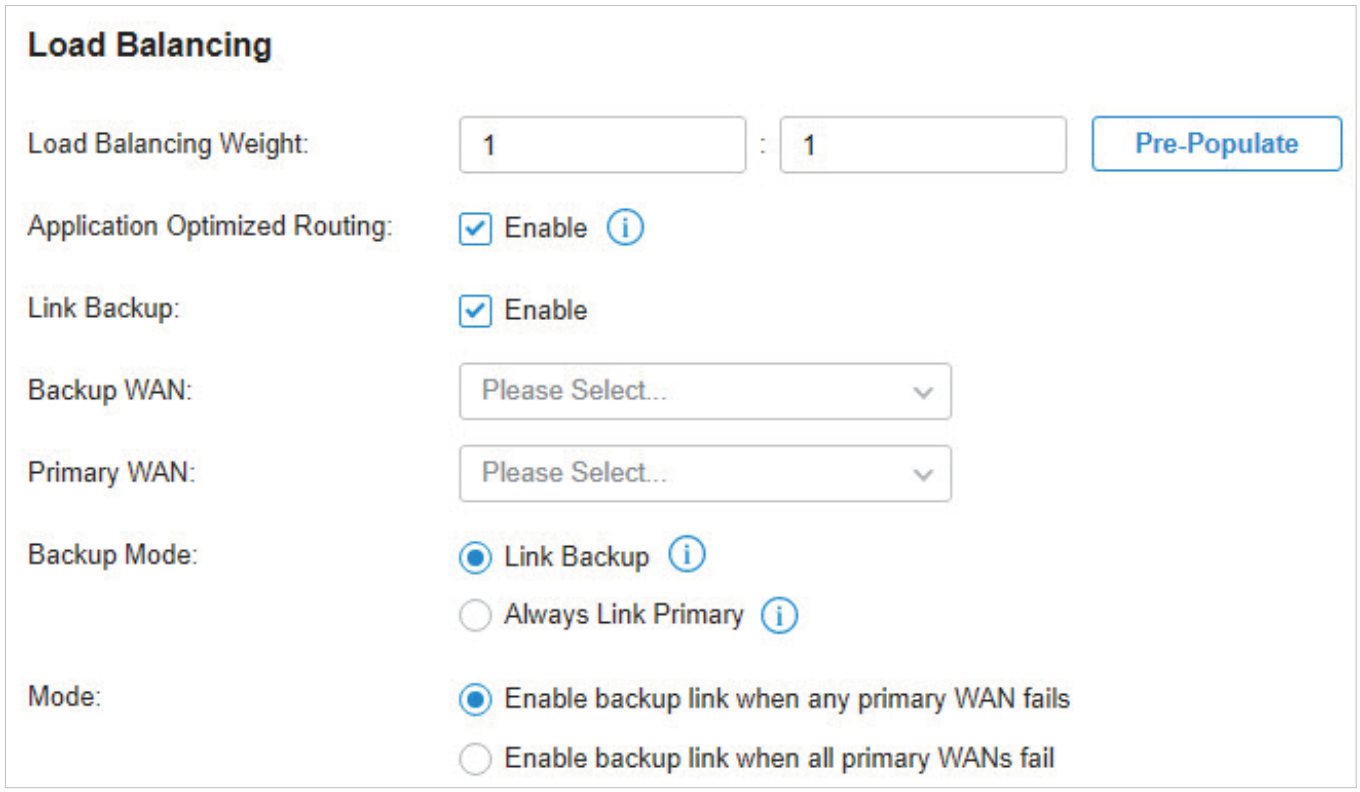
Connection Mode	Connect Automatically: The gateway activates the connection automatically when the connection is down. You need to specify the Redial Interval, which decides how often the gateway tries to redial after the connection is down. Connect Manually: You can manually activate or terminate the connection. Time-Based: During the specified period, the gateway will automatically activate the connection. You need to specify the Time Range when the connection is up.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When the connection type is PPTP, MTU can be set in the range of 576-1420 bytes. The default value is 1420.
VLAN	Add the WAN port to a VLAN and you need to specify the VLAN. Generally, you don't need to manually configure it unless required by your ISP.
QoS Tag	The QoS (Quality of Service) function helps to prioritize the internet traffic based on your needs. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 1 to 7. None means the packet will be forwarded without any operation. QoS Tag is only available when VLAN is enabled.
Secondary Connection	Select the connection type required by your ISP. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection. You need to specify the IP Address, Subnet Mask, Default Gateway (Optional), Primary DNS Server (Optional), and Secondary DNS Server (Optional) provided by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.
MAC Address	Use Default MAC Address: The WAN port uses the default MAC address to set up the internet connection. It's recommended to use the default MAC address unless required otherwise. Customize MAC Address: The WAN port uses a customized MAC address to set up the internet connection and you need to specify the MAC address. Typically, this is required when your ISP bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

Select WAN Mode > Configure WAN Connections > (Optional) Configure Load Balancing

Note:

Loading Balancing is only available when you configure more than one WAN port.

Go to Settings > Wired Networks > Internet to load the following page. In Load Balancing, configure the following parameters and click Apply.



Load Balancing Weight	Specify the ratio of network traffic that each WAN port carries. Alternatively, you can click Pre-Populate to test the speed of WAN ports and automatically fill in the appropriate ratio according to test result.
Application Optimized Routing	With Application Optimized Routing enabled, the router will consider the source IP address and destination IP address (or destination port) of the packets as a whole and record the WAN port they pass through. Then the packets with the same source IP address and destination IP address (or destination port) will be forwarded to the recorded WAN port. This feature ensures that multi-connected applications work properly.
Link Backup	With Link Backup enabled, the router will switch all the new sessions from dropped lines automatically to another to keep an always on-line network.
Backup WAN / Primary WAN	The backup WAN port backs up the traffic for the primary WAN ports under the specified condition.
Backup Mode	Link Backup: The system will switch all the new sessions from dropped line automatically to another to keep an always on-link network. Always Link Primary: Traffic is always forwarded through the primary WAN port unless it fails. The system will try to forward the traffic via the backup WAN port when it fails, and switch back when it recovers.
Mode	Select whether to enable backup link when any primary WAN fails or all primary WANs fail.

4. 3. 2 Configure LAN Networks

Overview

The **LAN** function allows you to configure wired internal network. Based on 802.1Q VLAN, Omada Controller provides a convenient and flexible way to separate and deploy the network. The network can be logically segmented by departments, application, or types of users, without regard to geographic locations.

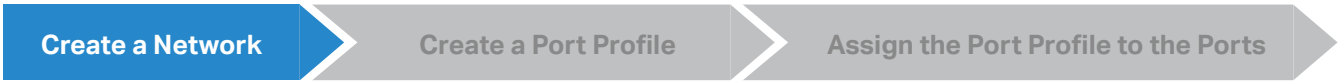
Configuration

To create a LAN, follow the guidelines:

1) Create a Network with specific purpose. For Layer 2 isolation, create a network as **VLAN.** To realize inter-VLAN routing, create a network as **Interface**, which is configured with a VLAN interface.

2) Create a port profile for the network. The profile defines how the packets in both ingress and egress directions are handled.

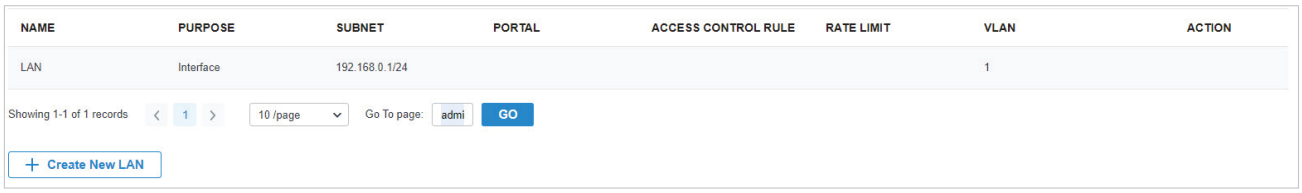
3) Assign the port profile to the desired ports of the switch to activate the LAN.



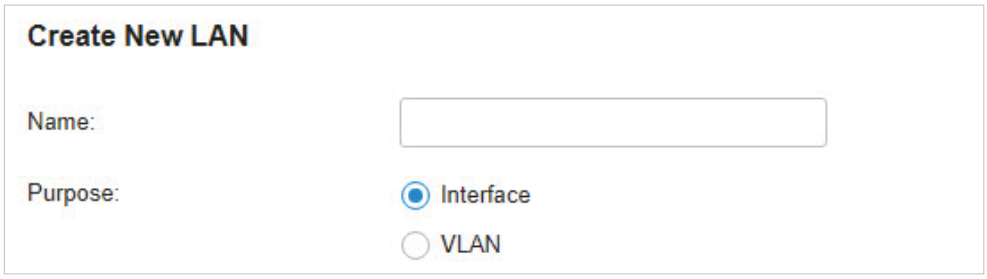
Note:

A default Network (default VLAN) named LAN is preconfigured as Interface and is associated with all LAN ports of the Omada Gateway and all switch ports. The VLAN ID of the default Network is 1. The default Network can be edited, but not deleted.

1. Go to Settings > Wired Networks > LAN > Networks to load the following page.



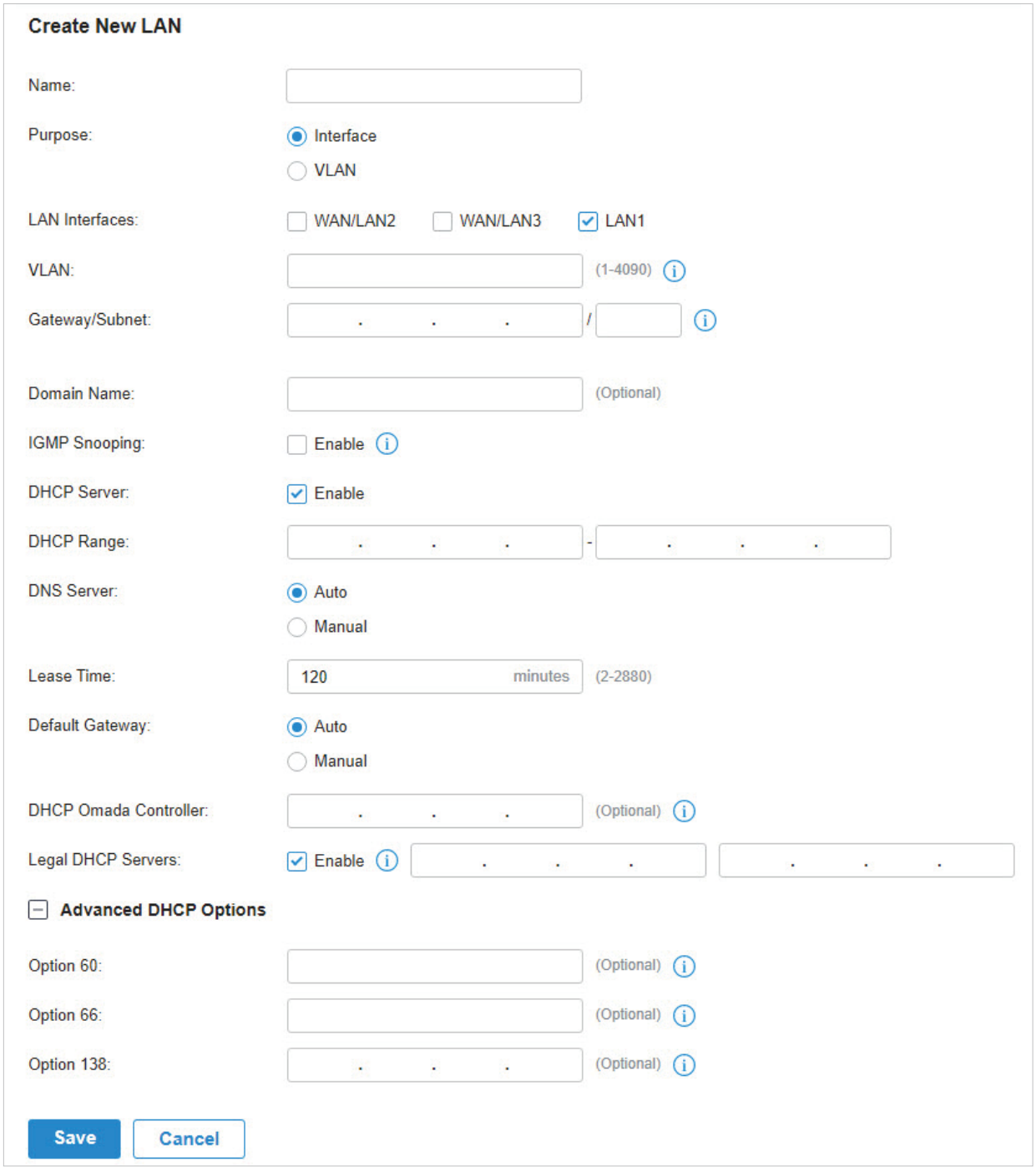
2. Click + Create New LAN to load the following page, enter a name to identify the network, and select the purpose for the network.



Purpose	Interface: Create the network with a Layer 3 interface, which is required for inter-VLAN routing. VLAN: Create the network as a Layer 2 VLAN.

3. Configure the parameters according to the purpose for the network.

■ Interface

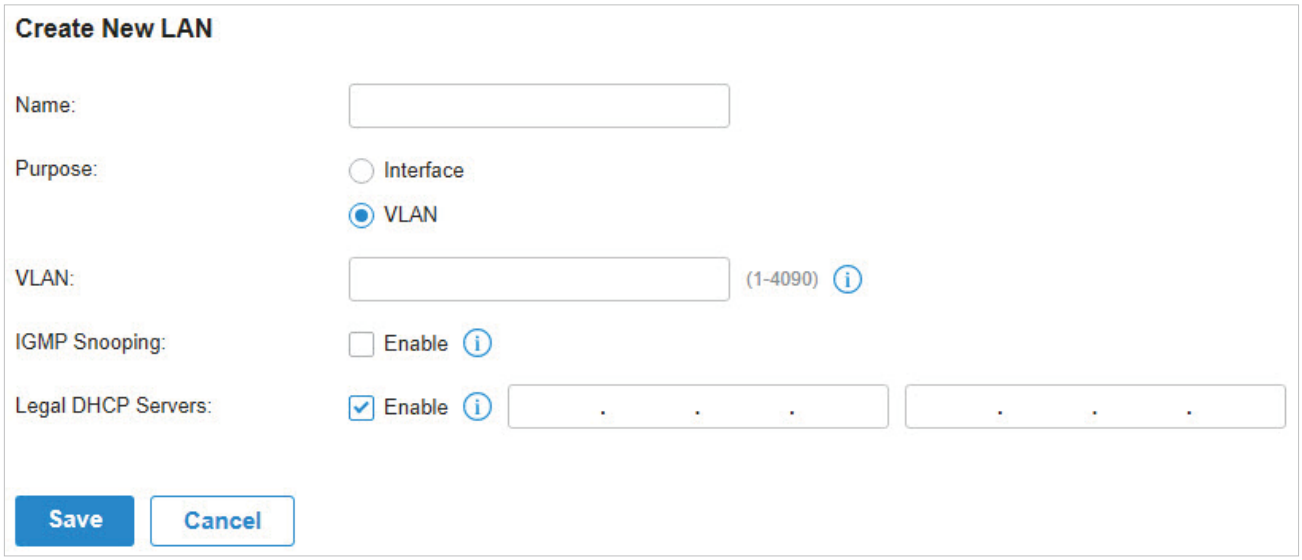


LAN Interface	Select the physical interfaces of the Omada Gateway that this network will be associated with.

VLAN	Enter a VLAN ID with the values between 1 and 4090. Each VLAN can be uniquely identified by VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.
Gateway/Subnet	Enter the IP address and subnet mask in the CIDR format. The CIDR Notation here includes the IP address and subnet mask of the default gateway. The summary of the information that you entered will show up below in realtime.
Domain Name	Enter the domain name.
IGMP Snooping	Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.
DHCP Server	Click the checkbox to allow the Omada Gateway to serve as the DHCP server for this network. A DHCP server assigns IP addresses, DNS server, default gateway, and other parameters to all devices in the network. Uncheck the box if there is already a DHCP server in the network.
DHCP Range	Enter the starting and ending IP addresses of the DHCP address pool in the fields provided. For quick operation, click the Update DHCP Range beside the Gateway/Subnet entry to get the IP address range populated automatically, and edit the range according to your needs.
DNS Server	Select a method to configure the DNS server for the network. Auto: The DHCP server automatically assigns DNS server for devices in the network. It uses the IP address specified in the Gateway/Subnet entry as the DNS server address. Manual: Specify DNS servers manually. Enter the IP address of a server in each DNS server field.
Lease TIme	Specify how long a client can use the IP address assigned from this address pool.
Default Gateway	Enter the IP address of the default gateway. Auto: The DHCP server automatically assigns default gateway for devices in the network. It uses the IP address specified in the Gateway/Subnet entry as the default gateway address. Manual: Specify default gateway manually. Enter the IP address of the default gateway in the field.
DHCP Omada Controller	Enter the IP address of the Omada Controller. The DHCP server uses this IP address as Option 138 in DHCP packets to tell clients where the controller is.
Legal DHCP Servers	Click the checkbox to specify legal DHCP servers for the network. With legal DHCP servers configured, Omada Gateways and Switches ensure that clients get IP addresses only from the DHCP servers specified here.
Option 60	Enter the value for DHCP Option 60. DHCP clients use this field to optionally identify the vendor type and configuration of a DHCP client. Mostly it is used in the scenario where the APs apply for different IP addresses from different servers according to the needs.
Option 66	Enter the value for DHCP Option 66. It specifies the TFTP server information and supports a single TFTP server IP address.

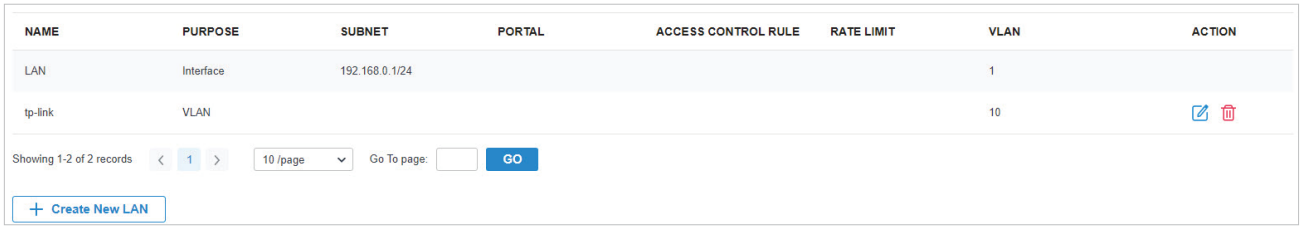
Option 138	Enter the value for DHCP Option 138. It is used in discovering the devices by the Omada controller.

- VLAN



VLAN	Enter a VLAN ID with the values between 1 and 4090. Each VLAN can be uniquely identified by VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.
IGMP Snooping	Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.
Legal DHCP Servers	Click the checkbox to specify legal DHCP servers for the network. With legal DHCP servers configured, Omada Gateways and Switches ensure that clients get IP addresses only from the DHCP servers specified here.

4. Click Save. The new LAN is added to the LAN list. You can click in the ACTION column to edit the LAN. You can click in the ACTION column to delete the LAN.



Create a Network | **Create a Port Profile** | Assign the Port Profile to the Ports

Note:

- Three default port profiles are preconfigured on the controller. They can be viewed, but not edited or deleted.

  All: In the All profile, all networks except the default network (LAN) are configured as Tagged Network, and the native network is the default network (LAN). This profile is assigned to all switch ports by default.

  Disable: In the Disable profile, no networks are configured as the native network, Tagged Networks and Untagged Networks. With this profile assigned to a port, the port does not belong to any VLAN.

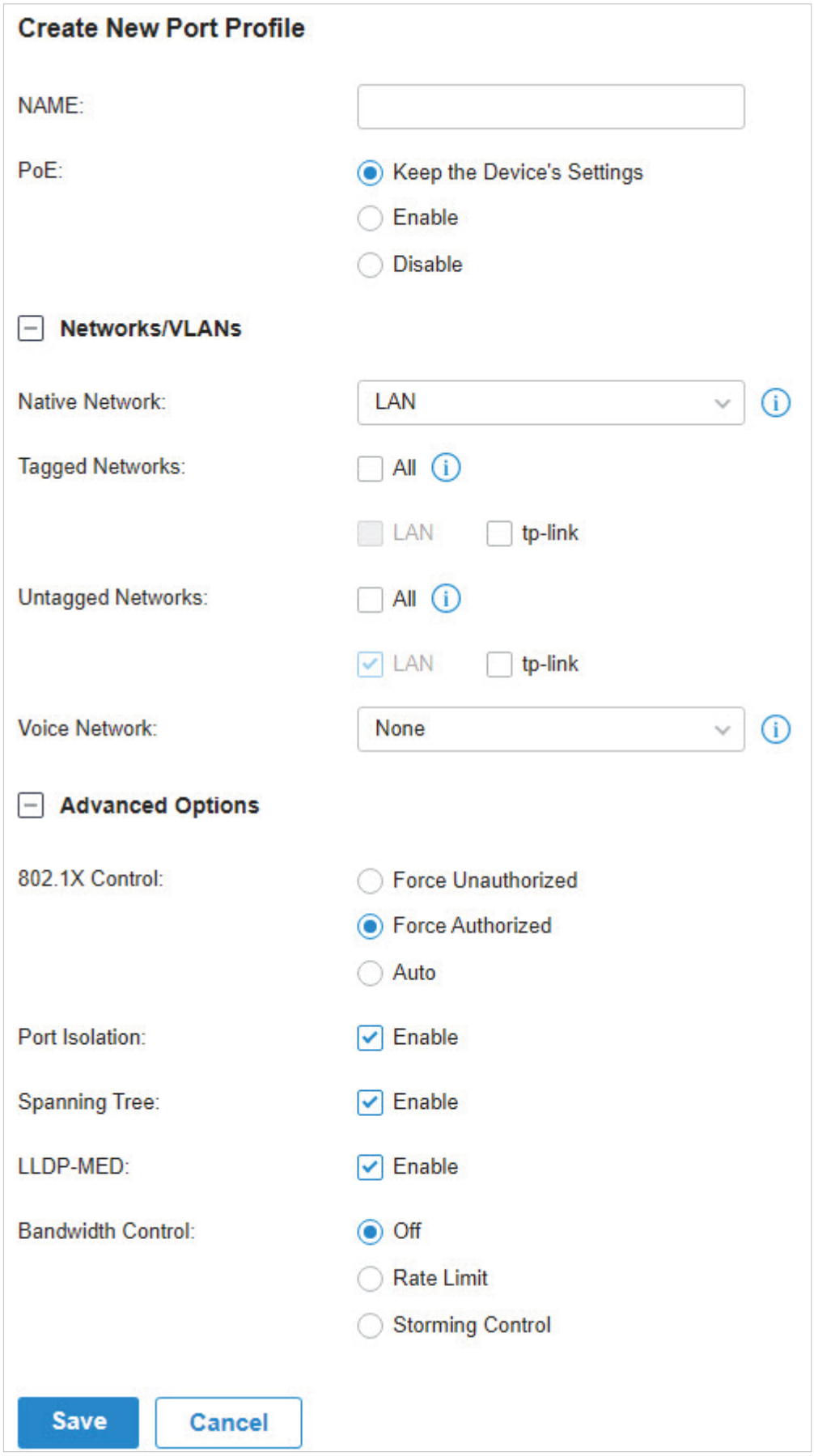
  LAN: In the LAN profile, the native network is the default network (LAN), and no networks are configured as Tagged Networks and Untagged Networks.

- When a network is created, the system will automatically create a profile with the same name and configure the network as the native network for the profile. In this profile, no networks are configured as Tagged Networks and Untagged Networks. The profile can be viewed, but not edited or deleted.

1. Go to Wired Networks > LAN > Profiles to load the following page.



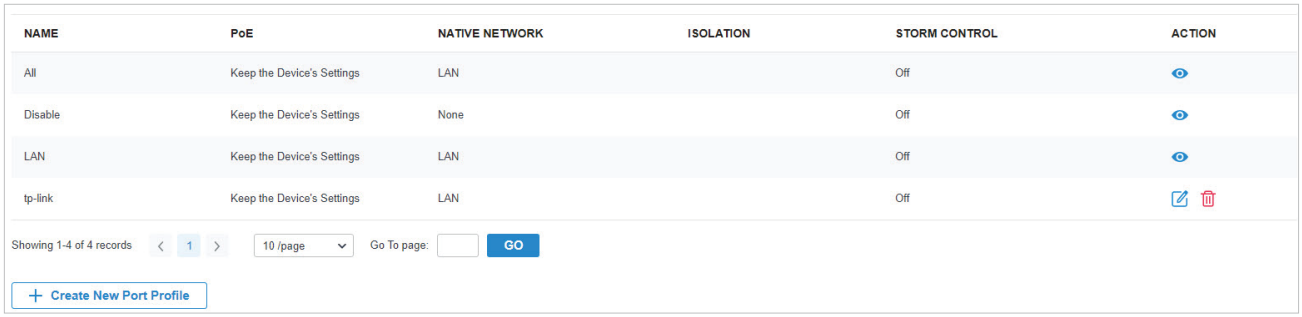
2. Click + Create New Port Profile to load the following page, and configure the following parameters.



Name	Enter a name to identify the port profile.
PoE	Select the PoE mode for the ports. Keep the Device's Settings: PoE keep enabled or disabled according to the switches' settings. By default, the switches enable PoE on all PoE ports. Enable: Enable PoE on PoE ports. Disable: Disable PoE on PoE ports.
Native Network	Select the native network from all networks. The native network determines the Port VLAN Identifier (PVID) for switch ports. When a port receives an untagged frame, the switch inserts a VLAN tag to the frame based on the PVID, and forwards the frame in the native network. Each physical switch port can have multiple networks attached, but only one of them can be native.
Tagged Networks	Select the Tagged Networks. Frames sent out of a Tagged Network are kept with VLAN tags. Usually networks that connect the switch to network devices like routers and other swithes, or VoIP devices like IP phones should be configured as Tagged Networks.
Untagged Networks	Select the Untagged Networks. Frames that sent out of an Untagged Network are stripped of VLAN tags. Usually networks that connect the switch to endpoint devices like computers should be configured as Untagged Networks. Note that the native network is untagged.
Voice Network	Select the network that connects VoIP devices like IP phones as the Voice Network. Omada Switches will prioritize the voice traffic by changing its 802.1p priority. To configure a network as Voice Network, configure it as Tagged Network first, and then enable LLDP-MED. Only tagged networks can be configured as Voice Network, and Voice Network will take effect with LLDP-MED enabled.
802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to **Settings** > **Authentication** > **802.1X**. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Spanning Tree	Click the checkbox to enable Spanning Tree. It helps to ensure that you do not create loops when you have redundant paths in the network. If you want to enable Spanning Tree for the switch, you also need to select the Spanning Tree protocol in the Device Config page. For details, refer to Configure and Monitor Switches.

LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP devices.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the set rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Broadcast Threshold	When Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	When Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
UL-Frame Threshold	When Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations..
Action	When Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.

3. Click Save. The new port profile is added to the profile list. You can click in the ACTION column to edit the port profile. You can click in the ACTION column to delete the port profile.

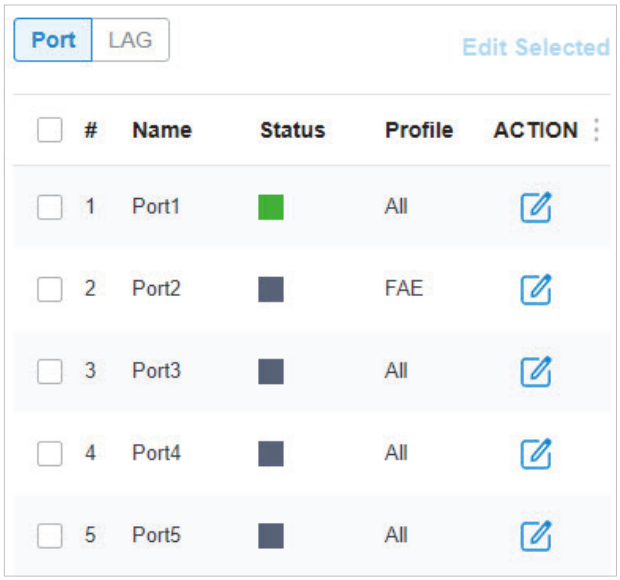


Create a Network > Create a Port Profile > **Assign the Port Profile to the Ports**

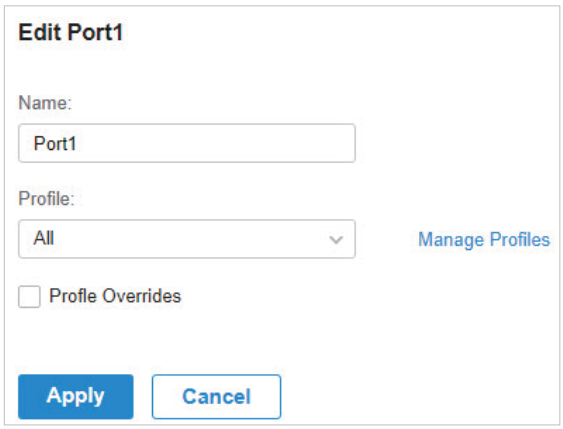
Note:

By default, there is a port profile named All, which is assigned to all switch ports by default. In the All profile, all networks except the default network (LAN) are configured as Tagged Network, and the native network is the default network (LAN).

1. Go to Settings > Wired Networks > LAN > Networks, and click beside the switch in the devices list to reveal the Properties window. Go to Ports, you can either click in the Action column to assign the port profile to a single port, or select the desired ports and click Edit Selected on the top to assign the port profile to multiple ports in batch.



2. Select the profile from the drop-down list to assign the port profile to the desired ports of the switch. You can enable profile overrides to customize the settings for the ports, and all the configuration here overrides the port profile. For details, refer to Configure and Monitor Omada Managed Devices.



4. 4 Configure Wireless Networks

Wireless networks enable your wireless clients to access the internet. Once you set up a wireless network, your EAPs typically broadcast the network name (SSID) in the air, through which your wireless clients connect to the wireless network and access the internet.

A WLAN group is a combination of wireless networks. Configure each group so that you can flexibly apply these groups of wireless networks to different EAPs according to your needs.

After setting up basic wireless networks, you can further configure WLAN Schedule, 802.11 Rate Control, and MAC Filter among other advanced settings.

4. 4. 1 Set Up Basic Wireless Networks

Configuration

To create, configure and apply wireless networks, follow these steps:

4) Create a WLAN group.

5) Create Wireless Networks

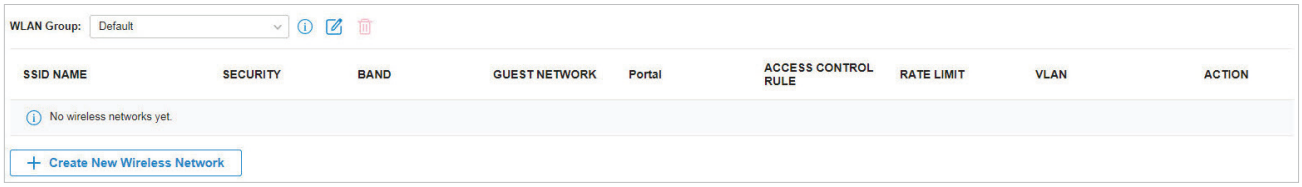
6) Apply the WLAN group to your EAPs



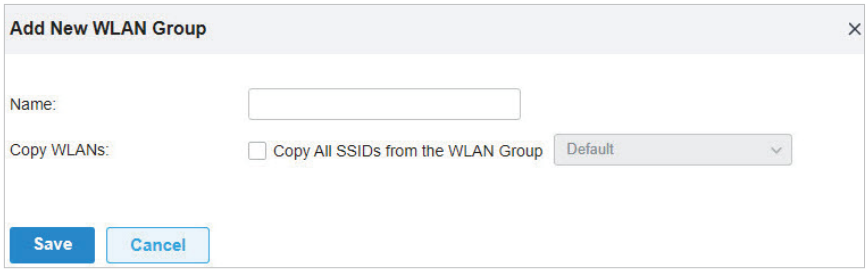
Note:

By default, there is a WLAN group named Default, which is applied to all EAPs. If you simply want to configure wireless networks for the default WLAN group and apply it to all your EAPs, skip this step.

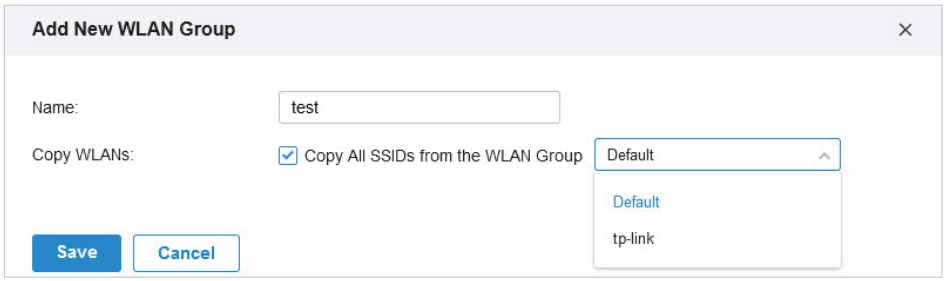
3. Go to Settings > Wireless Networks to load the following page.



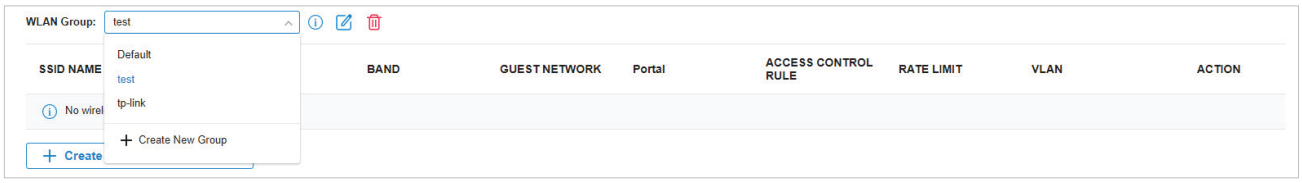
4. Select + Create New Group from the drop-down list of WLAN Group to load the following page. Enter a name to identify the WLAN group.



5. (Optional) If you want to create a new WLAN group based on an existing one, check Copy All SSIDs from the WLAN Group and select the desired WLAN group. Then you can further configure wireless networks based on current settings.

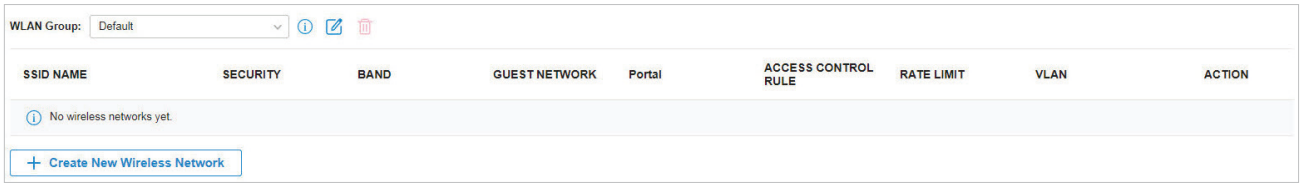


6. Click Save. The new WLAN Group is added to the WLAN Group list. You can select a WLAN Group from the list to further create and configure its wireless networks. You can click to edit the name of the WLAN Group. You can click to delete the WLAN Group.

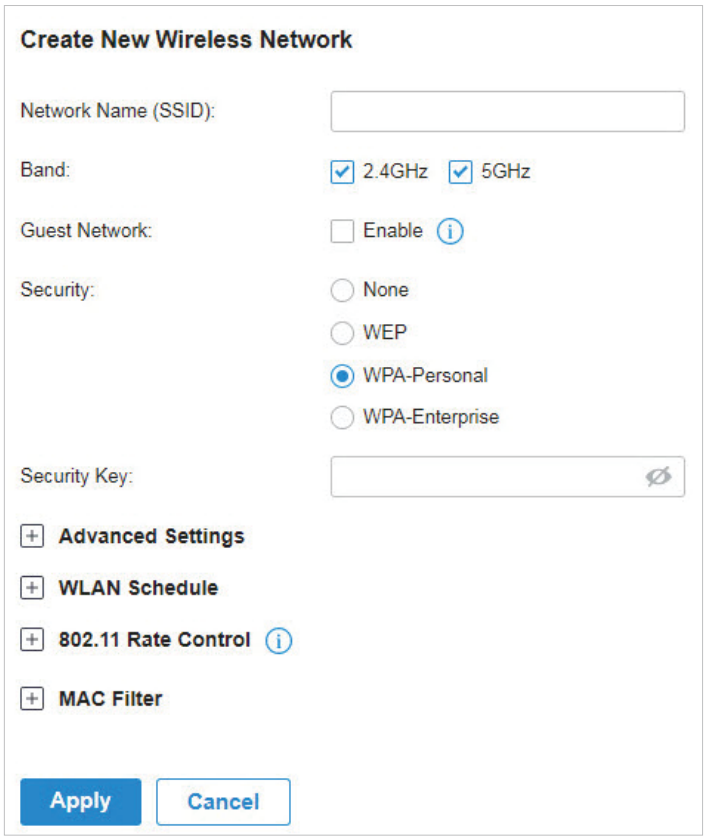


Create a WLAN Group → Create Wireless Networks → Apply the WLAN Group

1. Select the WLAN group for which you want to configure wireless networks from the drop-down list of WLAN Group.



2. Click + Create New Wireless Network to load the following page. Configure the basic parameters for the network.



Network Name (SSID)	Enter the network name (SSID) to identify the wireless network. The users of wireless clients choose to connect to the wireless network according to the SSID, which appears on the WLAN settings page of wireless clients.
Band	Enable 2.4 GHz and/or 5 GHz radio band for the wireless network.
Guest Network	With Guest Network enabled, all the clients connecting to the SSID are blocked from reaching any private IP subnet.

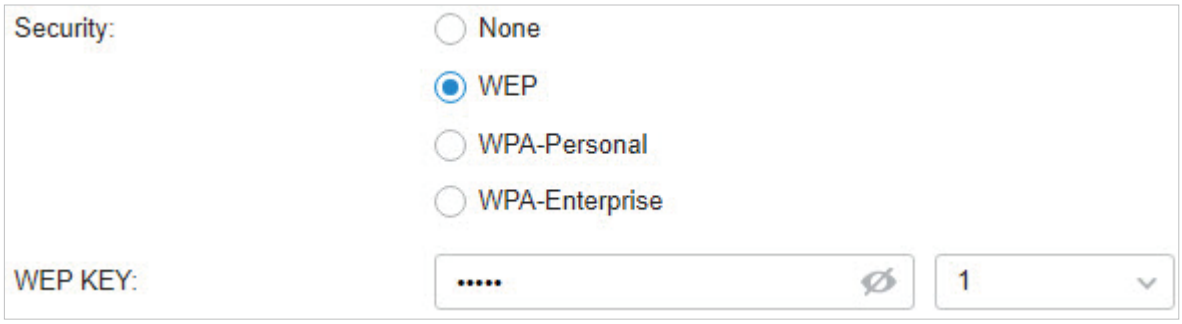
3. Select the security strategy for the wireless network.

- **None**

  With None selected, the hosts can access the wireless network without authentication, which is applicable to lower security requirements.

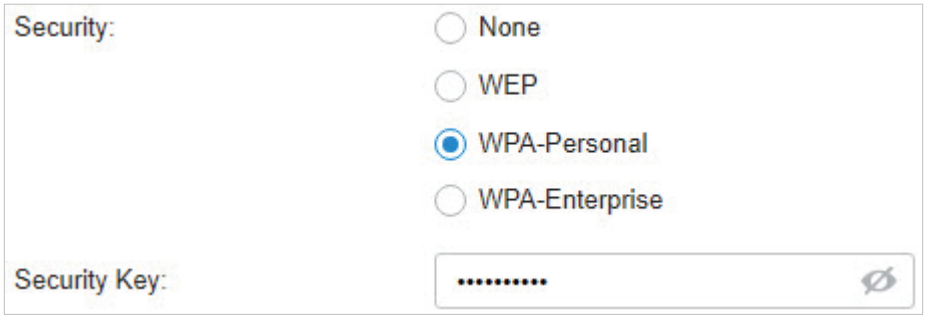
- **WEP**

  Traffic is encrypted with a WEP Key, which you need to specify. WEP is not recommended because it's insecure.



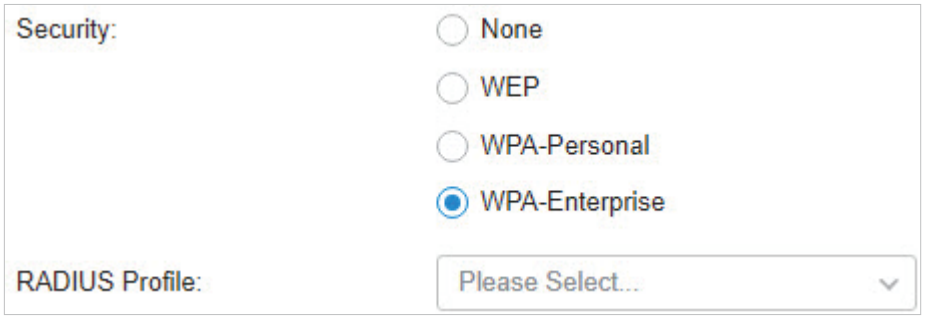
- **WPA-Personal**

  Traffic is encrypted with a Security Key, which you need to specify. WPA-Personal is more secure than WEP.

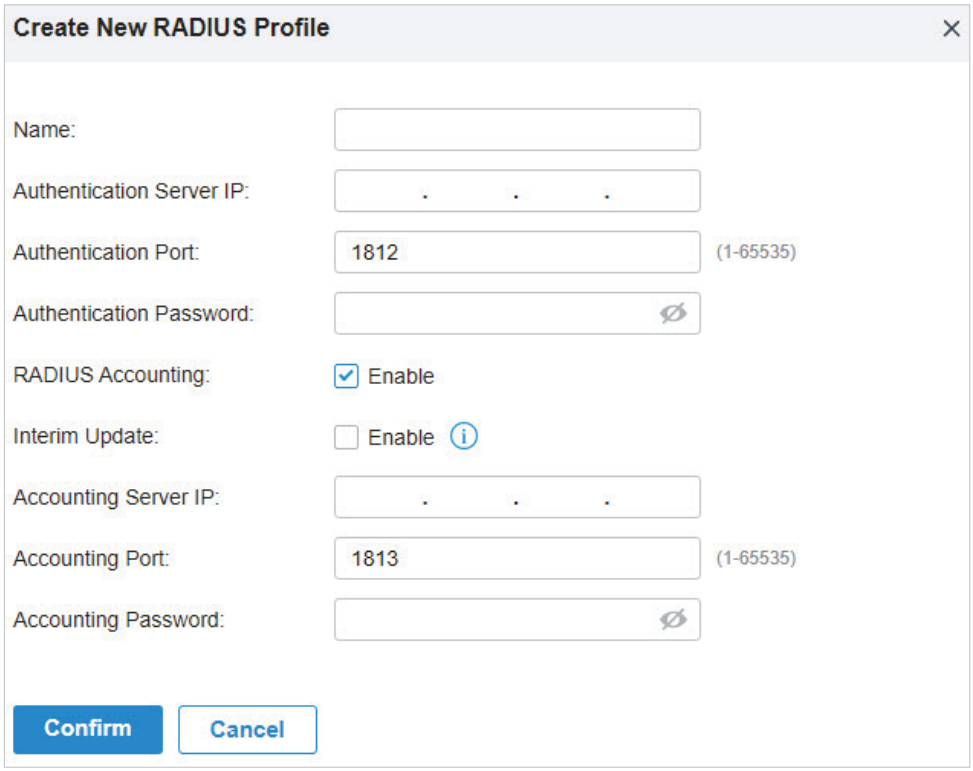


- **WPA-Enterprise**

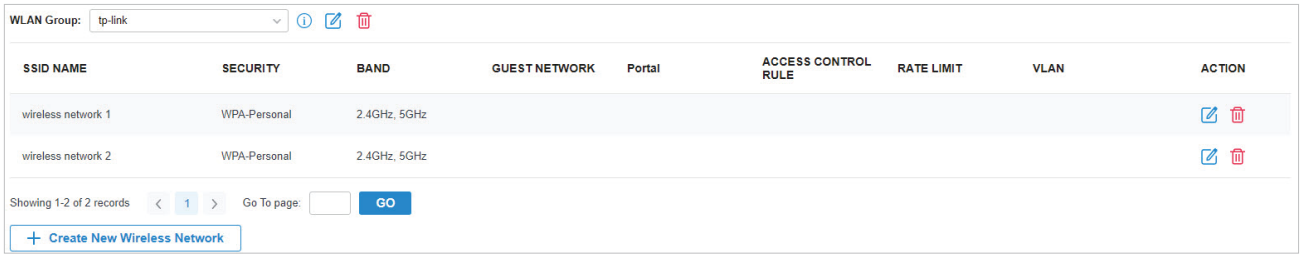
  WPA-Enterprise requires an authentication server to authenticate wireless clients, and probably an accounting server to record the traffic statistics.



Select a RADIUS Profile, which records the settings of the authentication server and accounting server. You can create a RADIUS Profile by clicking + Create New Radius Profile from the drop-down list of RADIUS Profile. For details, refer to Authentication.



4. (Optional) You can also configure Advanced Settings, WLAN Schedule, 802.11 Rate Control, and MAC Filter according to your needs. Related topics are covered later in this chapter.
5. Click Apply. The new wireless network is added to the wireless network list under the WLAN group. You can click in the ACTION column to edit the wireless network. You can click in the ACTION column to delete the wireless network.



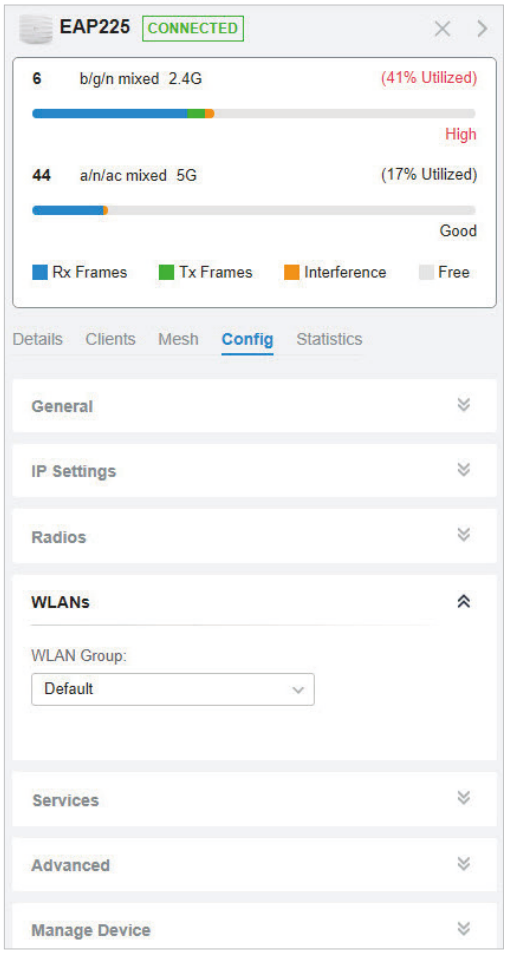
Create a WLAN Group > Create Wireless Networks > **Apply the WLAN Group**

Note:

By default, there is a WLAN group named Default, which is applied to all EAPs. If you simply want to configure wireless networks for the default WLAN group and apply it to all your EAPs, skip this step.

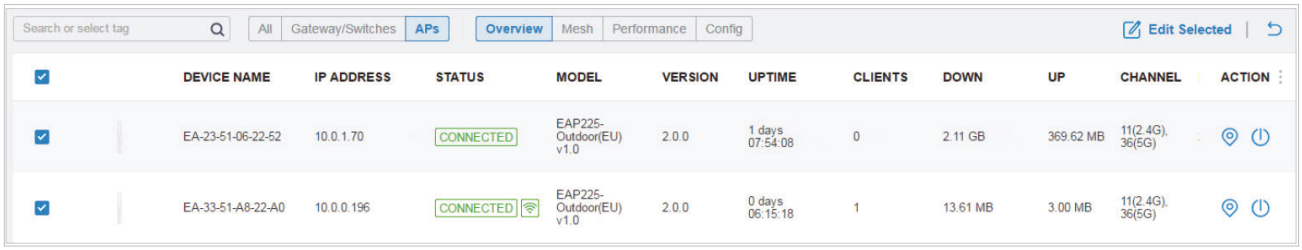
Apply to a Single EAP

Go to Devices, select the EAP which you want to apply the WLAN group to. In the Properties window, go to Config > WLANs, select the WLAN group which you want to apply to the EAP.

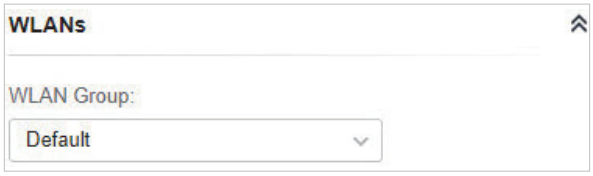


Apply to EAPs in batch

1. Go to Devices, select the APs tab, click , select Batch Config, check the boxes of EAPs which you want to apply the WLAN group to, and click Edit Selected.

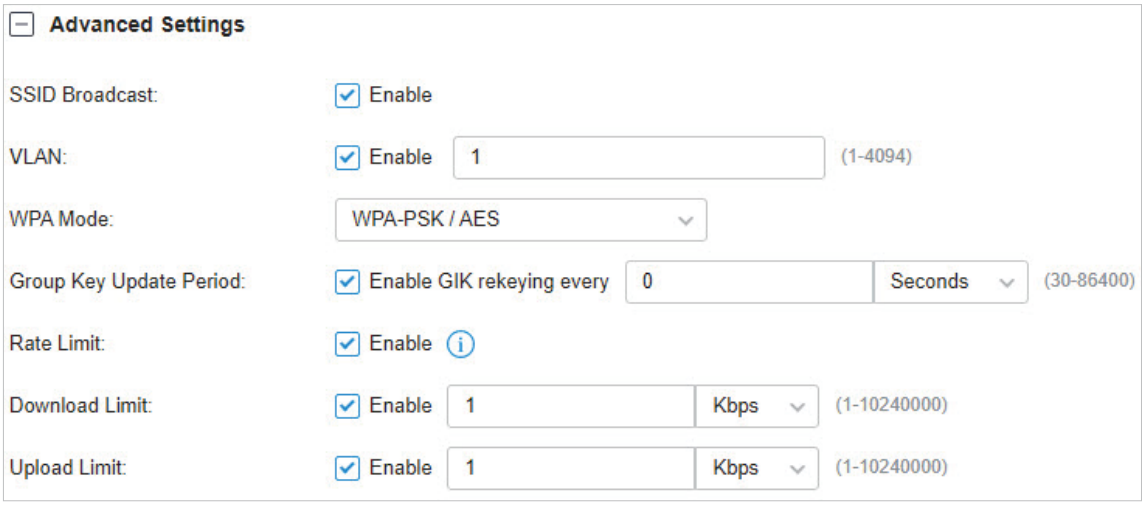


2. In the Properties window, go to Config > WLANs, select the WLAN group which you want to apply to the EAP.



4. 4. 2 Advanced Settings

Go to Settings > Wireless Networks, click in the ACTION column of the wireless network which you want to configure, and click + Advanced Settings to load the following page. Configure the parameters and click Apply.



SSID Broadcast	With SSID Broadcast enabled, EAPs broadcast the SSID (network name) in the air so that wireless clients can connect to the wireless network, which is identified by the SSID. With SSID Broadcast disabled, users of wireless clients must enter the SSID manually to connect to the wireless network.
VLAN	To set a wireless VLAN for the wireless network, enable this option and set a VLAN ID from 1 to 4094. With this option enabled, traffic in different wireless networks is marked with different VLAN tags according to the configured VLAN IDs. Then the EAPs work together with the switches which also support 802.1Q VLAN, to distribute the traffic to different VLANs according to the VLAN tags. As a result, wireless clients in different VLANs cannot directly communicate with each other.

WEP Mode	If you select WEP as the security strategy, you can select the WEP Mode including the WEP authentication type, the WEP key format, and the WEP key length. Select the WEP authentication type. Open System: Wireless clients can pass the authentication and connect to the wireless network without any password. However, the correct password is required for data transmission. Shared Key: The correct password is required for wireless clients to pass the authentication, connect to the wireless network, and transmit data. Auto: EAPs automatically decide whether to use Open System or Shared Key in the authentication process. Select the WEP key format. ASCII: ASCII format stands for any combination of keyboard characters of the specified length. Hexadecimal: Hexadecimal format stands for any combination of hexadecimal digits (0-9, A-F) with the specified length. Select the WEP key length. 64Bit: The WEP key is 10 hexadecimal digits or 5 ASCII characters. 128Bit: The WEP key is 26 hexadecimal digits or 13 ASCII characters. 152Bit: The WEP key is 32 hexadecimal digits or 16 ASCII characters.
WPA Mode	If you select WPA-Personal or WPA-Enterprise as the security strategy, you can select the WPA Mode including the version of WPA, and the encryption type. Select the version of WPA according to your needs. Select the encryption type. Some encryption type is only available under certain circumstances. TKIP: TKIP stands for Temporal Key Integrity Protocol. AES: AES stands for Advanced Encryption Standard. We recommend that you select AES as the encryption type for it is more secure than TKIP. Auto: EAPs automatically decide whether to use TKIP or AES in the authentication process.
Group Key Update Period	If you select WPA-Personal or WPA-Enterprise as the security strategy, you can specify whether and how often the security key changes. If you want the security key to change periodically, enable GIK rekeying and specify the time period.
Rate Limit	You can limit the download and upload rate of each client to balance bandwidth usage. Download Limit: Set the download rate for each client to receive the traffic. Upload Limit: Set the upload rate for each client to transmit the traffic.

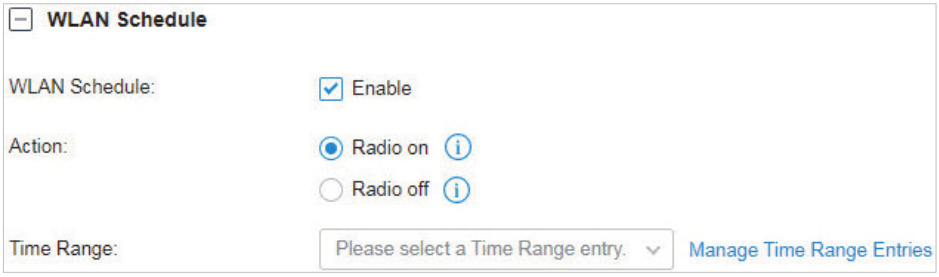
4. 4. 3 WLAN Schedule

Overview

WLAN Schedule can turn on or off your wireless network in the specific time period as you desire.

Configuration

Go to Settings > Wireless Networks, click in the ACTION column of the wireless network which you want to configure, and click + WLAN Schedule to load the following page. Enable WLAN schedule and configure the parameters .Then click Apply.



Action	Radio On: Turn on your wireless network within the time range you set, and turn it off beyond the time range. Radio Off: Turn off your wireless network within the time range you set, and turn it on beyond the time range.
Time Range	Select the Time Range for the action to take effect. You can create a Time Range entry by clicking + Create New Time Range Entry from the drop-down list of Time Range. For details, refer to Create Profiles.

4. 4. 4 802.11 Rate Control

Overview

Note:

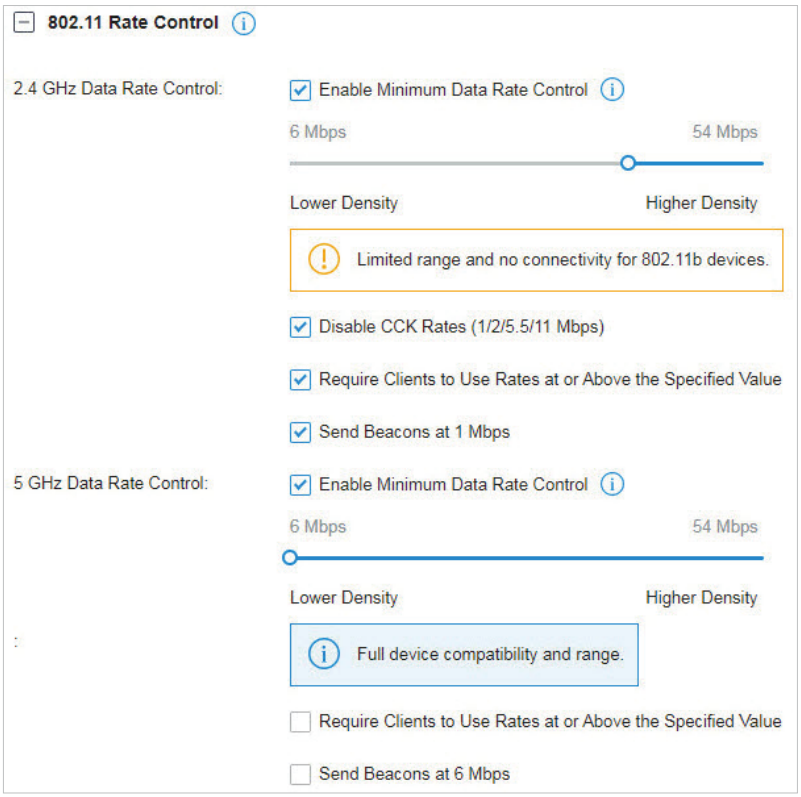
802.11 Rate Control is only available for certain devices.

802.11 Rate Control can improve performance for higher-density networks by disabling lower bit rates and only allowing the higher. However, 802.11 Rate Control might make some legacy devices incompatible with your networks, and limit the range of your wireless networks.

Configuration

Go to Settings > Wireless Networks, click in the ACTION column of the wireless network which you want to configure, and click + 802.11 Rate Control to load the following page. Select 2.4 GHz and/or 5

GHz band to enable minimum data rate control according to your needs, move the slider to determine what bit rates your wireless network allows, and configure the parameters. Then click Apply.



Disable CCK Rates (1/2/5.5/11 Mbps)	Select whether to disable CCK (Complementary Code Keying), the modulation scheme which works with 802.11b devices. Disable CCK Rates (1/2/5.5/11 Mbps) is only available for 2.4 GHz band.
Require Clients to Use Rates at or Above the Specified Value	Select whether or not to require clients to use rates at or above the value that the slider indicates.
Send Beacons at 1 Mbps/6 Mbps	Select whether or not to send Beacons at the minimum rate of 1Mbps for 2.4 GHz band or 6Mbps for 5 GHz band.

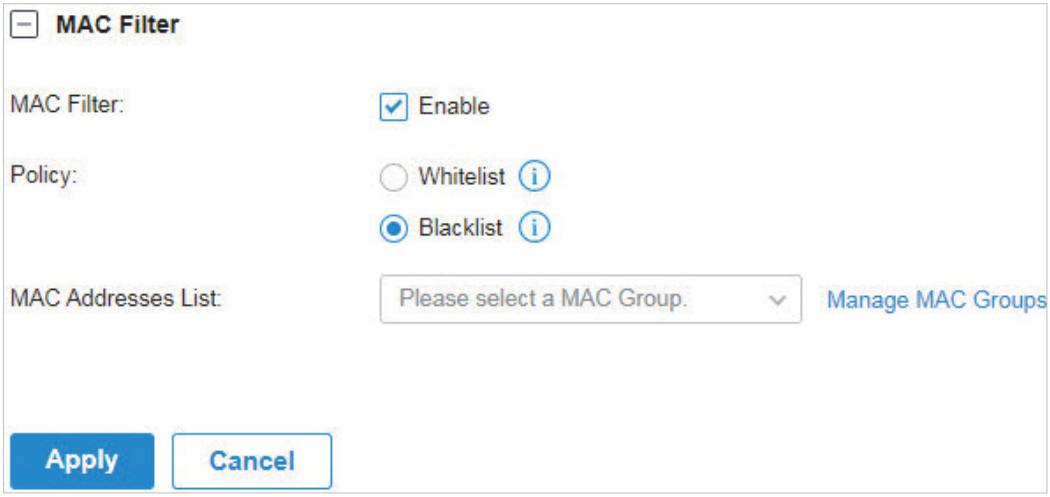
4. 4. 5 MAC Filter

Overview

MAC Filter allows or blocks connections from wireless clients of specific MAC addresses.

Configuration

Go to Settings > Wireless Networks, click in the ACTION column of the wireless network which you want to configure, and click + MAC Filter to load the following page. Enable MAC Filter and configure the parameters .Then click Apply.



Policy	Whitelist: Allow the connection of the clients whose MAC addresses are in the specified MAC Address List, while blocking others. Blacklist: Block the connection of the clients whose MAC address are in the specified MAC Addresses List, while allowing others.
MAC Address List	Select the MAC Group which you want to allow or block according to the policy. You can create new MAC group by clicking + Create New MAC Group from the drop-down list of MAC Address List. For details, refer to Create Profiles.

4. 5 Network Security

Network Security is a portfolio of features designed to improve the usability and ensure the safety of your network and data. Network security services include ACL, URL Filtering, and Attack Defense, which implement policies and controls on multiple layers of defenses in the network.

4. 5. 1 ACL

Overview

ACL (Access Control List) allows a network administrator to create rules to restrict access to network resources. ACL rules filter traffic based on specified criteria such as source IP addresses, destination IP addresses, and port numbers, and determine whether to forward the matched packets. These rules can be applied to specific clients or groups whose traffic passes through the gateway, switches and EAPs.

The system filters traffic against the rules in the list sequentially. The first match determines whether the packet is accepted or dropped, and other rules are not checked after the first match. Therefore, the order of the rules is critical. By default, the rules are prioritized by their created time. The rule created earlier is checked for a match with higher priority. To reorder the rules, select a rule and drag it to a new position. If no rules match, the device forwards the packet because of an implicit Permit All clause.

The system provides three types of ACL:

- **Gateway ACL**

  After Gateway ACLs are configured on the controller, they can be applied to the gateway to control traffic which is sourced from LAN ports and forwarded to the WAN ports.

  You can set the Network, IP address, port number of a packet as packet-filtering criteria in the rule.

- **Switch ACL**

  After Switch ACLs are configured on the controller, they can be applied to the switch to control inbound and outbound traffic through switch ports.

  You can set the Network, IP address, port number and MAC address of a packet as packet-filtering criteria in the rule.

- **EAP ACL**

  After EAP ACLs are configured on the controller, they can be applied to the EAPs to control traffic in wireless networks.

  You can set the Network, IP address, port number and SSID of a packet as packet-filtering criteria in the rule.

Configuration

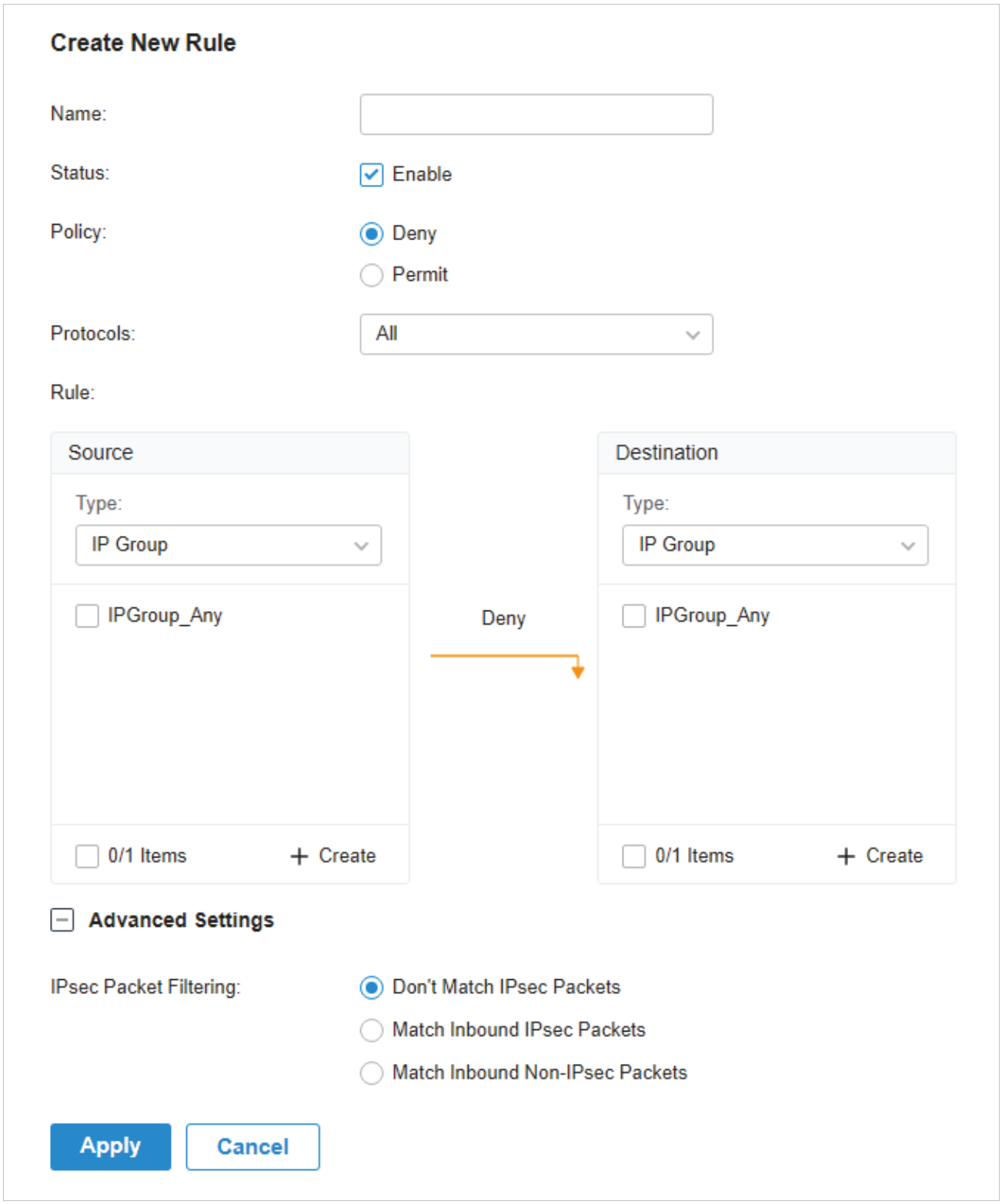
To complete the ACL configuration, follow these steps:

7) Create an ACL with the specified type.

8) Define packet-filtering criteria of the rule, including protocols, source, and destination, and determine whether to forward the matched packets.

■ **Configuring Gateway ACL**

3. Go to Settings > Network Security > ACL. On Gateway ACL tab, click + Create New Rule to load the following page.



4. Define packet-filtering criteria of the rule, including protocols, source, and destination, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the ACL.
Status	Click the checkbox to enable the ACL.
Policy	Select the action to be taken when a packet matches the rule. Permit: Forward the matched packet. Deny: Discard the matched packet.
Protocols	Select one or more protocol types to which the rule applies from the drop-down list. The default is All, indicating that packets of all protocols will be matched. When you select one of TCP and UDP or both of them, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.

From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The gateway will examine whether the packets are sourced from the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the source IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the source IP address and port number of the packet are in the IP-Port Group.

From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

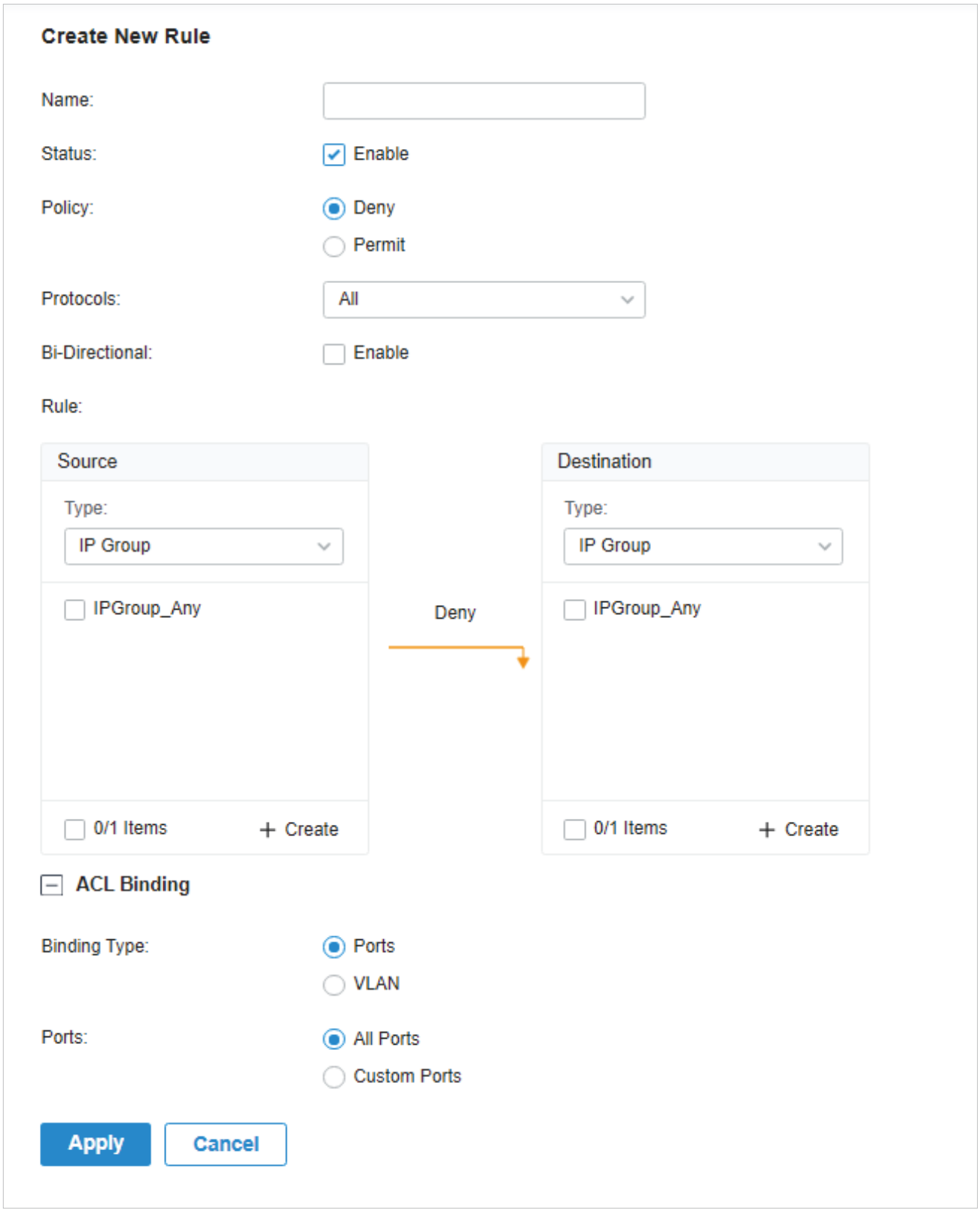
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the destination IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the destination IP address and port number of the packet are in the IP-Port Group.

You can determine whether the ACL is applied to the packets that are encrypted with IPsec protocols in the Advanced Settings.

IPsec packet filtering	Select whether to match IPsec packets. Three options are available: Don't Match IPsec Packets, Match Inbound IPsec Packets, Match Inbound Non-IPsec Packets.

Configuring Switch ACL

1. Go to Settings > Network Security > ACL. Under the Switch ACL tab, click + Create New Rule to load the following page.



2. Define packet-filtering criteria of the rule, including protocols, source, and destination, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters.

Name	Enter a name to identify the ACL.
Status	Click the checkbox to enable the ACL.
Policy	Select the action to be taken when a packet matches the rule. Permit: Forward the matched packet. Deny: Discard the matched packet.
Protocols	Select one or more protocol types to which the rule applies from the drop-down list. The default is All, indicating that packets of all protocols will be matched. When you select one of TCP and UDP or both of them, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.
Bi-Directional	Click the checkbox to enable the switch to create another symmetric ACL with the name "xxx_reverse", where "xxx" is the name of the current ACL. The two ACLs target at packets with the opposite direction of each other.

From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The switch will examine whether the packets are sourced from the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address and port number of the packet are in the IP-Port Group.
MAC Group	Select the MAC Group you have created. If no MAC Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source MAC address of the packet is in the MAC Group.

From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

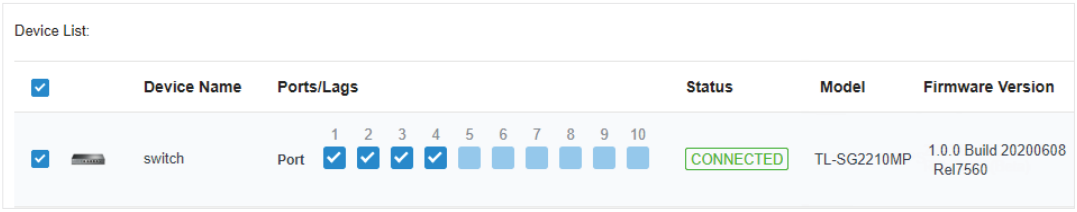
Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The switch will examine whether the packets are forwarded to the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address of the packet is in the IP Group.

IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address and port number of the packet are in the IP-Port Group.
MAC Group	Select the MAC Group you have created. If no MAC Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination MAC address of the packet is in the MAC Group.

3. Bind the switch ACL to a switch port or a VLAN and click Apply. Note that a switch ACL takes effect only after it is bound to a port or VLAN.

Binding Type Specify whether to bind the ACL to ports or a VLAN.

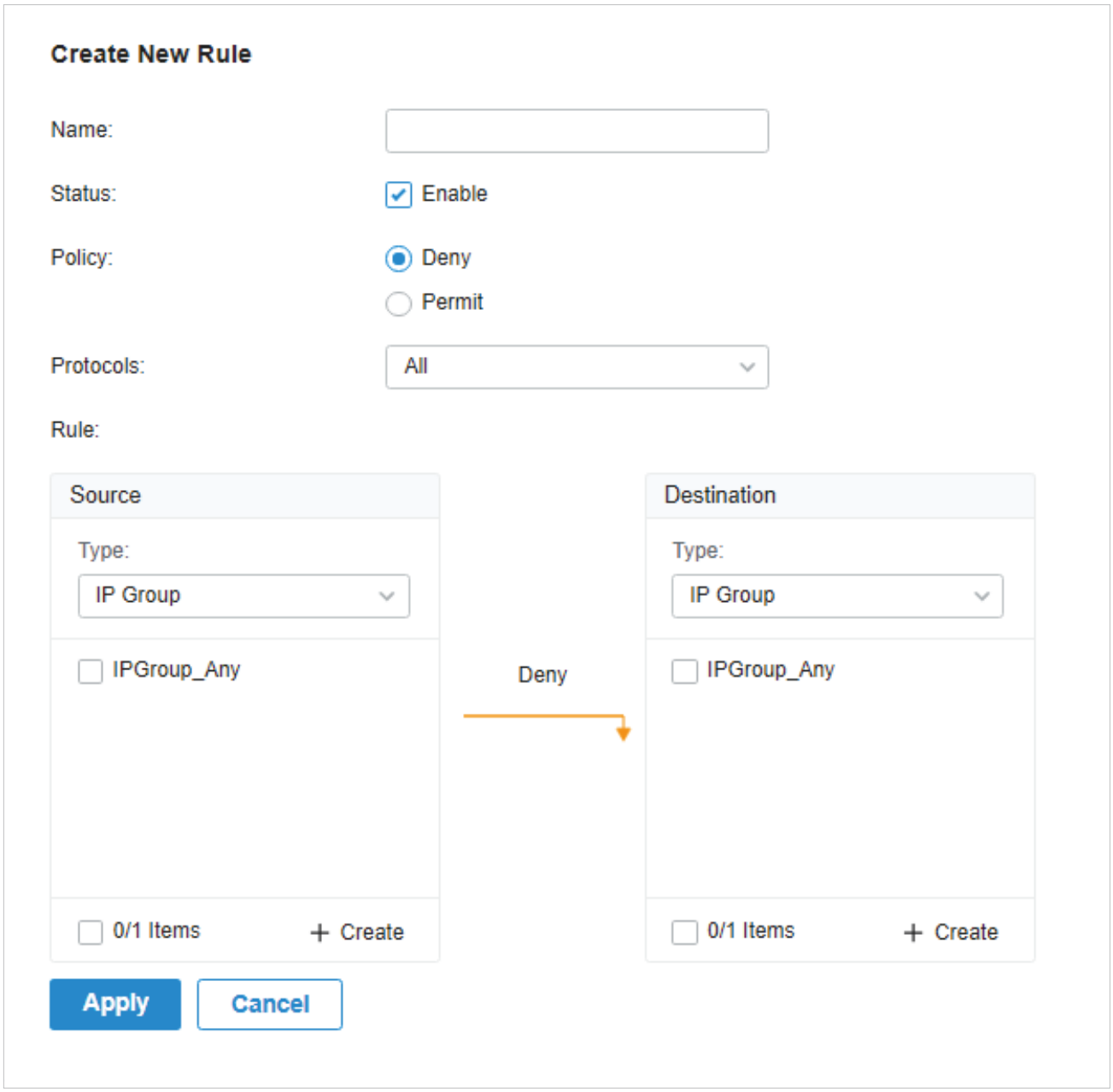
Ports: Select All ports or Custom ports as the interfaces to be bound with the ACL. With All ports selected, the rule is applied to all ports of the switch. With Custom ports selected, the rule is applied to the selected ports of the switch. Click the ports from the Device List to select the binding ports.



VLAN: Select a VLAN from the drop-down list as the interface to be bound with the ACL. If no VLANs have been created, you can select the default VLAN 1 (LAN), or go to Settings > Wired Networks > LAN to create one.

Configuring EAP ACL

1. Go to Settings > Network Security > ACL. Under the EAP ACL tab, click + Create New Rule to load the following page.



2. Define packet-filtering criteria of the rule, including protocols, source, and destination, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the ACL.
Status	Click the checkbox to enable the ACL.

Policy	Select the action to be taken when a packet matches the rule. Permit: Forward the matched packet. Deny: Discard the matched packet.
Protocols	Select one or more protocol types to which the rule applies from the drop-down list. The default is All, indicating that packets of all protocols will be matched. When you select one of TCP and UDP or both of them, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.

From the Source drop-down list, choose one of these options to specify the source of the packets to which this ACL applies:

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The EAP will examine whether the packets are sourced from the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The EAP will examine whether the source IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The EAP will examine whether the source IP address and port number of the packet are in the IP-Port Group.
SSID	Select the SSID you have created. If no SSIDs have been created, go to Settings > Wireless Networks to create one. The EAP will examine whether the SSID of the packet is the SSID selected here.

From the Destination drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The EAP will examine whether the packets are forwarded to the selected network.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The EAP will examine whether the destination IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The EAP will examine whether the destination IP address and port number of the packet are in the IP-Port Group.

4. 5. 2 URL Filtering

Overview

URL Filtering allows a network administrator to create rules to block or allow certain websites, which protects it from web-based threats, and deny access to malicious websites.

In URL filtering, the system compares the URLs in HTTP, HTTPS and DNS requests against the lists of URLs that are defined in URL Filtering rules, and intercepts the requests that are directed at a blocked URLs. These rules can be applied to specific clients or groups whose traffic passes through the gateway and EAPs.

The system filters traffic against the rules in the list sequentially. The first match determines whether the packet is accepted or dropped, and other rules are not checked after the first match. Therefore, the order of the rules is critical. By default, the rules are prioritized based on the sequence they are created. The rule created earlier is checked for a match with a higher priority. To reorder the rules, select a rule and drag it to a new position. If no rules match, the device forwards the packet because of an implicit Permit All clause.

Note that URL Filtering rules take effects with a higher priority over ACL rules. That is, the system will process the URL Filtering rule first when the URL Filtering rule and ACL rules are configured at the same time.

Configuration

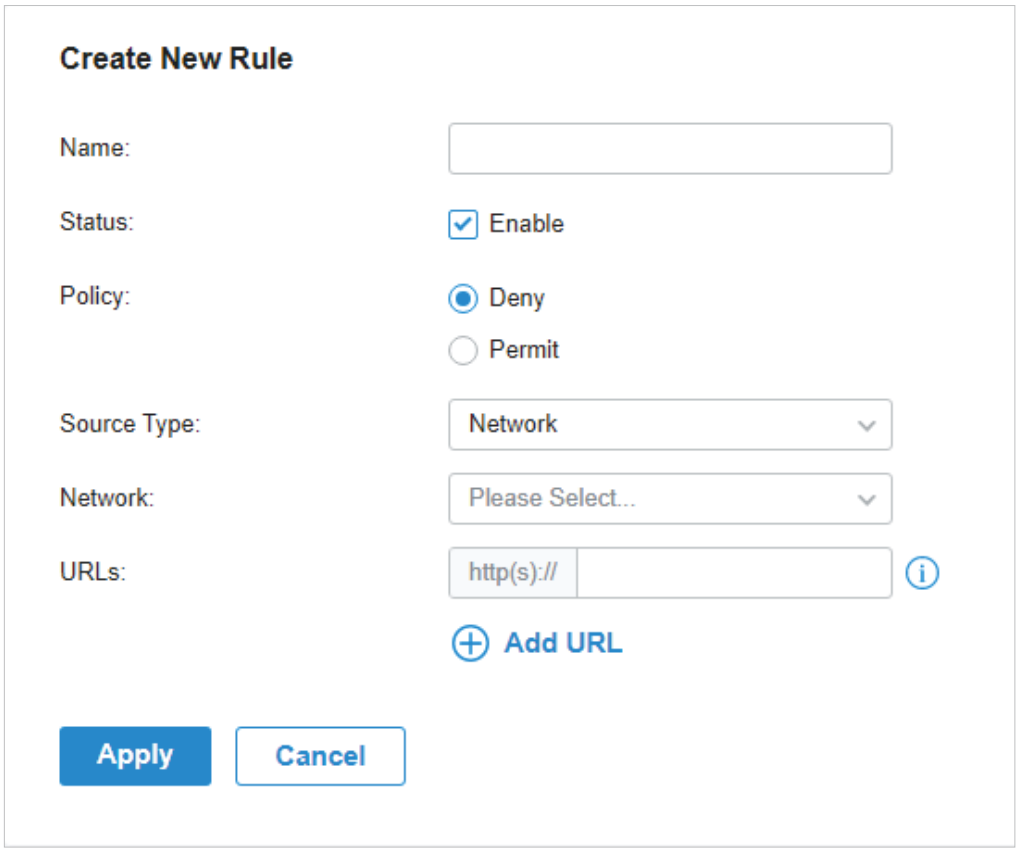
To complete the URL Filtering configuration, follow these steps:

1) Create a new URL Filtering rule with the specified type.

2) Define filtering criteria of the rule, including source, and URLs, and determine whether to forward the matched packets.

Configuring Gateway Rules

1. Go to Settings > Network Security > URL Filtering. Under the Gateway Rules tab, click + Create New Rule to load the following page.



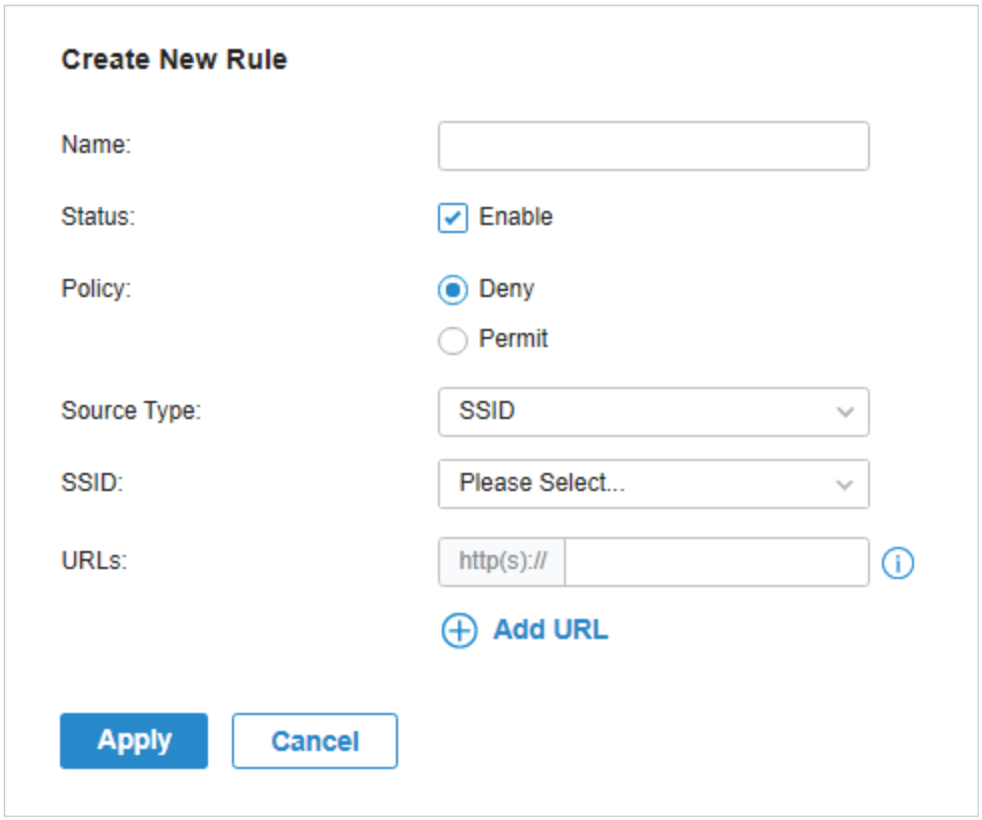
2. Define filtering criteria of the rule, including source and URLs, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the URL Filtering rule.
Status	Click the checkbox to enable the URL Filtering rule.
Policy	Select the action to be taken when a packet matches the rule. Deny: Discard the matched packet and the clients cannot access the URLs. Permit: Forward the matched packet and clients can access the URLs.
Source Type	Select the source of the packets to which this rule applies. Network: With Network selected, select the network you have created from the Network drop-down list. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The gateway will filter the packets sourced from the selected network. IP Group: With IP Group selected, select the IP Group you have created from the IP Group drop-down list. If no IP Groups have been created, click +Create New IP Group on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the source IP address of the packet is in the IP Group.

URLs	Enter the URL address using up to 128 characters. URL address should be given in a valid format. The URL which contains a wildcard(*) is supported. One URL with a wildcard(*) can match mutiple subdomains. For example, with *.tp-link.com specified, community.tp-link.com will be matched.

■ Configuring EAP Rules

1. Go to Settings > Network Security > URL Filtering. On EAP Rules tab, click + Create New Rule to load the following page.



2. Define filtering criteria of the rule, including source and URLs, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the URL Filtering rule.
Status	Click the checkbox to enable the URL Filtering rule.
Policy	Select the action to be taken when a packet matches the rule. Deny: Discard the matched packet and the clients cannot access the URLs. Permit: Forward the matched packet and clients can access the URLs.
Source Type	Select the SSID of the packets to which this rule applies.

URLs	Enter the URL address using up to 128 characters. URL address should be given in a valid format. The URL which contains a wildcard(*) is supported. One URL with a wildcard(*) can match mutiple subdomains. For example, with *.tp-link.com specified, community.tp-link.com will be matched.

4. 5. 3 Attack Defense

Overview

Attacks initiated by utilizing inherent bugs of communication protocols or improper network deployment have negative impacts on networks. In particular, attacks on a network device can cause the device or network paralysis.

With the Attack Defense feature, the gateway can identify and discard various attack packets in the network, and limit the packet receiving rate. In this way, the gateway can protect itself and the connected network against malicious attacks.

The gateway provides two types of Attack Defense:

- **Flood Defense**

If an attacker sends a large number of fake packets to a target device, the target device is busy with these fake packets and cannot process normal services. Flood Defense detects flood packets in real time and limits the receiving rate of the packets to protect the device.

Flood attacks include TCP SYN flood attacks, UDP flood attacks, and ICMP flood attacks.

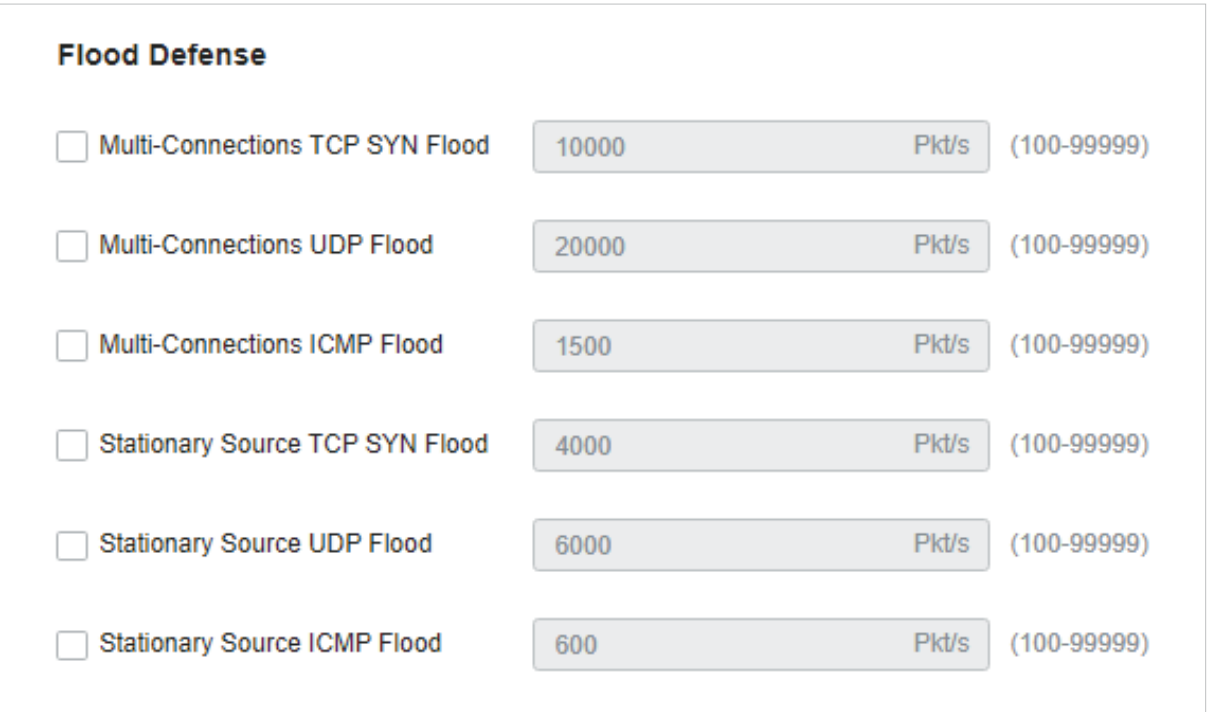
- **Packet Anomaly Defense**

Anomalous packets are packets that do not conform to standards or contain errors that make them unsuitable for processing. Packet Anomaly Defense discards the illegal packets directly.

Configuration

Configuring Flood Defense

Go to Settings > Network Security > Attack Defense. In the Flood Defense, click the checkbox and set the corresponding limit of the rate at which specific packets are received.

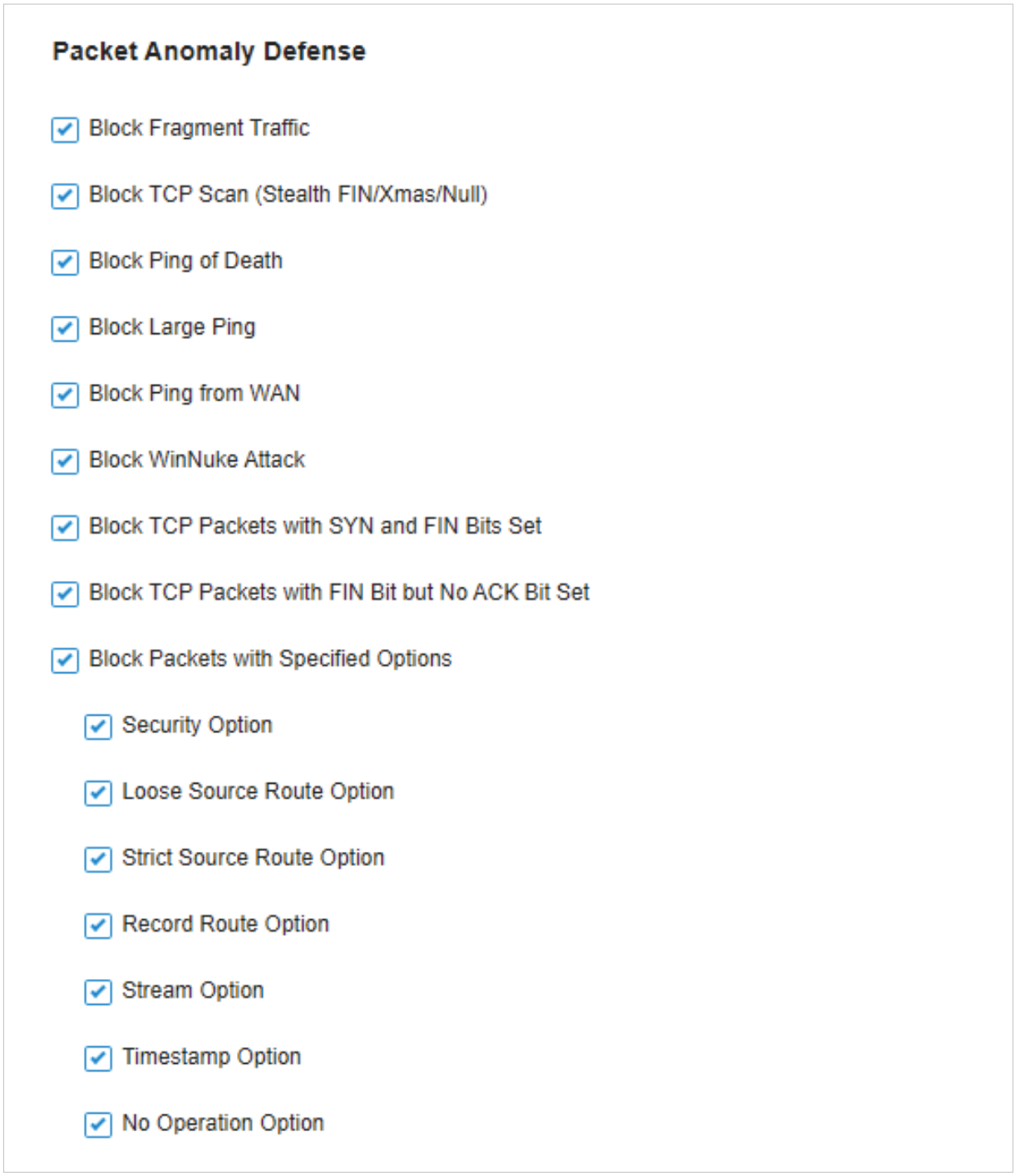


Multi-Connections TCP SYN Flood	A TCP SYN flood attack occurs when the attacker sends the target system with a succession of SYN (synchronize) requests. When the system responds, the attacker does not complete the connections, thus leaving the connection half-open and flooding the system with SYN messages. No legitimate connections can then be made. With this feature enabled, the gateway limits the rate of receiving TCP SYN packets from all the clients to the specified rate.
Multi-Connections UDP Flood	A UDP flood attack occurs when the attacker sends a large number of UDP packets to a target host in a short time, the target host is busy with these UDP packets and cannot process normal services. With this feature enabled, the gateway limits the rate of receiving UDP packets from all the clients to the specified rate.
Multi-Connections ICMP Flood	If an attacker sends many ICMP Echo messages to the target device, the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected. With this feature enabled, the system limits the rate of receiving ICMP packets from all the clients to the specified rate.

Stationary Source TCP SYN Flood	A TCP SYN flood attack occurs when the attacker sends the target system with a succession of SYN (synchronize) requests. When the system responds, the attacker does not complete the connections, thus leaving the connection half-open and flooding the system with SYN messages. No legitimate connections can then be made. With this feature enabled, the gateway limits the rate of receiving TCP SYN packets from a single client to the specified rate.
Stationary Source UDP Flood	A UDP flood attack occurs when the attacker sends a large number of UDP packets to a target host in a short time, the target host is busy with these UDP packets and cannot process normal services. With this feature enabled, the gateway limits the rate of receiving UDP packets from a single client to the specified rate.
Stationary Source ICMP Flood	If an attacker sends many ICMP Echo messages to the target device, the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected. With this feature enabled, the system limits the rate of receiving ICMP packets from a single clients to the specified rate.

- **Configuring Packet Anomaly Defense**

  Go to Settings > Network Security > Attack Defense. In the Packet Anomaly Defense, click the checkbox and set the corresponding limit of the rate at which specific packets are received.



Block Fragment Traffic	With this option enabled, the fragmented packets without the first part of the packet will be discarded.

Block TCP Scan (Stealth FIN/Xmas/Null)	With this option enabled, the gateway will block the anomalous packets in the following attack scenarios: Stealth FIN Scan: The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal. Xmas Scan: The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1. Null Scan: The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all control fields set to 0 are considered illegal.
Block Ping of Death	With this option enabled, the gateway will block Ping of Death attack. Ping of Death attack means that the attacker sends abnormal ping packets which are smaller than 64 bytes or larger than 65535 bytes to cause system crash on the target computer.
Block Large Ping	With this option enabled, the router will block the ping packets which are larger than 1024 packets to protect the system from Large Ping attack.
Block Ping from WAN	With this option enabled, the router will block the ICMP request from WAN.
Block WinNuke Attack	With this option enabled, the router will block WinNuke attacks. WinNuke attack refers to a remote DoS (denial-of-service) attack that affects some Windows operating systems, such as the Windows 95. The attacker sends a string of OOB (Out of Band) data to the target computer on TCP port 137, 138 or 139, causing system crash or Blue Screen of Death.
Block TCP Packets with SYN and FIN Bits Set	With this option enabled, the router will filter the TCP packets with both SYN Bit and FIN Bit set.
Block TCP Packets with FIN Bit but No ACK Bit Set	With this option enabled, the router will filter the TCP packets with FIN Bit set but without ACK Bit set.
Block Packets with Specified Options	With this option enabled, the router will filter the packets with specified IP options including Security Option, Loose Source Route Option, Strict Source Route Option, Record Route Option, Stream Option, Timestamp Option, and No Operation Option. You can choose the options according to your needs.

4. 6 Transmission

Transmission helps you control network traffic in multiple ways. You can add policies and rules to control transmission routes and limit the session and bandwidth.

4. 6. 1 Routing

Overview

- **Static Route**

  Network traffic is oriented to a specific destination, and Static Route designates the next hop or interface where to forward the traffic.

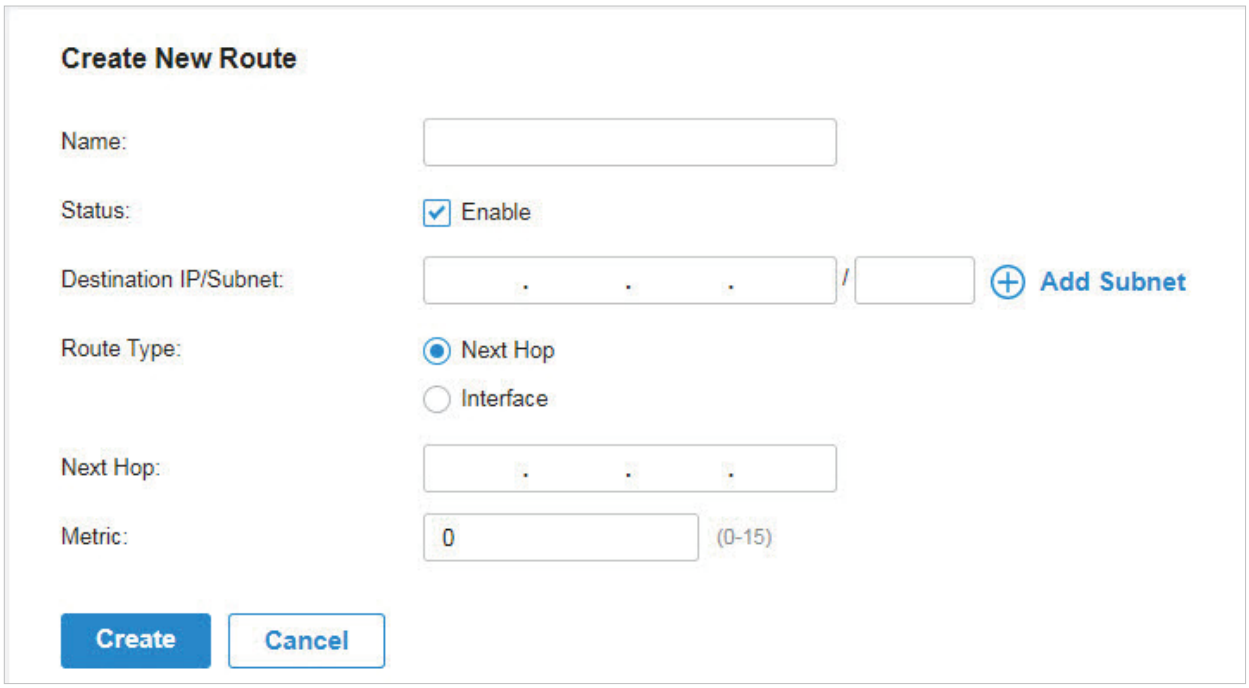
- **Policy Routing**

  Policy Routing designates which WAN port the router uses to forward the traffic based on the source, the destination, and the protocol of the traffic.

Configuration

- **Static Route**

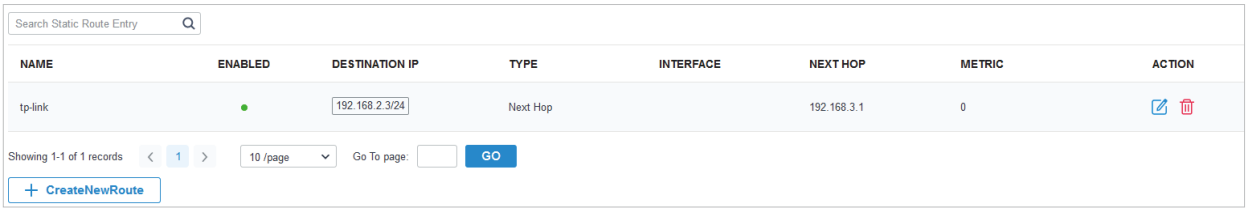
3. Go to Setting > Transmission > Routing > Static Route. Click + Create New Route to load the following page and configure the parameters.



Name	Enter the name to identify the Static Route entry.
Status	Enable or disable the Static Route entry.

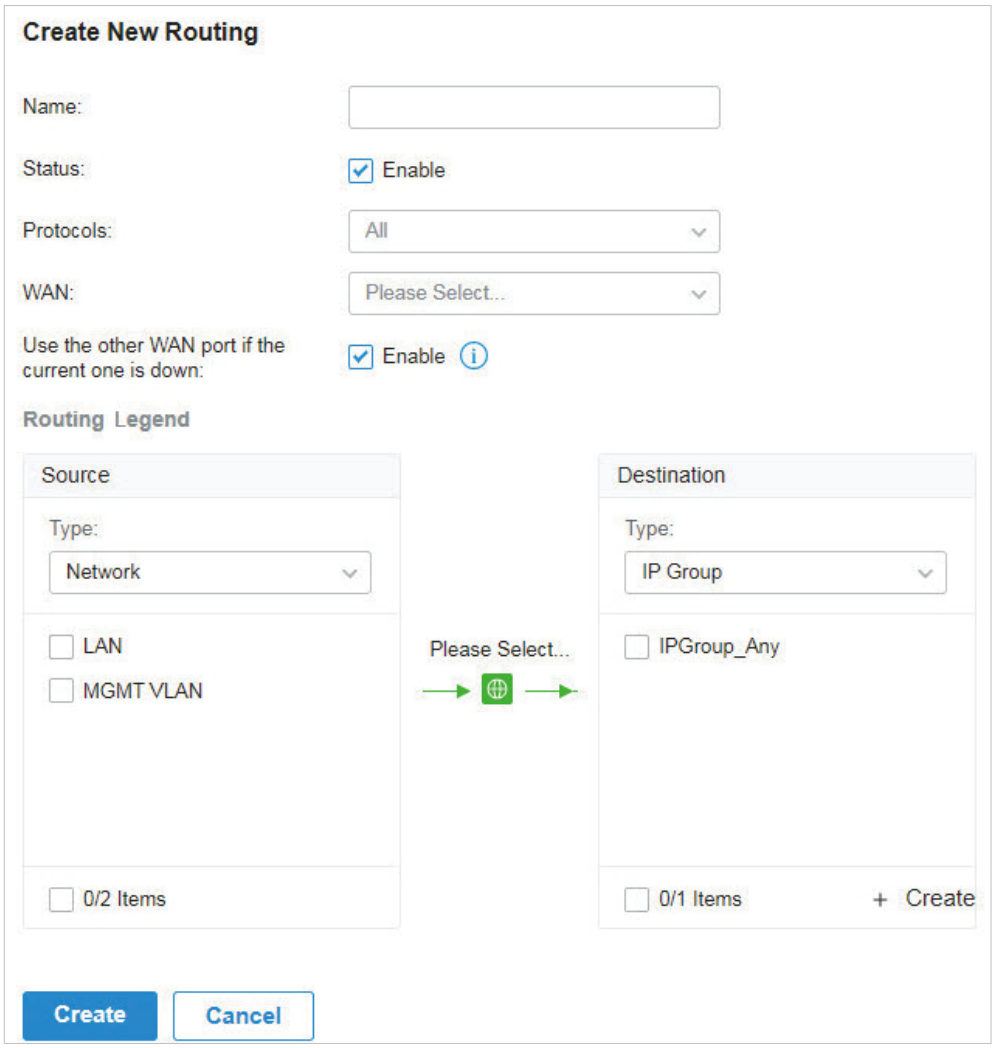
Destination IP/Subnet	Destination IP/Subnet identifies the network traffic which the Static Route entry controls. Specify the destination of the network traffic in the format of 192.168.0.1/24. You can click + Add Subnet to specify multiple Destination IP/Subnets and click to delete them.
Route Type	Next Hop: With Next Hop selected, your devices forward the corresponding network traffic to a specific IP address. You need to specify the IP address as Next Hop. Interface: With Interface selected, your devices forward the corresponding network traffic through a specific interface. You need to specify the Interface according to your needs.
Metric	Define the priority of the Static Route entry. A smaller value means a higher priority. If multiple entries match the Destination IP/Subnet of the traffic, the entry of higher priority takes precedence. In general, you can simply keep the default value.

4. Click Create. The new Static Route entry is added to the table. You can click to edit the entry. You can click to delete the entry.



Policy Routing

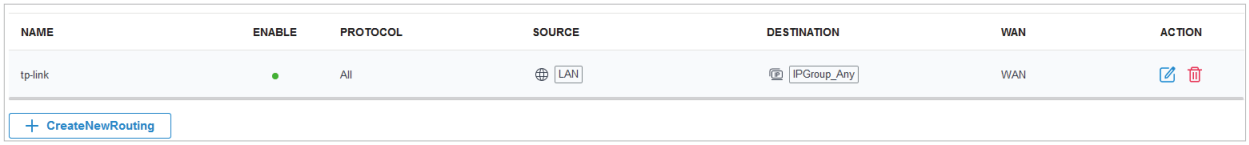
1. Go to Setting > Transmission > Routing > Policy Routing. Click + Create New Routing to load the following page and configure the parameters.



Name	Enter the name to identify the Policy Routing entry.
Status	Enable or disable the Policy Routing entry.
Protocols	Select the protocols of the traffic which the Policy Routing entry controls. The Policy Routing entry takes effect only when the traffic matches the criteria of the entry including the protocols.
WAN	Select the WAN port to forward the traffic through. If you want to forward the traffic through the other WAN port when the current WAN is down, enable Use the other WAN port if the current WAN is down.

Routing Legend	The Policy Routing entry takes effect only when the traffic using specified protocols matches the source and destination which are specified in the Routing Legend. Select the type of the traffic source and destination. Network: Select the LAN Interfaces for the traffic source or destination. IP Group: Select the IP Group for the traffic source or destination. You can click + Create to create a new IP Group.

2. Click Create. The new Policy Routing entry is added to the table. You can click to edit the entry. You can click to delete the entry.



4. 6. 2 NAT

Overview

- **Port Forwarding**

  You can configure Port Forwarding to allow internet users to access local hosts or use network services which are deployed in the LAN.

  Port Forwarding helps establish network connections between a host on the internet and the other in the LAN by letting the traffic pass through the specific port of the gateway. Without Port Forwarding, hosts in the LAN are typically inaccessible from the internet for the sake of security.

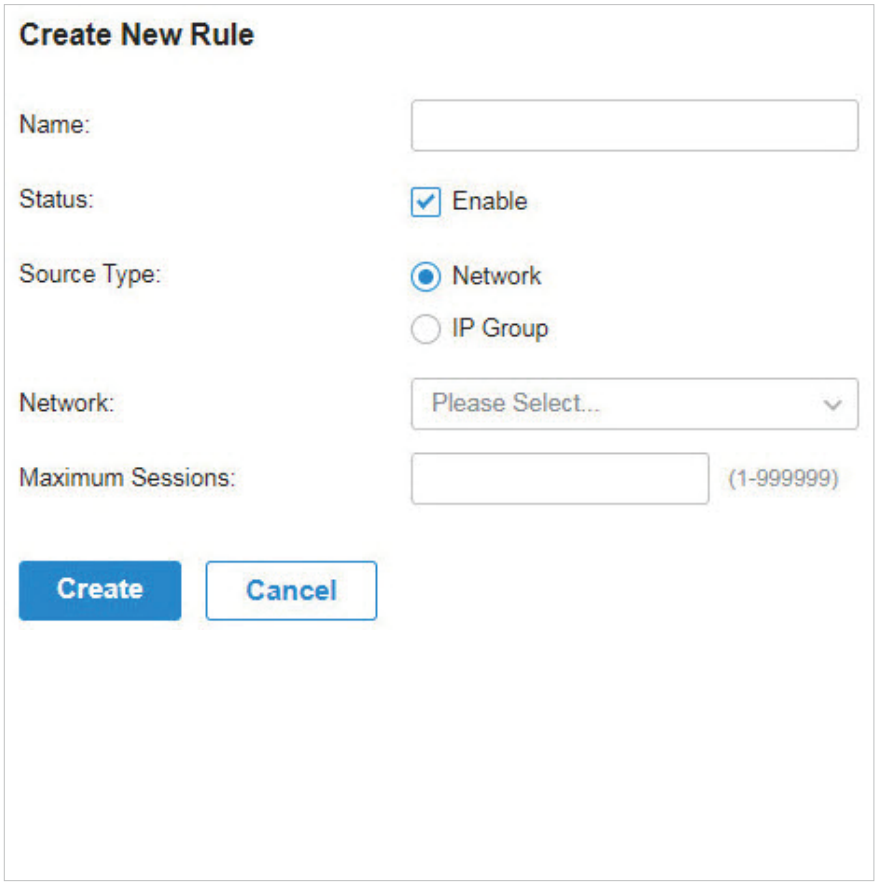
- **ALG**

  ALG ensures that certain application-level protocols function appropriately through your gateway.

Configuration

■ Port Forwarding

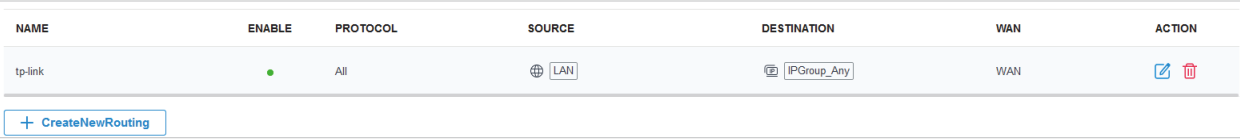
1. Go to Setting > Transmission > NAT > Port Forwarding. Click + Create New Rule to load the following page and configure the parameters.



Name	Enter the name to identify the Port Forwarding rule.
Status	Enable or disable the Port Forwarding rule.
Source IP	Any: The rule applies to traffic from any source IP address. Limited IP Address: The rule only applies to traffic from specific IP addresses. With this option selected, specify the IP addresses and subnets according to your needs.
Interface	Select the interface which the rule applies to. Traffic which is received through the interface is forwarded according to the rule.
DMZ	With DMZ enabled, all the traffic is forwarded to the Destination IP in the LAN, port to port. You need to specify the Destination IP. With DMZ disabled, only the traffic which matches the Source Port and the Protocol is forwarded. The traffic is forwarded to the Destination Port of the Destination IP in the LAN. You need to specify the Source Port, Destination IP, Destination Port, and Protocol.

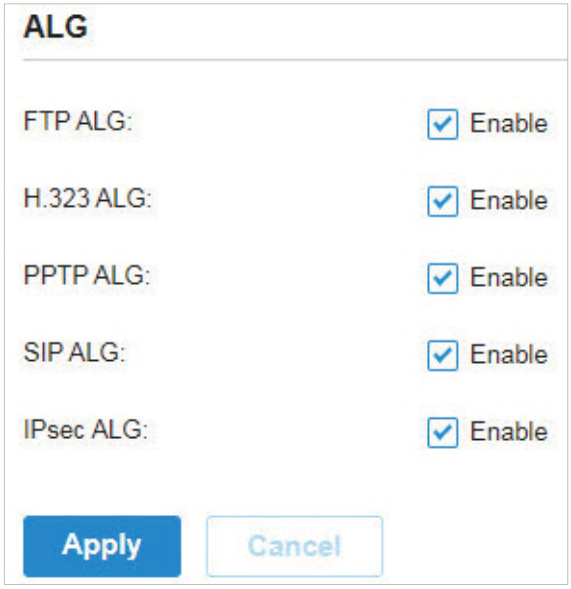
Source Port	The gateway uses the Source Port to receive the traffic from the internet. Only the traffic which matches the Source Port and the Protocol is forwarded.
Destination IP	The traffic is forwarded to the host of the Destination IP in the LAN.
Destination Port	The traffic is forwarded to the Destination Port of the host in the LAN.
Protocol	Network traffic is transmitted using either TCP or UDP protocol. Only the traffic which matches the Source Port and the Protocol is forwarded. If you want both TCP traffic and UDP traffic to be forwarded, select All.

2. Click Create. The new Port Forwarding entry is added to the table. You can click to edit the entry. You can click to delete the entry.



ALG

Go to Setting > Transmission > NAT > ALG. Enable or disable certain types of ALG according to your needs and click Apply.



FTP ALG	FTP ALG allows the FTP server and client to transfer data using the FTP protocol in one of the following scenarios: • The FTP server is in the LAN, while the FTP client is on the internet. • The FTP server is on the internet, while the FTP client is in the LAN. • The FTP server and FTP client are in different LANs.

H.323 ALG	H.323 ALG allows the IP phones and multimedia devices to set up connections using the H.323 protocol in one of the following scenarios: • One of the endpoints is in the LAN, while the other is on the internet. • The endpoints are in different LANs.
PPTP ALG	PPTP ALG allows the PPTP server and client to set up a PPTP VPN in one of the following scenarios: • The PPTP server is in the LAN, while the PPTP client is on the internet. • The PPTP server is on the internet, while the PPTP client is in the LAN. • The PPTP server and PPTP client are in different LANs.
SIP ALG	SIP ALG allows the IP phones and multimedia devices to set up connections using the SIP protocol in one of the following scenarios: • One of the endpoints is in the LAN, while the other is on the internet. • The endpoints are in different LANs.
IPsec ALG	IPsec ALG allows the IPsec endpoints to set up an IPsec VPN in one of the following scenarios: • One of the endpoints is in the LAN, while the other is on the internet. • The endpoints are in different LANs.

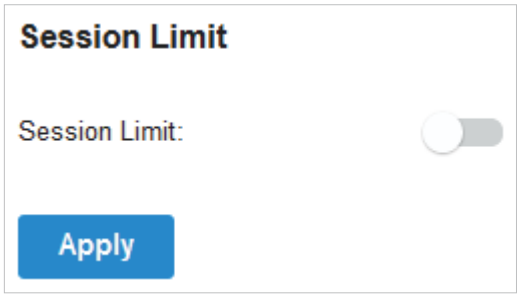
4. 6. 3 Session Limit

Overview

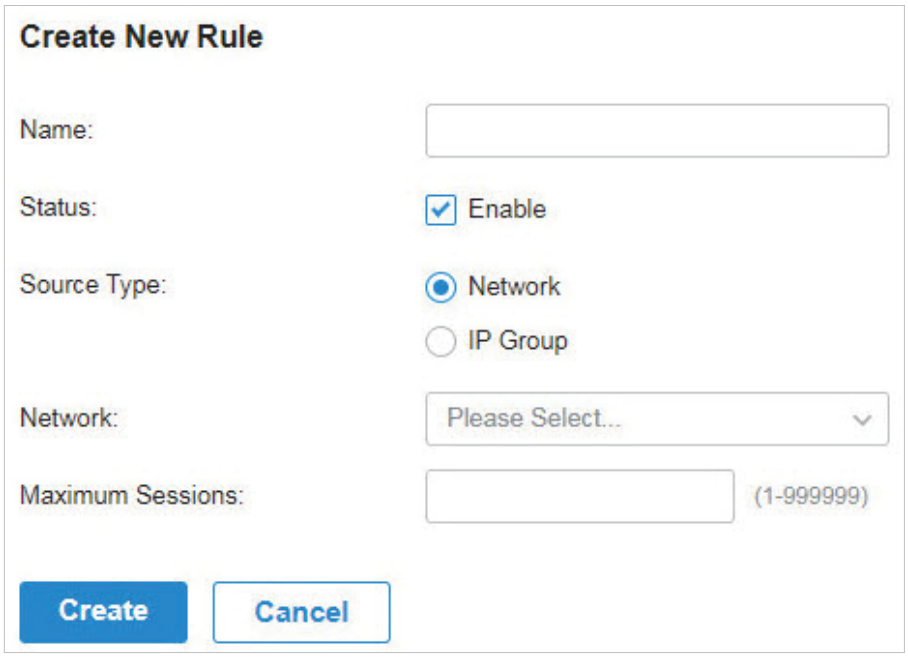
Session Limit optimizes network performance by limiting the maximum sessions of specific sources.

Configuration

1. Go to Setting > Transmission > Session Limit. In Session Limit, enable Session Limit globally and click Apply.

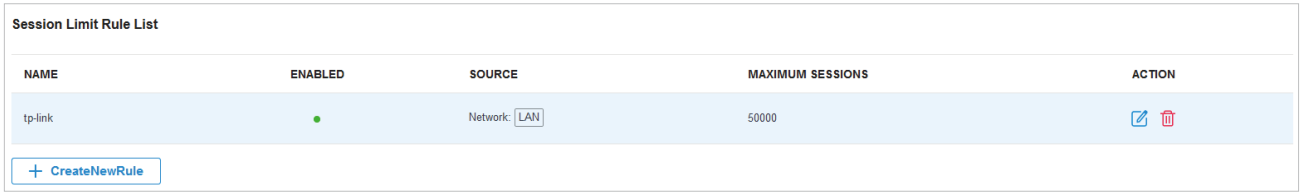


2. In Session Limit Rule List, click + Create New Rule to load the following page and configure the parameters.



Name	Enter the name to identify the Session Limit rule.
Status	Enable or disable the Session Limit rule.
Source Type	Network: Limit the maximum sessions of specific LAN networks. With this option selected, select the networks, which you can customize in Wired Networks > LAN Networks. For detailed configuration of networks, refer to Configure LAN Networks. IP Group: Limit the maximum sessions of specific IP Groups. With this option selected, select the IP Groups, which you can customize in Profiles > Groups. For detailed configuration of IP groups, refer to Create Profiles.
Maximum Sessions	Enter the maximum sessions of the specific sources.

3. Click Create. The new Session Limit rule is added to the list. You can click to edit the rule. You can click to delete the rule.



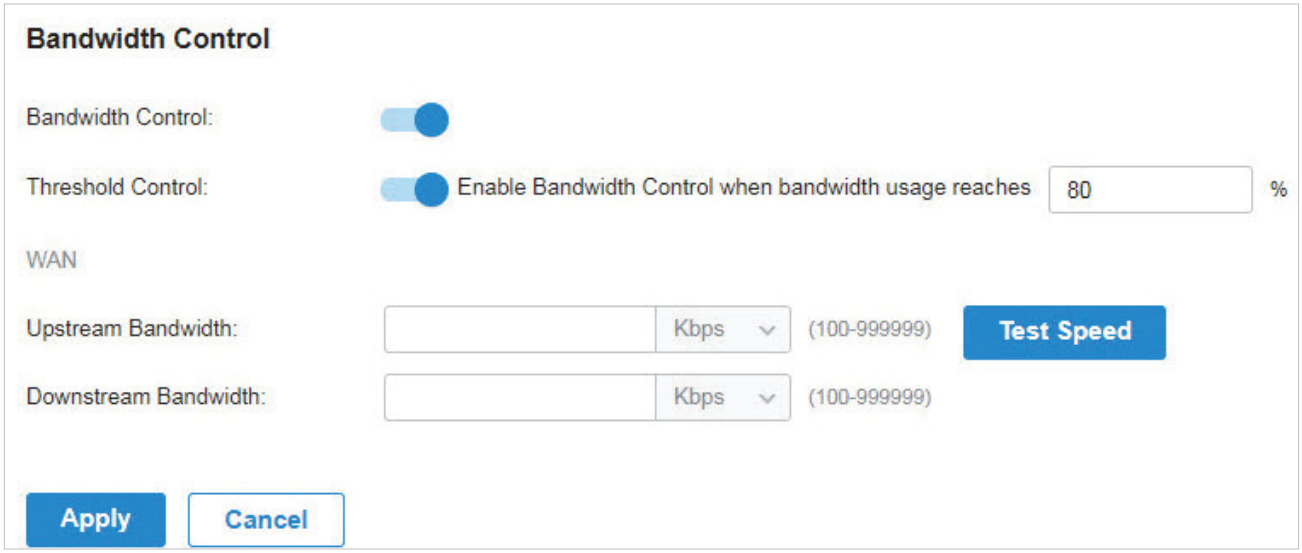
4. 6. 4 Bandwidth Control

Overview

Bandwidth Control optimizes network performance by limiting the bandwidth of specific sources.

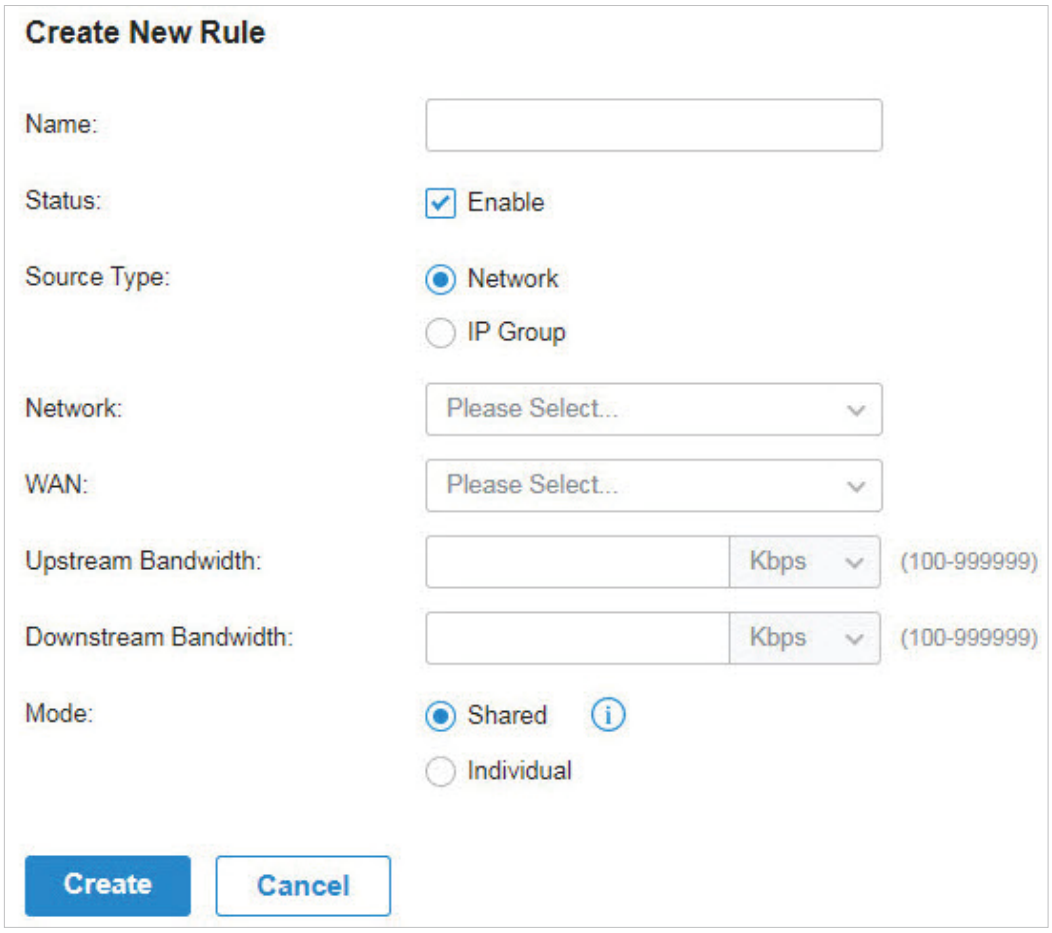
Configuration

1. Go to Setting > Transmission > Bandwidth Control. In Bandwidth Control, enable Bandwidth Control globally and configure the parameters. Then click Apply.



Threshold Control	With Threshold Control enabled, Bandwidth Control takes effect only when total bandwidth usage reaches the specified percentage. You need to specify the total Upstream Bandwidth and Downstream Bandwidth of the WAN ports. It's recommended to use the Test Speed tool to decide the actual Upstream Bandwidth and Downstream Bandwidth.

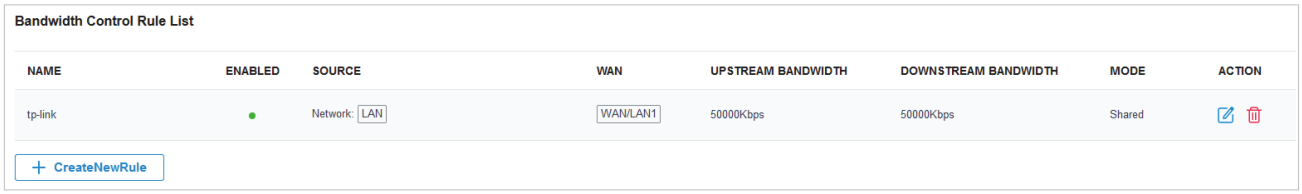
2. In Bandwidth Control Rule List, click + Create New Rule to load the following page and configure the parameters.



Name	Enter the name to identify the Bandwidth Control rule.
Status	Enable or disable the Bandwidth Control rule.
Source Type	Network: Limit the maximum bandwidth of specific LAN networks. With this option selected, select the networks, which you can customize in Wired Networks > LAN Networks. For detailed configuration of networks, refer to Configure LAN Networks. IP Group: Limit the maximum bandwidth of specific IP Groups. With this option selected, select the IP Groups, which you can customize in Profiles > Groups. For detailed configuration of IP groups, refer to Create Profiles.
WAN	Select the WAN port which the rule applies to.
Upstream Bandwidth	Specify the limit of Upstream Bandwidth, which the specific local hosts use to transmit traffic to the internet through the gateway.
Downstream Bandwidth	Specify the limit of Downstream Bandwidth, which the specific local hosts use to receive traffic from the internet through the gateway.

Mode	Specify the bandwidth control mode for the specific local hosts. Shared: The total bandwidth for all the local hosts is equal to the specified values. Individual: The bandwidth for each local host is equal to the specified values.

3. Click Create. The new Bandwidth Control rule is added to the list. You can click to edit the rule. You can click to delete the rule.



4. 7 Configure VPN

Overview

VPN (Virtual Private Network) gives remote LANs or users secure access to LAN resources over a public network such as the internet. Virtual indicates the VPN connection is based on the logical end-to-end connection instead of the physical end-to-end connection. Private indicates users can establish the VPN connection according to their requirements and only specific users are allowed to use the VPN connection.

The core of VPN connection is to realize tunnel communication, which fulfills the task of data encapsulation, data transmission and data decompression via the tunneling protocol. The gateway supports common tunneling protocols that a VPN uses to keep the data secure:

- **IPsec**

IPsec (IP Security) can provide security services such as data confidentiality, data integrity and data authentication at the IP layer. IPsec uses IKE (Internet Key Exchange) to handle negotiation of protocols and algorithms based on the user-specified policy, and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more paths between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

- **PPTP**

PPTP (Point-to-Point Tunneling Protocol) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP uses the username and password to validate users.

- **L2TP**

L2TP (Layer 2 Tunneling Protocol) provides a way for a dialup user to make a virtual Point-to-Point Protocol (PPP) connection to an L2TP network server (LNS), which can be a security gateway. L2TP sends PPP frames through a tunnel between an L2TP access concentrator (LAC) and the LNS. Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. L2TP uses the username and password to validate users.

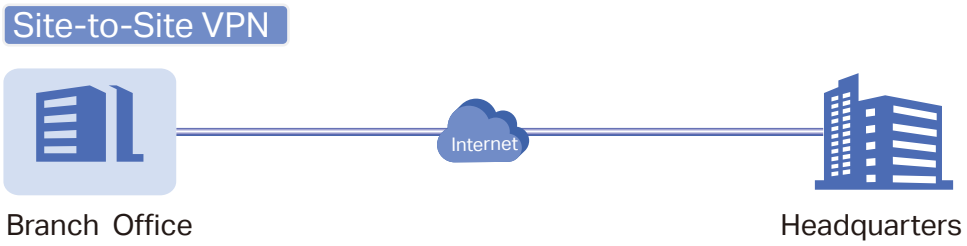
- **OpenVPN**

OpenVPN uses OpenSSL for encryption of UDP and TCP for traffic transmission. OpenVPN uses a client-server connection to provide secure communications between a server and a remote client over the internet. One of the most important steps in setting up OpenVPN is obtaining a certificate which is used for authentication. Omada SDN controller supports generating the certificate which can be downloaded as a file on your computer. With the certificate imported, the remote clients are checked out by the certificate and granted access to the LAN resources.

There are many variations of virtual private networks, with the majority based on two main models:

- **Site-to-Site VPN**

  A Site-to-Site VPN creates a connection between two networks at different geographic locations. Typically, headquarters set up Site-to-Site VPN with the subsidiary to provide the branch office with access to the headquarters' network.



  Omada managed gateway supports two types of Site-to-Site VPNs:

  - Auto IPsec

    The controller automatically creates an IPsec VPN tunnel between two sites on the same controller. The VPN connection is bidirectional. That is, creating an Auto IPsec VPN from site A to site B also provides connectivity from site B to site A, and nothing is needed to be configured on site B.

  - Manual IPsec

    You create an IPsec VPN tunnel between two peer routers over internet manually, from a local router to a remote router that supports IPsec. Omada managed gateway on this site is the local peer router.

- **Client-to-Site VPN**

  A Client-to-Site VPN creates a connection to the LAN from a remote host. It is useful for teleworkers and business travelers to access their central LAN from a remote location without compromising privacy and security.

  The first step to build a Client-to-Site VPN connection is to determine the role of the gateways and which VPN tunneling protocol to use:

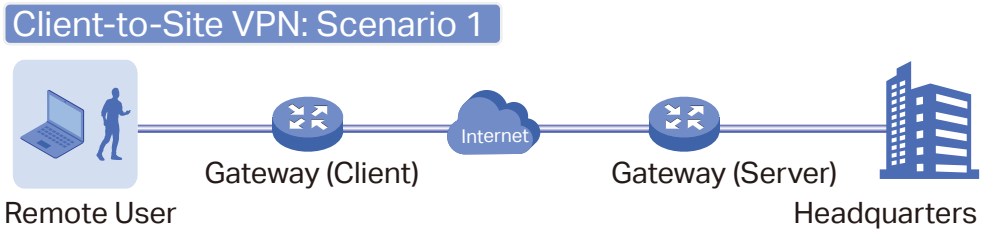
  - VPN Server

    The gateway on the central LAN works as a VPN server to provide a remote host with access to the local network. The gateway which functions as a VPN server can use L2TP, PPTP, IPsec, or OpenVPN as the tunneling protocol.

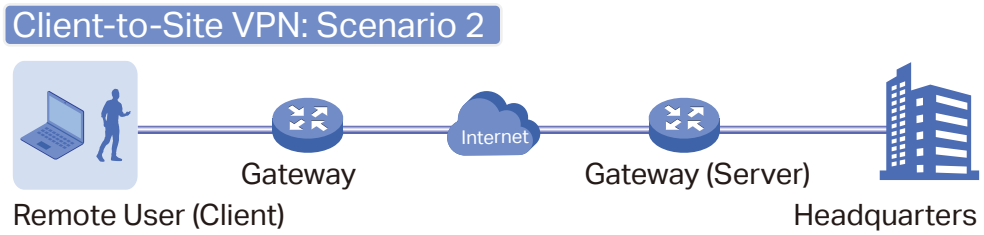
  - VPN Client

    Either the remote user's gateway or the remote user's laptop or PC works as the VPN client.

When the remote user's gateway works as the VPN client, the gateway helps create VPN tunnels between its connected hosts and the VPN server. The gateway which functions as a VPN client can use L2TP, PPTP, or OpenVPN as the tunneling protocol.



When the remote user's laptop or PC works as the VPN client, the laptop or PC uses a VPN client software program to create VPN tunnels between itself and the VPN server. The VPN client software program can use L2TP, PPTP, IPsec, or OpenVPN as the tunneling protocol.

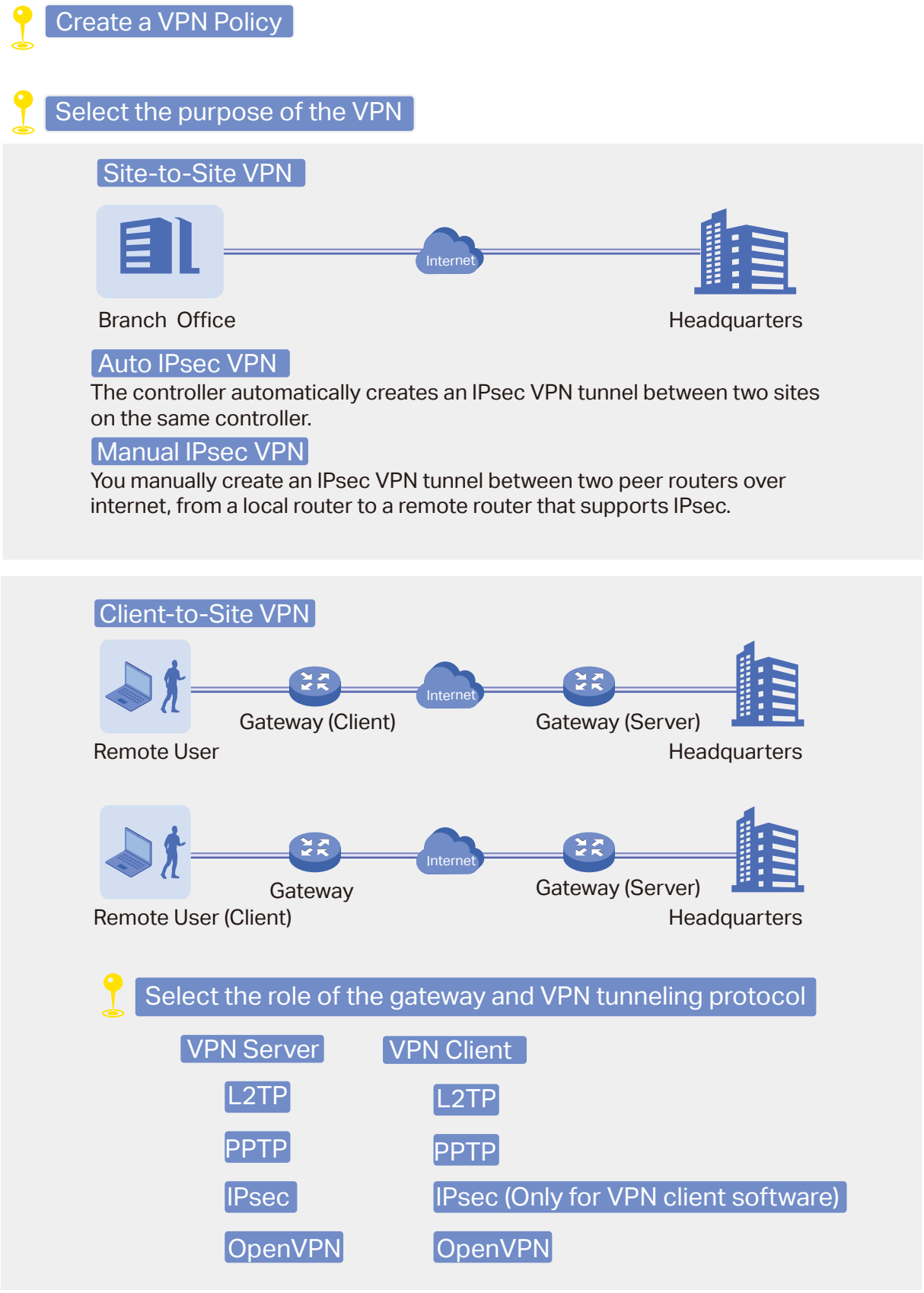


Note:

In scenario 1, you need to configure VPN client and VPN server separately on the gateways, while remote hosts can access the local networks without running VPN client software.

In scenario 2, you need to configure VPN server on the gateway, and then configure the VPN client software program on the remote user's laptop or PC, while the remote user's gateway doesn't need any VPN configuration.

Here is the infographic to provide a quick overview of VPN solutions.



Configuration

To complete the VPN configuration, follow these steps:

3) Create a new VPN policy and select the purpose of the VPN according to your needs. Select Site-to-Site if you want the network connected to another. Select Client-to-Site if you want some hosts connected to the network.

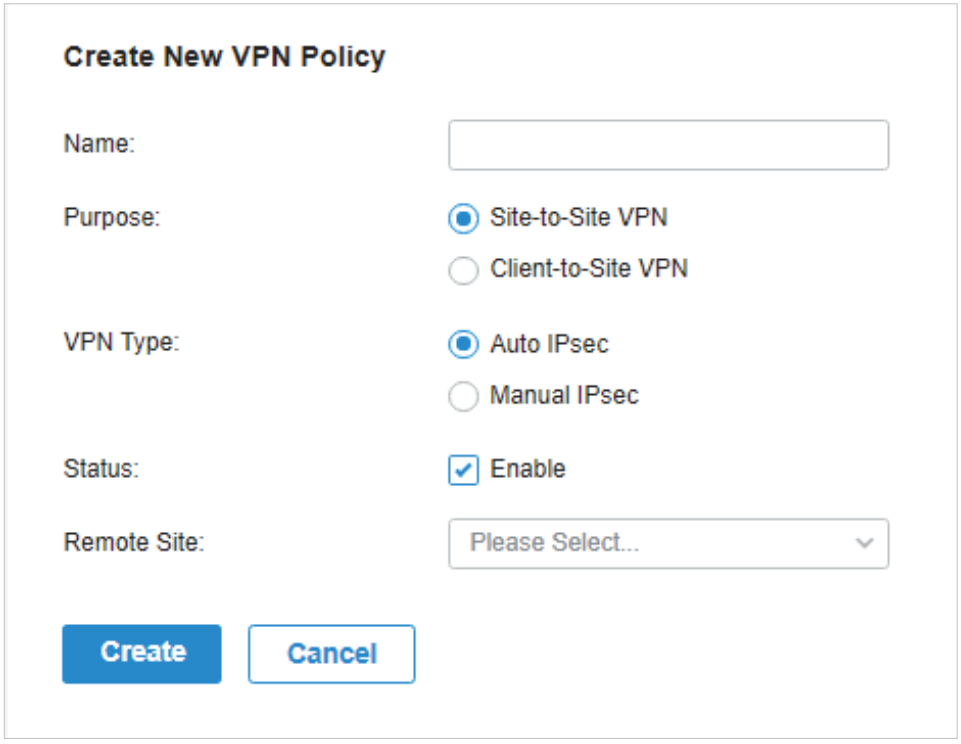
4) Select the VPN tunneling protocol and configure the VPN policy based on the protocol.

■ **Configuring Site-to-Site VPN**

Omada managed gateway supports two types of Site-to-Site VPNs: Auto IPsec and Manual IPsec.

- Configuring Auto IPsec VPN

4. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.

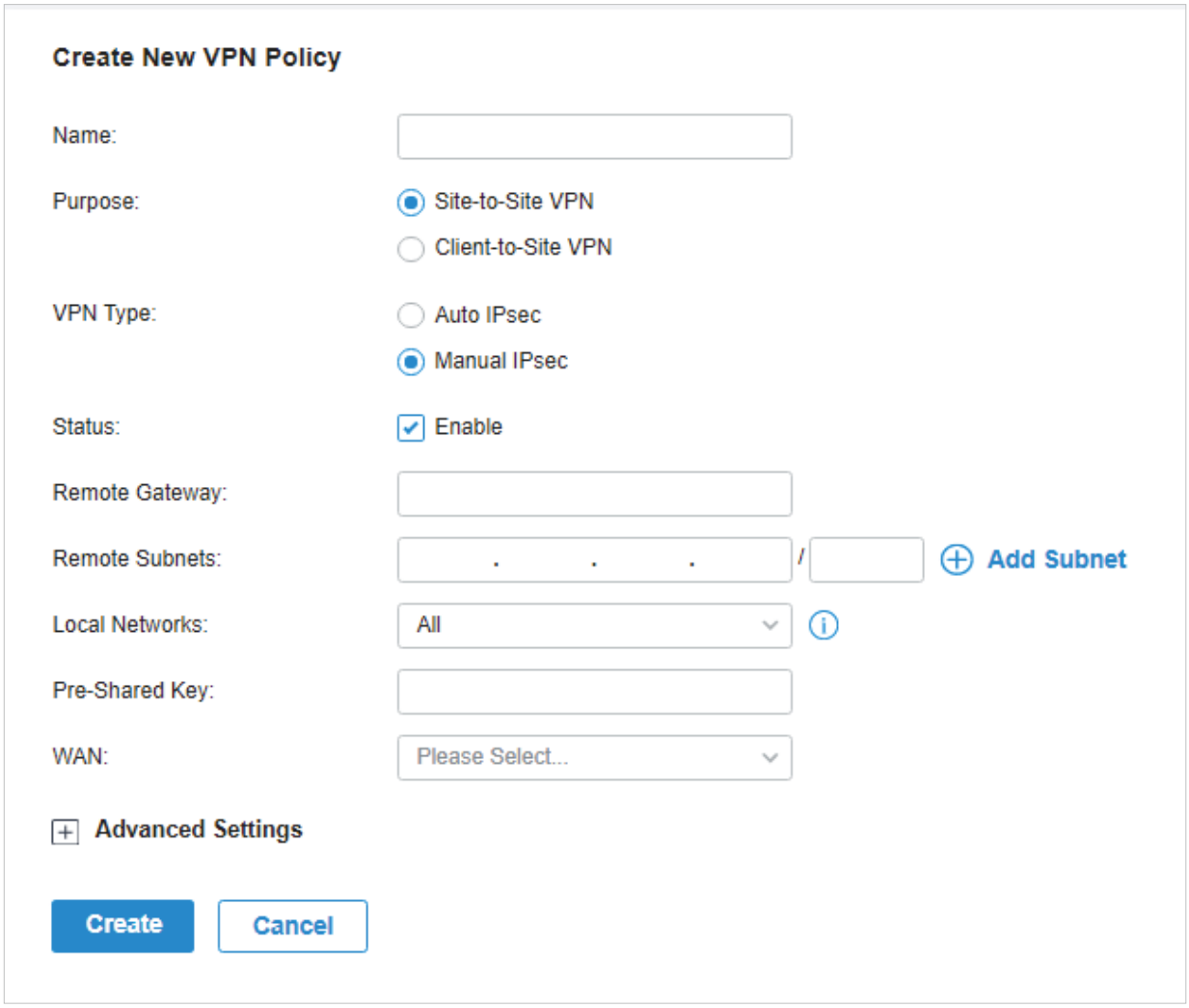


5. Enter a name to identify the VPN policy and select the purpose as Site-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Site-to-Site VPN.
VPN Type	Select the VPN type as Auto IPsec.
Status	Click the checkbox to enable the VPN policy.
Remote Site	Select the site on the other end of the Auto IPsec VPN tunnel. Make sure that the selected remote site has an online Omada managed gateway within the same controller.

- Configuring Manual IPsec VPN

1. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.

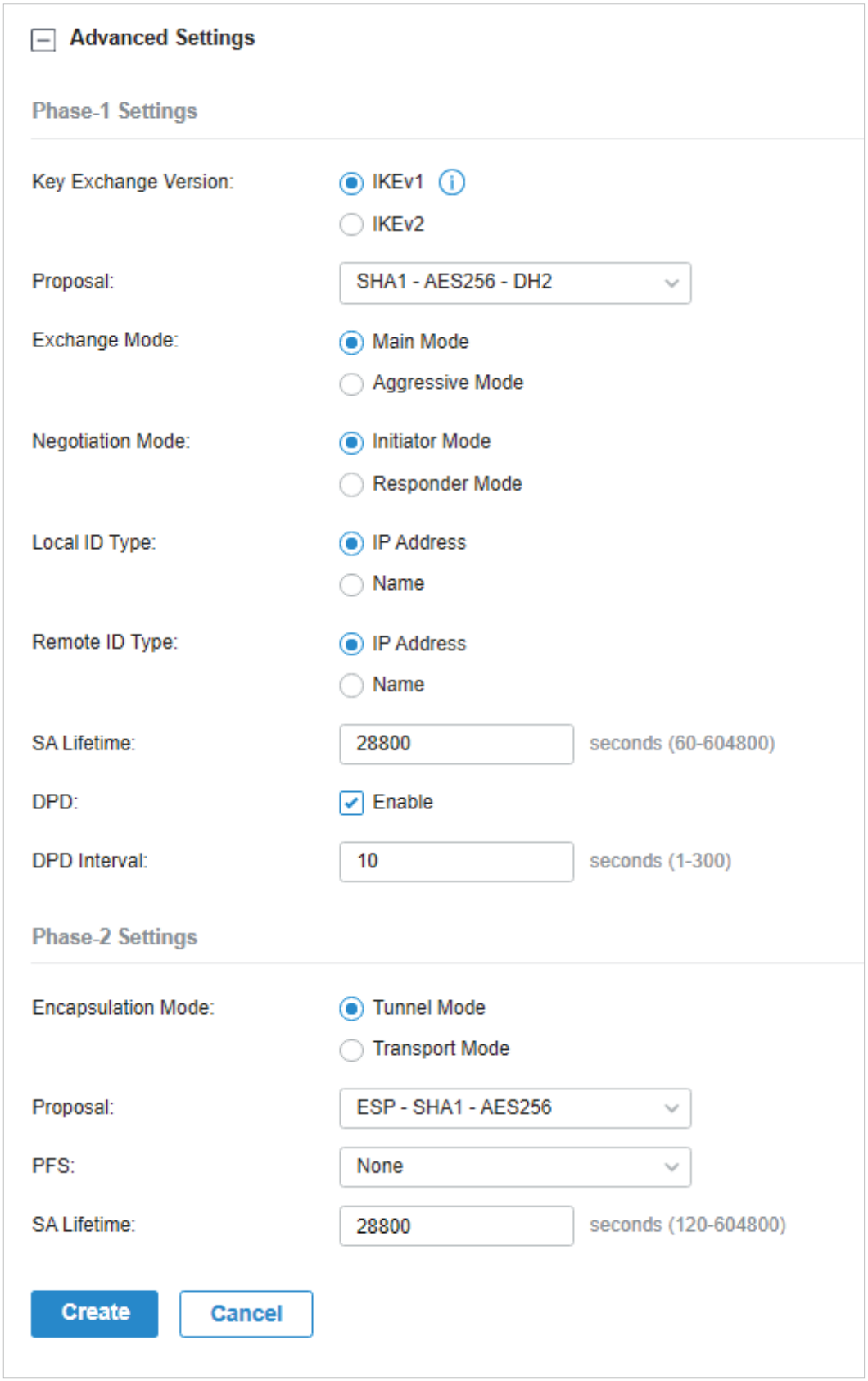


2. Enter a name to identify the VPN policy and select the purpose as Site-to-Site VPN. Refer to the following table to configure the basic parameters and click Create.

Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Site-to-Site VPN.
VPN Type	Select the VPN type as Manual IPsec.
Status	Click the checkbox to enable the VPN policy.
Remote Gateway	Enter an IP address or a domain name as the gateway on the remote peer of the VPN tunnel.
Remote Subnets	Enter the IP address range of LAN on the remote peer of the VPN tunnel.
Local Networks	Select the networks on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local networks.

Pre-Shared Key	Enter the pre-shared key(PSK). Both peer gateways must use the same pre-shared secret key for authentication. A pre-shared key is a string of characters that is used as an authentication key. Both peer gateways create a hash value based on the same pre-shared key and other information. The hash values are then exchanged and verified to authenticate the other party. The pre-shared keys should be long and random for security. Short or predictable pre-shared keys can be easily broken in brute-force attacks. To maintain a high level of security, administrators are recommended to update the pre-shared key periodically.
WAN	Select the WAN port on which the IPsec VPN tunnel is established.

3. Click Advanced Settings to load the following page.



Advanced settings include Phase-1 settings and Phase-2 settings. Phase-1 is used to set up a secure encrypted channel which the two peers can negotiate Phase-2, and then establish the IKE Security Associations (IKE SA). Phase-2 is used to negotiate about a set of parameters that

define what traffic can go through the VPN, and how to encrypt and authenticate the traffic, then establish the IPsec Security Associations (IPsec SA).

Refer to the following table to complete the configurations according to your actual needs and click Create.

For Phase-1 Settings:

Phase-1 Settings	The IKE version you select determines the available Phase-1 settings and defines the negotiation process . Both VPN gateways must be configured to use the same IKE version and Phase-1 settings.
Internet Key Exchange Version	Select the version of Internet Key Exchange (IKE) protocol which is used to set up security associations for IPsec. Both IKEv1 and IKEv2 are supported with Omada managed gateways, but IKEv1 is available only when the VPN policy is applied to a single Remote Subnet and a single Local Network. Note that both peer gateways must be configured to use the same IKE version.
Proposal	Specify the proposal for IKE negotiation phase-1. An IKE proposal lists the encryption algorithm, authentication algorithm and Diffie-Hellman (DH) groups to be negotiated with the remote IPsec peer— Authentication algorithms verify the data integrity and authenticity of a message. The types of authentication includes MD5 and SHA1. Encryption algorithms protect the data from being read by a third-party. The types of encryption algorithm includes DES, 3DES, AES128, AES192, and AES256. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. The DH group includes DH1, DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH25, and DH26. Note that both peer gateways must be configured to use the same Proposal.
Exchange Mode	Specify the IKE Exchange Mode when IKEv1 is selected. Main Mode: This mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection. Aggressive Mode: This mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.
Negotiation Mode	Specify the IKE Negotiation Mode as Initiator Mode or Responder Mode. Initiator Mode: This mode means that the local device initiates a connection to the peer. Responder Mode: This mode means that the local device waits for the connection request initiated by the peer.

Local ID Type	Specify the type of Local ID which indicates the authentication identifier sent to the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Local ID field to use the name as the ID for authentication. Note that the type and value of Local ID should be the same as Remote ID given for the remote peer of the VPN tunnel.
Local ID	When the Local ID Type is configured as Name, enter a name for the local device as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
Remote ID Type	Specify the type of Remote ID which indicates the authentication identifier received from the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Remote ID field to use the name as the ID for authentication. Note that the type and value of Remote ID should be the same as Local ID given for the remote peer of the VPN tunnel.
Remote ID	When the Remote ID Type is configured as Name, enter a name of the remote peer as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
SA Lifetime	Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.
DPD	Check the box to enable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.
DPD Interval	Specify the interval between sending DPD requests with DPD enabled. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA.

For Phase-2 Settings:

Phase-2 Settings	The purpose of Phase 2 negotiations is to establish the Phase-2 SA (also called the IPsec SA). The IPsec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic.
Encapsulation Mode	Specify the Encapsulation Mode as Tunnel Mode or Transport Mode. When both ends of the tunnel are hosts, either mode can be chosen. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, Tunnel Mode is recommended to ensure safety.

Proposal	Specify the proposal for IKE negotiation phase-2. An IPsec proposal lists the encryption algorithm, authentication algorithm and protocol to be negotiated with the remote IPsec peer. Note that both peer gateways must be configured to use the same Proposal.
PFS	Select the DH group to enable PFS (Perfect Forward Security) for IKE mode, then the key generated in phase-2 will be irrelevant with the key in phase-1, which enhance the network security. With None selected, it means PFS is disabled and the key in phase-2 will be generated based on the key in phase-1.
SA Lifetime	Specify IPsec SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related IPsec SA will be deleted.

■ Configuring Client-to-Site VPN

Omada managed gateway supports seven types of client-to-Site VPNs depending on the role of your Omada managed gateway and the protocol that you used:

Configuring the gateway as a VPN server using L2TP

Configuring the gateway as a VPN server using PPTP

Configuring the gateway as a VPN server using IPsec

Configuring the gateway as a VPN server using OpenVPN

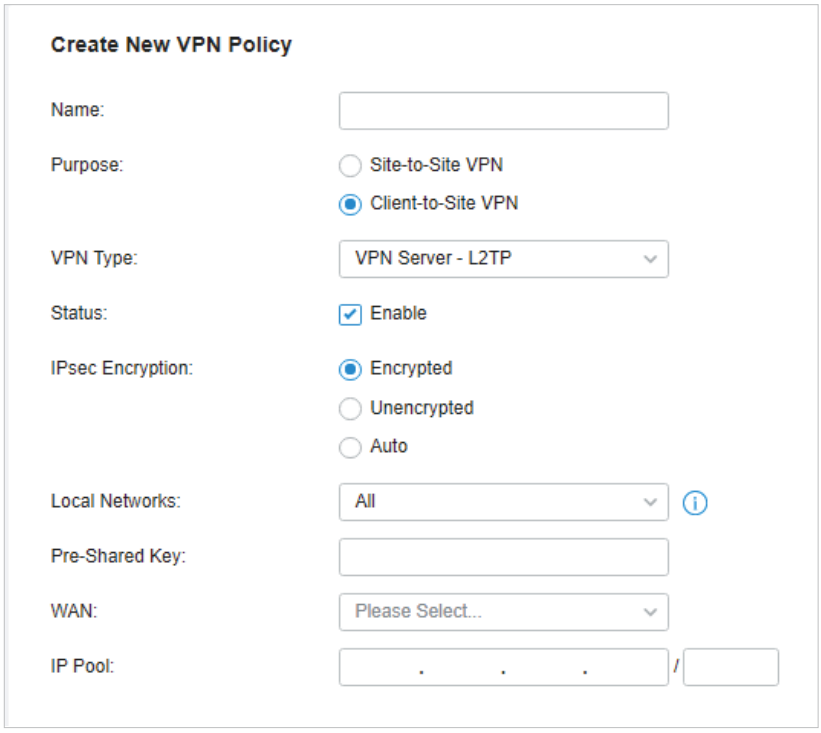
Configuring the gateway as a VPN client using L2TP

Configuring the gateway as a VPN client using PPTP

Configuring the gateway as a VPN client using OpenVPN

- Configuring the gateway as a VPN server using L2TP

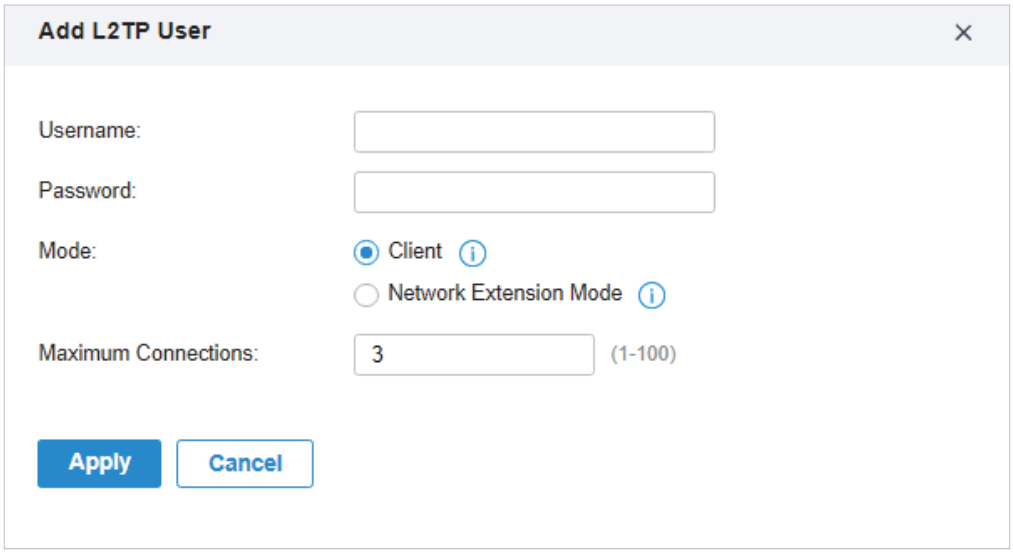
1. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

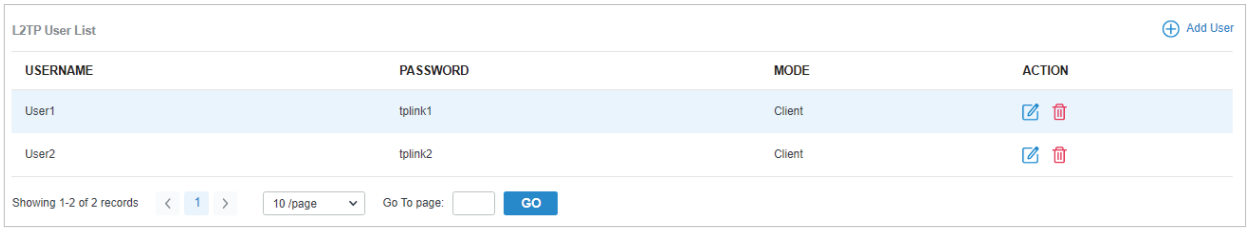
Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - L2TP.
Status	Click the checkbox to enable the VPN policy.
IPsec Encryption	Specify whether to enable the encryption for the tunnel. Encrypted: Select Encrypted to encrypt the L2TP tunnel by IPsec (L2TP over IPsec). With Encrypted selected, enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication. Unencrypted: With Unencrypted selected, the L2TP tunnel will not be encrypted by IPsec. Auto: With Auto selected, the L2TP server will determine whether to encrypt the tunnel according to the client 's encryption settings. And enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication.
Local Networks	Select the networks on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local networks.
Pre-shared Key	Enter the pre-shared secret key when IPsec Encryption is selected as Encrypted and Auto. Both peer routers must use the same pre-shared secret key for authentication.
WAN	Select the WAN port on which the L2TP VPN tunnel is established. Each WAN port supports only one L2TP VPN tunnel when the gateway works as a L2TP server.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.

3. Create the VPN users accounts to validate remote hosts in the L2TP User List. Click ⊕ Add User to load the following page.



Username	Enter the username used for the VPN tunnel. The L2TP client use the username for the validation before accessing the network.
Password	Enter the password of user. The L2TP client use the password for the validation before accessing the network.
Mode	Specify the connection mode for the L2TP users. Client: This mode allows the client to request for an IP address and the server supplies the IP addresses from the VPN IP Pool. With this mode selected, set maximum number of concurrent VPN connections with the same account in Maximum Connections. Network Extension Mode: This mode allows only clients from the configured subnet to connect to the server and obtain VPN services. With this mode selected, specify the subnet in Remote Subnets.
Maximum Connections	With Client mode selected, set maximum number of concurrent VPN connections with the same account.
Remote Subnets	With Network Extension Mode selected, only clients from the configured subnet are allowed to connect to the server and obtain VPN services. Click ⊕ Add Subnet to specify the subnet.

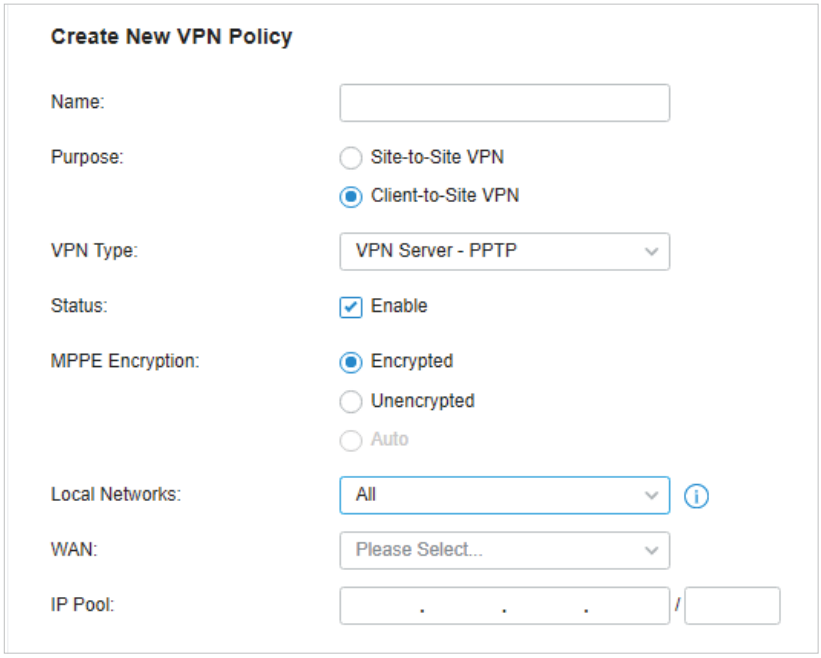
To edit or delete the L2TP users, click the icon in the Action column.



	View and edit the account information of users.
	Delete the L2TP user.

- Configuring the gateway as a VPN server using PPTP

1. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.

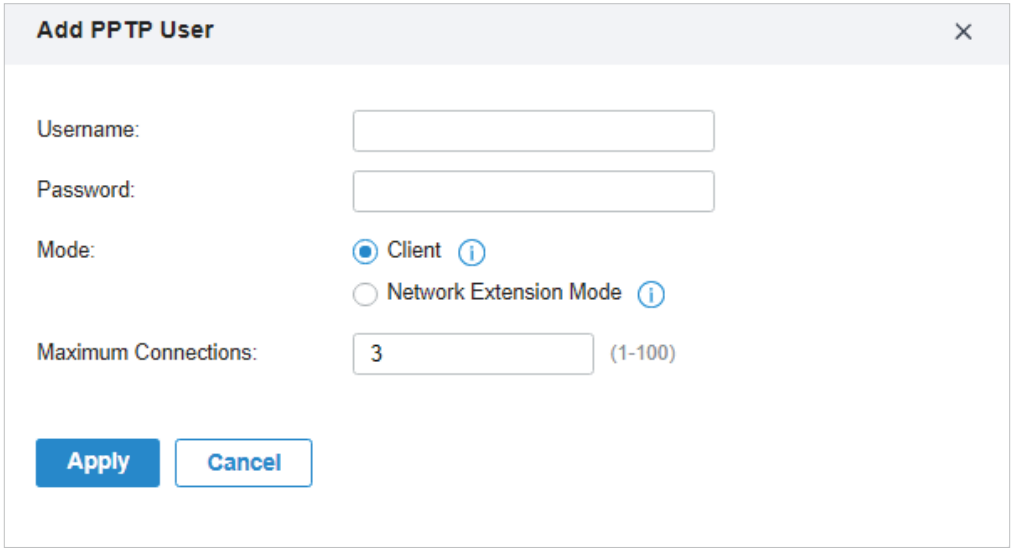


2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - PPTP.
Status	Click the checkbox to enable the VPN policy.

MPPE Encryption	Specify whether to enable MPPE (Microsoft Point-to-Point Encryption) for the tunnel. Encrypted: With Encrypted selected, the PPTP tunnel will be encrypted by MPPE. Unencrypted: With Unencrypted selected, the PPTP tunnel will be not encrypted by MPPE.
Local Networks	Select the networks on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local networks.
WAN	Select the WAN port on which the PPTP VPN tunnel is established. Each WAN port supports only one PPTP VPN tunnel when the gateway works as a PPTP server.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.

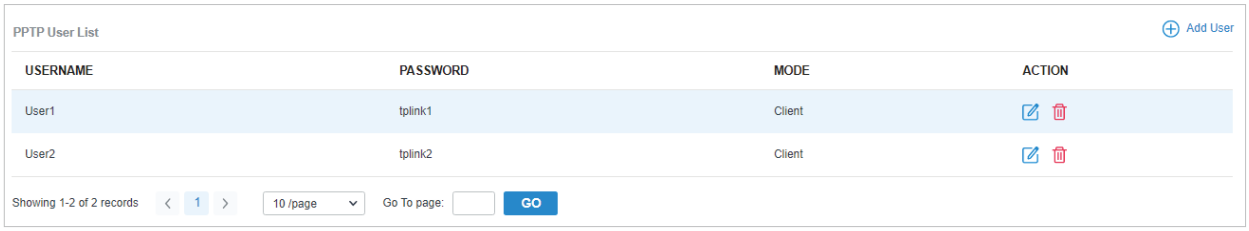
3. Create the VPN users accounts to validate remote hosts in the PPTP User List. Click ⊕ Add User to load the following page.



Username	Enter the username used for the VPN tunnel. The PPTP client use the username for the validation before accessing the network.
Password	Enter the password of user. The PPTP client use the password for the validation before accessing the network.
Mode	Specify the connection mode for the PPTP users. Client: This mode allows the client to request for an IP address and the server supplies the IP addresses from the VPN IP Pool. With this mode selected, set maximum number of concurrent VPN connections with the same account in Maximum Connections. Network Extension Mode: This mode allows only clients from the configured subnet to connect to the server and obtain VPN services. With this mode selected, specify the subnet in Remote Subnets.

Maximum Connections	With Client mode selected, set maximum number of concurrent VPN connections with the same account.
Remote Subnets	With Network Extension Mode selected, only clients from the configured subnet are allowed to connect to the server and obtain VPN services. Click ⊕ Add Subnet to specify the subnet..

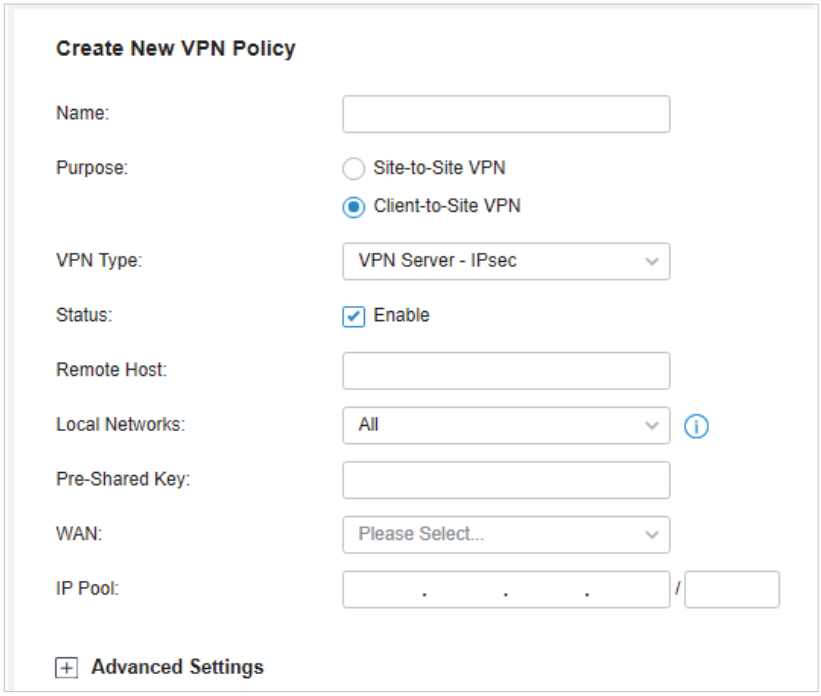
To edit or delete the PPTP users, click the icon in the Action column.



	View and edit the account information of users.
	Delete the PPTP user.

- Configuring the gateway as a VPN server using IPsec

1. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.

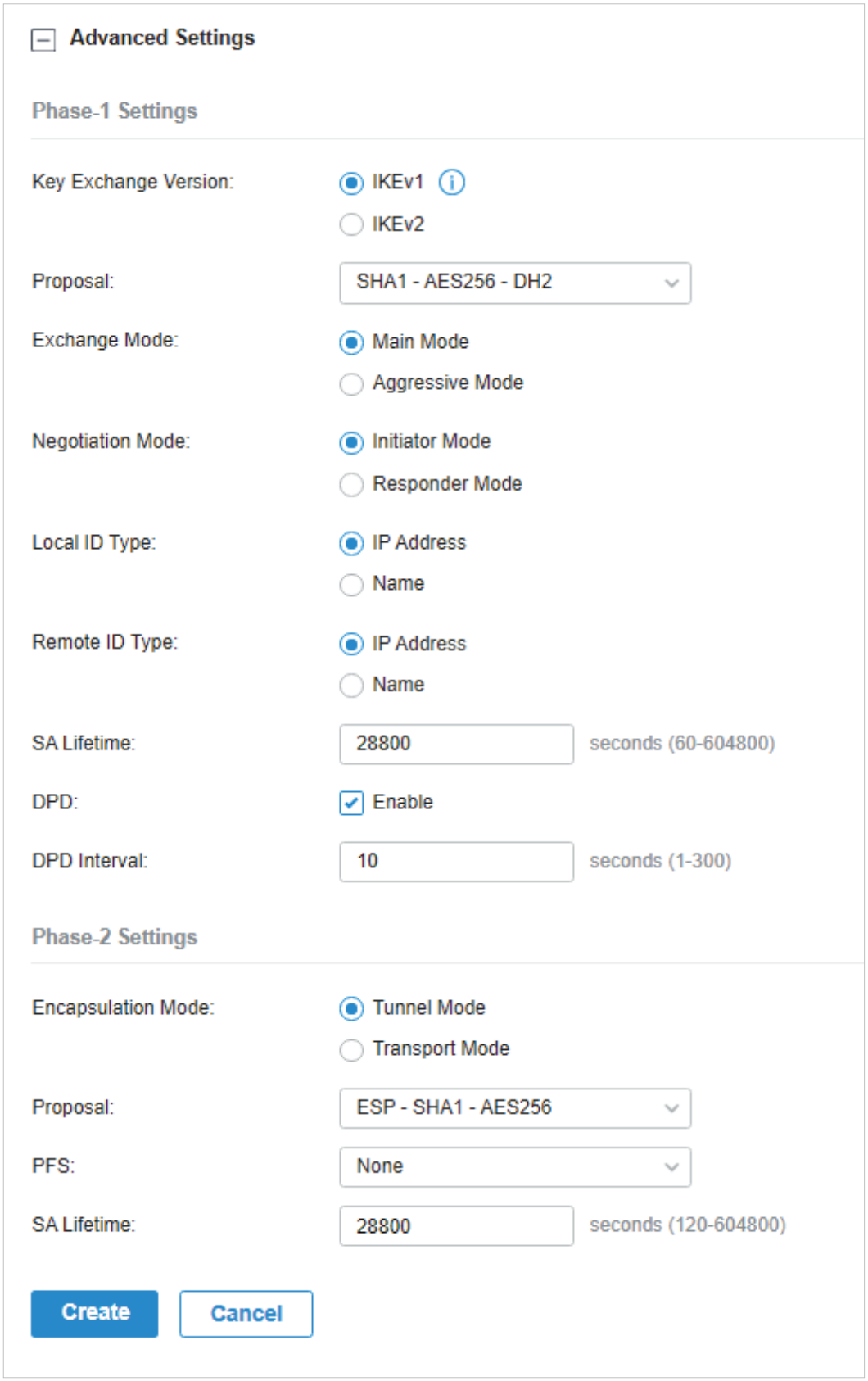


2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the basic parameters and click Create.

Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.

VPN Type	Select the VPN type as VPN Server - IPsec.
Status	Click the checkbox to enable the VPN policy.
Remote Host	Enter an IP address or a domain name of the host on the remote peer of the VPN tunnel. 0.0.0.0 represents any IP address.
Local Networks	Select the networks on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local networks.
Pre-Shared Key	Enter the pre-shared key(PSK). Both peer gateways must use the same pre-shared secret key for authentication. A pre-shared key is a string of characters that is used as an authentication key. Both VPN peers create a hash value based on the same pre-shared key and other information. The hash values are then exchanged and verified to authenticate the other party. The pre-shared keys should be long and random for security. Short or predictable pre-shared keys can be easily broken in brute-force attacks. To maintain a high level of security, administrators are recommended to update the pre-shared key periodically.
WAN	Select the WAN port on which the IPsec VPN tunnel is established.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.

3. Click Advanced Settings to load the following page.



Advanced settings include Phase-1 settings and Phase-2 settings. Phase-1 is used to set up a secure encrypted channel which the two peers can negotiate Phase-2, and then establish the IKE Security Associations (IKE SA). Phase-2 is used to negotiate about a set of parameters that

define what traffic can go through the VPN, and how to encrypt and authenticate the traffic, then establish the IPsec Security Associations (IPsec SA).

Refer to the following table to complete the configurations according to your actual needs and click Create.

For Phase-1 Settings:

Phase-1 Settings	The IKE version you select determines the available Phase-1 settings and defines the negotiation process . Both VPN gateways must be configured to use the same IKE version and Phase-1 settings.
Internet Key Exchange Version	Select the version of Internet Key Exchange (IKE) protocol which is used to set up security associations for IPsec. Both IKEv1 and IKEv2 are supported with Omada managed gateways, but IKEv1 is available only when the VPN policy is applied to a single Remote Subnet and a single Local Network. Note that both VPN peers must be configured to use the same IKE version.
Proposal	Specify the proposal for IKE negotiation phase-1. An IKE proposal lists the encryption algorithm, authentication algorithm and Diffie-Hellman (DH) groups to be negotiated with the remote IPsec peer— Authentication algorithms verify the data integrity and authenticity of a message. The types of authentication includes MD5 and SHA1. Encryption algorithms protect the data from being read by a third-party. The types of encryption algorithm includes DES, 3DES, AES128, AES192, and AES256. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. The DH group includes DH1, DH2, DH5, DH14, DH15, DH16, DH19, DH20, DH21, DH25, and DH26. Note that both VPN peers must be configured to use the same Proposal.
Exchange Mode	Specify the IKE Exchange Mode when IKEv1 is selected. Main Mode: This mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection. Aggressive Mode: This mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.
Negotiation Mode	Specify the IKE Negotiation Mode as Initiator Mode or Responder Mode. Initiator Mode: This mode means that the local device initiates a connection to the peer. Responder Mode: This mode means that the local device waits for the connection request initiated by the peer.

Local ID Type	Specify the type of Local ID which indicates the authentication identifier sent to the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Local ID field to use the name as the ID for authentication. Note that the type and value of Local ID should be the same as Remote ID given for the remote peer of the VPN tunnel.
Local ID	When the Local ID Type is configured as Name, enter a name for the local device as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
Remote ID Type	Specify the type of Remote ID which indicates the authentication identifier received from the peer for IKE negotiation. IP Address: Select IP Address to use the IP address for authentication. Name: Select Name, and then enter the name in the Remote ID field to use the name as the ID for authentication. Note that the type and value of Remote ID should be the same as Local ID given for the remote peer of the VPN tunnel.
Remote ID	When the Remote ID Type is configured as Name, enter a name of the remote peer as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
SA Lifetime	Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.
DPD	Check the box to enable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.
DPD Interval	Specify the interval between sending DPD requests with DPD enabled. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA.

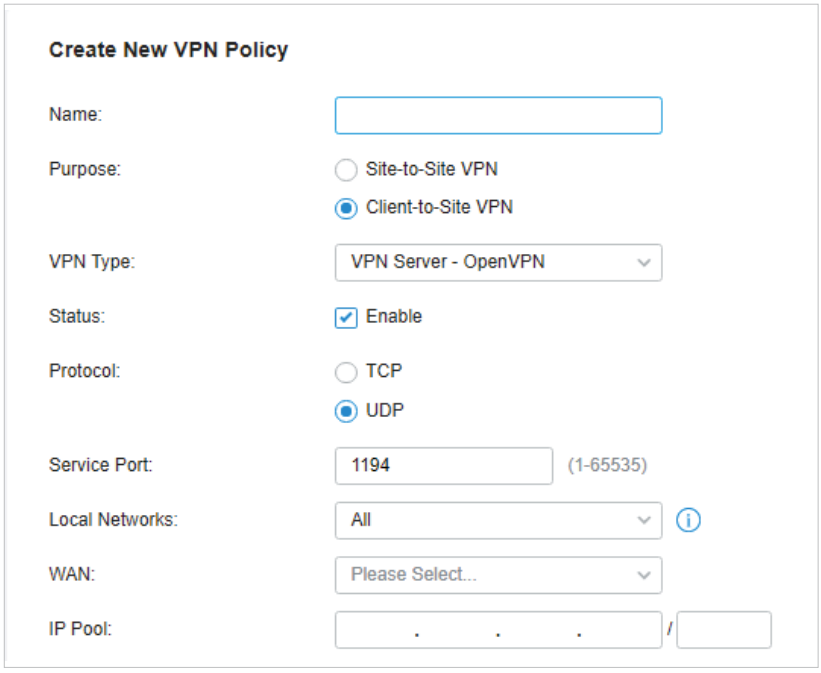
For Phase-2 Settings:

Phase-2 Settings	The purpose of Phase 2 negotiations is to establish the Phase-2 SA (also called the IPsec SA). The IPsec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic.
Encapsulation Mode	Specify the Encapsulation Mode as Tunnel Mode or Transport Mode. When both ends of the tunnel are hosts, either mode can be chosen. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, Tunnel Mode is recommended to ensure safety.

Proposal	Specify the proposal for IKE negotiation phase-2. An IPsec proposal lists the encryption algorithm, authentication algorithm and protocol to be negotiated with the remote IPsec peer. Note that both peer gateways must be configured to use the same Proposal.
PFS	Select the DH group to enable PFS (Perfect Forward Security) for IKE mode, then the key generated in phase-2 will be irrelevant with the key in phase-1, which enhance the network security. With None selected, it means PFS is disabled and the key in phase-2 will be generated based on the key in phase-1.
SA Lifetime	Specify IPsec SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related IPsec SA will be deleted.

- Configuring the gateway as a VPN server using OpenVPN

1. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.

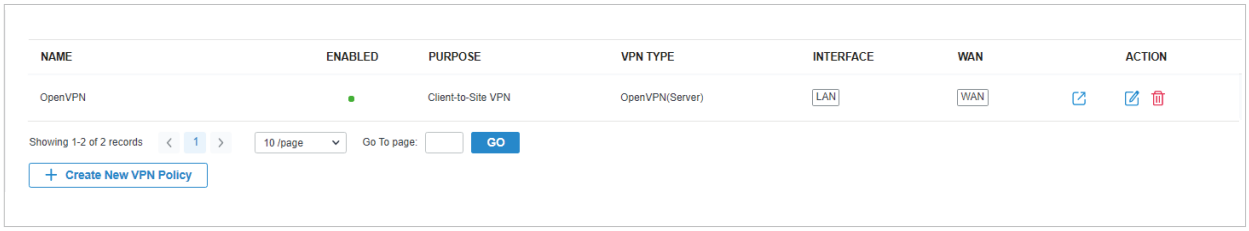


2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - OpenVPN.
Status	Click the checkbox to enable the VPN policy.
Protocol	Select the communication protocol for the gateway which works as an OpenVPN Server. Two communication protocols are available: TCP and UDP.
Service Port	Enter a VPN service port to which a VPN device connects.

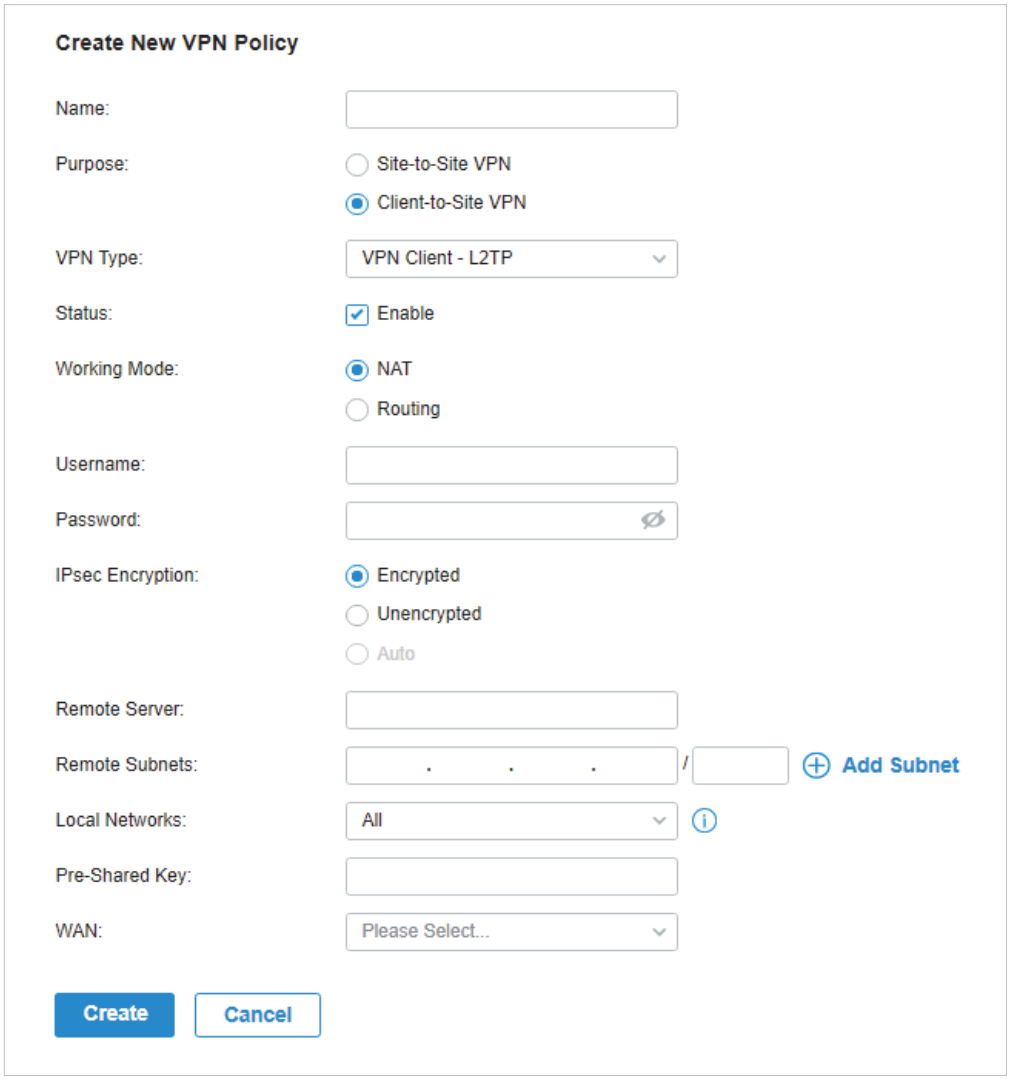
Local Networks	Select the networks on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local networks.
WAN	Select the WAN port on which the VPN tunnel is established. Each WAN port supports only one OpenVPN tunnel when the gateway works as a OpenVPN server.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router.

3. After clicking Create to save the VPN policy, go to VPN Policy List and click in the Action column to export the OpenVPN file that ends in .ovpn which is to be used by the remote client. The exported OpenVPN file contains the certificate and configuration information.



- Configuring the gateway as a VPN client using L2TP

1. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



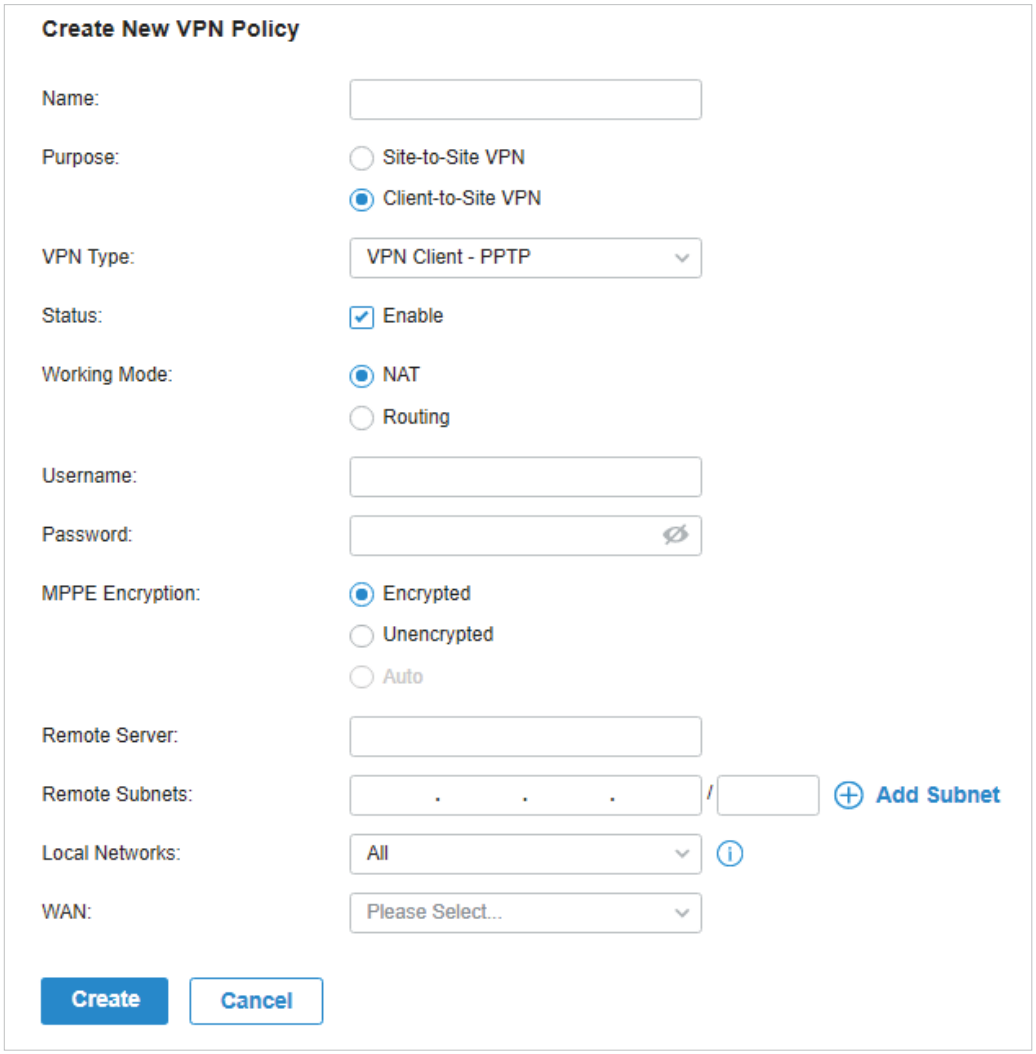
2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Client - L2TP.
Status	Click the checkbox to enable the VPN policy.
Working Mode	Specify the Working Mode as NAT or Routing. NAT: With NAT (Network Address Translation) mode selected, the L2TP client uses the assigned IP address as its source addresses of original IP header when forwarding L2TP packets. Routing: With Routing selected, the L2TP client uses its own IP address as its source addresses of original IP header when forwarding L2TP packets.

Username	Enter the username used for the VPN tunnel. This username should be the same as that of the L2TP server.
Password	Enter the password of user. This password should be the same as that of the L2TP server.
IPsec Encryption	Specify whether to enable the encryption for the tunnel. Encrypted: Select Encrypted to encrypt the L2TP tunnel by IPsec (L2TP over IPsec). With Encrypted selected, enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication. Unencrypted: With Unencrypted selected, the L2TP tunnel will be not encrypted by IPsec.
Remote Server	Enter the IP address or domain name of the L2TP server.
Remote Subnets	Enter the IP address and subnet mask to specify the remote network. It's always the IP address range of LAN on the remote peer of the VPN tunnel.
Local Networks	Select the networks on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local networks.
Pre-shared Key	Enter the pre-shared secret key when the L2TP tunnel is encrypted by IPsec. Both peer gateways must use the same pre-shared secret key for authentication.
WAN	Select the WAN port on which the VPN tunnel is established.

- Configuring the gateway as a VPN client using PPTP

1. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



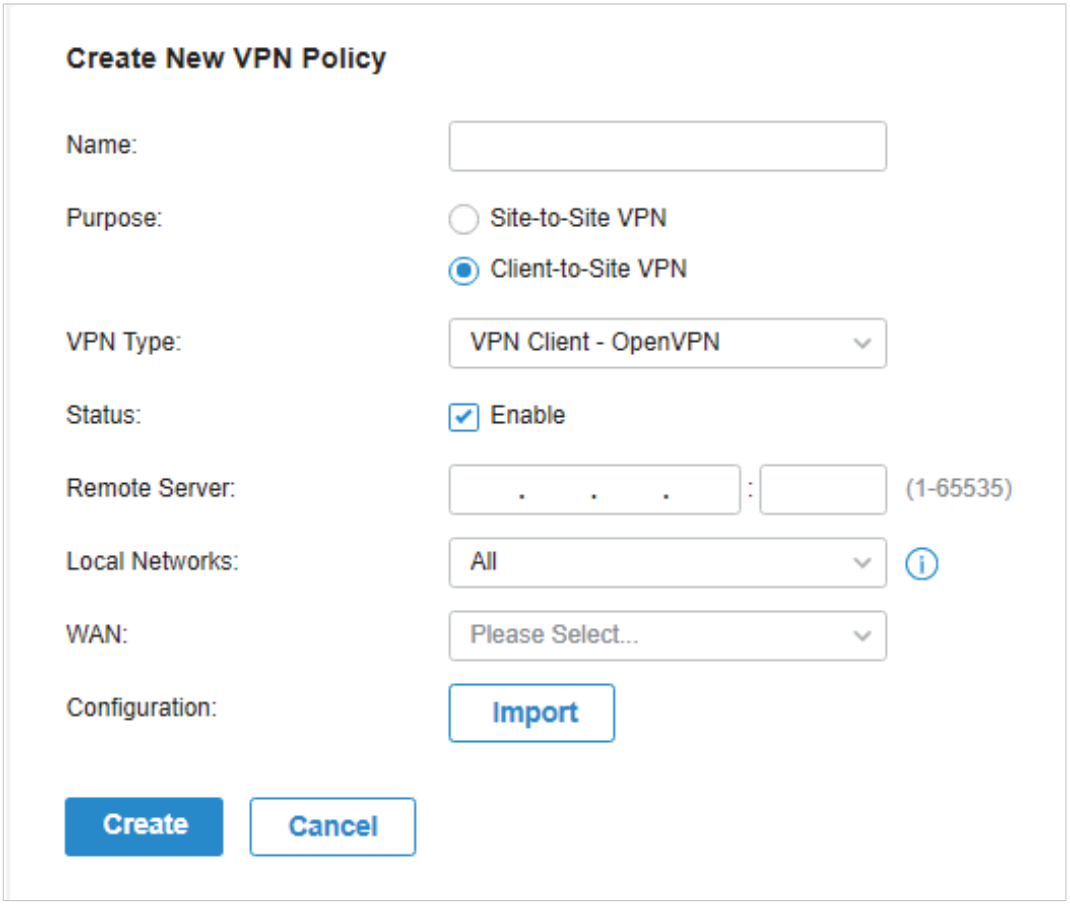
2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Client - PPTP.
Status	Click the checkbox to enable the VPN policy.
Working Mode	Specify the Working Mode as NAT or Routing. NAT: With NAT (Network Address Translation) mode selected, the PPTP client uses the assigned IP address as its source addresses of original IP header when forwarding PPTP packets. Routing: With Routing selected, the PPTP client uses its own IP address as its source addresses of original IP header when forwarding PPTP packets.

Username	Enter the username used for the VPN tunnel. This username should be the same as that of the PPTP server.
Password	Enter the password of user. This password should be the same as that of the PPTP server.
MPPE Encryption	Specify whether to enable the encryption for the tunnel. Encrypted: Select Encrypted to encrypt the PPTP tunnel by MPPE. Unencrypted: With Unencrypted selected, the PPTP tunnel will be not encrypted by MPPE.
Remote Server	Enter the IP address or domain name of the PPTP server.
Remote Subnets	Enter the IP address and subnet mask to specify the remote network. It's always the IP address range of LAN on the remote peer of the VPN tunnel.
Local Networks	Select the networks on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local networks.
WAN	Select the WAN port on which the VPN tunnel is established.

- Configuring the gateway as a VPN client using OpenVPN

1. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

Name	Enter a name to identify the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Client - OpenVPN.
Status	Click the checkbox to enable the VPN policy.
Remote Server	Enter the IP address or domain name of the OpenVPN server.
Local Networks	Select the networks on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local networks.
WAN	Select the WAN port on which the VPN tunnel is established.
Configuration	Click Import to import the OpenVPN file that ends in .ovpn generated by the OpenVPN server. Only one file can be imported. If the certificate file and configuration file are generated singly by the OpenVPN server, combine two files and import the whole file.

4. 8 Create Profiles

Profiles section is used to configure and record your custom settings for site configurations. It includes Time Range and Groups profiles. In Time Range section, you can configure time templates for wireless schedule, PoE schedule, etc. In Groups section, you can configure groups based on IP, IP-Port and MAC addresses for ACL, Routing, NAT, etc. After creating the profiles, you can apply them to multiply configurations for different sites, saving you from repeatedly setting up the same information.

4. 8. 1 Time Range

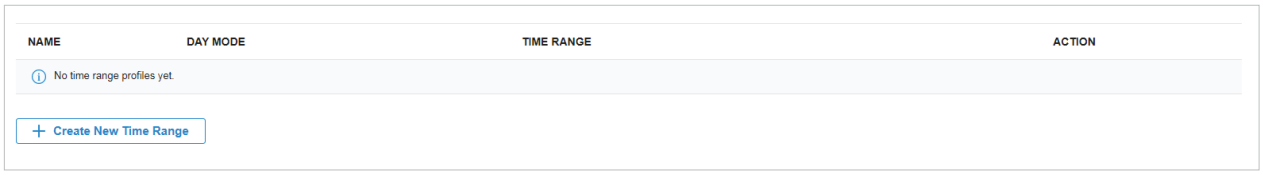
Overview

Time Range section allows you to customize time-related configurations. You can set different time range templates which can be shared and applied to wireless schedule, PoE schedule, etc. in site configuration.

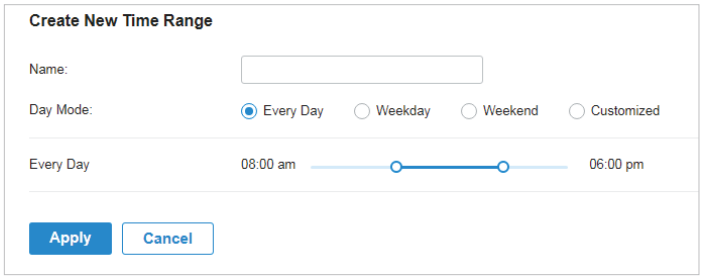
Configuration

To configure the time range profiles, follow these steps:

3. Go to Settings > Profiles >Time Range. Click +Create New Time Range to add a new time range entry. By default, there is no entry in the list.



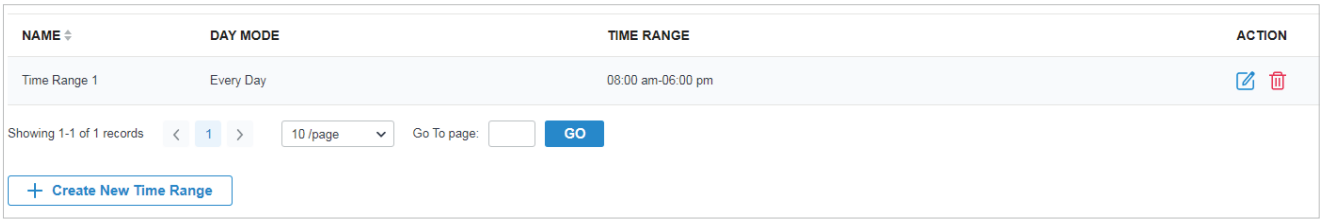
4. Enter a Name for the new entry, select the Day Mode, and specify the time range. Click Apply to save the entry. After saving the newly added entry, you can apply them to site configuration. To apply the customized time range profiles in configuration, refer to WLAN Schedule, and PoE Schedule.



Name	Enter a name for the new entry, and it is a string with 1 to 64 ASCII symbols.

Day Mode	Select Every Day, Weekday, Weekend, or Customized first before specifying the time range for each day. Every Day: You only need to set the time range once, and it will repeat every day. Weekday: You only need to set the time range once, and it will repeat every weekday from Monday to Friday. Weekend: You only need to set the time range once, and it will repeat every Saturday and Sunday. Customized: You are able to set different time range for the chosen day(s) based on your needs. When a day is not chosen, the WiFi is open all day by default.

You can view the name, day mode and time range in the list.



To edit or delete the time range entry, click the icon in the Action column.

	Edit the parameters in the entry.
	Delete the entry.

4. 8. 2 Groups

Overview

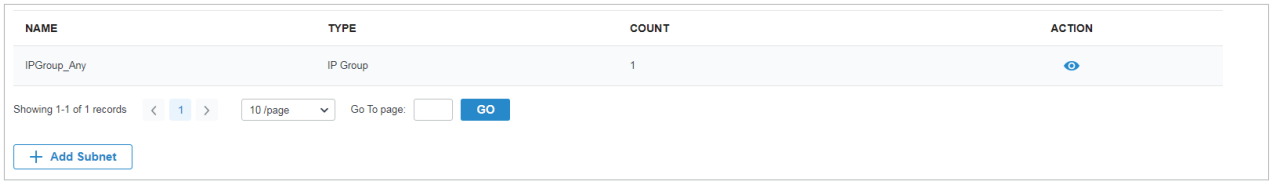
Groups section allows you to customize client groups based on IP, IP-Port, or MAC Address. You can set different rules for the groups profiles which can be shared and applied to ACL, Routing, NAT, etc. in site configuration.

Configuration

To configure the group profiles, follow these steps:

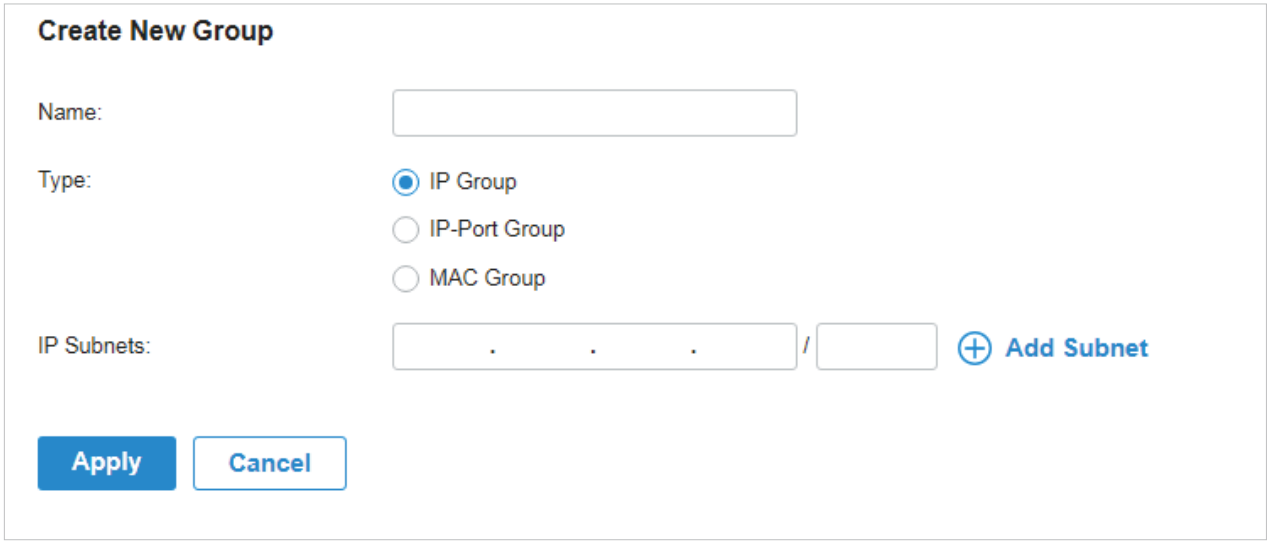
Add a New Group | Configure Group Profiles | Apply

1. Go to Settings > Profiles > Groups. By default, there is an entry covering all IPs, and it is not editable and deletable. Click +Add Subnet to add a new group entry.



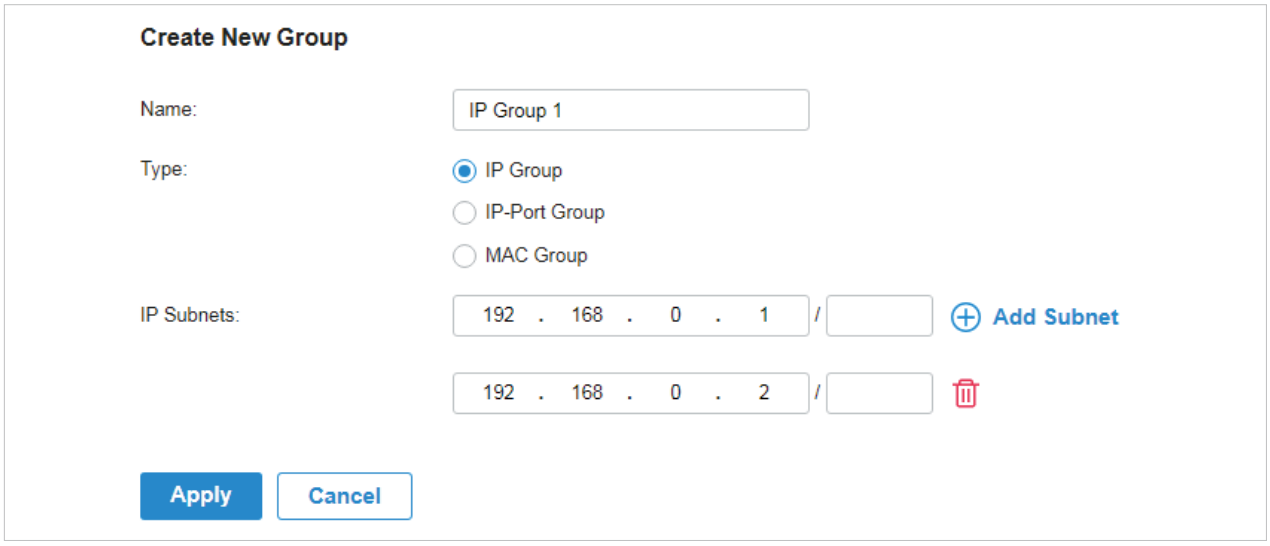
Add a New Group | Configure Group Profiles | Apply

2. Enter a name for the new group profile entry, and select the type for the new entry.



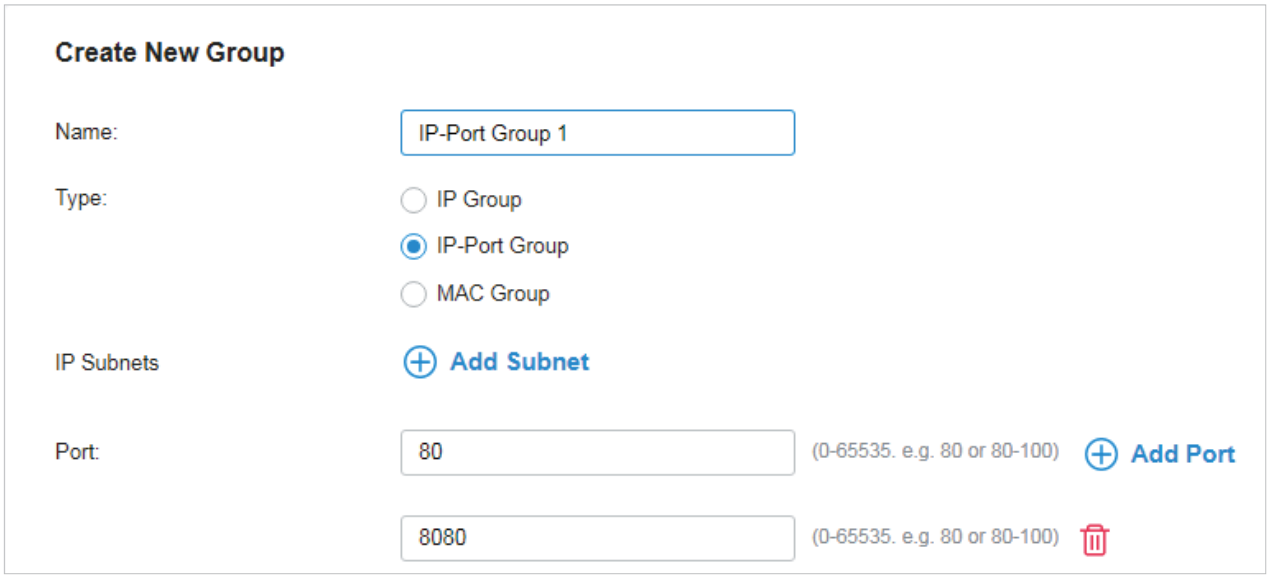
- **Based on IP Group**

  To configure a group profile based on IP Group, you are required to specify the IP subnets, while subnet mask is optional. You can click +Add Subnet to add new subnets, and click to delete them.



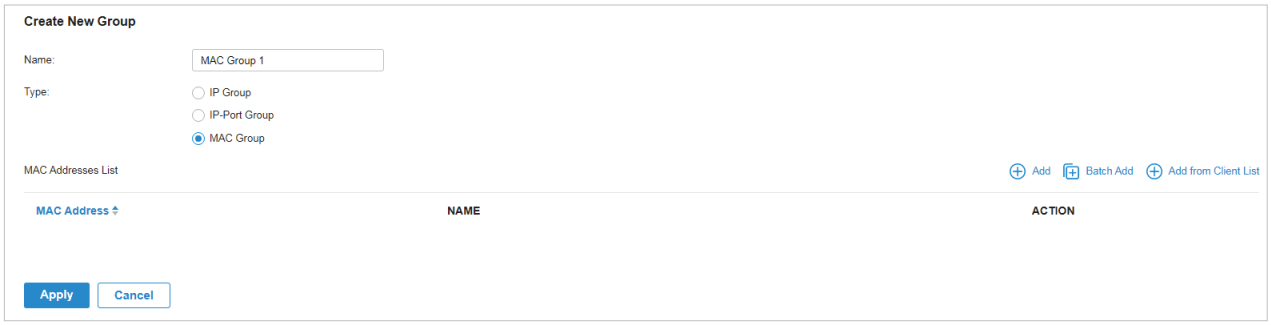
- **Based on IP-Port Group**

  To configure a group profile based on IP-Port Group, you are required to specify the port(s) for the entry, while it is optional to specify the IP subnet(s). If you only specify the port(s) without entering any IP subnet, it means the group contains the specified port(s) for all IPs. You can click +Add Subnet to add new IP subnets, click +Add Port to add ports, and click to delete them.



Based on MAC Group

To configure a group profile based on MAC Group, you are required to enter MAC Address(es) in the MAC Addresses List. There are three ways to add MAC address(es) to the MAC Addresses List.



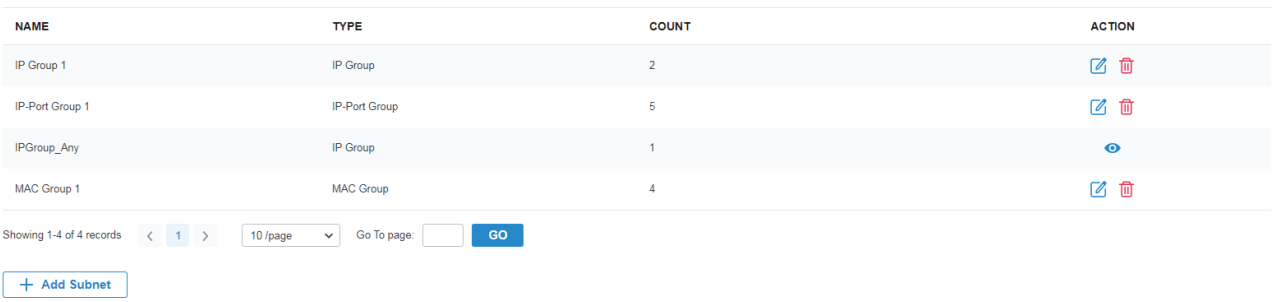
Add	Add MAC address singly.
Batch Add	Add MAC addresses in batches. You can enter the MAC addresses and names in the input box or import them with files in the format of Excel, txt, and text. If you want to use the newly added MAC address(es) and names when they conflict with the existing ones, click the to allow it to override the curent MAC Access Control List. Note: 1. Each MAC address and name should be entered on a new line. The MAC address and name should be separated by a space. 2. Octets in a MAC address should be separated by a hyphen. For example, AA-BB-CC-DD-EE-FF.
Add from Client List	Add MAC addresses from the clients that are connected to the devices controlled by the Omada SDN Controller.

Add a New Group > Configure Group Profiles Based on Type > Apply

3. Click Apply to save the entry.

   After saving the newly added entry, you can apply them to site configuration. To apply the customized profiles in configuration, refer to ACL, Routing, NAT.

You can view the name, type, and count in the list.



To view, edit or delete the group entry, click the icon in the Action column.

	View and edit the parameters in the entry. You cannot change the type when editing the entry.
	Delete the entry.

4. 9 Authentication

Authentication is a portfolio of features designed to authorize network access to clients, which enhances the network security. Authentication sevices include Portal, 802.1X and MAC-Based Authentication, covering all the needs to authenticate both wired and wireless clients.

4. 9. 1 Portal

Overview

Portal authentication provides convenient authentication services to the clients that only need temporary access to the network, such as the customers in a restaurant or in a supermarket. To access the network, these clients need to enter the authentication login page and use the correct login information to pass the authentication. In addition, you can customize the authentication login page and specify a URL which the authenticated clients will be redirected to.

Portal authentication can work with Pre-Authentication and Authentication-Free Policy, which grant specific network access to the users with valid identities. Pre-Authentication policies allow unauthenticated clients to access the specific network resources. Authentication-Free policies allow the specific clients to access the specific network resources without authentication.

Portal authentication takes effect on SSIDs and LAN networks. EAPs authenticate wireless clients which connect to the SSID with Portal configured, and the gateway authenticates wired clients which connect to the network with Portal configured. To make Portal authentication available for wired and wireless clients, ensure that both the gateway and EAPs are connected and working properly.

The controller provides six types of Portal authentication:

- **No Authentication**

  With this authentication type configured, clients can pass the authentication and access the network without providing any login information. Clients just need to accept the terms (if configured) and click the Login button.

- **Simple Password**

  With this authentication type configured, clients are required to enter the correct password to pass the authentication. All clients use the same password which is configured in the controller.

- **Hotspot**

  With this authentication type configured, clients can access the network after passing any type of the authentication:

  - **Voucher**

    Clients can use the unique voucher codes generated by the controller within a predefined time usage. Voucher codes can be printed out from the controller, so you can print the codes and distribute them to your costumers to tie the network access to consumption.

- **Local User**

  Clients are required to enter the correct username and password of the login account to pass the authentication.

- **SMS**

  Clients can get verification codes using their mobile phones and enter the received codes to pass the authentication.

- **RADIUS**

  Clients are required to enter the correct username and password which are stored in the RADIUS server to pass the authentication.

- **External RADIUS Server**

  Clients are required to enter the correct username and password created on the RADIUS server to pass the authentication.

- **External Portal Server**

  The option of External Portal Server is designed for the developers. They can customize their own authentication type like Google account authentication according to the interface provided by Omada Controller.

- **Facebook**

  With Facebook Portal configured, when clients connect to your Wi-Fi, they will be redirected to your Facebook page. To access the internet, clients need to log in their account or enter the password code in the Facebook page.

Configuration

To complete the Portal configuration, follow these steps:

5) Click to enable Portal.

6) Select the SSIDs and LAN networks for the portal to take effect on and configure basic parameters including authentication type, authentication timeout and so on.

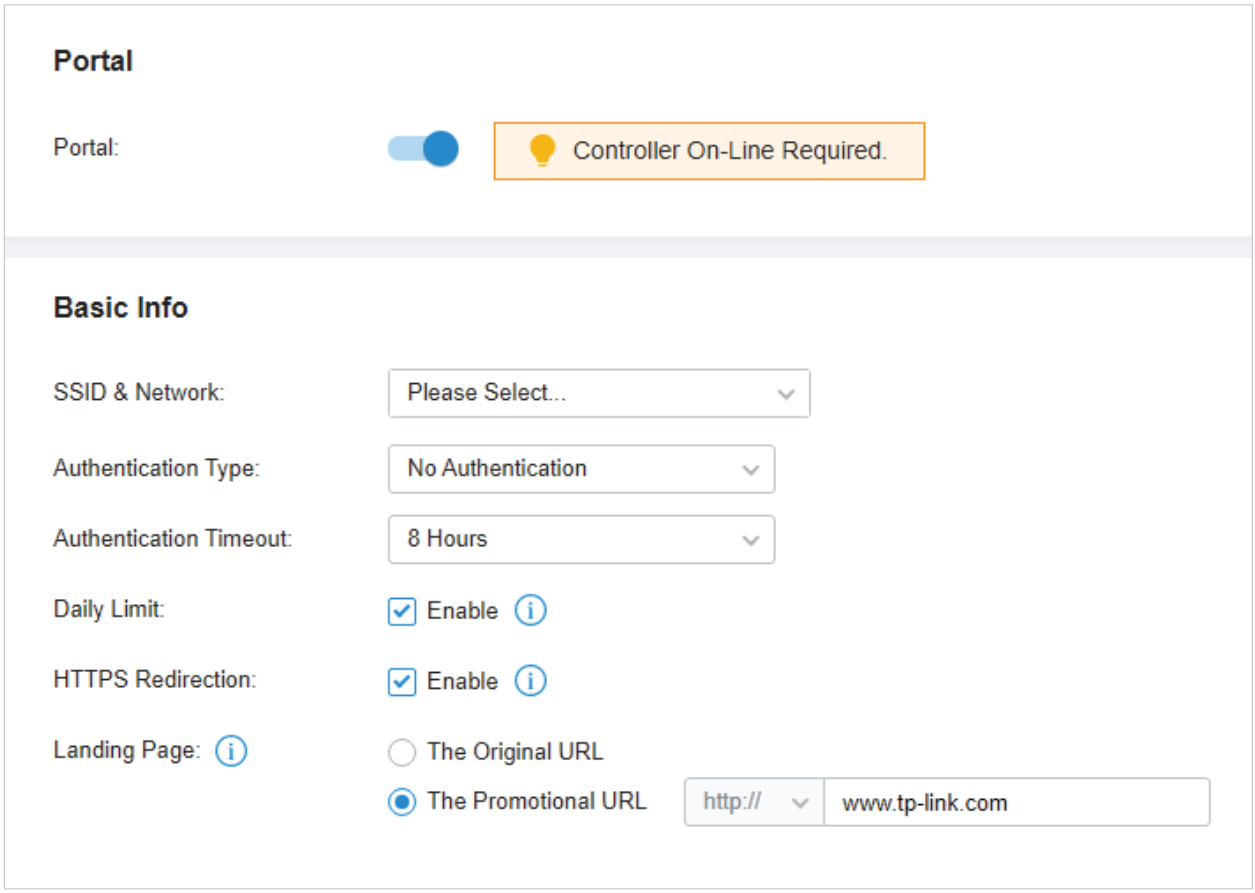
7) Customize the Portal page including the background picture, logo picture and so on.

8) Configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed.

The following part introduces how to configure each type of Portal authentication: No Authentication, Simple Password, Hotspot (Voucher, Local User, SMS, RADIUS), External RADIUS Server, External Portal Server and Facebook.

Configuring Portal with No Authentication

4. Go to Settings > Authentication > Portal. Click to enable Portal and load the following page.

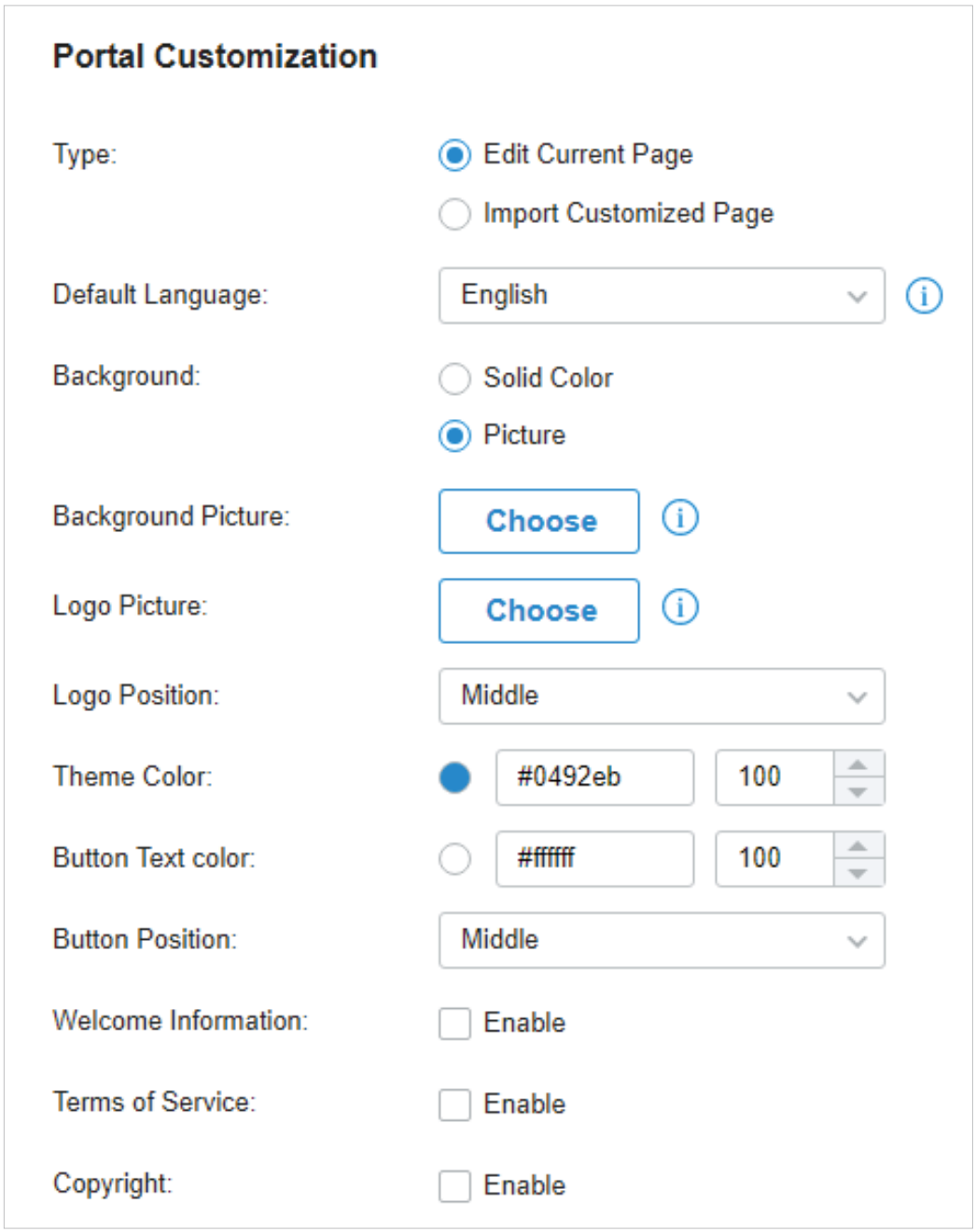


5. Select the SSIDs and LAN networks for the portal to take effect on and configure basic parameters including authentication type, authentication timeout and so on.

SSID & LAN Network	Select one or more SSIDs or LAN networks for the portal. The clients connected to the selected SSIDs or LAN networks have to log into a web page to establish verification before accessing the network.
Authentication Type	Select the type of Portal authentication as No Authentication.
Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.
Daily Limit	Click the checkbox to enable Daily Limit. With this feature enabled, after authentication times out, clients cannot get authenticated again until the next day. With this feature disabled, after authentication times out, clients can get authenticated again without limit.
HTTPS Redirection	Click the checkbox to enable HTTPS Redirection. With this feature enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this feature disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.

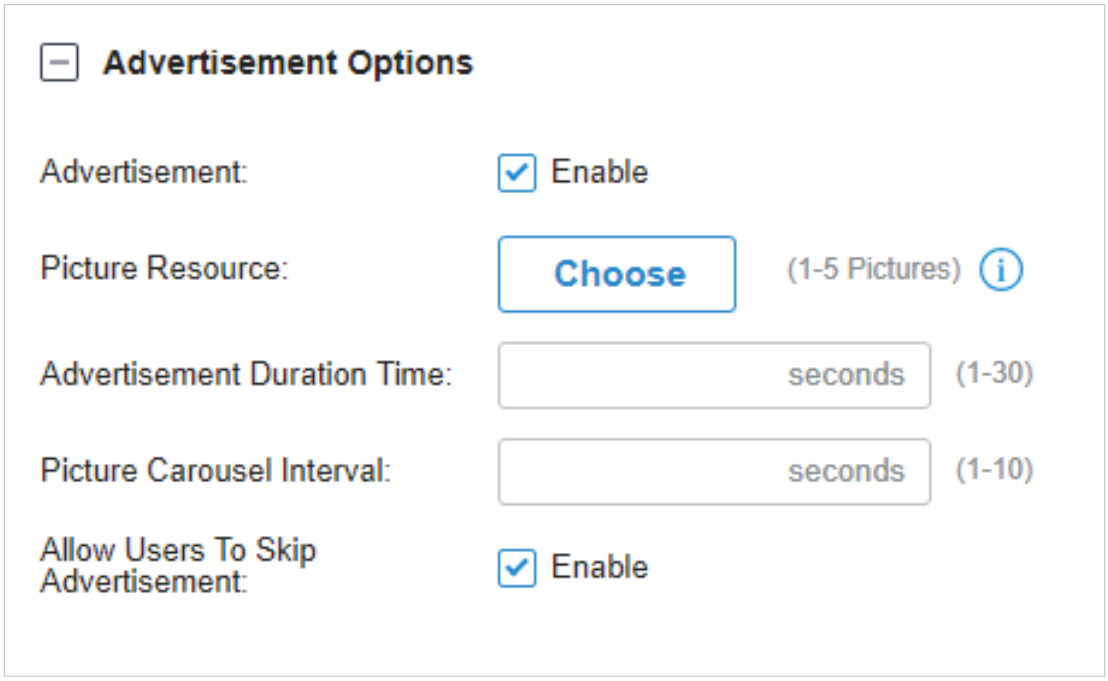
Landing Page	Select which page the client will be redirected to after a successful authentication. The Original URL: Clients are directed to the URL they request for after they pass Portal authentication. The Promotional URL: Clients are directed to the specified URL after they pass Portal authentication.

6. In the Portal Customization section, customize the Portal page including the background picture, logo picture and so on.



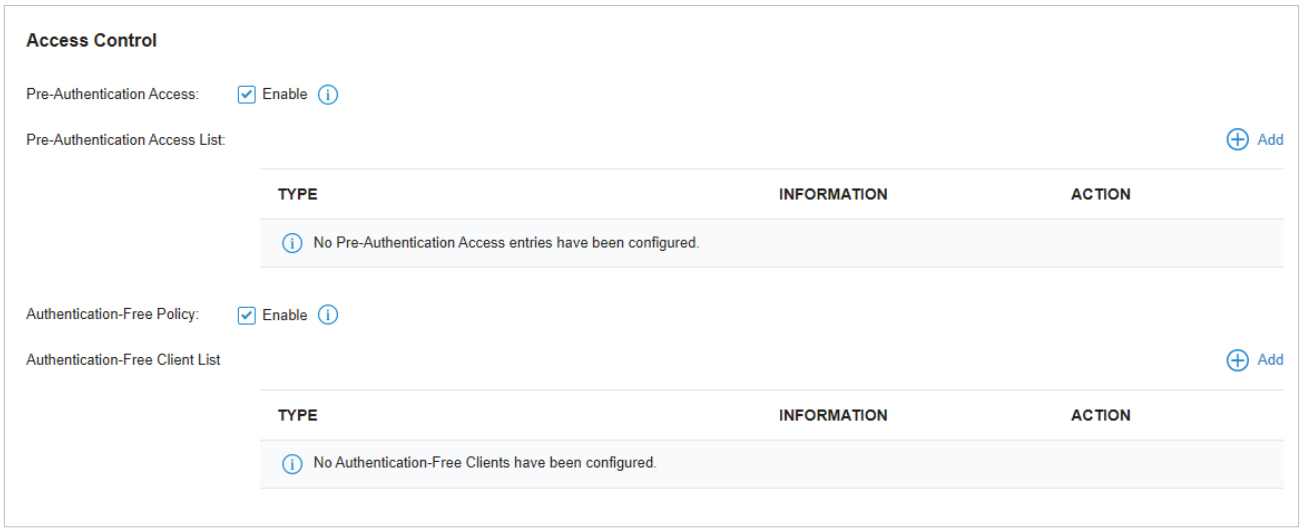
Type	Select the type of the Portal page. Edit Current Page: Edit the related parameters to customize the Portal page based on the provided page. Import Customized Page: Click Import to import your unique Portal page for branding it as per your business.
Default Language	Select the default language displayed on the Portal page. The controller automatically adjusts the language displayed on the Portal page according to the system language of the clients. If the language is not supported, the controller will use the default language specified here.
Background	Select the background type. Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker. Picture: Click Choose and select a picture from your PC as the background.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Position	Select the logo position in the Portal page.
Theme Color	Configure your desired background color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Text Color	Configure your desired text color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Position	Select the button position in the Portal page.
Welcome Information	Click the checkbox and enter text as the welcome information. And you can configure your desired text color for the welcome information by entering the hexadecimal HTML color code manually or through the color picker.
Terms of Service	Click the checkbox and enter text as the terms of service in the following box.
Copyright	Click the checkbox and enter text as the copyright in the following box.

Click Advertisement Options and customize advertisement pictures on the authentication page.



Advertisement	Click the checkbox to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears.
Picture Resource	Click Choose and select pictures from your PC as the advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Enter the duration time for the advertisement pictures. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Enter the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Click the checkbox to allow users to skip the advertisement.

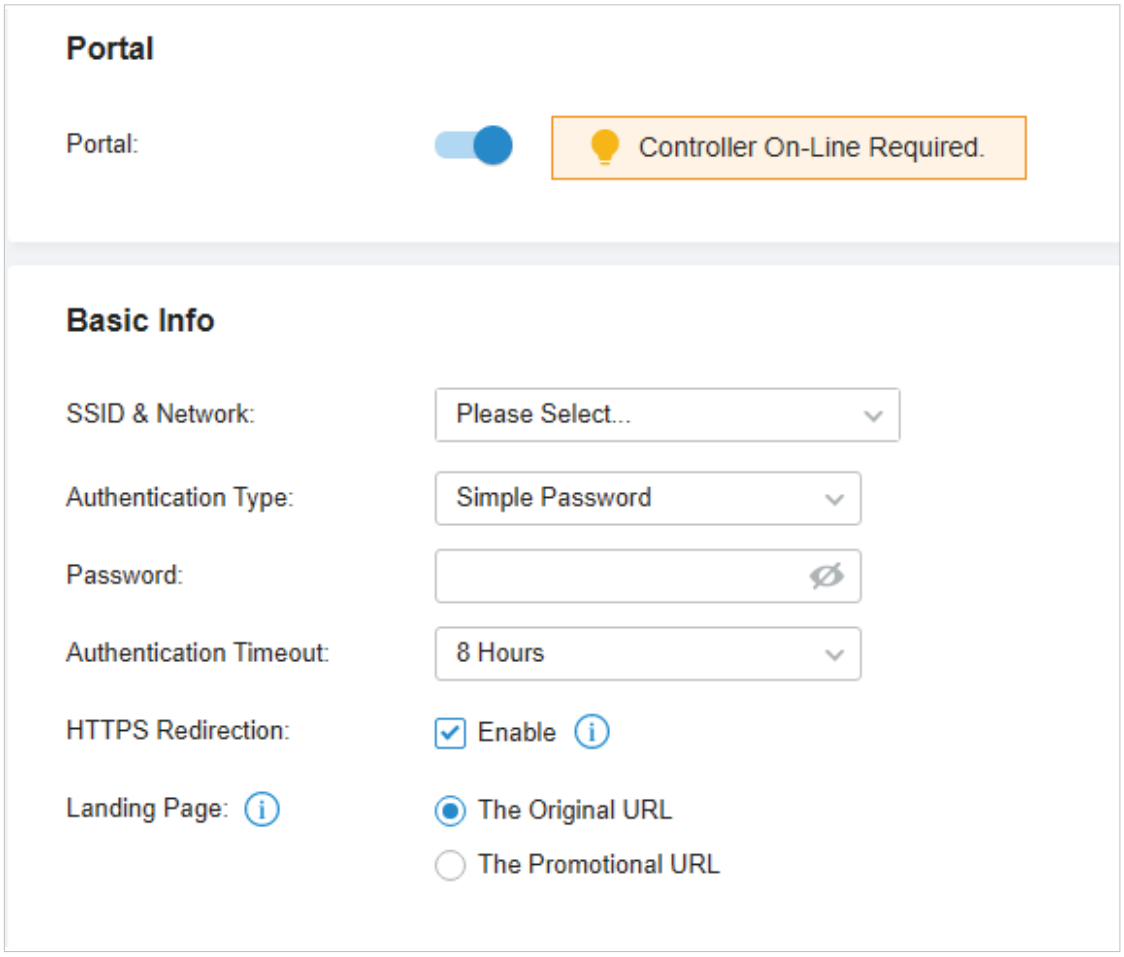
7. In the Access Control section, configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed.



Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click ⊕ Add to configure the IP range or URL which unauthenticated clients are allowed to access.
Authentication-Free Policy	Click the checkbox to enable Authentication-Free Policy. With this feature enabled, you can allow certain clients to access the internet without Portal authentication.
Authentication-Free Client List	Click ⊕ Add and enter the IP address or MAC address of Authentication-Free clients.

Configuring Portal with Simple Password

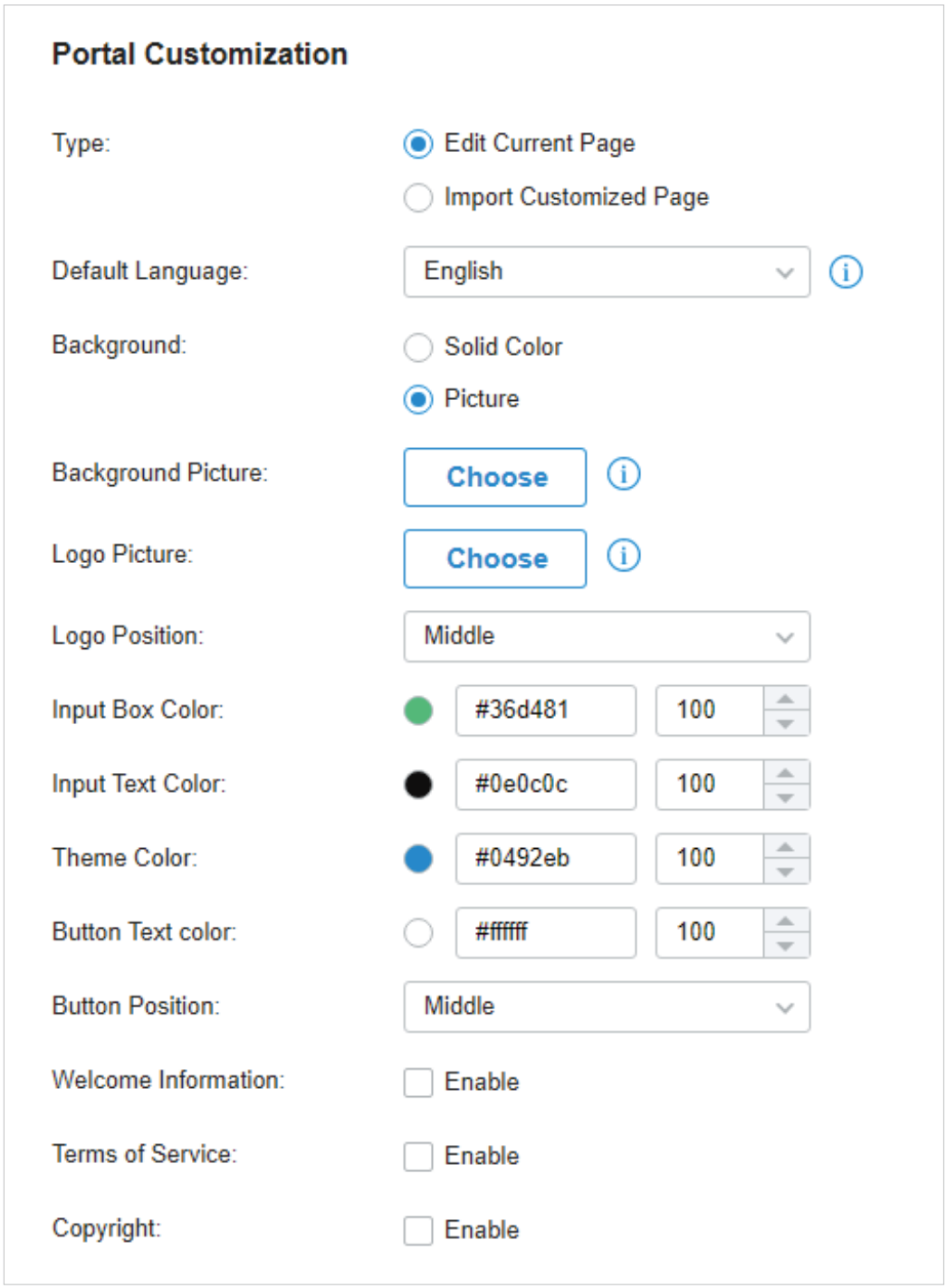
1. Go to Settings > Authentication > Portal. Click to enable Portal and load the following page.



2. Select the SSIDs and LAN networks for the portal to take effect on and configure basic parameters including authentication type, authentication timeout and so on.

SSID & LAN Network	Select one or more SSIDs or LAN networks for the portal. The clients connected to the selected SSIDs or LAN networks have to log into a web page to establish verification before accessing the network.
Authentication Type	Select the type of Portal authentication as Simple Password.
Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.
HTTPS Redirection	Click the checkbox to enable HTTPS Redirection. With this feature enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this feature disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Landing Page	Select which page the client will be redirected to after a successful authentication. The Original URL: Clients are directed to the URL they request for after they pass Portal authentication. The Promotional URL: Clients are directed to the specified URL here after they pass Portal authentication.

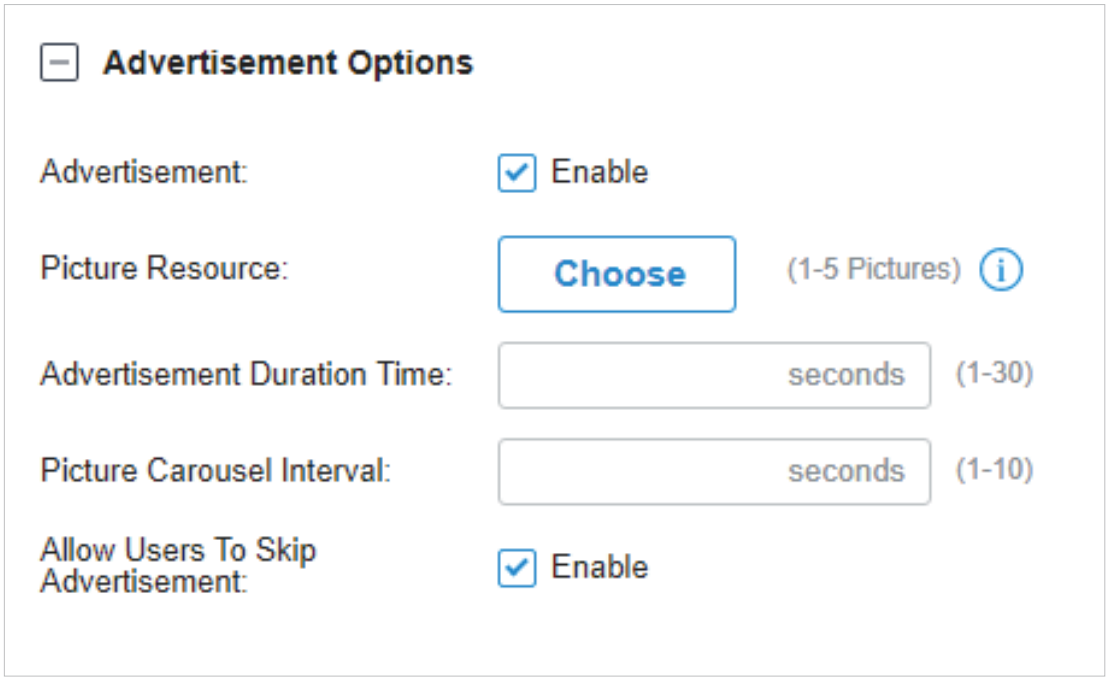
3. In the Portal Customization section, customize the Portal page including the background picture, logo picture and so on.



Type	Select the type of the Portal page. Edit Current Page: Edit the related parameters to customize the portal page based on the provided page. Import Customized Page: Click Import to import your unique Portal page for branding it as per your business.

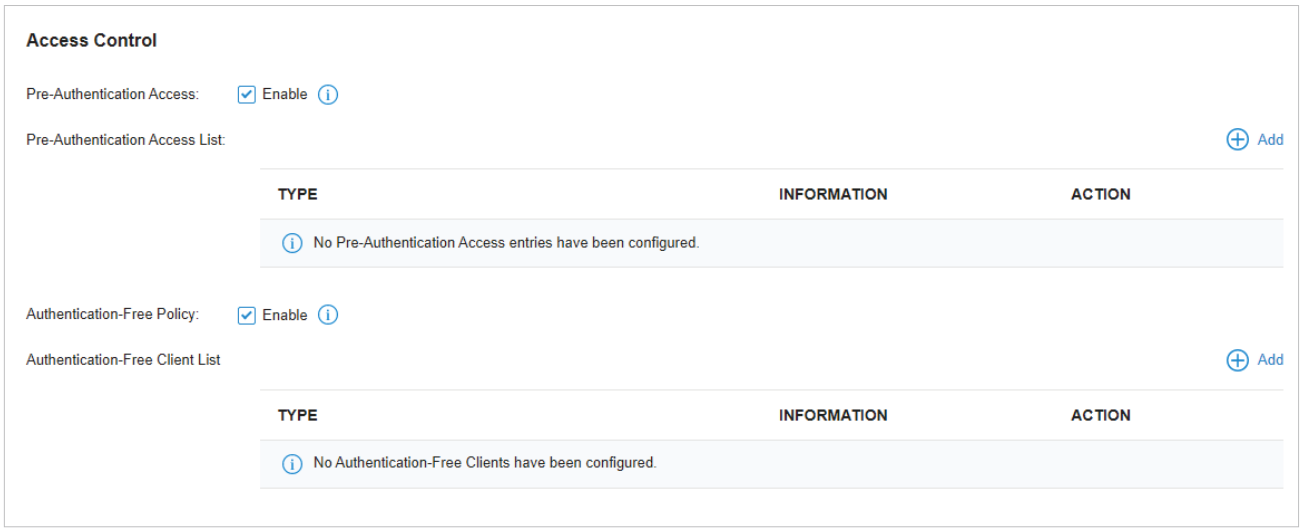
Default Language	Select the default language displayed on the Portal page. The controller automatically adjusts the language displayed on the Portal page according to the system language of the clients. If the language is not supported, the controller will use the default language specified here.
Background	Select the background type. Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker. Picture: Click Choose and select a picture from your PC as the background.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Position	Select the logo position in the Portal page.
Input Box Color	Configure your desired color of the input box for password by entering the hexadecimal HTML color code manually or through the color picker.
Input Text Color	Configure your desired color of the input text for password by entering the hexadecimal HTML color code manually or through the color picker.
Theme Color	Configure your desired background color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Text Color	Configure your desired text color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Position	Select the button position in the Portal page.
Welcome Information	Click the checkbox and enter text as the welcome information. And you can configure your desired text color for the welcome information by entering the hexadecimal HTML color code manually or through the color picker.
Terms of Service	Click the checkbox and enter text as the terms of service in the following box.
Copyright	Click the checkbox and enter text as the copyright in the following box.

Click Advertisement Options and customize advertisement pictures on the authentication page.



Advertisement	Click the checkbox to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears.
Picture Resource	Click Choose and select pictures from your PC as the advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Enter the duration time for the advertisement pictures. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Enter the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Click the checkbox to allow users to skip the advertisement.

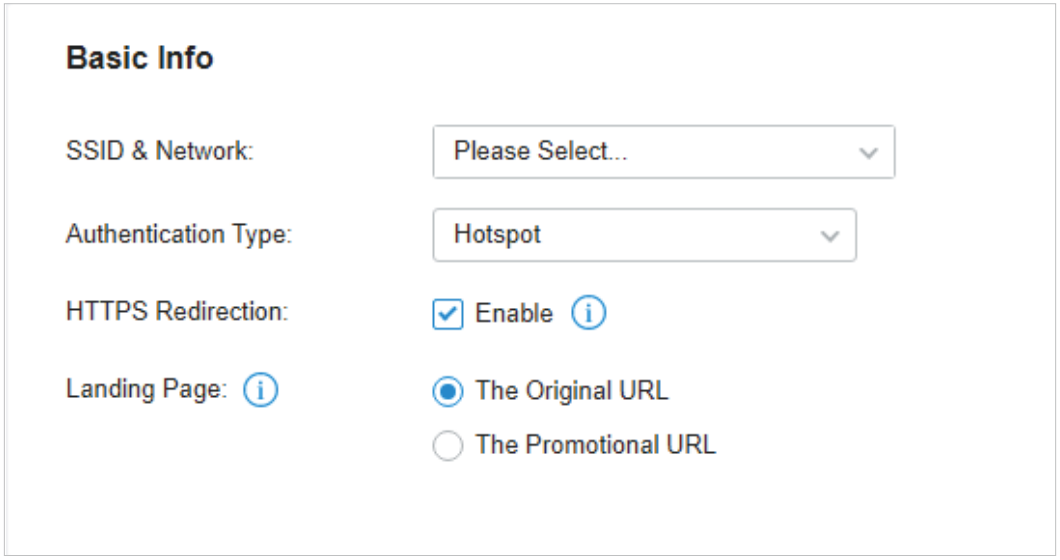
4. In the Access Control section, configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed.



Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click ⊕ Add to configure the IP range or URL which unauthenticated clients are allowed to access.
Authentication-Free Policy	Click the checkbox to enable Authentication-Free Policy. With this feature enabled, you can allow certain clients to access the internet without Portal authentication.
Authentication-Free Client List	Click ⊕ Add and enter the IP address or MAC address of Authentication-Free clients.

■ Configuring Portal with Hotspot

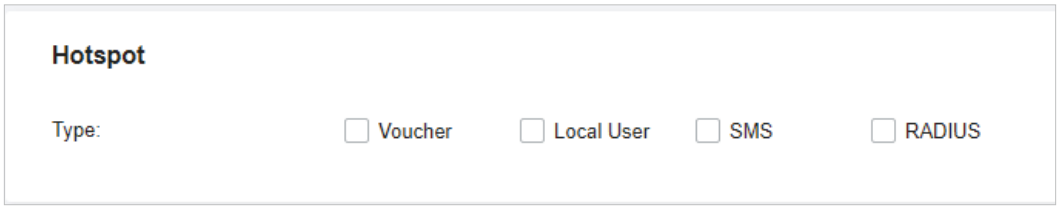
1. Go to Settings > Authentication > Portal. Click ◯ to enable Portal and load the following page.



2. Select the SSIDs and LAN networks for the portal to take effect on and configure basic parameters.

SSID & LAN Network	Select one or more SSIDs or LAN networks for the portal. The clients connected to the selected SSIDs or LAN networks have to log into a web page to establish verification before accessing the network.
Authentication Type	Select the type of Portal authentication as Hotspot.
HTTPS Redirection	Click the checkbox to enable HTTPS Redirection. With this feature enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this feature disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Landing Page	Select which page the client will be redirected to after a successful authentication. The Original URL: Clients are directed to the URL they request for after they pass Portal authentication. The Promotional URL: Clients are directed to the specified URL after they pass Portal authentication.

3. In the Hotspot section, select one or more types of Hotspot to authenticate clients.



- **Configuring Voucher Portal**

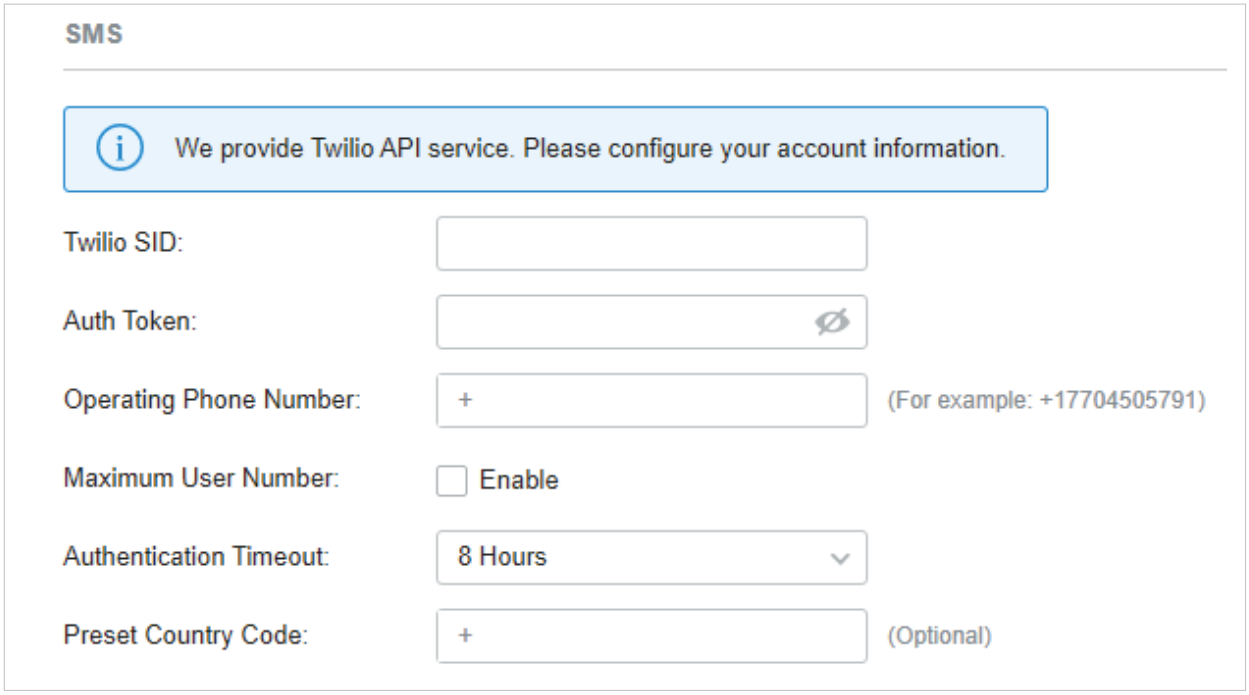
Voucher	Select Voucher and click **Voucher Manager** to manage the voucher codes. Refer to Vouchers for detailed information about how to create vouchers.

- **Configuring Local Portal**

Local User	Select Local User and click **User Management** to manage the information of the login accounts. Refer to Local Users for detailed information about how to create Local Users.

- **Configuring SMS Portal**

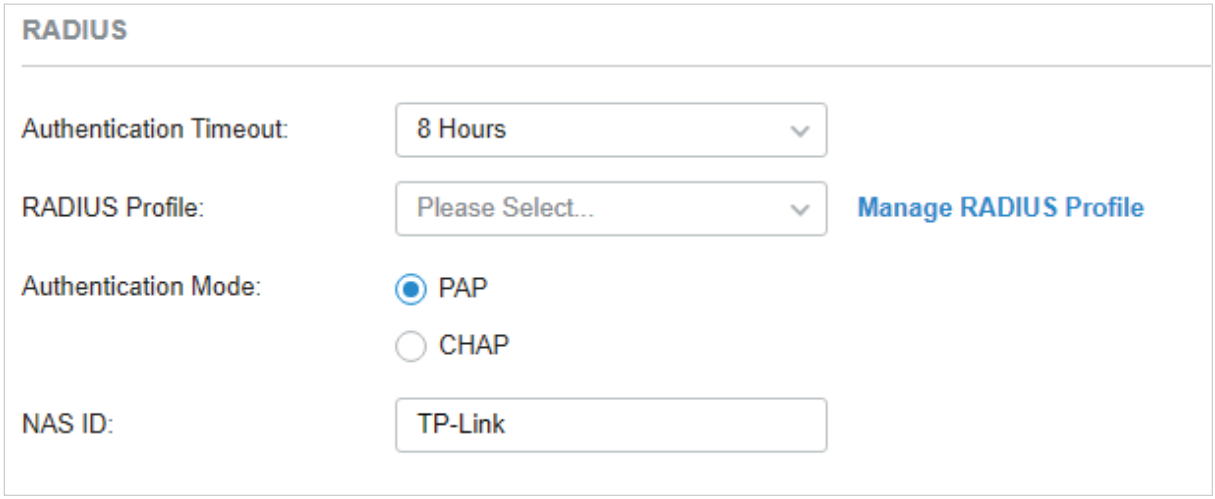
  Select SMS and configure the required parameters in the SMS section.



SMS	Clients can get verification codes using their mobile phones and enter the received codes to pass the authentication.
Twilio SID	Enter the Account SID for Twilio API Credentials.
Auth Token	Enter the Authentication Token for Twilio API Credentials.
Operating Phone Number	Enter the phone number that is used to send verification messages to the clients.
Maximum User Numbers	Click the checkbox and enter the maximum number of users allowed to be authenticated using the same phone number at the same time.
Authentication Timeout	Select the login duration. The client needs to log in again on the web authentication page to access the network.
Preset Country Code	Enter the default country code that will be filled automatically on the authentication page.

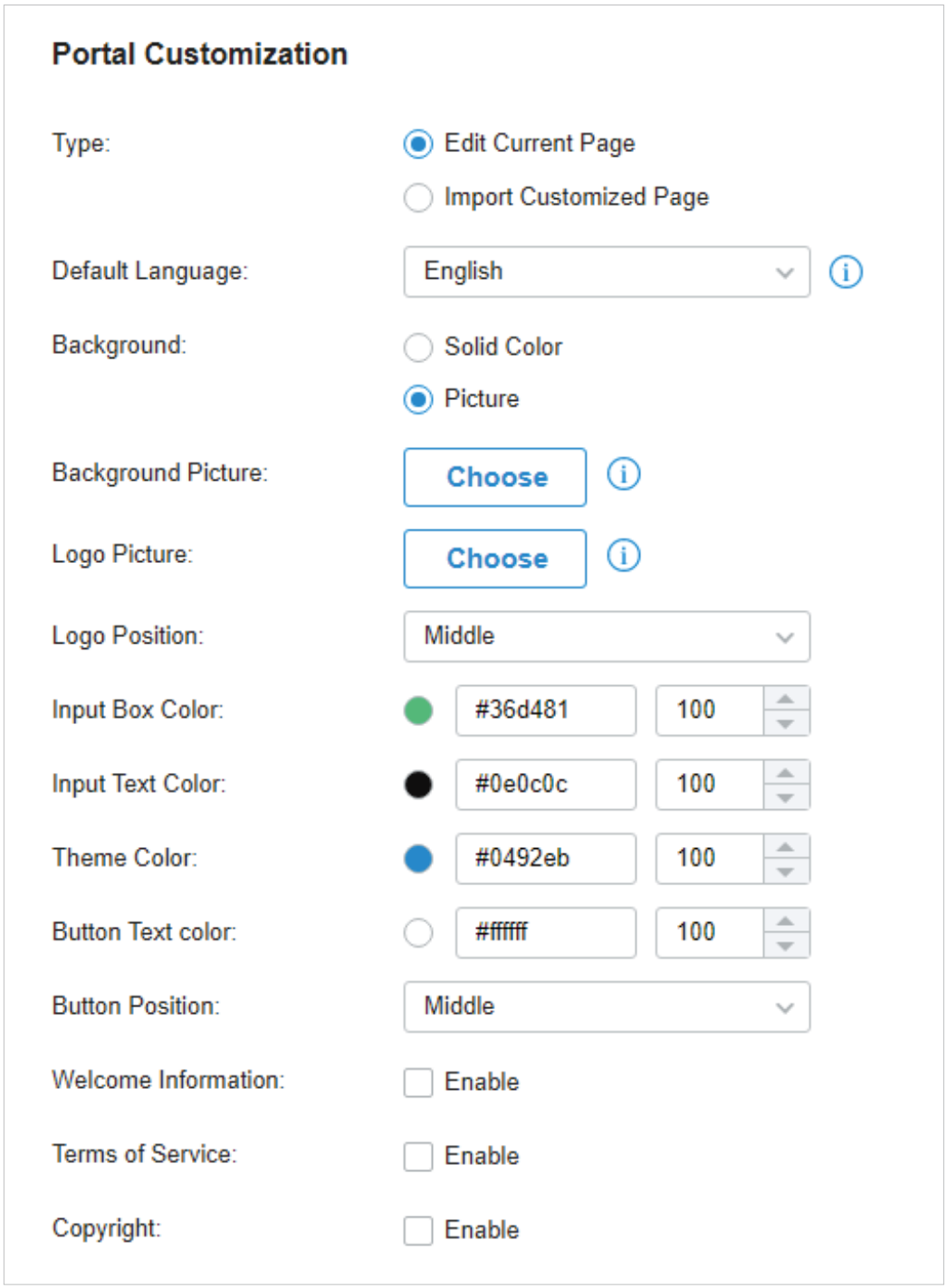
- **Configuring RADIUS Portal**

  Select RADIUS and configure the required parameters in the RADIUS section.



RADIUS	Clients are required to enter the correct username and password which are stored in the RADIUS server to pass the authentication.
RADIUS Profile	Select the RADIUS profile you have created. If no RADIUS profiles have been created, click + Create New RADIUS Profile from the drop-down list or **Manage RADIUS Profile** to create one. The RADIUS profile records the information of the RADIUS server which provides a method for storing the authentication information centrally.
Authentication Mode	Select the authentication protocol for the RADIUS server. Two authentication protocols are available: PAP and CHAP.
NAS ID	Configure a Network Access Server Identifier (NAS ID) on the portal. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups.

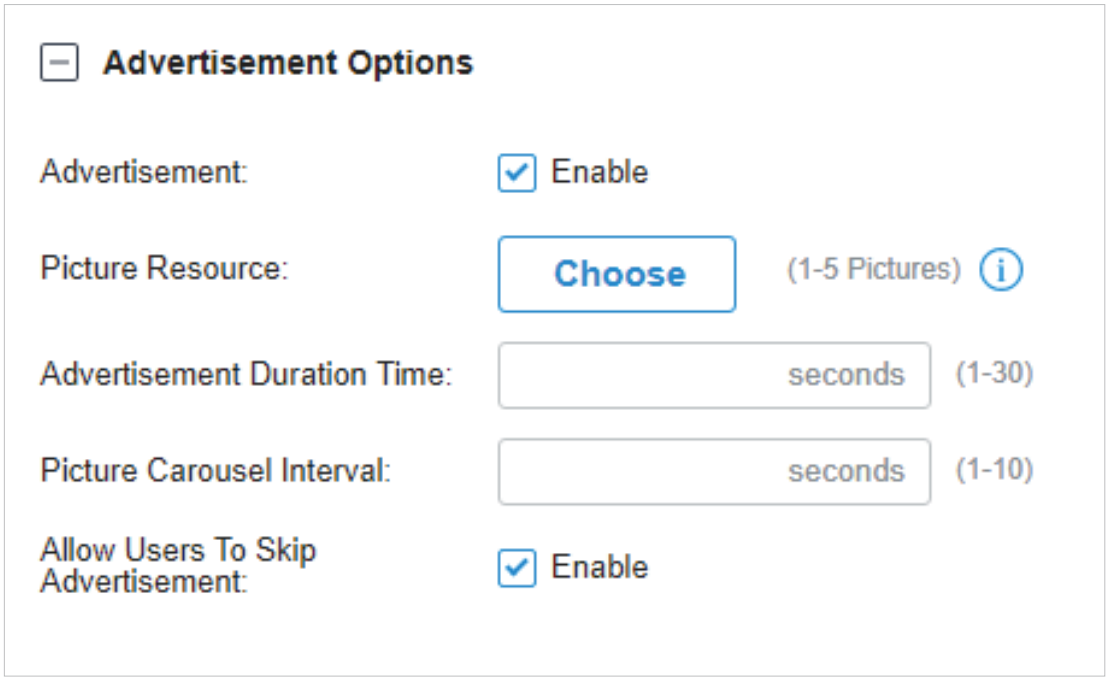
4. In the Portal Customization section, customize the Portal page including the background picture, logo picture and so on.



Type	Select the type of the Portal page. Edit Current Page: Edit the related parameters to customize the portal page based on the provided page. Import Customized Page: Click Import to import your unique Portal page for branding it as per your business.

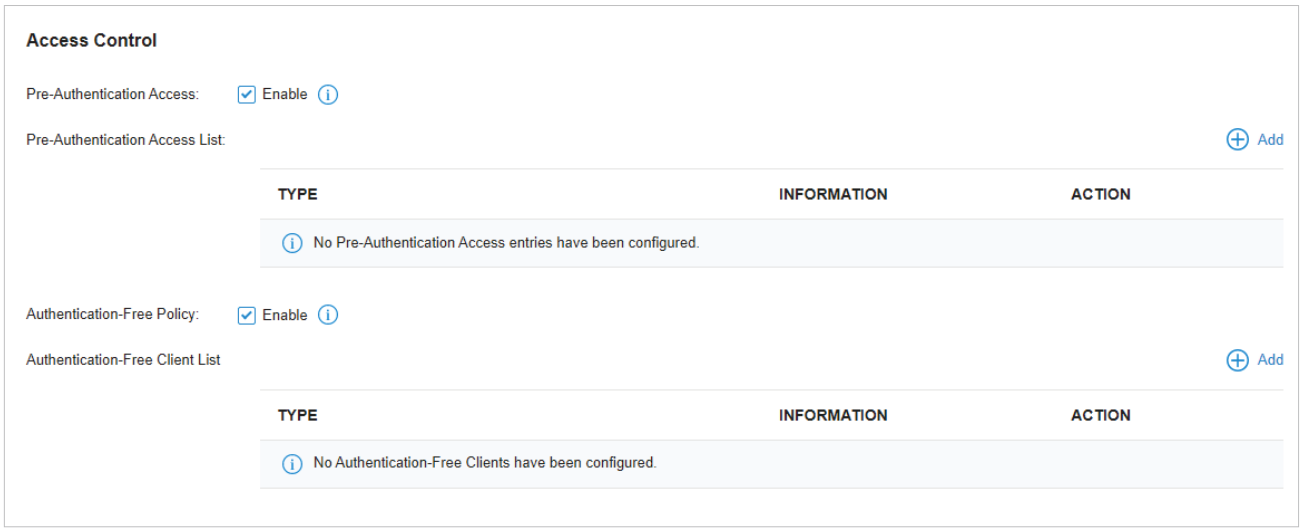
Default Language	Select the default language displayed on the Portal page. The controller automatically adjusts the language displayed on the Portal page according to the system language of the clients. If the language is not supported, the controller will use the default language specified here.
Background	Select the background type. Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker. Picture: Click Choose and select a picture from your PC as the background.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Position	Select the logo position in the Portal page.
Input Box Color	Configure your desired color of the input box for password by entering the hexadecimal HTML color code manually or through the color picker.
Input Text Color	Configure your desired color of the input text for password by entering the hexadecimal HTML color code manually or through the color picker.
Theme Color	Configure your desired background color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Text Color	Configure your desired text color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Position	Select the button position in the Portal page.
Welcome Information	Click the checkbox and enter text as the welcome information. And you can configure your desired text color for the welcome information by entering the hexadecimal HTML color code manually or through the color picker.
Terms of Service	Click the checkbox and enter text as the terms of service in the following box.
Copyright	Click the checkbox and enter text as the copyright in the following box.

Click Advertisement Options and customize advertisement pictures on the authentication page.



Advertisement	Click the checkbox to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears.
Picture Resource	Click Choose and select pictures from your PC as the advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Enter the duration time for the advertisement pictures. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Enter the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Click the checkbox to allow users to skip the advertisement.

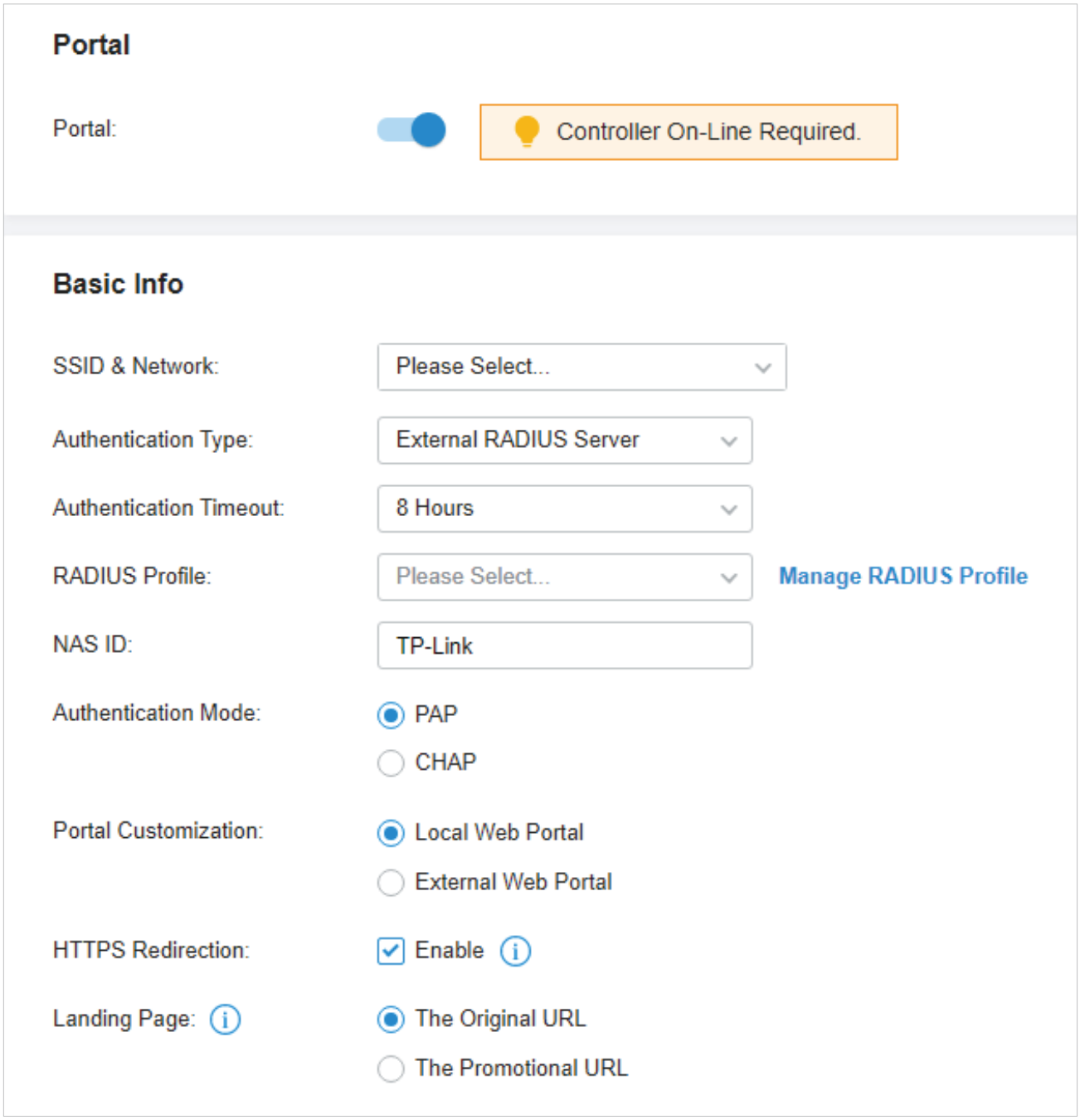
5. In the Access Control section, configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed.



Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click ⊕ Add to configure the IP range or URL which unauthenticated clients are allowed to access.
Authentication-Free Policy	Click the checkbox to enable Authentication-Free Policy. With this feature enabled, you can allow certain clients to access the internet without Portal authentication.
Authentication-Free Client List	Click ⊕ Add and enter the IP address or MAC address of Authentication-Free clients.

■ Configuring Portal with External RADIUS Server

1. Go to Settings > Authentication > Portal. Click to enable Portal and load the following page.

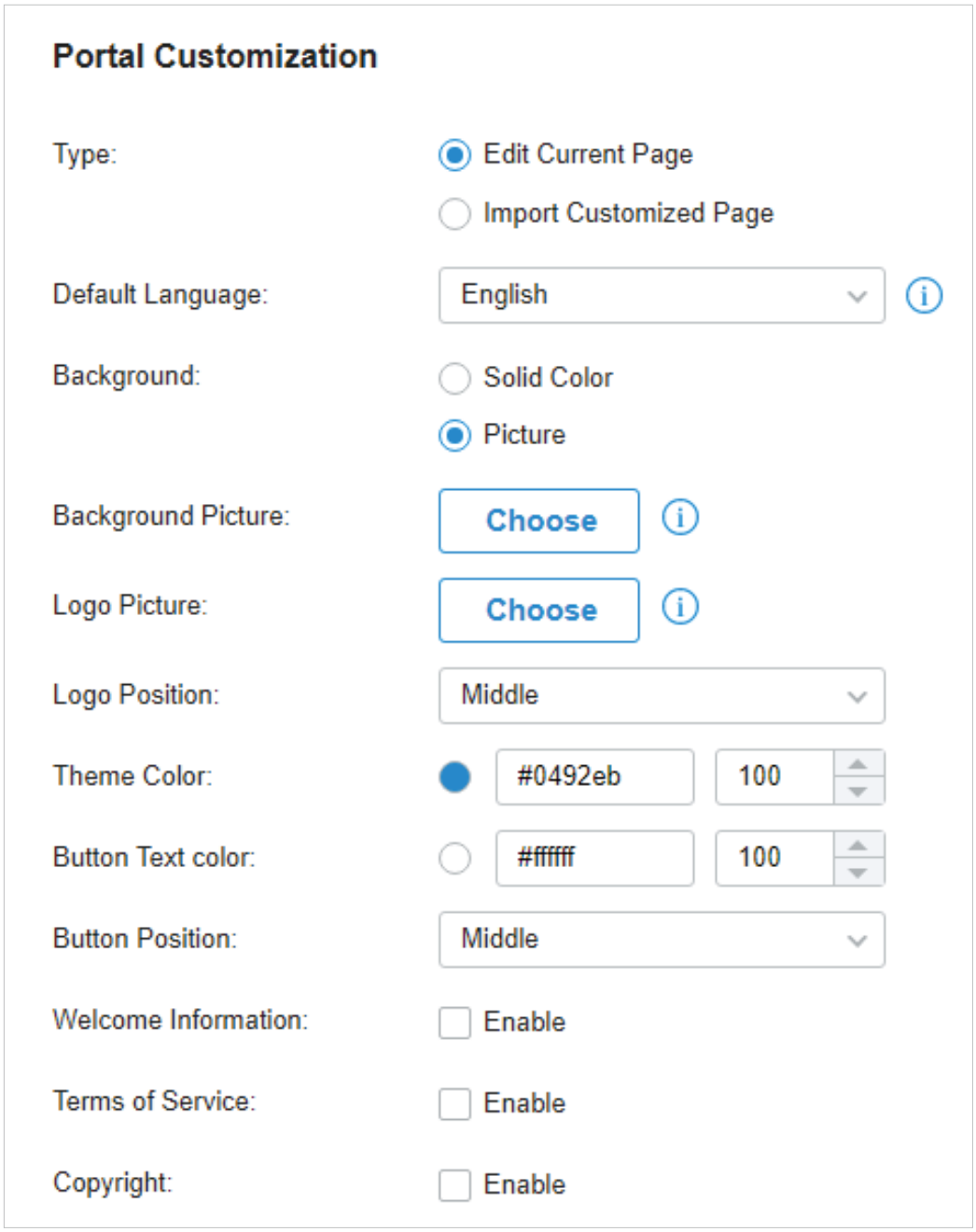


2. Select the SSIDs and LAN networks for the portal to take effect on and configure basic parameters including authentication type, authentication timeout and so on.

SSID & LAN Network	Select one or more SSIDs or LAN networks for the portal. The clients connected to the selected SSIDs or LAN networks have to log into a web page to establish verification before accessing the network.
Authentication Type	Select the type of Portal authentication as External RADIUS Server.
Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.

RADIUS Profile	Select the RADIUS profile you have created. If no RADIUS profiles have been created, click + Create New RADIUS Profile from the drop-down list or Manage RADIUS Profile to create one. The RADIUS profile records information of the RADIUS server including the IP address, port and so on.
NAS ID	Configure a Network Access Server Identifier (NAS ID) on the portal. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups.
Authentication Mode	Select the authentication protocol for the RADIUS server.
Portal Customization	Select Local Web Portal or External Web Portal. The authentication login page of Local Web Portal is provided by the built-in portal server of the controller. The External Web Portal is provided by external portal server. Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field.
HTTPS Redirection	Click the checkbox to enable HTTPS Redirection. With this feature enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this feature disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Landing Page	Select which page the client will be redirected to after a successful authentication. The Original URL: Clients are directed to the URL they request for after they pass Portal authentication. The Promotional URL: Clients are directed to the specified URL here after they pass Portal authentication.

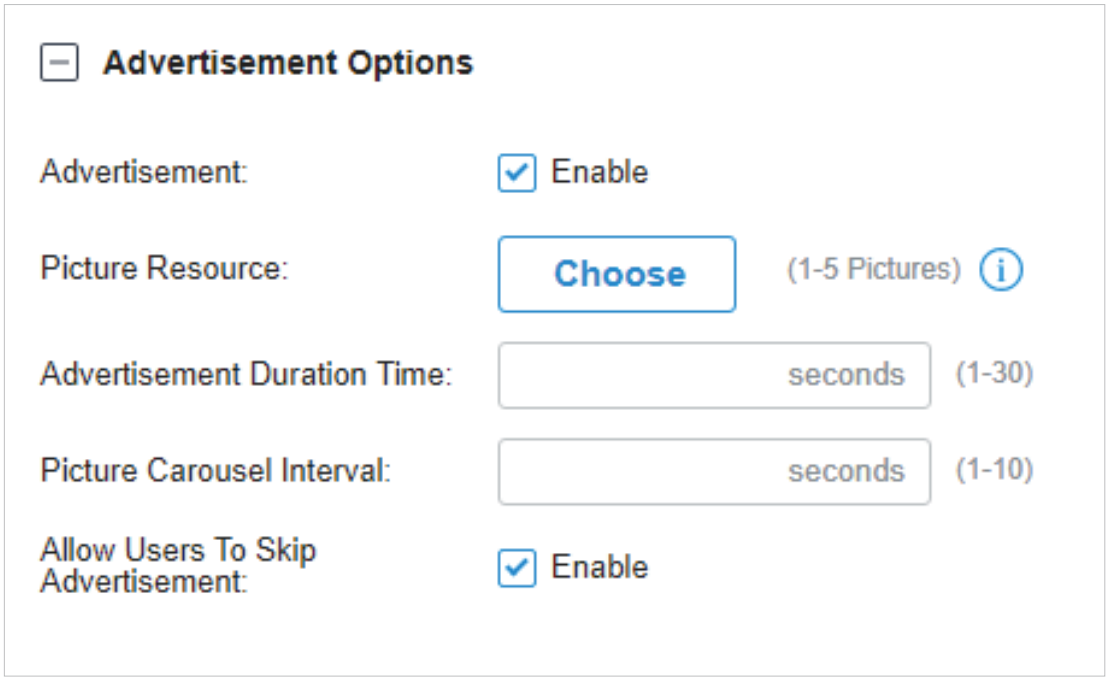
3. If you choose Local Web Portal which is provided by the built-in portal server of the controller, customize the Portal page in the Portal Customization section, including the background picture, logo picture and so on.



Type	Select the type of the Portal page. Edit Current Page: Edit the related parameters to customize the portal page based on the provided page. Import Customized Page: Click Import to import your unique Portal page for branding it as per your business.

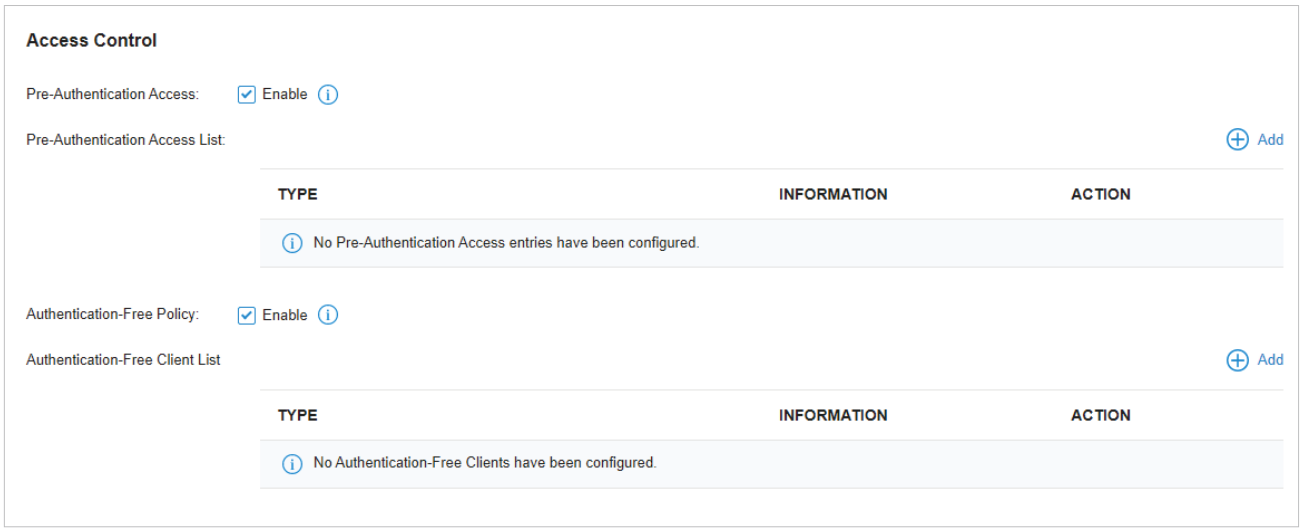
Default Language	Select the default language displayed on the Portal page. The controller automatically adjusts the language displayed on the Portal page according to the system language of the clients. If the language is not supported, the controller will use the default language specified here.
Background	Select the background type. Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker. Picture: Click Choose and select a picture from your PC as the background.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Position	Select the logo position in the Portal page.
Theme Color	Configure your desired background color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Text Color	Configure your desired text color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Position	Select the button position in the Portal page.
Welcome Information	Click the checkbox and enter text as the welcome information. And you can configure your desired text color for the welcome information by entering the hexadecimal HTML color code manually or through the color picker.
Terms of Service	Click the checkbox and enter text as the terms of service in the following box.
Copyright	Click the checkbox and enter text as the copyright in the following box.

Click Advertisement Options and customize advertisement pictures on the authentication page.



Advertisement	Click the checkbox to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears.
Picture Resource	Click Choose and select pictures from your PC as the advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Enter the duration time for the advertisement pictures. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Enter the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Click the checkbox to allow users to skip the advertisement.

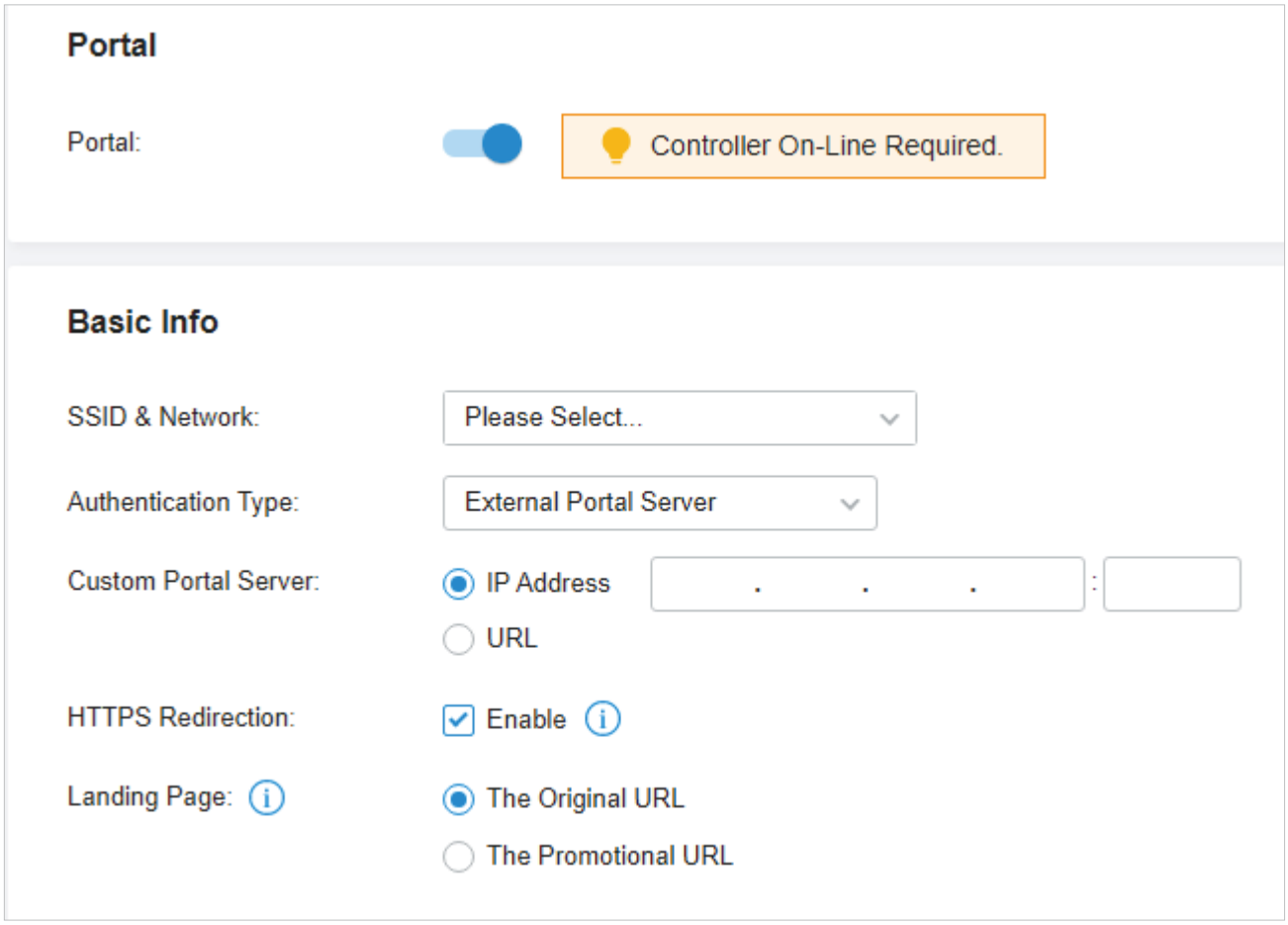
4. **In the Access Control section, configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed.**



Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click ⊕ Add to configure the IP range or URL which unauthenticated clients are allowed to access.
Authentication-Free Policy	Click the checkbox to enable Authentication-Free Policy. With this feature enabled, you can allow certain clients to access the internet without Portal authentication.
Authentication-Free Client List	Click ⊕ Add and enter the IP address or MAC address of Authentication-Free clients.

Configuring Portal with External Portal Server

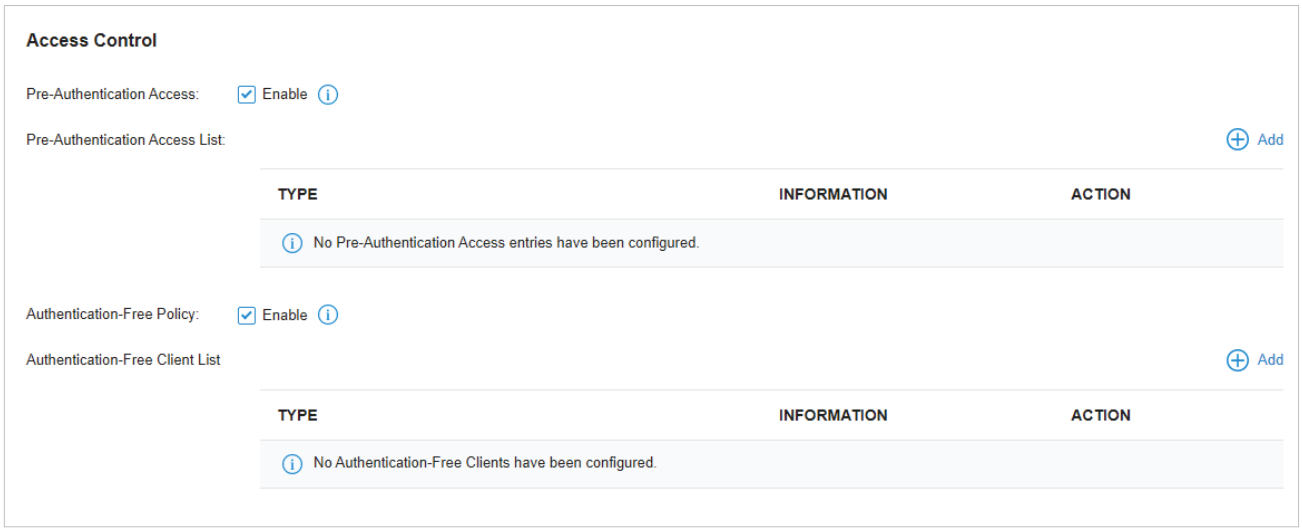
1. Go to Settings > Authentication > Portal. Click to enable Portal and load the following page.



2. Select the SSIDs and LAN networks for the portal to take effect on and configure basic parameters including authentication type, custom portal server and so on.

SSID & LAN Network	Select one or more SSIDs or LAN networks for the portal. The clients connected to the selected SSIDs or LAN networks have to log into a web page to establish verification before accessing the network.
Authentication Type	Select the type of Portal authentication as External Portal Server.
Custom Portal Server	Specify the IP address or URL that redirect to an external portal server.
HTTPS Redirection	Click the checkbox to enable HTTPS Redirection. With this feature enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this feature disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Landing Page	Select which page the client will be redirected to after a successful authentication. The Original URL: Clients are directed to the URL they request for after they pass Portal authentication. The Promotional URL: Clients are directed to the specified URL here after they pass Portal authentication.

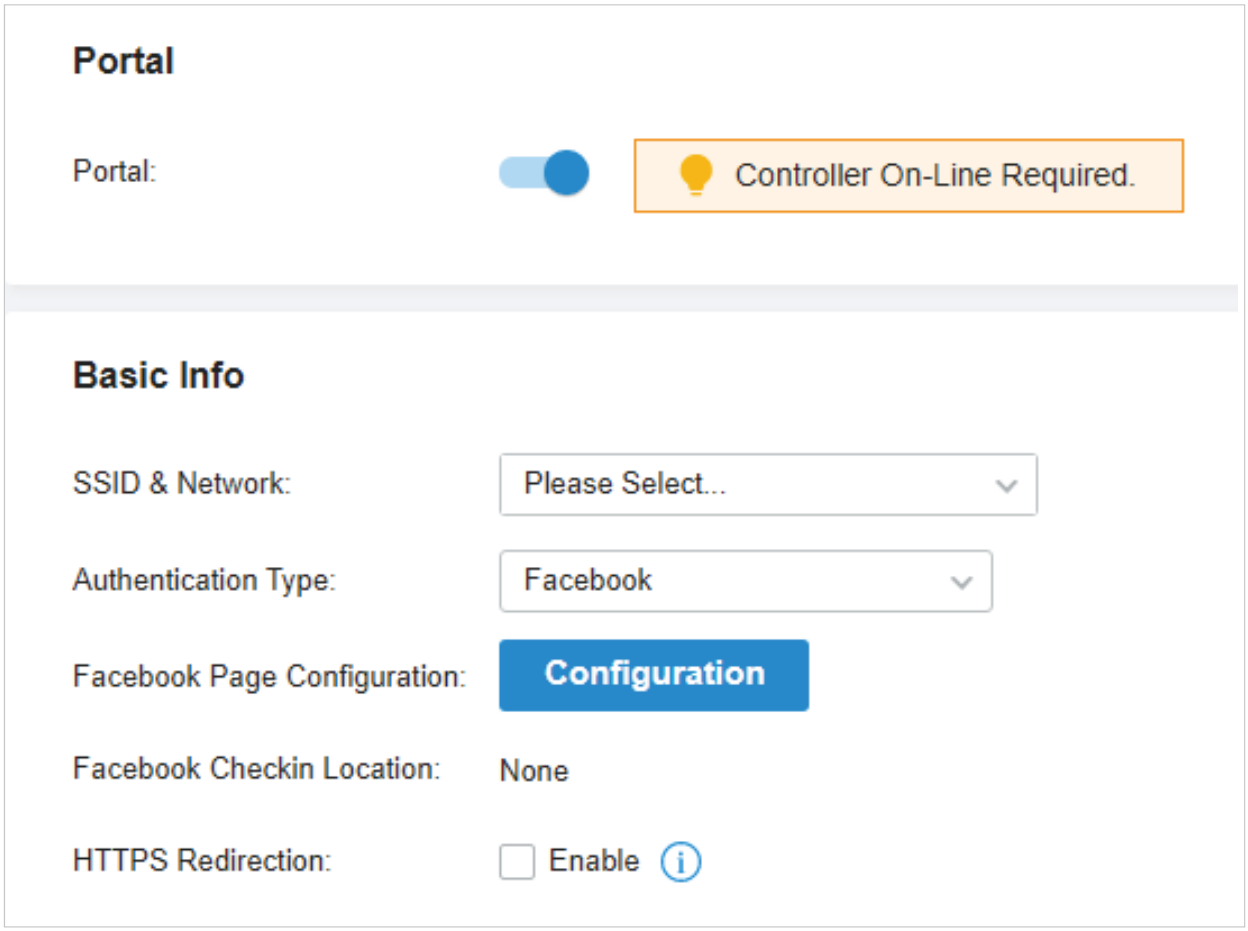
3. **In the Access Control section, configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed.**



Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click ⊕ Add to configure the IP range or URL which unauthenticated clients are allowed to access.
Authentication-Free Policy	Click the checkbox to enable Authentication-Free Policy. With this feature enabled, you can allow certain clients to access the internet without Portal authentication.
Authentication-Free Client List	Click ⊕ Add and enter the IP address or MAC address of Authentication-Free clients.

■ Configuring Portal with Facebook

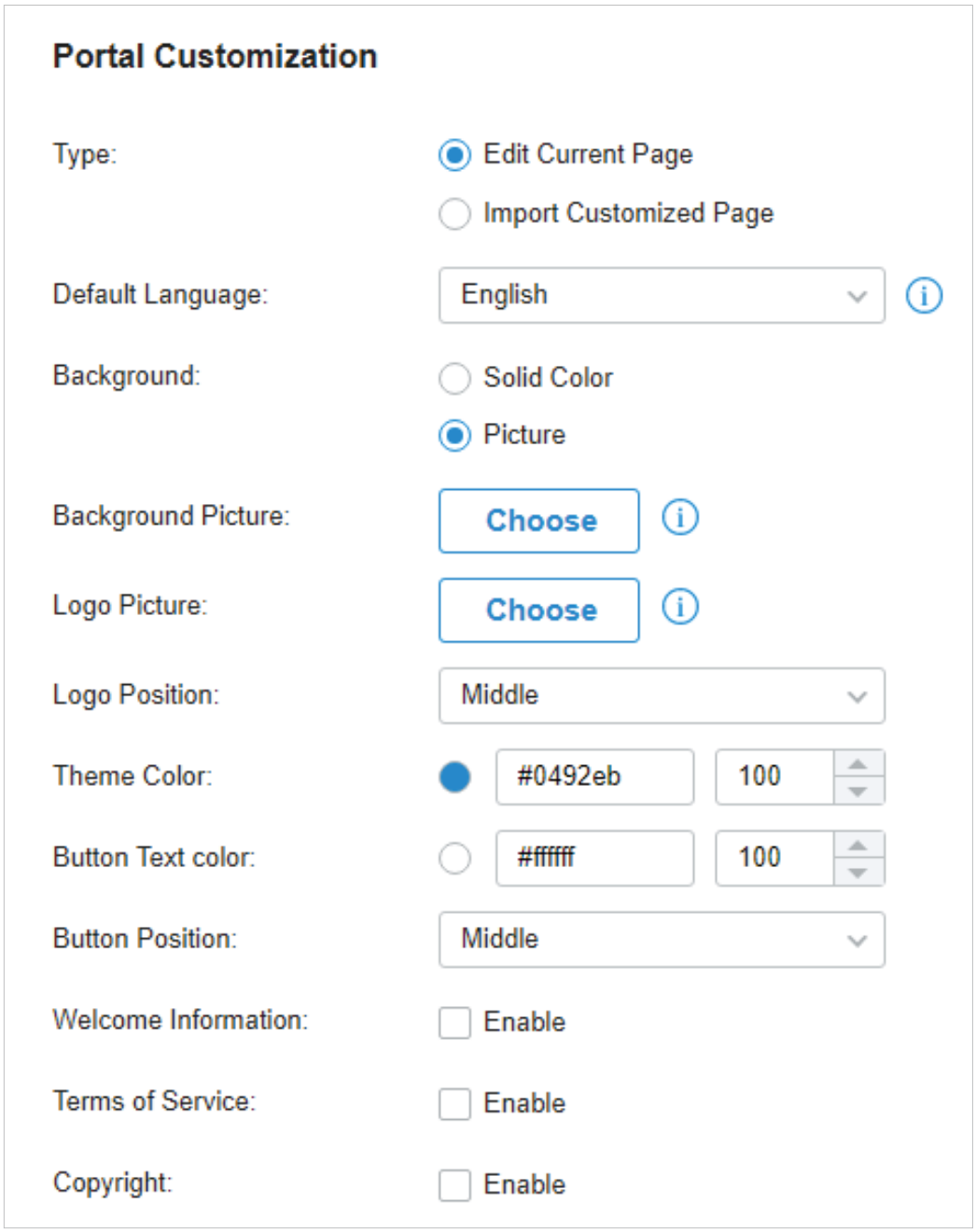
1. Go to Settings > Authentication > Portal. Click to enable Portal and load the following page.



2. Select the SSIDs and LAN networks for the portal to take effect on and configure basic parameters.

SSID & LAN Network	Select one or more SSIDs or LAN networks for the portal. The clients connected to the selected SSIDs or LAN networks have to log into a web page to establish verification before accessing the network.
Authentication Type	Select the type of Portal authentication as Facebook.
Facebook Page Configuration:	Click Configuration to specify the Facebook Page.
Facebook Checkin Location	When the Omada Controller successfully obtain the Facebook page, it will display the name of the Facebook page here.
HTTPS Redirection	Click the checkbox to enable HTTPS Redirection. With this feature enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this feature disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.

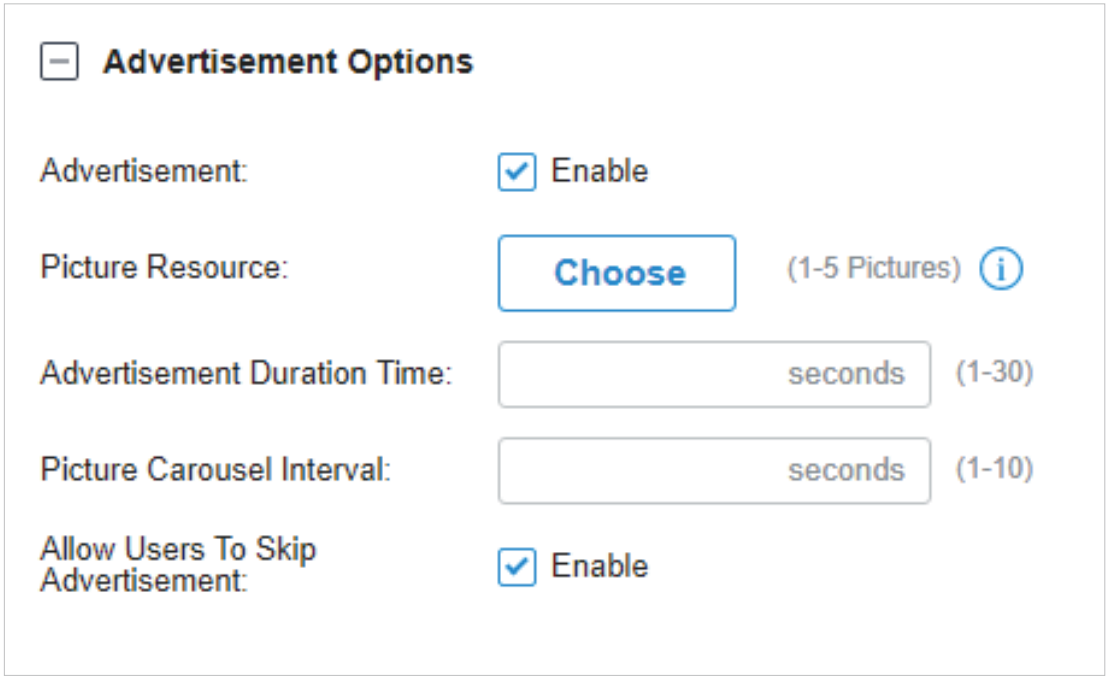
3. In the Portal Customization section, customize the Portal page including the background picture, logo picture and so on.



Type	Select the type of the Portal page. Edit Current Page: Edit the related parameters to customize the portal page based on the provided page. Import Customized Page: Click Import to import your unique Portal page for branding it as per your business.
Default Language	Select the default language displayed on the Portal page. The controller automatically adjusts the language displayed on the Portal page according to the system language of the clients. If the language is not supported, the controller will use the default language specified here.

Background	Select the background type. Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker. Picture: Click Choose and select a picture from your PC as the background.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Position	Select the logo position in the Portal page.
Theme Color	Configure your desired background color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Text Color	Configure your desired text color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Position	Select the button position in the Portal page.
Welcome Information	Click the checkbox and enter text as the welcome information. And you can configure your desired text color for the welcome information by entering the hexadecimal HTML color code manually or through the color picker.
Terms of Service	Click the checkbox and enter text as the terms of service in the following box.
Copyright	Click the checkbox and enter text as the copyright in the following box.

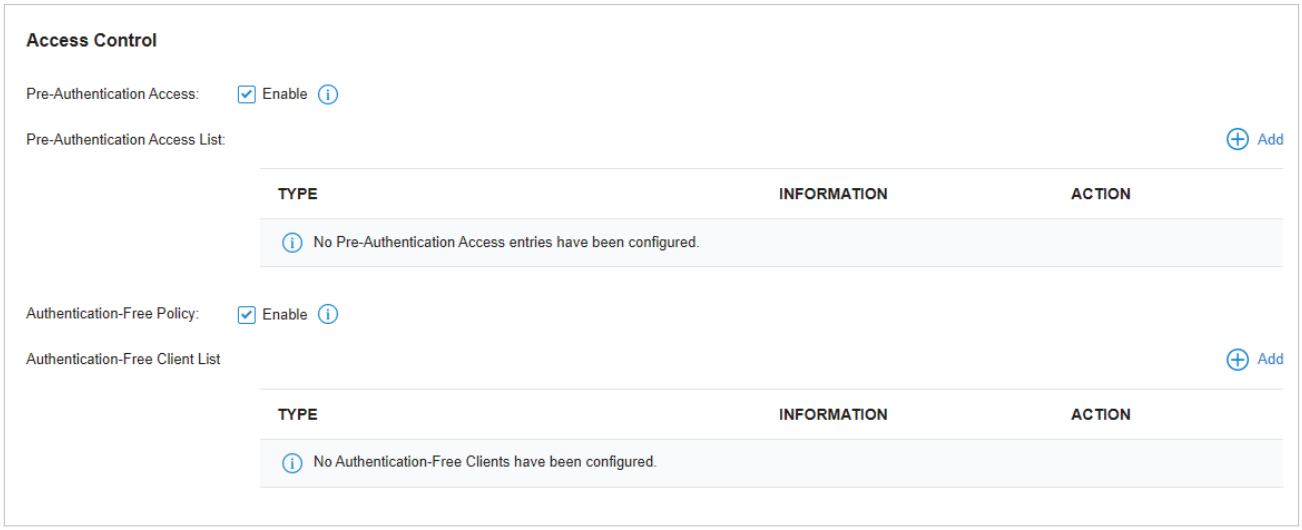
Click Advertisement Options and customize advertisement pictures on the authentication page.



Advertisement	Click the checkbox to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears.

Picture Resource	Click Choose and select pictures from your PC as the advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Enter the duration time for the advertisement pictures. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Enter the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Click the checkbox to allow users to skip the advertisement.

4. In the Access Control, configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed.



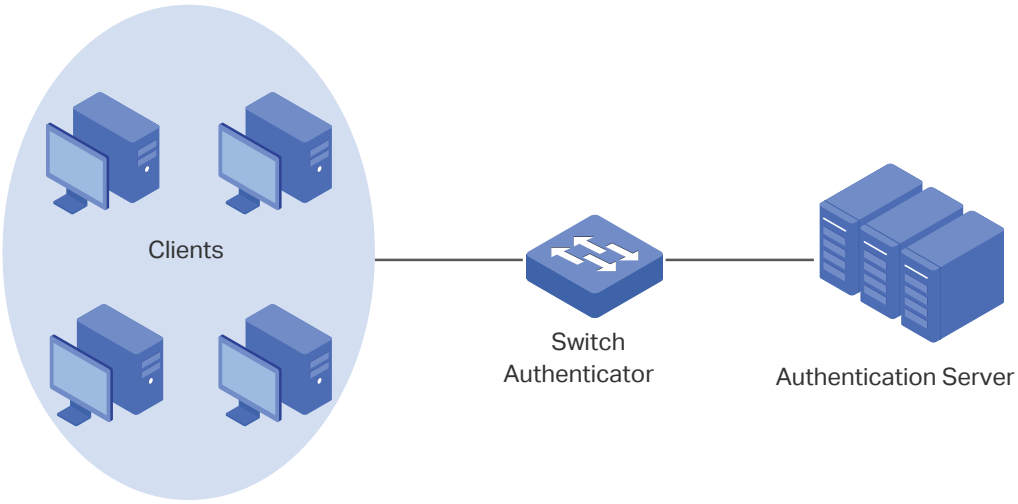
Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click Add to configure the IP range or URL which unauthenticated clients are allowed to access.
Authentication-Free Policy	Click the checkbox to enable Authentication-Free Policy. With this feature enabled, you can allow certain clients to access the internet without Portal authentication.
Authentication-Free Client List	Click Add and enter the IP address or MAC address of Authentication-Free clients.

4. 9. 2 802.1X

Overview

802.1X provides port-based authentication service to restrict unauthorized clients from accessing to the network through publicly accessible switch ports. An 802.1X-enabled port allows only authentication messages and forbids normal traffic until the client passes the authentication.

802.1X authentication uses client-server model which contains three device roles: client/supplicant, authenticator and authentication server. This is described in the figure below:



- **Client**

  A client, usually a computer, is connected to the authenticator via a physical port. We recommend that you install TP-Link 802.1X authentication client software on the client hosts, enabling them to request 802.1X authentication to access the LAN.

- **Authenticator**

  An authenticator is usually a network device that supports 802.1X protocol. As the above figure shows, the switch is an authenticator.

  The authenticator acts as an intermediate proxy between the client and the authentication server. The authenticator requests user information from the client and sends it to the authentication server; also, the authenticator obtains responses from the authentication server and sends them to the client. The authenticator allows authenticated clients to access the LAN through the connected ports but denies the unauthenticated clients.

- **Authentication Server**

  The authentication server is usually the host running the RADIUS server program. It stores information of clients, confirms whether a client is legal and informs the authenticator whether a client is authenticated.

Based on authenticated identity, 802.1X can also deliver customized services. For example, 802.1X and VLAN Assignment together make it possible to assign different authenticated users to different VLANs automatically.

Configuration

To complete the 802.1X configuration, follow these steps:

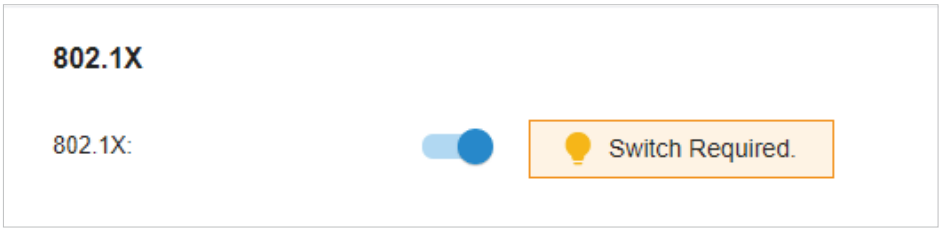
1) Click to enable 802.1X.

2) Select the RADIUS profile you have created and configure other parameters.

3) Select the ports on which 802.1X Authentication will take effect.

Enable 802.1X > Configure RADIUS Profile and Parameters > Select the Ports

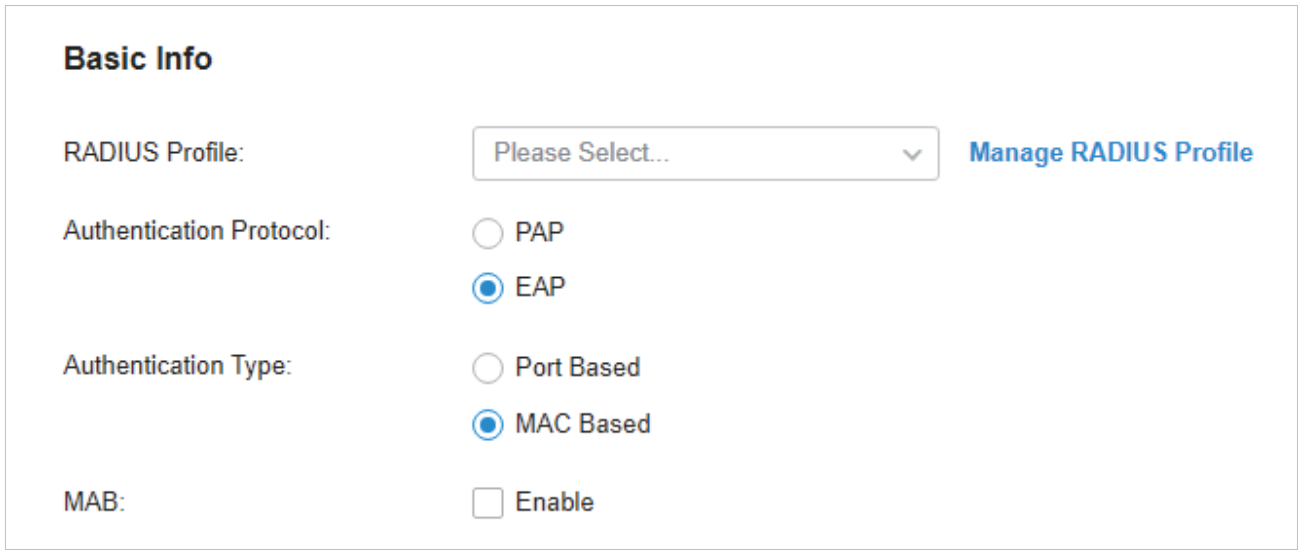
Go to Settings > Authentication > 802.1X. Click to enable 802.1X.



Enable 802.1X > Configure RADIUS Profile and Parameters > Select the Ports

Select the RADIUS profile you have created. If no RADIUS profiles have been created, click + Create New RADIUS Profile from the drop-down list or Manage RADIUS Profile to create one. The RADIUS

profile records the information of the RADIUS server which acts as the authentication server during 802.1X authentication.



Authentication Protocol	Select the authentication protocol for exchanging messages between the switch and RADIUS server. As a bridge between the client and RADIUS server, the switch forwards messages for them. It uses EAP packets to exchange messages with the client, and processes the messages according to the specified authentication protocol before forwarding them to the RADIUS server. PAP: The EAP packets are converted to other protocol (such as RADIUS) packets, and transmitted to the RADIUS server. EAP: The EAP packets are encapsulated in other protocol (such as RADIUS) packets, and transmitted to the authentication server. To use this authentication mechanism, the RADIUS server should support EAP attributes.
Authentication Type	Select the 802.1X authentication type. Port Based: After a client connected to the port gets authenticated successfully, other clients can access the network via the port without authentication. MAC Based: Clients connected to the port need to be authenticated individually. The RADIUS server distinguishes clients by their MAC addresses.
VLAN Assignment	This feature allows the RADIUS server to send the VLAN configurations to the port dynamically. After the port is authenticated, the RADIUS server assigns the VLAN based on the username of the client connecting to the port. The username-to-VLAN mappings must be already stored in the RADIUS server database. This feature is available only when the 802.1X authentication type is Port Based.
MAB	MAB (MAC Authentication Bypass) allows clients to be authenticated without any client software installed. MAB is useful for authenticating devices without 802.1X capability like IP phones. When MAB is enabled on a port, the switch will learn the MAC address of the client automatically and send the authentication server a RADIUS access request frame with the client's MAC address as the username and password. MAB takes effect only when 802.1X authentication is enabled on the port.

Enable 802.1X > Configure RADIUS Profile and Parameters > Select the Ports

Select the ports to enable 802.1X authentication or MAB for them. To enable 802.1X authentication, click the unselected ports. 802.1X-enabled ports will be marked with ☑. To enable MAB, click the ports marked with ☑. You can enable MAB only on 802.1X-enabled ports. MAB-enabled ports will be marked with ☑.



Note:

- You are not recommended to enable 802.1X authentication on the switch ports which connects to network devices without 802.1X capability like the router and APs.
- The switch authenticates wired clients which connect to the port with 802.1X enabled. And the gateway authenticates wired clients which connect to the network with Portal configured. Wired clients should pass Portal and 802.1X authentication to access the internet when both are configured.

4. 9. 3 MAC-Based Authentication

Overview

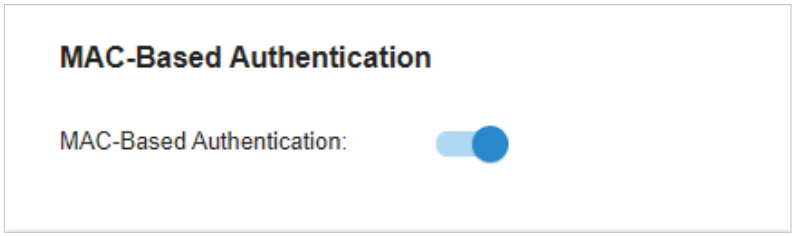
MAC-Based Authentication allows or disallows clients access to wireless networks based on the MAC addresses of the clients. In this authentication method, the controller takes wireless clients' MAC addresses as their usernames and passwords for authentication. The RADIUS server authenticates the MAC addresses against its database which stores the allowed MAC addresses. Clients can access the wireless networks configured with MAC-based authentication after passing authentication successfully.

Note:

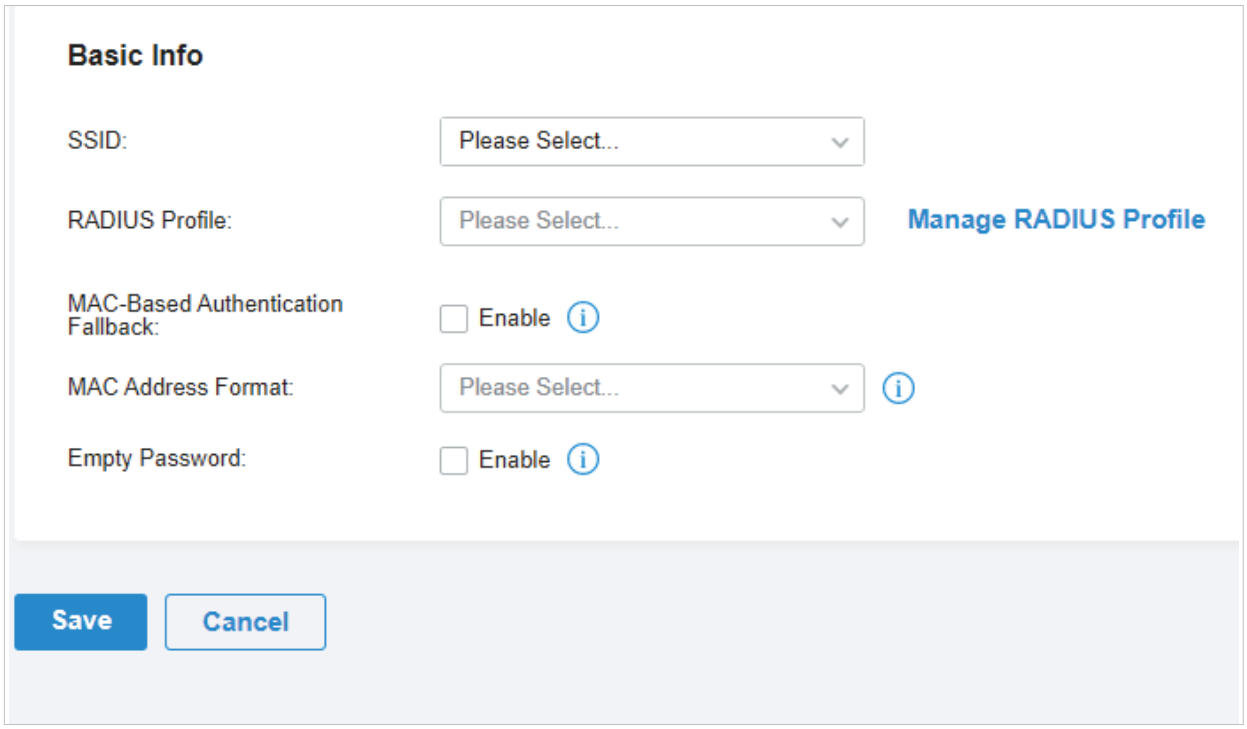
Both MAC-Based Authentication and Portal authentication can authenticate wireless clients. If both are configured on a wireless network, a wireless client needs to pass MAC-Based Authentication first and then Portal authentication for internet access. You can enable MAC-Based Authentication Fallback to allow clients bypass MAC-Based Authentication, which means the client needs to pass either of the two authentication. The client tries MAC-Based Authentication first, and is allowed to try portal authentication if it failed the MAC-Based Authentication.

Configuration

1. Go to Settings > Authentication > MAC-Based Authentication. Click ◯ to enable MAC-Based Authentication.



2. In the Basic Info, select the SSIDs, RADIUS Profile and other required parameters. Refer to the following table to configure the required parameters and click Save.



SSID	Select one or more SSIDs for MAC-based authentication to take effect.
RADIUS Profile	Select the RADIUS profile you have created. If no RADIUS profiles have been created, click + Create New RADIUS Profile from the drop-down list or Manage RADIUS Profile to create one. The RADIUS profile records the information of the RADIUS server which acts as the authentication server during MAC-Based Authentication.
MAC-Based Authentication Fallback	For the wireless network configured with both MAC-Based Authentication and Portal, if you enable this feature, a wireless client needs to pass only one authentication. The client tries MAC-Based Authentication first, and is allowed to try Portal authentication if it failed the MAC-Based Authentication. If you disable this feature as default, a wireless client needs to pass both the MAC-Based Authentication and portal authentication for internet access, and will be denied if it fails either of the authentication.
MAC Address Format	Select clients' MAC address format which the controller uses for authentication. Then configure the MAC addresses in the specified format as usernames for the clients on the RADIUS server.
Empty Password	Click to allow a blank password for MAC-Based Authentication. With this option disabled, the password will be the same as the username.

4. 9. 4 RADIUS Profile

Overview

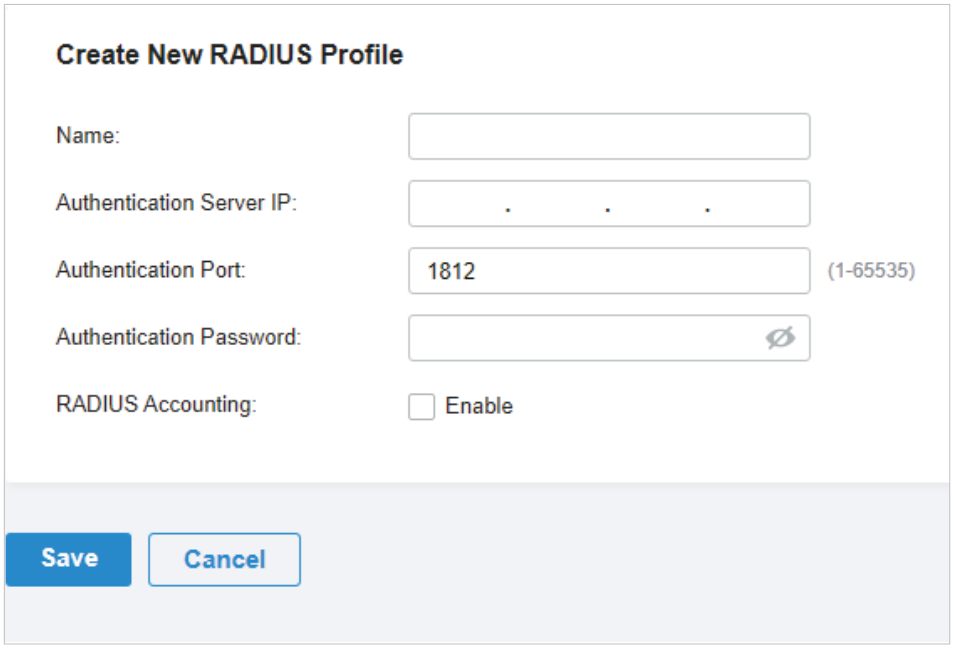
RADIUS (Remote Authentication Dial In User Service) is a client/server protocol that provides for the AAA (Authentication, Authorization, and Accounting) needs in modern IT environments.

In authentication services including 802.1X, Portal and MAC-Based Authentication, Omada devices operate as clients of RADIUS to pass user information to designated RADIUS servers. A RADIUS server maintains a database which stores the identity information of legal users. It authenticates users against the database when the users are requesting to access the network, and provides authorization and accounting services for them.

A RADIUS profile records your custom settings of a RADIUS server. After creating a RADIUS profile, you can apply it to multiple authentication policies like Portal and 802.1X, saving you from repeatedly entering the same information.

Configuration

1. Go to Settings > Authentication > RADIUS Profile. Click + Create New RADIUS Profile to load the following page.



2. Enter the information of the RADIUS servers. Refer to the following table to configure the required parameters and click Save.

Name	Enter a name to identify the RADIUS profile.
Authentication Server IP	Enter the IP address of the authentication server.
Authentication Port	Enter the UDP destination port on the authentication server for authentication requests.
Authentication Password	Enter the password that will be used to validate the communication between Omada devices and the RADIUS authentication server.
RADIUS Accounting	Click the checkbox to enable RADIUS Accounting to meet billing needs. This feature is only available for Omada EAPs with Portal to account for wireless clients.

Interim Update	Click the checkbox to enable Interim Update. By default, the RADIUS accounting process needs only start and stop messages to the RADIUS accounting server. With Interim Update enabled, Omada devices will periodically send an Interim Update (a RADIUS Accounting Request packet containing an “interim-update” value) to the RADIUS server. An Interim Update updates the user’s session duration and current data usage.
Interim Update Interval	Enter an appropriate interval between the updates of users’ session duration and current data usage.
Accounting Server IP	Enter the IP address of the RADIUS accounting server.
Accounting Port	Enter the UDP destination port on the RADIUS server for accounting requests.
Accounting Password	Enter the password that will be used to validate the communication between Omada devices and the RADIUS accounting server.

4. 10 Services

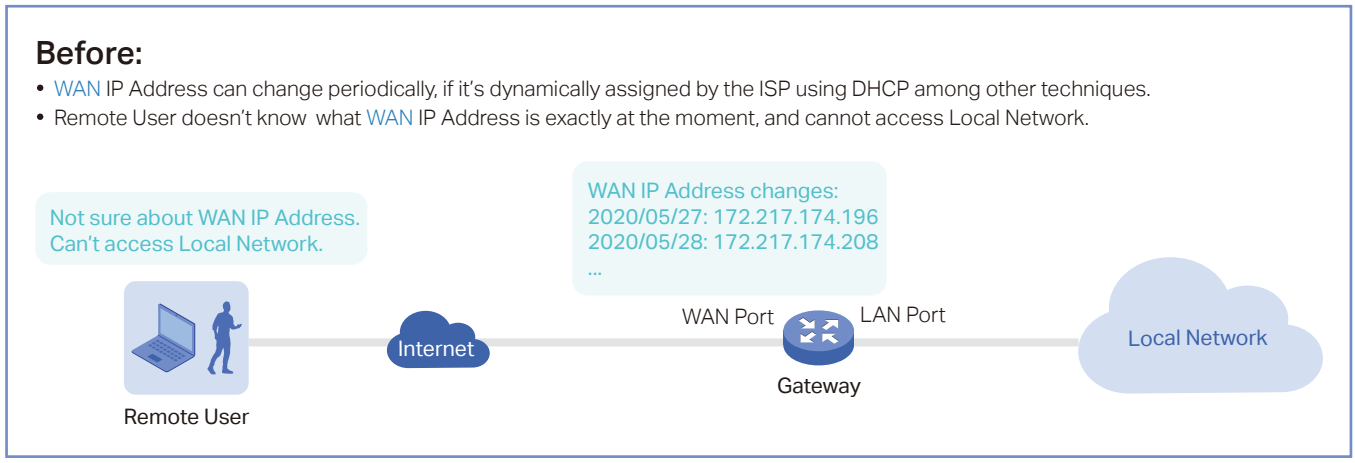
Services provide convenient network services and facilitate network management. You can configure servers or terminals in DDNS, SNMP, UPnP, and SSH, schedule the devices in Reboot Schedule and PoE Schedule, and export the running logs in Export Data.

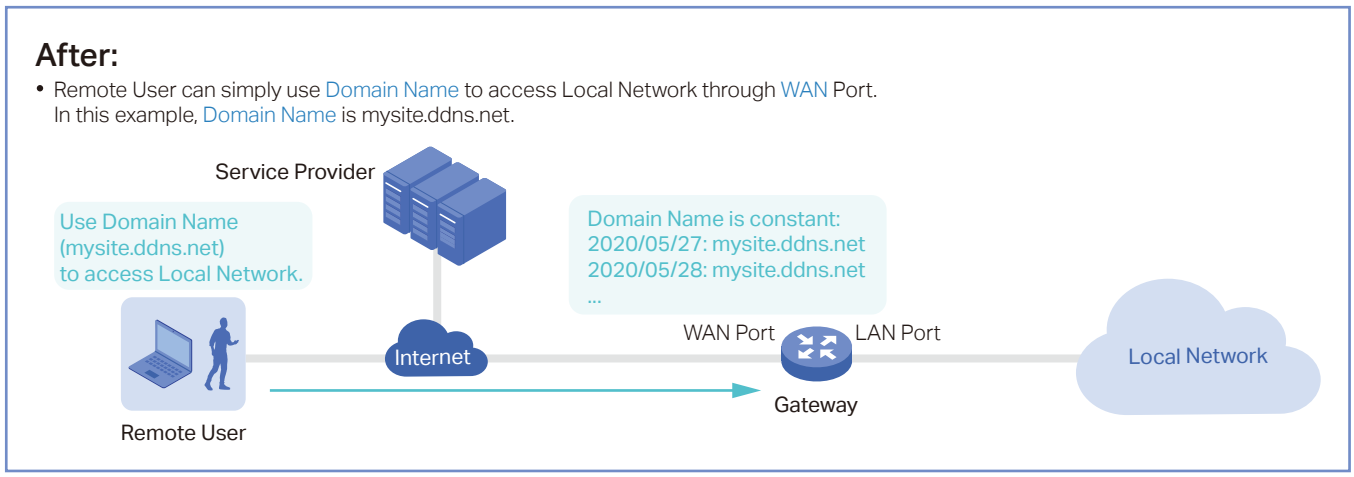
4. 10. 1 Dynamic DNS

Overview

WAN IP Address of your gateway can change periodically because your ISP typically employs DHCP among other techniques. This is where Dynamic DNS comes in. Dynamic DNS assigns a fixed domain name to the WAN port of your gateway, which facilitates remote users to access your local network through WAN Port.

Let's illustrate how Dynamic DNS works with the following figures.



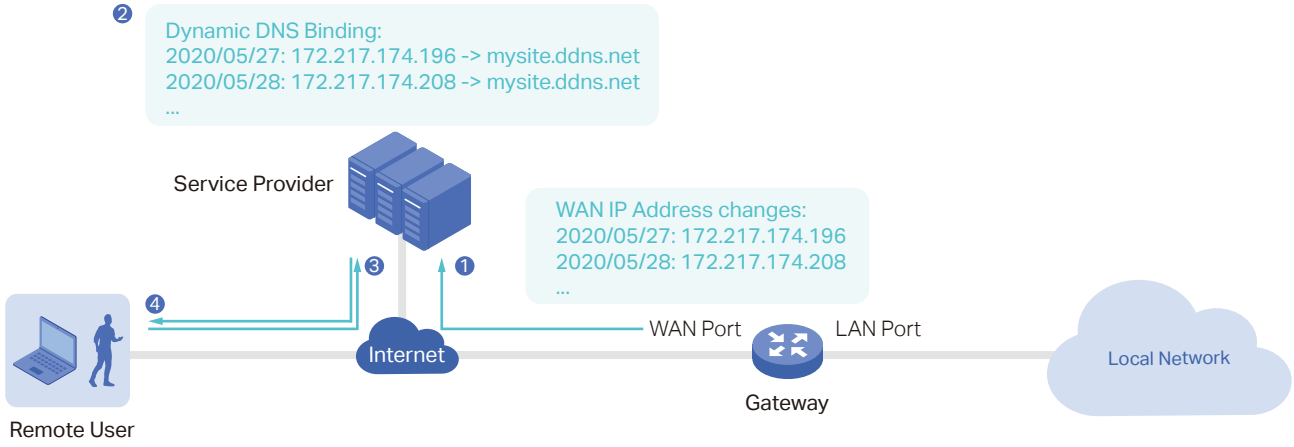


Prerequisite:

- Choose one Service Provider from the four that the controller supports, i.e. DynDNS, No-IP, Peanuthull, Comexe.
- Register at your Service Provider, then you get your Username and Password.
- Get your Domain Name from your Service Provider.

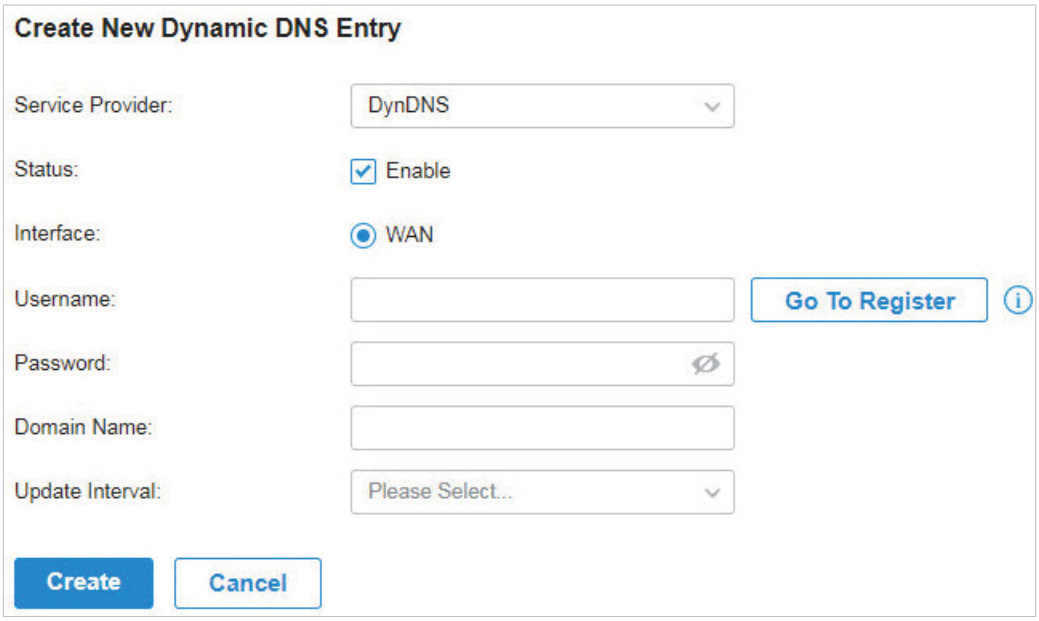
How Dynamic DNS works:

1. Gateway informs Service Provider of WAN IP Address.
2. Service Provider binds WAN IP Address with Domain Name and keeps it updated as WAN IP Address changes.
3. Remote User requests for WAN IP Address by sending Domain Name to Service Provider.
4. Service Provider replies with WAN IP Address, which Remote User actully uses to access Local Network through WAN Port.



Configuration

Go to Settings > Services > Dynamic DNS. Click + Create New Dynamic DNS Entry, to load the following page. Configure the parameters and click Create.



Service Provider	Select your service provider which Dynamic DNS works with.

Status	Enable or disable the Dynamic DNS entry.
Interface	Select the WAN Port which the Dynamic DNS entry applies to.
Username	Enter your username for the service provider. If you haven't registered at the service provider, click Go To Register.
Password	Enter your password for the service provider.
Domain Name	Enter the Domain Name which is provided by your service provider. Remote users can use the Domain Name to access your local network through WAN port.
Update Interval	Select how often the WAN IP address is updated with Domain Name.

4. 10. 2 SNMP

Overview

SNMP (Simple Network Management Protocol) provides a convenient and flexible method for you to configure and monitor network devices. Once you set up SNMP for the devices, you can centrally manage them with an NMS (Network Management Station).

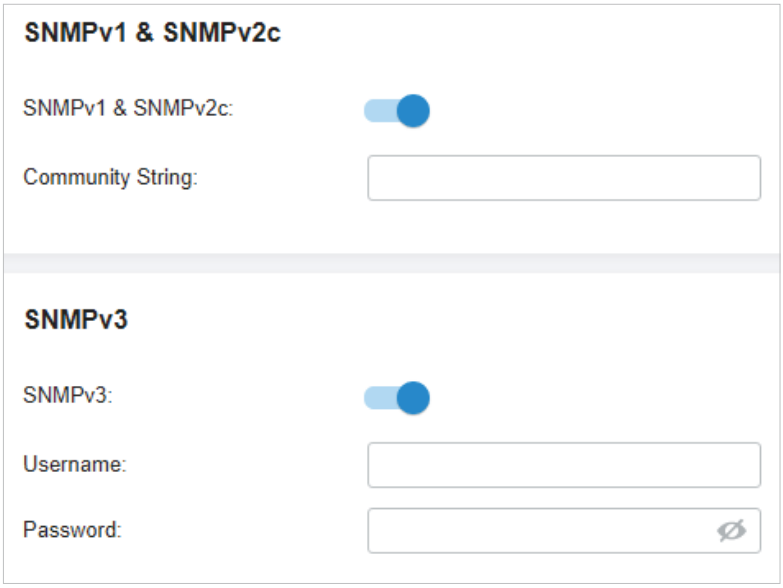
The controller supports multiple SNMP versions including SNMPv1, SNMPv2c and SNMPv3.

Note:

If you use an NMS to manage devices which are managed by the controller, you can only read but not write SNMP objects.

Configuration

Go to Settings > Services > SNMP and configure the parameters. Then click Apply.



SNMPv1 & SNMPv2c	Enable or disable SNMPv1 and SNMPv2c globally.
Community String	With SNMPv1 & SNMPv2c enabled, specify the Community String, which is used as a password for your NMS to access the SNMP agent. You need to configure the Community String correspondingly on your NMS.
SNMPv3	Enable or disable SNMPv3 globally.
Username	With SNMPv3 enabled, specify the username for your NMS to access the SNMP agent. You need to configure the username correspondingly on your NMS.
Password	With SNMPv3 enabled, specify the password for your NMS to access the SNMP agent. You need to configure the password correspondingly on your NMS.

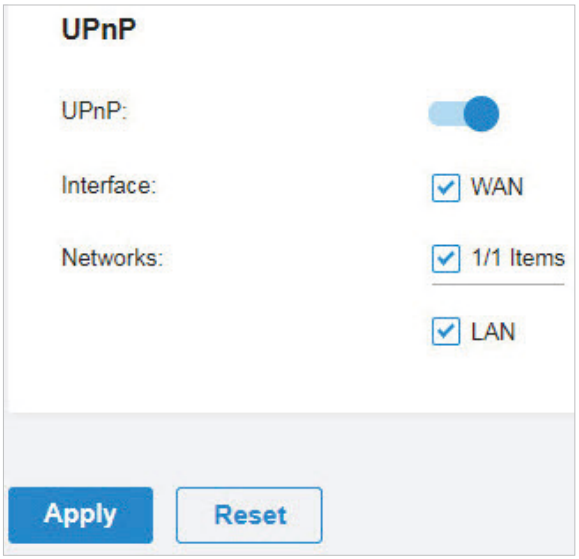
4. 10. 3 UPnP

Overview

UPnP (Universal Plug and Play) is essential for applications including multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) and remote assistance, etc. With the help of UPnP, the traffic between the endpoints of these applications can freely pass the gateway, thus realizing seamless connections.

Configuration

Go to Settings > Services > UPnP. Enable UPnP globally and configure the parameters. Then click Apply.



Interface	Select the WAN port where UPnP takes effect.
Networks	Select the LAN interface where UPnP takes effect.

4. 10. 4 SSH

Overview

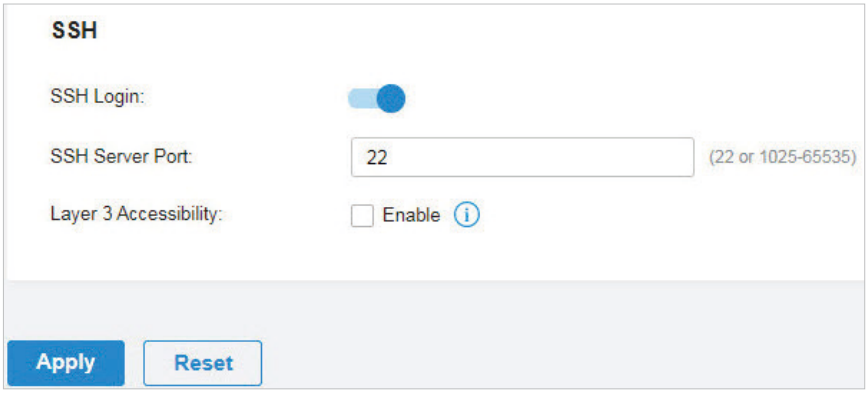
SSH (Secure Shell) provides a method for you to securely configure and monitor network devices via a command-line user interface on your SSH terminal.

Note:

If you use an SSH terminal to manage devices which are managed by the controller, you can only get the User privilege.

Configuration

Go to Settings > Services > SSH. Enable SSH Login globally and configure the parameters. Then click Apply.



SSH Server Port	Specify the SSH Sever Port which your network devices use for SSH connections. You need to configure the SSH Server Port correspondingly on your SSH terminal.
Layer 3 Accessibility	With this feature enabled, the SSH terminal from a different subnet can access your devices via SSH. With this feature disabled, only the SSH terminal in the same subnet can access your devices via SSH.

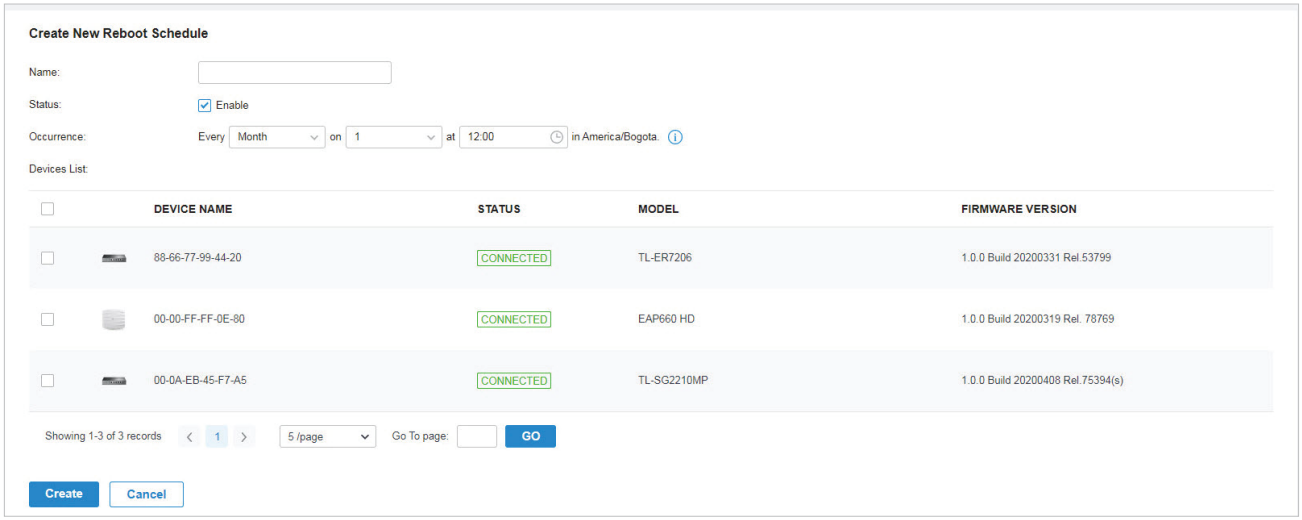
4. 10. 5 Reboot Schedule

Overview

Reboot Schedule can make your devices reboot periodically according to your needs. You can configure Reboot Schedule flexibly by creating multiple Reboot Schedule entries.

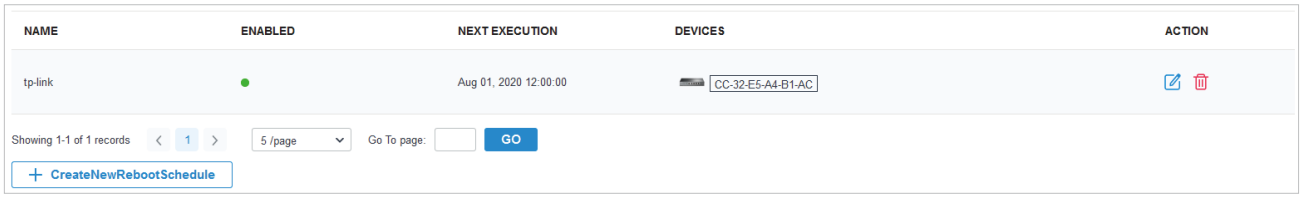
Configuration

3. Go to Settings > Services > Reboot Schedule. Click + Create New Reboot Schedule to load the following page and configure the parameters.



Name	Enter the name to identify the Reboot Schedule entry.
Status	Enable or disable the Reboot Schedule entry.
Occurrence	Specify the date and time for the devices to reboot.
Devices List	Select the devices which the Reboot Schedule applies to.

4. Click Create. The new Reboot Schedule entry is added to the table. You can click to edit the entry. You can click to delete the entry.



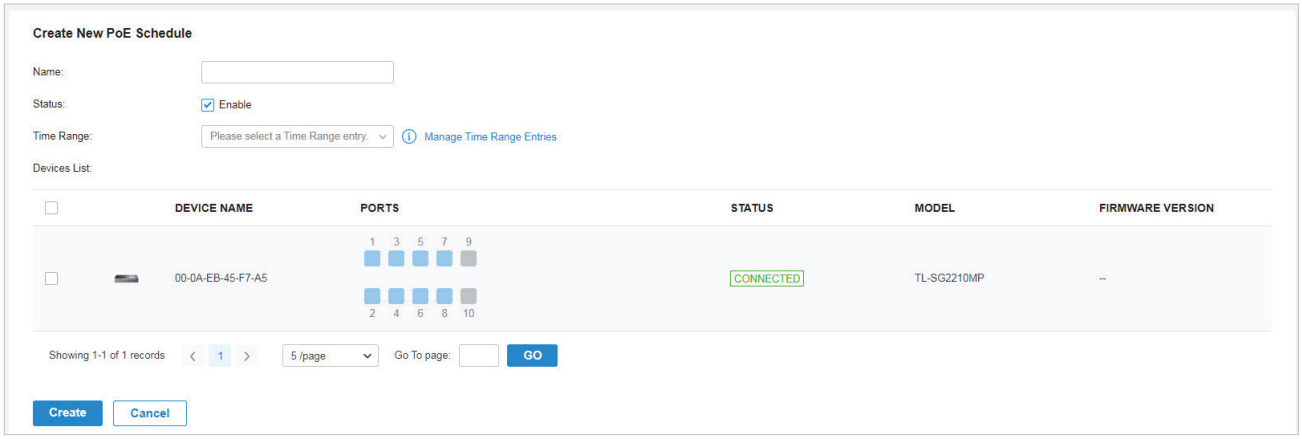
4. 10. 6 PoE Schedule

Overview

PoE Schedule can make PoE devices which are connected to your PoE switches power on and work only in the specific time period as you desire. You can configure PoE Schedule flexibly by creating multiple PoE Schedule entries.

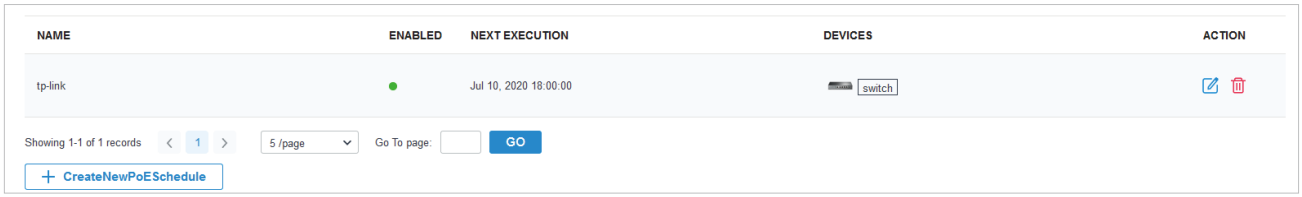
Configuration

5. Go to Settings > Services > PoE Schedule. Click + Create New PoE Schedule to load the following page and configure the parameters.



Name	Enter the name to identify the PoE Schedule entry.
Status	Enable or disable the PoE Schedule entry.
Time Range	Select the Time Range when the PoE devices work. You can create a Time Range entry by clicking + Create New Time Range Entry from the drop down list of Time Range. For details, refer to Profiles.
Devices List	Select the PoE switches and PoE ports which the PoE Schedule applies to. Your PoE devices connected to the selected ports of the switches work according to the PoE Schedule.

6. Click Create. The new PoE Schedule entry is added to the table. You can click to edit the entry. You can click to delete the entry.



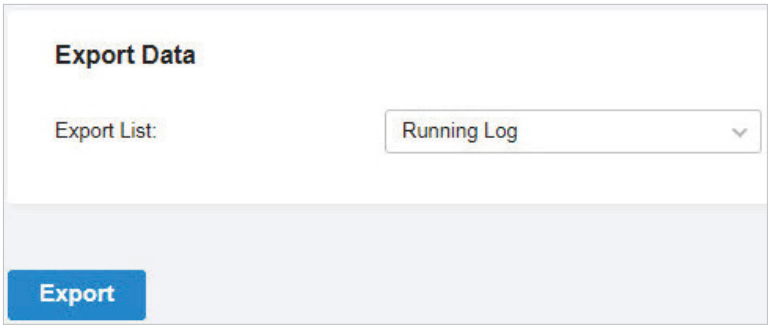
4. 10. 7 Export Data

Overview

You can export data to monitor or debug your devices.

Configuration

Go to Settings > Services > Export Data. Select the type of data from the export list and click Export.



Export List	Running Log: Export the day-to-day running log of the controller.



Configure the Omada SDN Controller

Controller Settings control the appearance and behavior of the controller and provide methods of data backup, restore and migration:

- Manage the Controller
- Manage Your Controller Remotely via Cloud Access
- Maintenance
- Migration

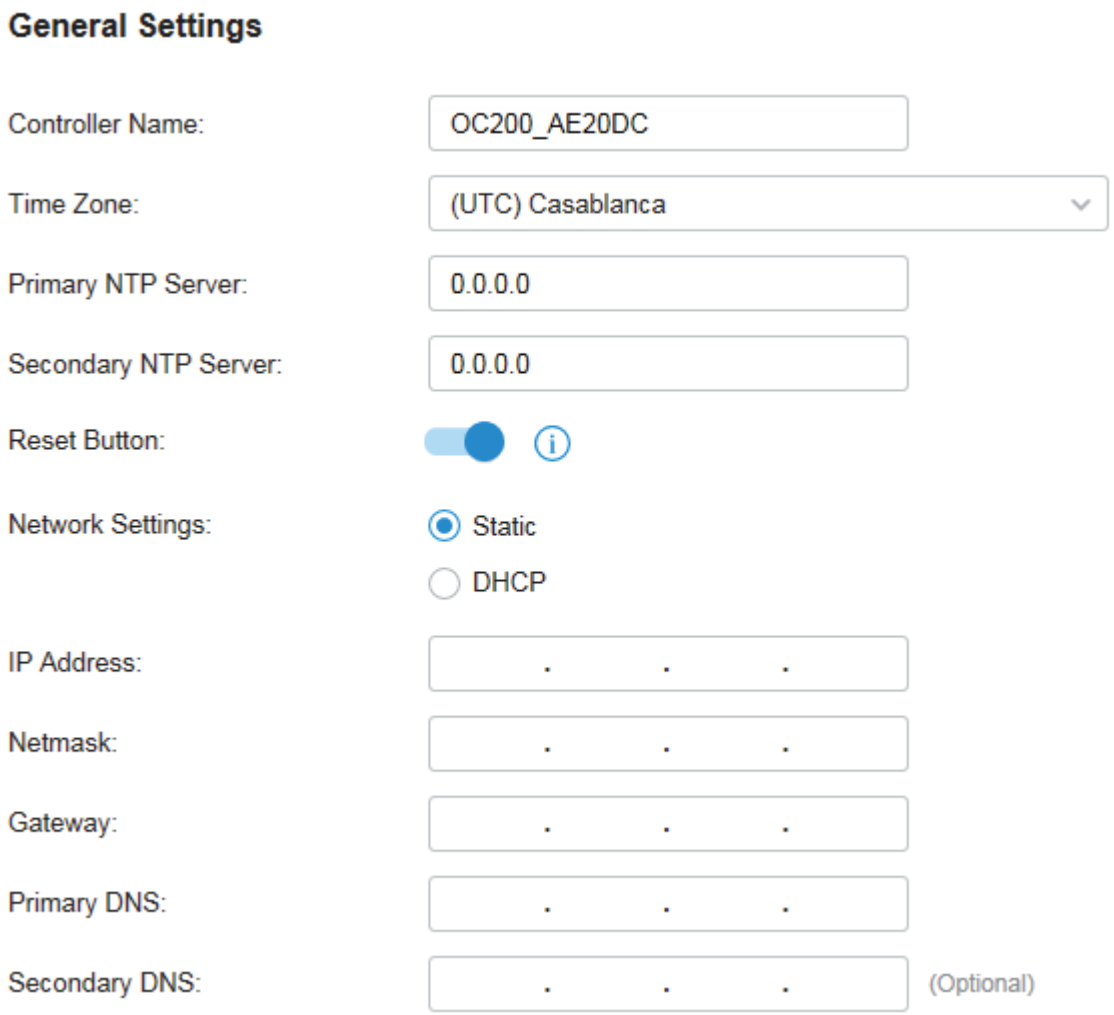
5. 1 Manage the Controller

5. 1. 1 General Settings

Configuration

Go to Settings > Controller. In General Settings, configure the parameters and click Save.

- **For Omada Hardware Controller**



Controller Name	Specify the Controller Name to identify the controller.
Time Zone	Select the Time Zone of the controller according to your region. For controller settings and statistics, time is displayed based on the Time Zone.
Primary NTP Server/ Secondary NTP Server	Enter the IP address of the primary and secondary NTP (Network Time Protocol) server. NTP servers assign network time to the controller.

Reset Button	With this feature enabled, the controller can be reset via reset button.
Network Settings	Select one way for the controller to get IP settings. Static: You need to specify the IP address, Netmask, Gateway, Primary DNS, and Secondary DNS for the controller. DHCP: The controller get IP settings from the DHCP server. If the controller fails to get IP settings from the DHCP server, it will use the Fallback IP Address and Fallback Netmask.

- **For Omada Software Controller / Omada Cloud-Based Controller**



Controller Name	Specify the Controller Name to identify the controller.
Time Zone	Select the Time Zone of the controller according to your region. For controller settings and statistics, time is displayed based on the Time Zone.

5. 1. 2 Mail Server

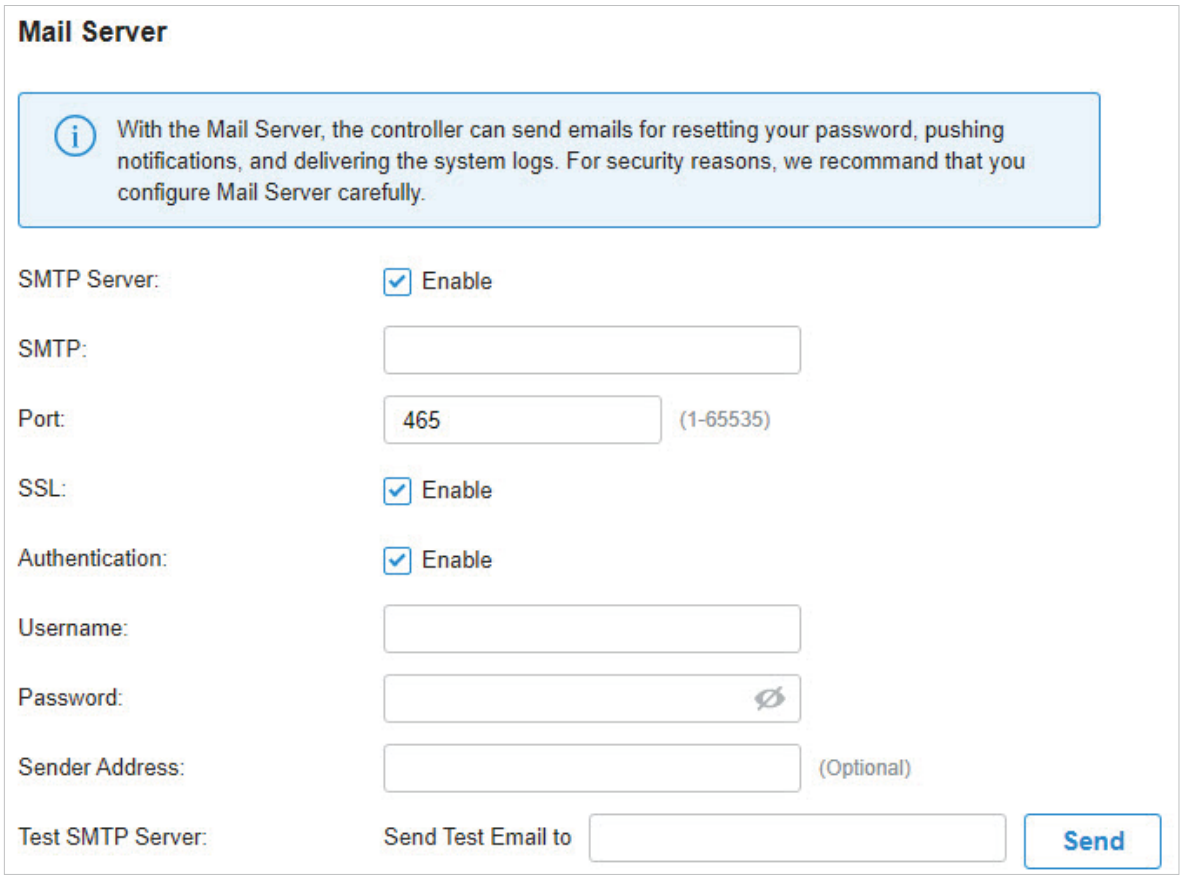
Overview

With the Mail Server, the controller 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 > Controller. In Mail Server, enable SMTP Server and configure the parameters. Then click Save.



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 the controller 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, the controller 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.

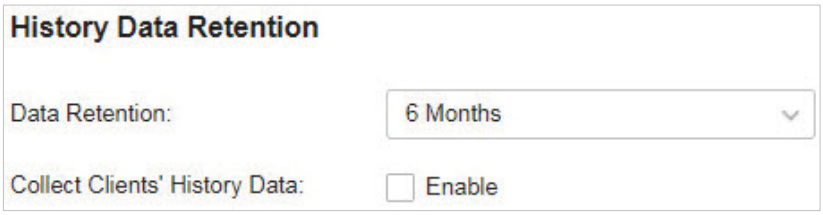
5. 1. 3 History Data Retention

Overview

With History Data Retention, you can specify how the controller retains its data.

Configuration

Go to Settings > Controller. In History Data Retention, configure the parameters and click Save.

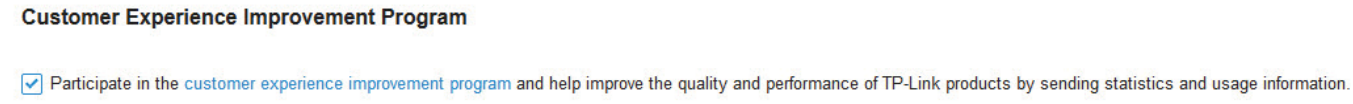


Data Retention	Select how long the controller retains its data. Any history data beyond the time range is dropped.
Collect Clients' History Data	With Collect Clients' History Data enabled, the history data of the clients are included in that of the controller.

5. 1. 4 Customer Experience Improvement Program

Configuration

Click the checkbox if you agree to participate in the customer experience improvement program and help improve the quality and performance of TP-Link products by sending statistics and usage information.



5. 1. 5 HTTPS Certificate

Overview

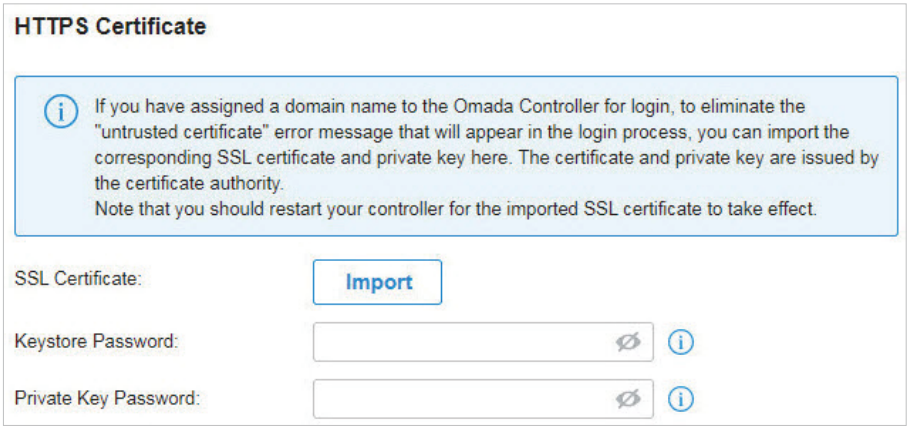
If you have assigned a domain name to the controller for login, to eliminate the "untrusted certificate" error message that will appear in the login process, you can import the corresponding SSL certificate and private key here. The certificate and private key are issued by the certificate authority.

Note:

- HTTPS Certificate configuration is only available for Omada Software Controller and Omada Hardware Controller.
- You need to restart you controller for the imported SSL certificate to take effect.

Configuration

Go to Settings > Controller. 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. Otherwise, leave it blank.
Private Key Password	Enter the private key password if your SSL certificate has the private key password. Otherwise, leave it blank.

5. 1. 6 Access Port Config

Overview

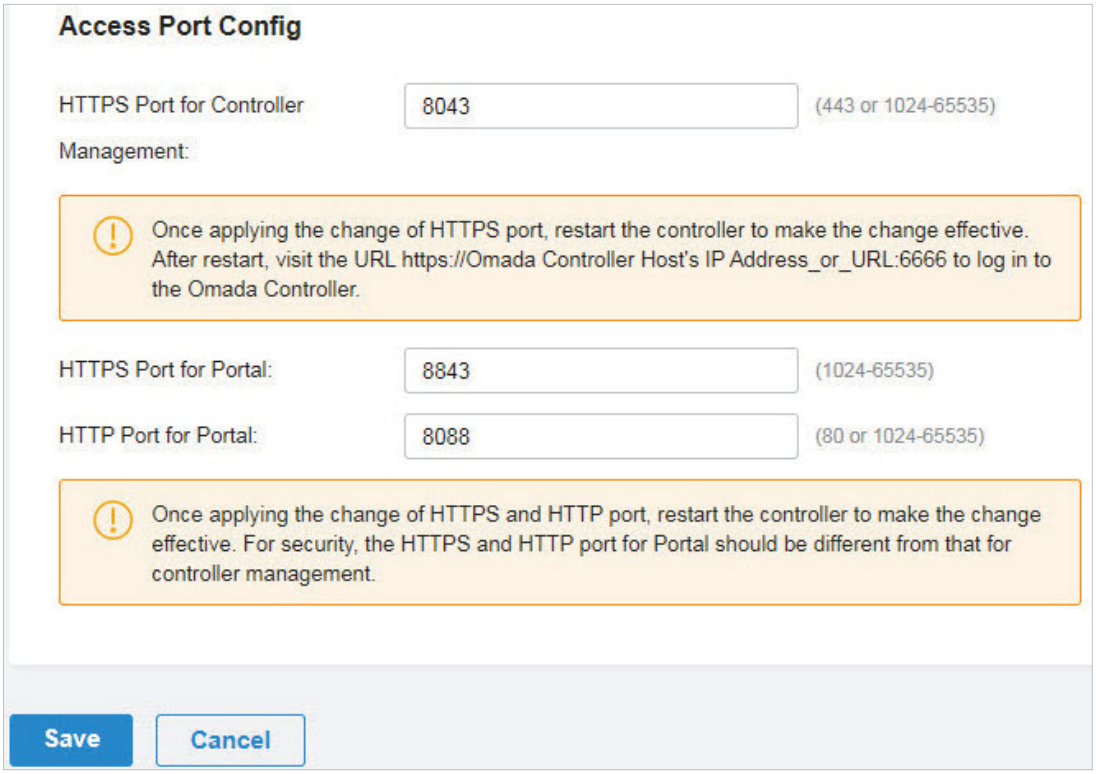
With Access Port Config, you can specify the port used by the controller for management and portal.

Note:

- Access Port Config is only available on Omada Software Controller and Omada Hardware Controller.
- Once applying the change of HTTPS and HTTP port, restart the controller to make the change effective.
- For security, the HTTPS and HTTP port for Potal should be different from that for controller management.

Configuration

Go to Settings > Controller. In Access Port Config, configure the parameters and click Save.



HTTPS Port for Controller Management	Specify the HTTPS port used by the controller for management. After setting the port, you can visit https://[Omada Controller Host's IP address or URL]:[Port] to log in to the Omada Controller.
HTTPS Port for Portal	Specify the HTTPS port used by the controller for Portal.
HTTP Port for Portal	Specify the HTTP port used by the controller for Portal.

5. 2 Manage Your Controller Remotely via Cloud Access

Overview

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

Configuration

To manage your controller from anywhere, follow these steps:

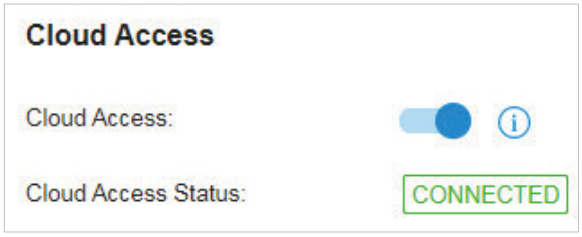
1. Prepare your controller for Cloud Access

■ **For Omada Software Controller / Omada Hardware Controller:**

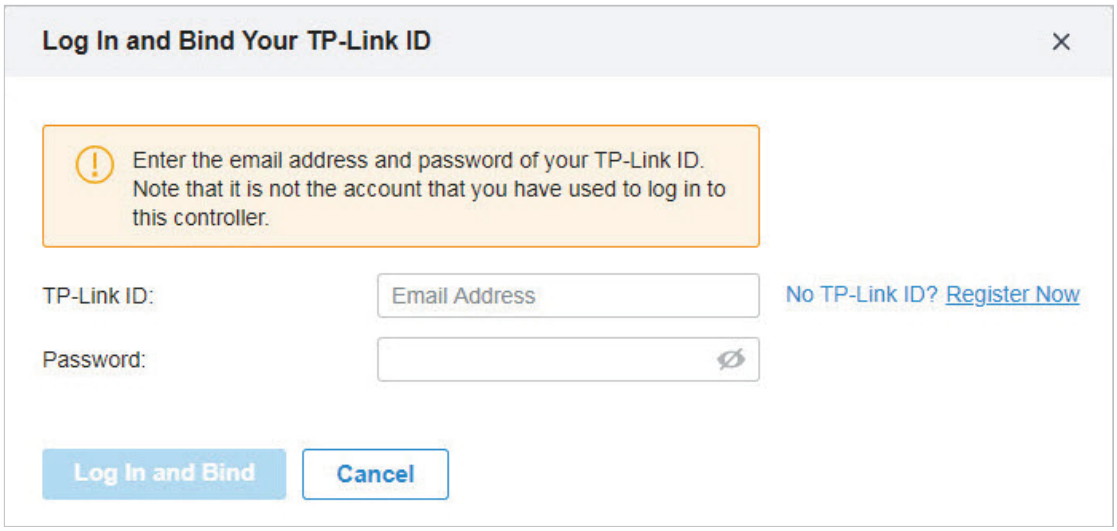
Note:

- Before you start, make sure your Omada Software Controller Host or Omada Hardware Controller 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.



■ **For Omada Cloud-Based Controller**

Your Omada Cloud-Based Controller is based on the Cloud, so it's naturally accessible through Cloud Service. No additional preparation is needed.

2. Access your controller through Cloud Service

Go to Omada Cloud and login with your TP-Link ID and password. A list of controllers that have been bound with your TP-Link ID will appear. Then click Launch to manage the controller.



5. 3 Maintenance

5. 3. 1 Controller Status

Go to Settings > Maintenance. In Controller Status, you can view the controller-related information and status.



Controller Name	Displays the controller name, which identifies the controller. You can specify the controller name in General Settings.
MAC Address	Displays the MAC address of the controller.
System Time	Displays the system time of the controller. The system time is based on the time zone which you configure in General Settings.
Uptime	Displays how long the controller has been working.
Controller Version	Displays the software version of the controller.

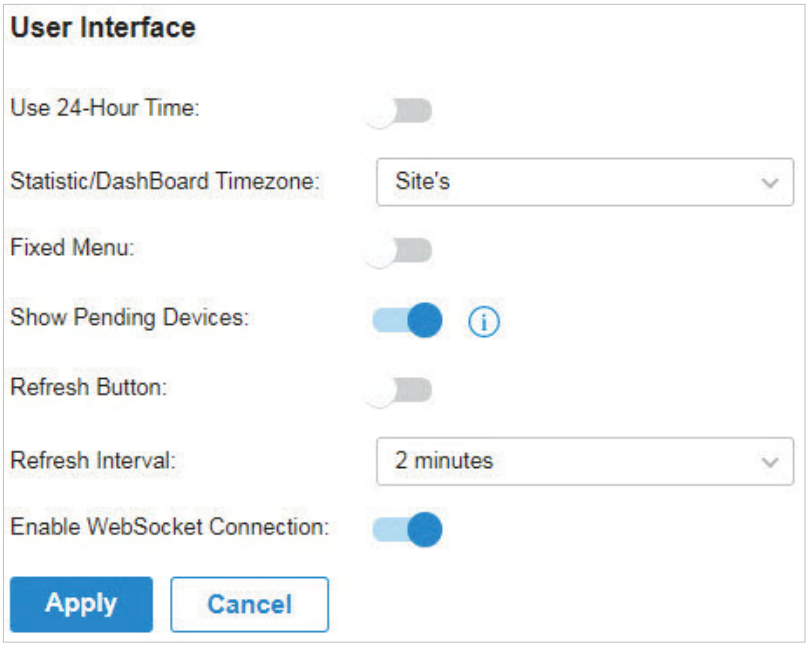
5. 3. 2 User Interface

Overview

You can customize the User Interface settings of the controller 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.
Statistic/Dashboard Timezone	Select which Timezone the time of statistics and the dashboard is based on. Site's: Site's Timezone is set in Site Configuration of the corresponding site. Browser's: Browser's Timezone is synchronized with the browser configuration. Controller's: Controller's Timezone is set in General Settings of the controller. UTC: UTC (Coordinated Universal Time) is the common time standard across the world.
Fixed Menu	With Fixed Menu enabled, the menu icons are fixed and do not prompt menu texts when your mouse hovers on them.
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.

Enable WebSocket Connection	With WebSocket Connection enabled, the controller updates in real time some part of its data on the web interface, which is transmitted using the WebSocket service, so that you don't need to refresh them manually.

5. 3. 3 Backup & Restore

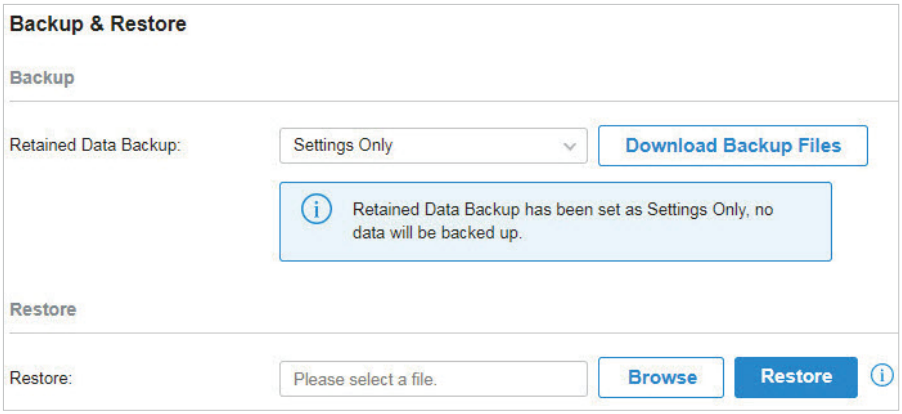
Overview

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

Configuration

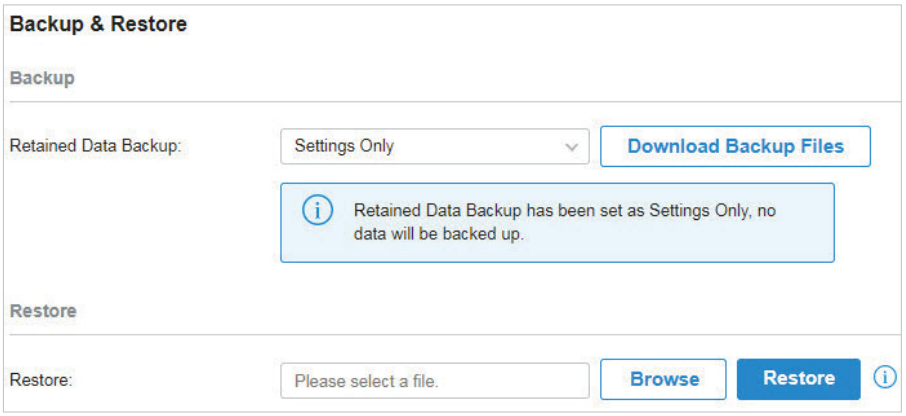
- **Backup**

Go to Settings > Maintenance. In Backup & Restore, select the time range in the drop-down menu of Retained Data Backup. 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.



5. 4 Migration

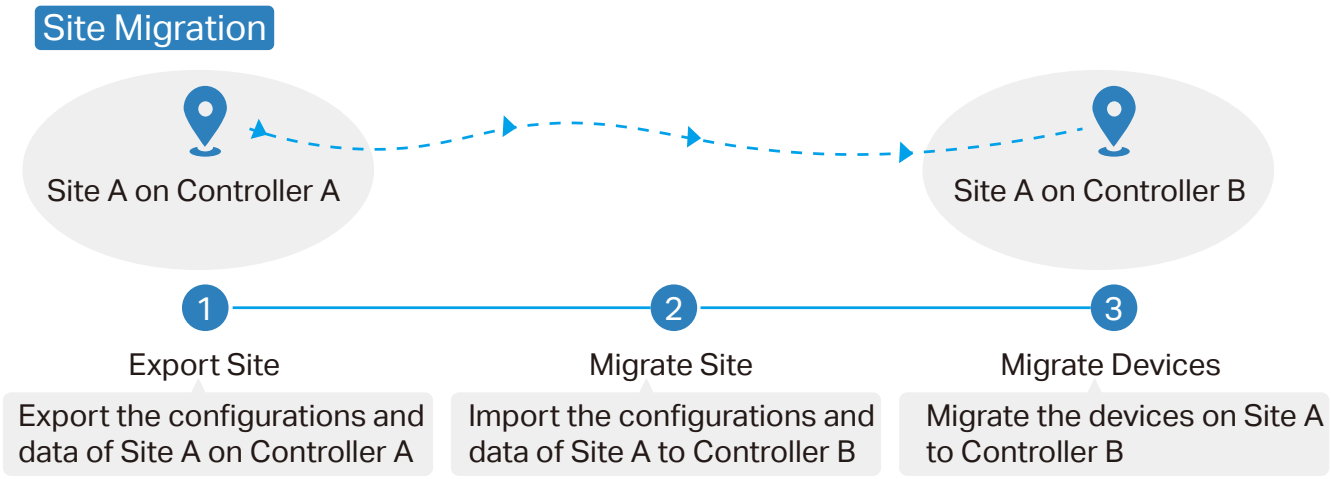
Migration services allow users to migrate the configurations and data to any other controller. Migration services include Site Migration and Controller Migration, covering all the needs to migrate both a single site and the whole controller.

5. 4. 1 Site Migration

Overview

Site Migration allows the administrators to export a site from the current controller to any other controller that has the same version. All the configurations and data of the site will be migrated to the target controller.

The process of migrating configurations and data from a site to another controller can be summarized in three steps: Export Site, Migrate Site and Migrate Devices.



Step1: Export Site

Export the configurations and data of the site to be migrated as a backup file.

Step2: Migrate Site

In the target controller, import the backup file of the original site.

Step3: Migrate Devices

Migrate the devices which are on the original site to the target controller.

Configuration

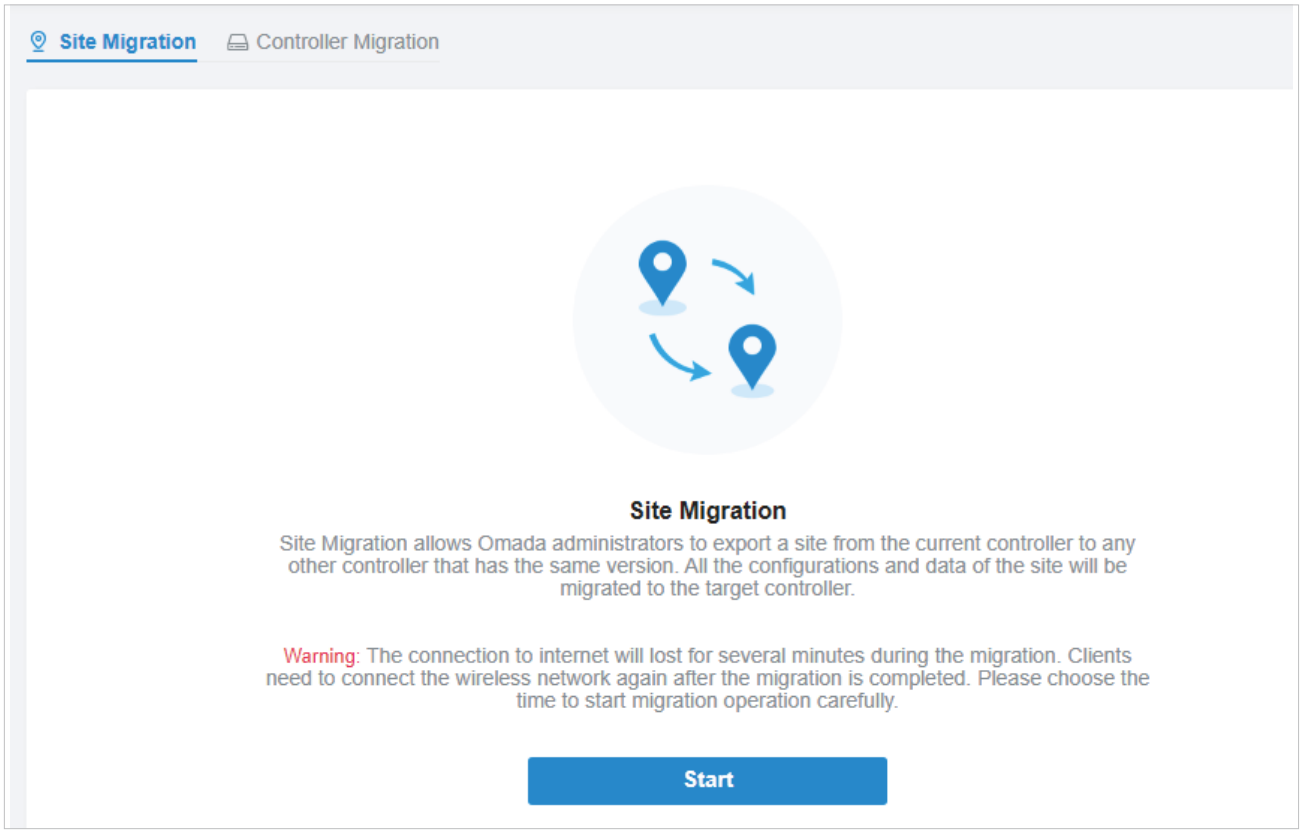
To migrate a site to anther controller, follow these steps below.

Note:

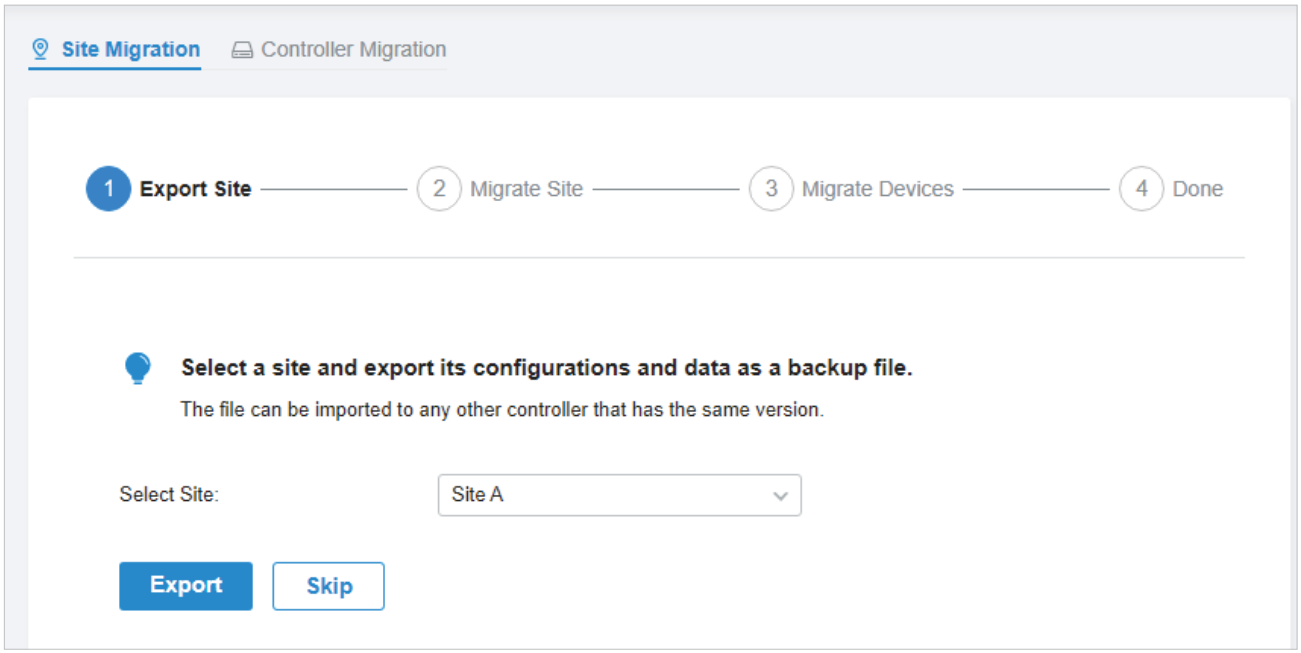
The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Export Site | Migrate Site | Migrate Devices

3. Go to Settings > Migration. On the Site Migration tab, click start button on the following page.

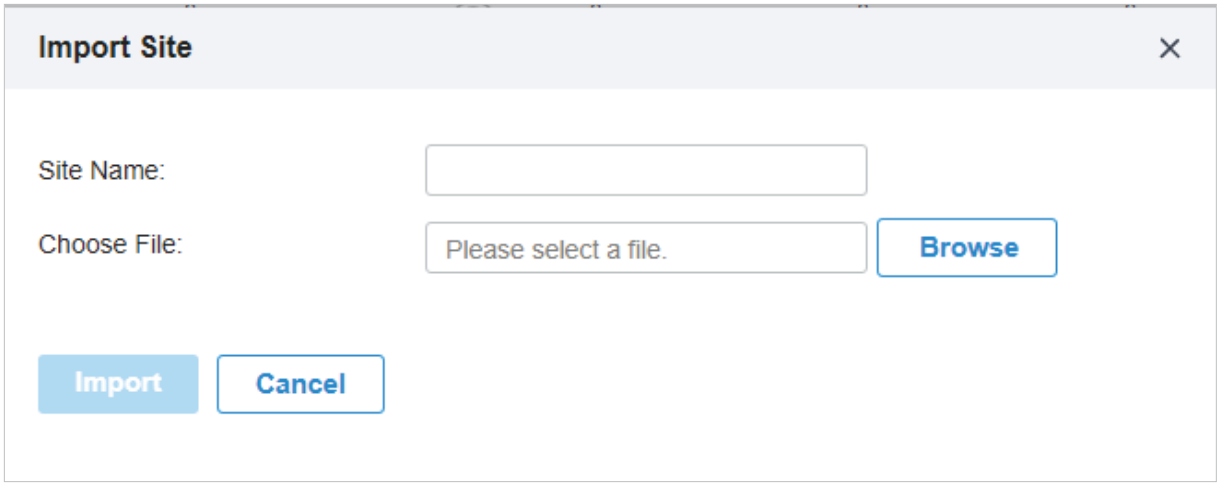


4. Select the site to be imported into the second controller in the Select Site drop-down list. Click Export to download the file of the current site. If you have backed up the file, click Skip.

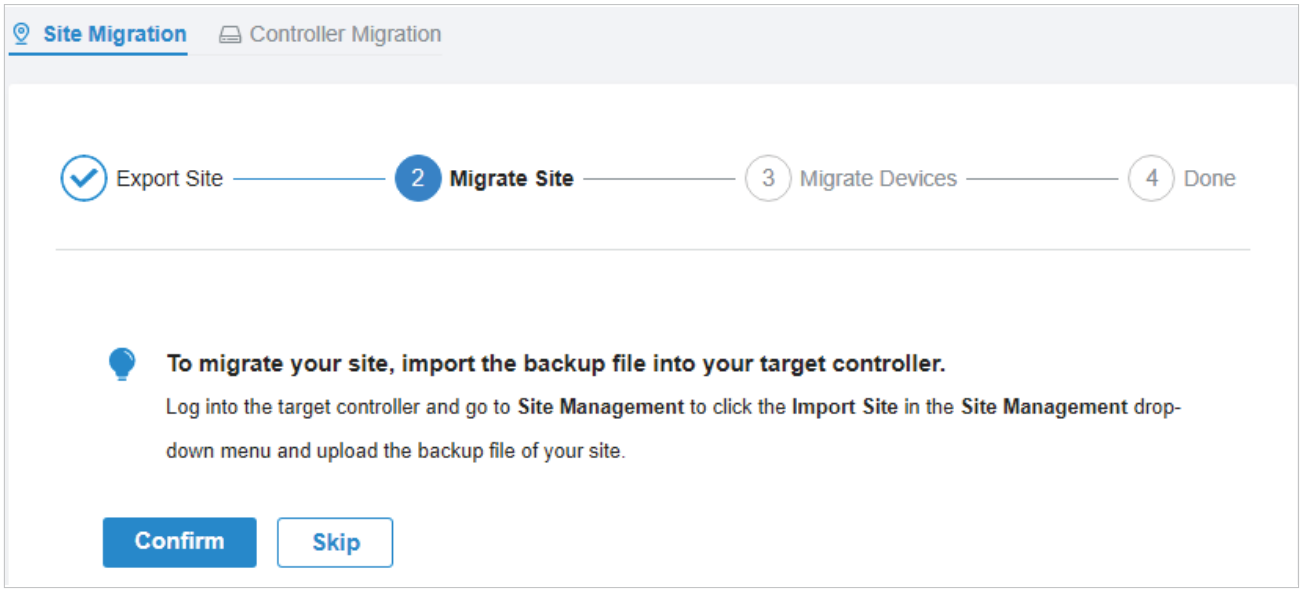




1. Start and log in to the target controller, click Sites: Site A the top right corner of the screen and select Import Site, and then the following window will pop up.

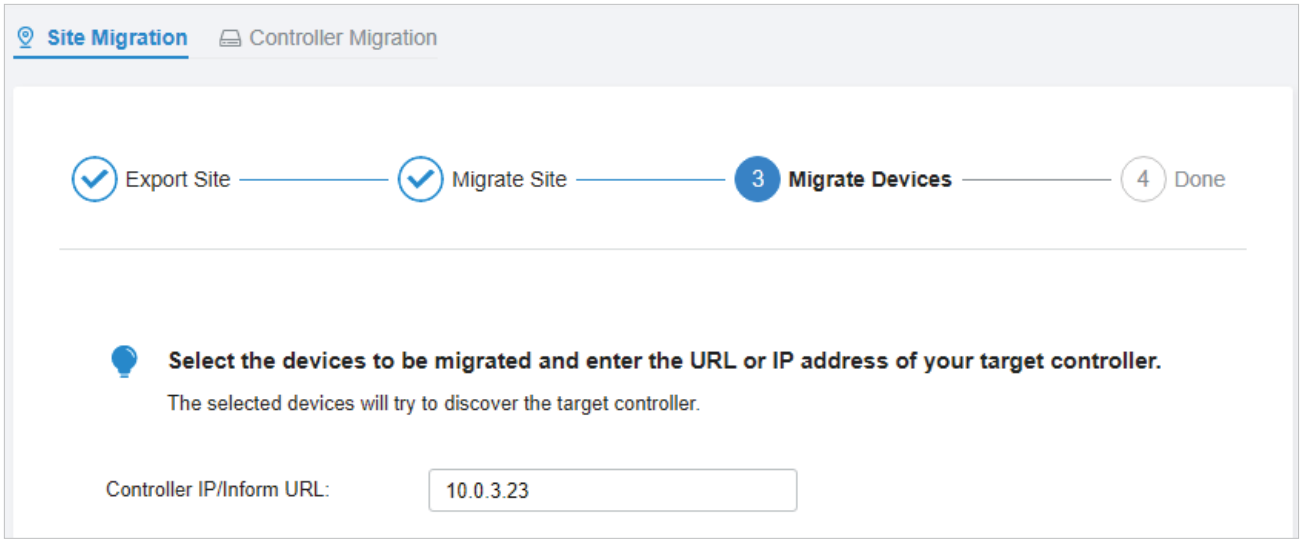


2. Enter a unique name for the new site. Click Browse to upload the file of the site to be imported and click Import to import the site.
3. After the file has been imported to the target controller, go back to the previous controller and click Confirm.





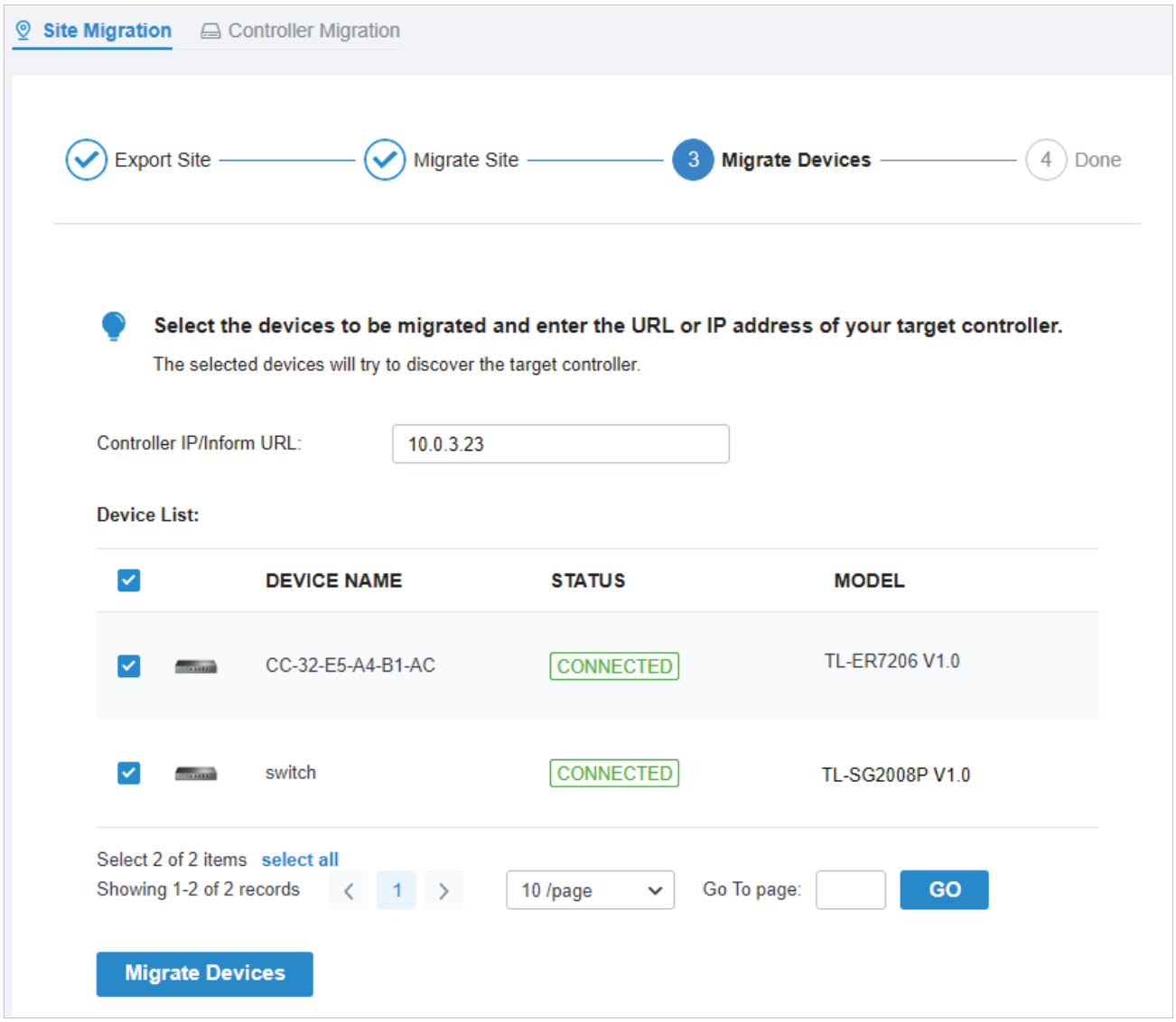
1. Enter the IP address or URL of your target controller into Controller IP/Inform URL input filed. In this case, the IP address of the target controller is 10.0.3.23.



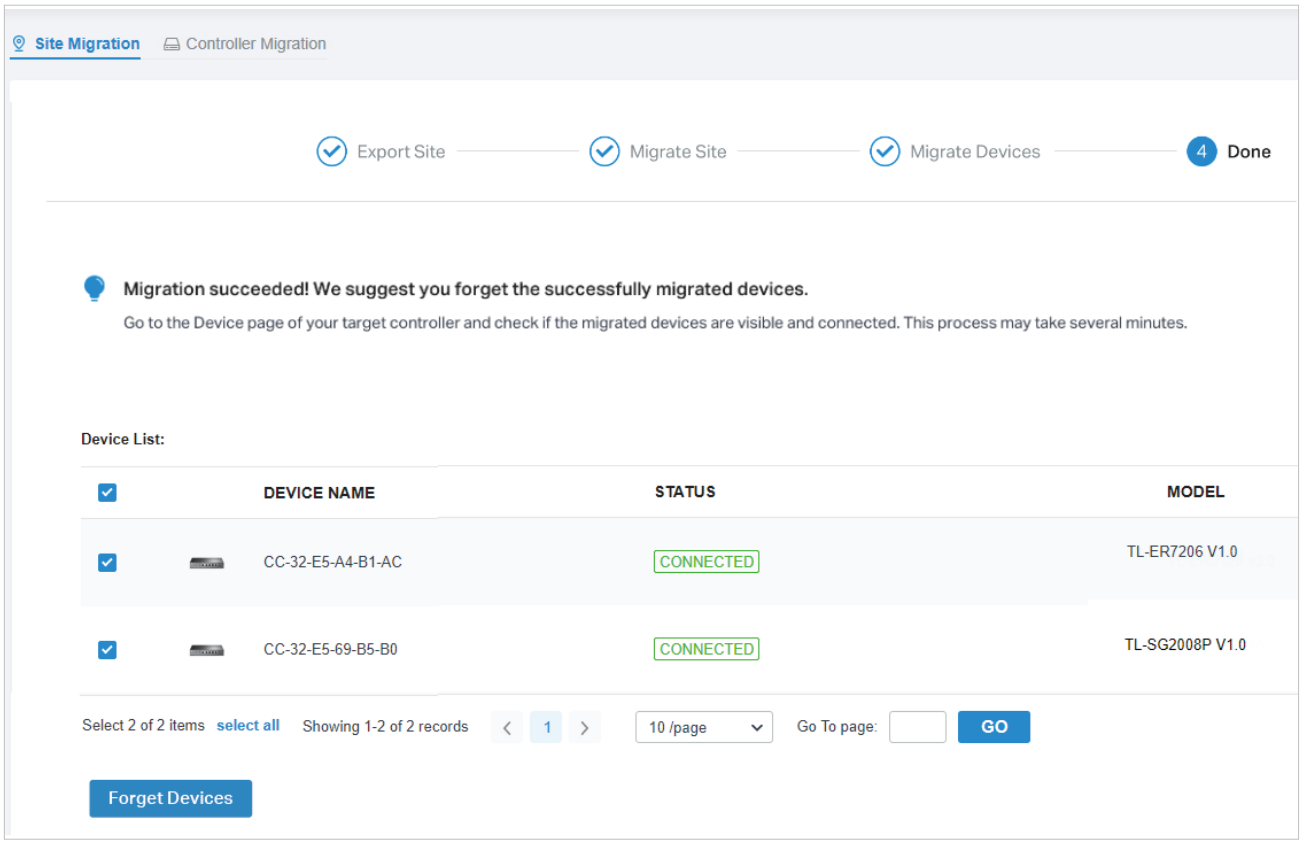
Note:

Make sure that you enter the correct IP address or URL of the target controller to establish the communication between Omada managed devices and your target controller. Otherwise Omada managed devices cannot be adopted by the target controller.

2. Select the devices that are to be migrated by clicking the box next to each device. By default, all the devices are selected. Click Migrate Devices to migrate the selected devices to the target controller.



3. Verify that all the migrated devices are visible and connected on the target controller. When all the migrated devices are in Connected status on the Device page on the target controller, click Forget Devices to finish the migration process.



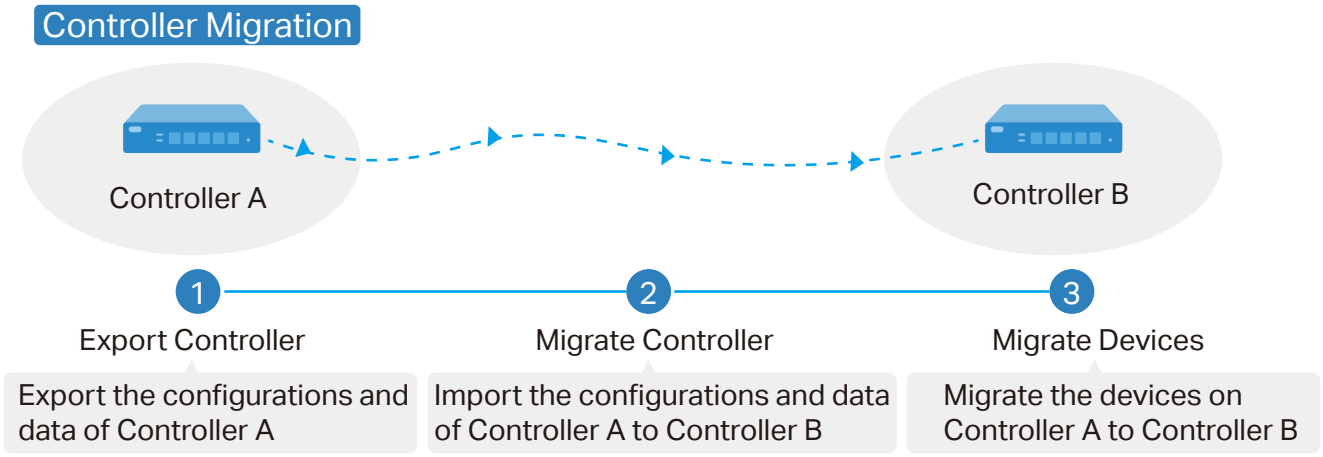
4. When the migration process is completed, all the configuration and data are migrated to the target controller. You can delete the previous site if necessary.

5. 4. 2 Controller Migration

Overview

Controller Migration allows Omada administrators to migrate the configurations and data from the current controller to any other controller that has the same version.

The process of migrating configurations and data from the current controller to another controller can be summarized in three steps: Export Controller, Migrate Controller and Migrate Devices.



Step1: Export Controller

Export the configurations and data of the current controller as a backup file.

Step2: Migrate Controller

In the target controller, import the backup file of the current controller.

Step3: Migrate Devices

Migrate the devices on the current controller to the target controller.

Configuration

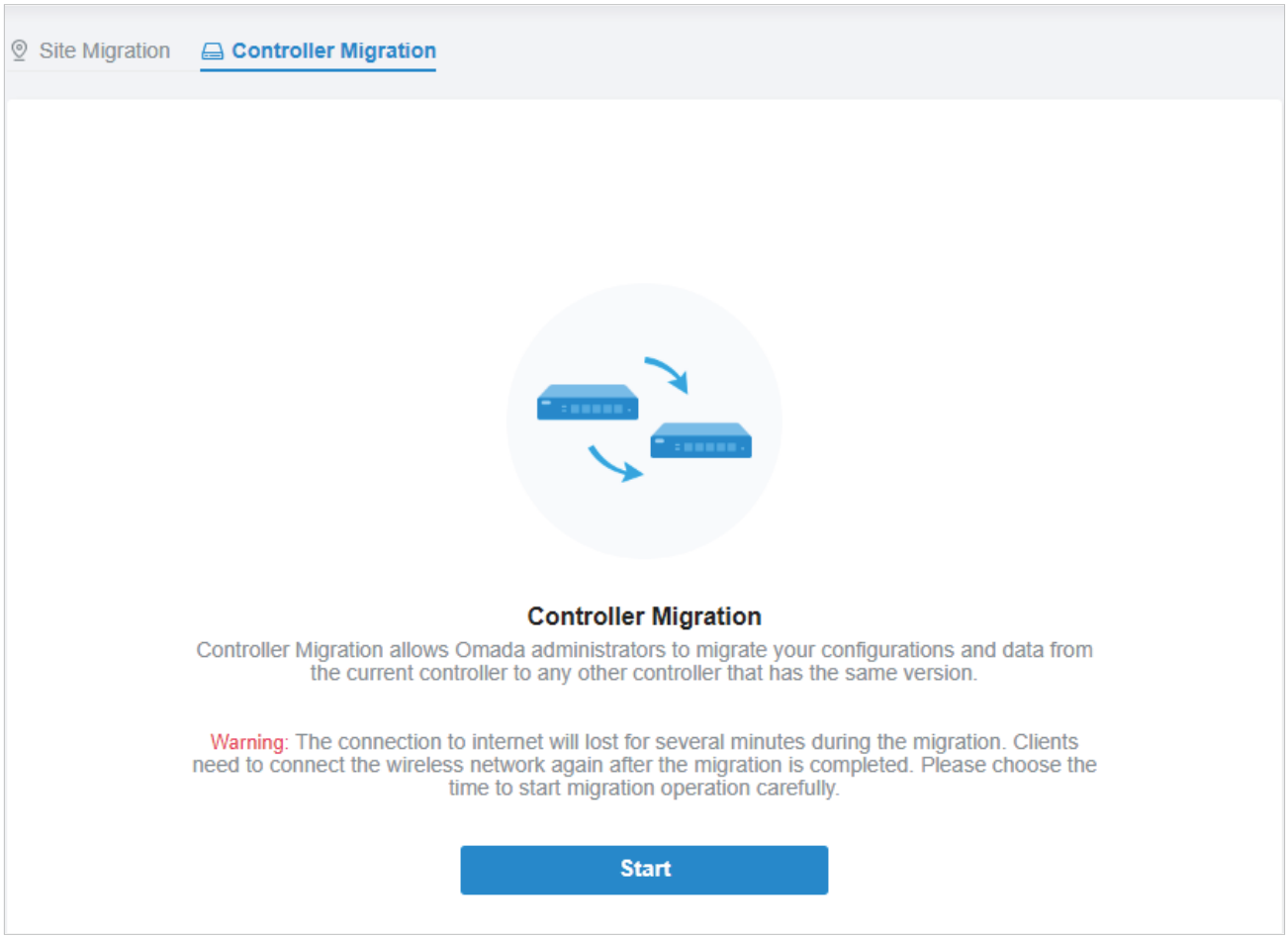
To migrate your controller, follow these steps below.

Note:

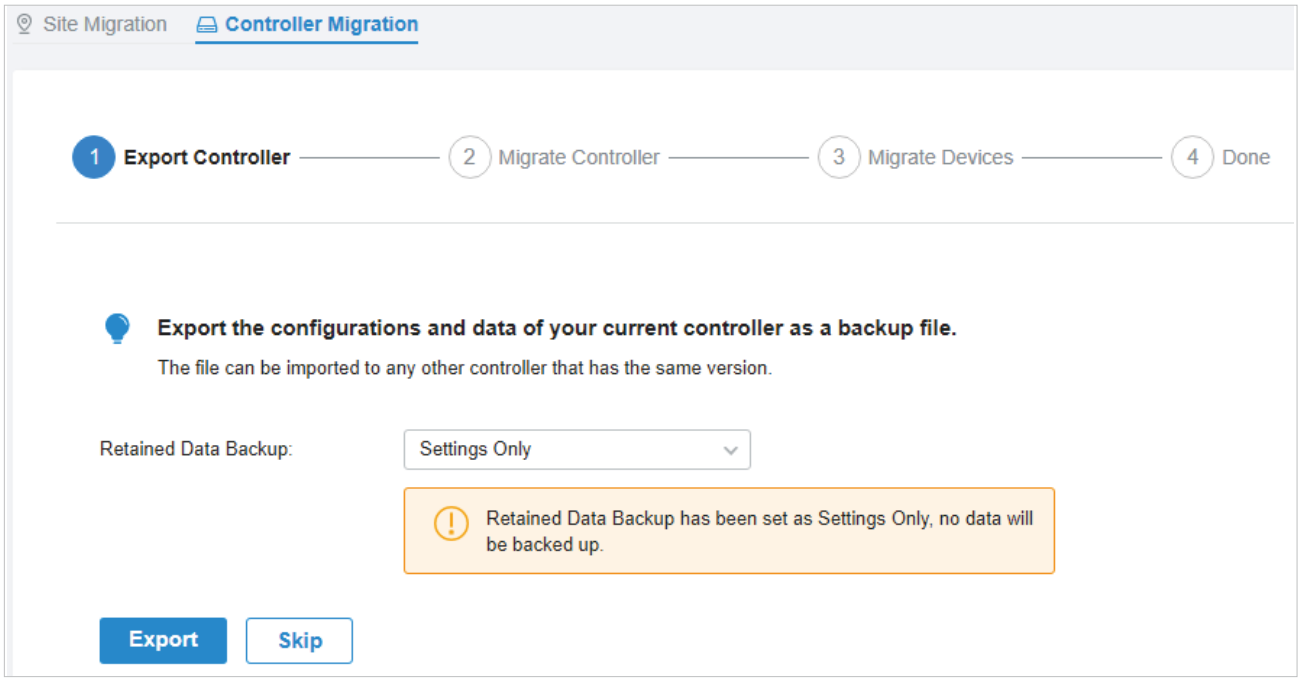
The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Export Controller | Migrate Controller | Migrate Devices

1. Go to Settings > Migration. On the Controller Migration tab, click start button on the following page.

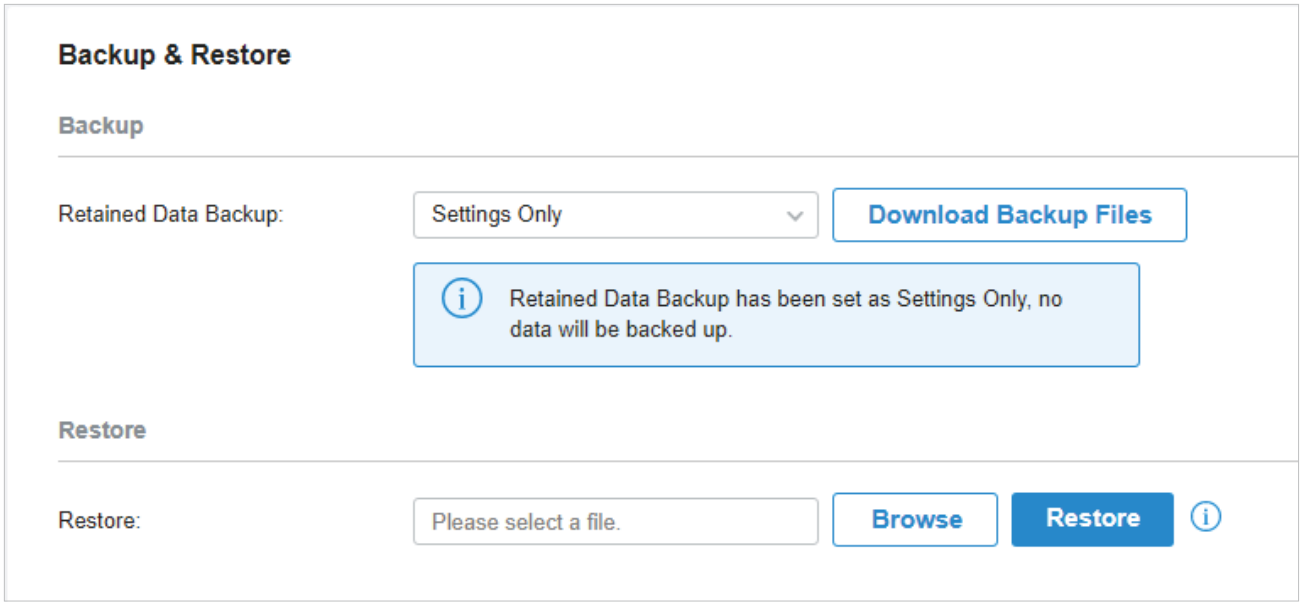


2. Select the length of time in days that data will be backed up in the Retained Data Backup, and click Export to export the configurations and data of your current controller as a backup file. If you have backed up the file, click Skip.

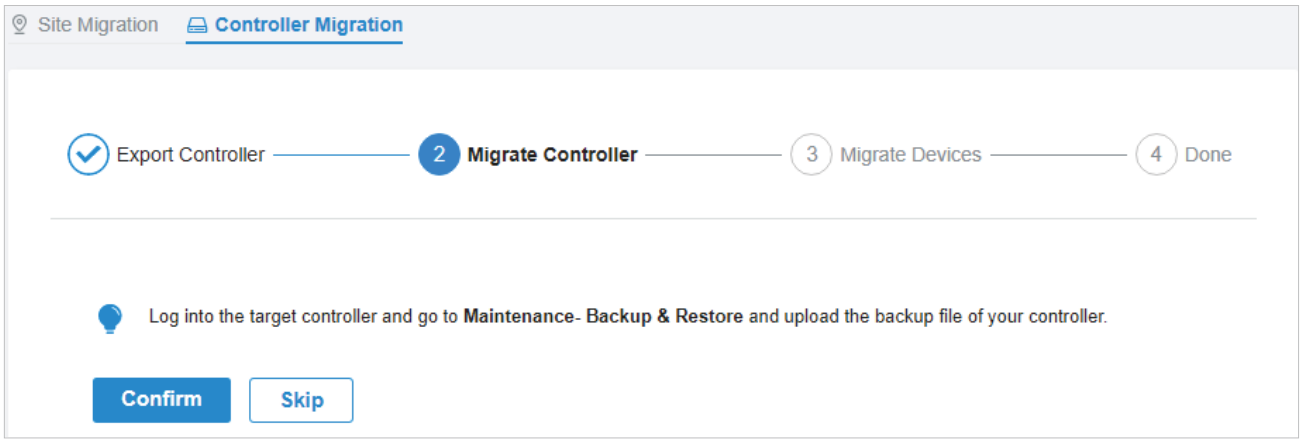


Export Controller > **Migrate Controller** > Migrate Devices

1. Log in to the target controller, go to Settings > Maintenance > Backup & Restore. Click Browse to locate and choose the backup file of the previous controller. Then click Restore to upload the file.

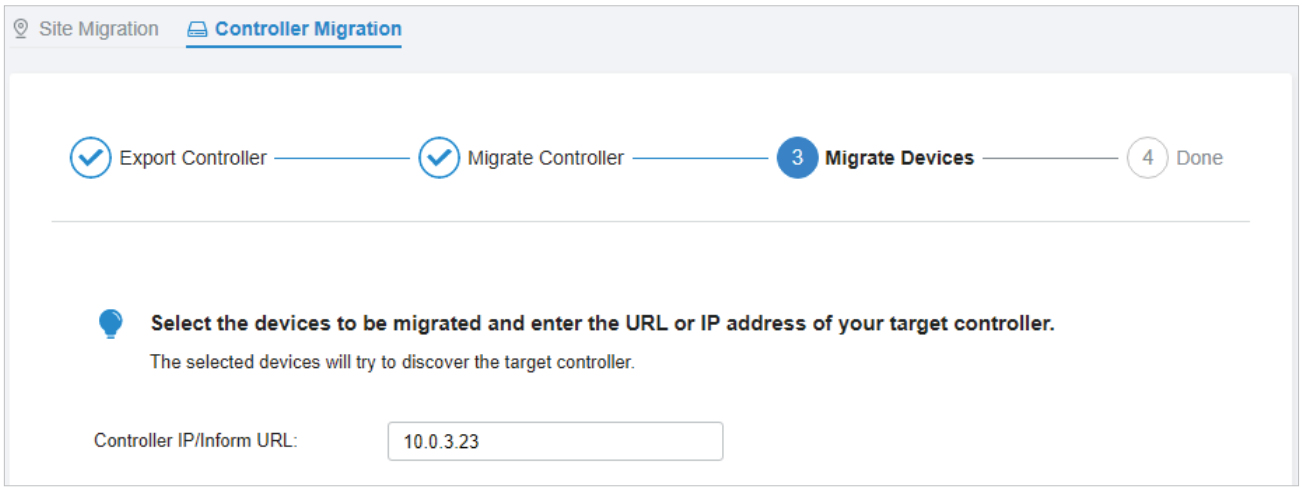


2. After the file has been imported to the target controller, go back to the previous controller and click Confirm.



Export Controller > Migrate Controller > Migrate Devices

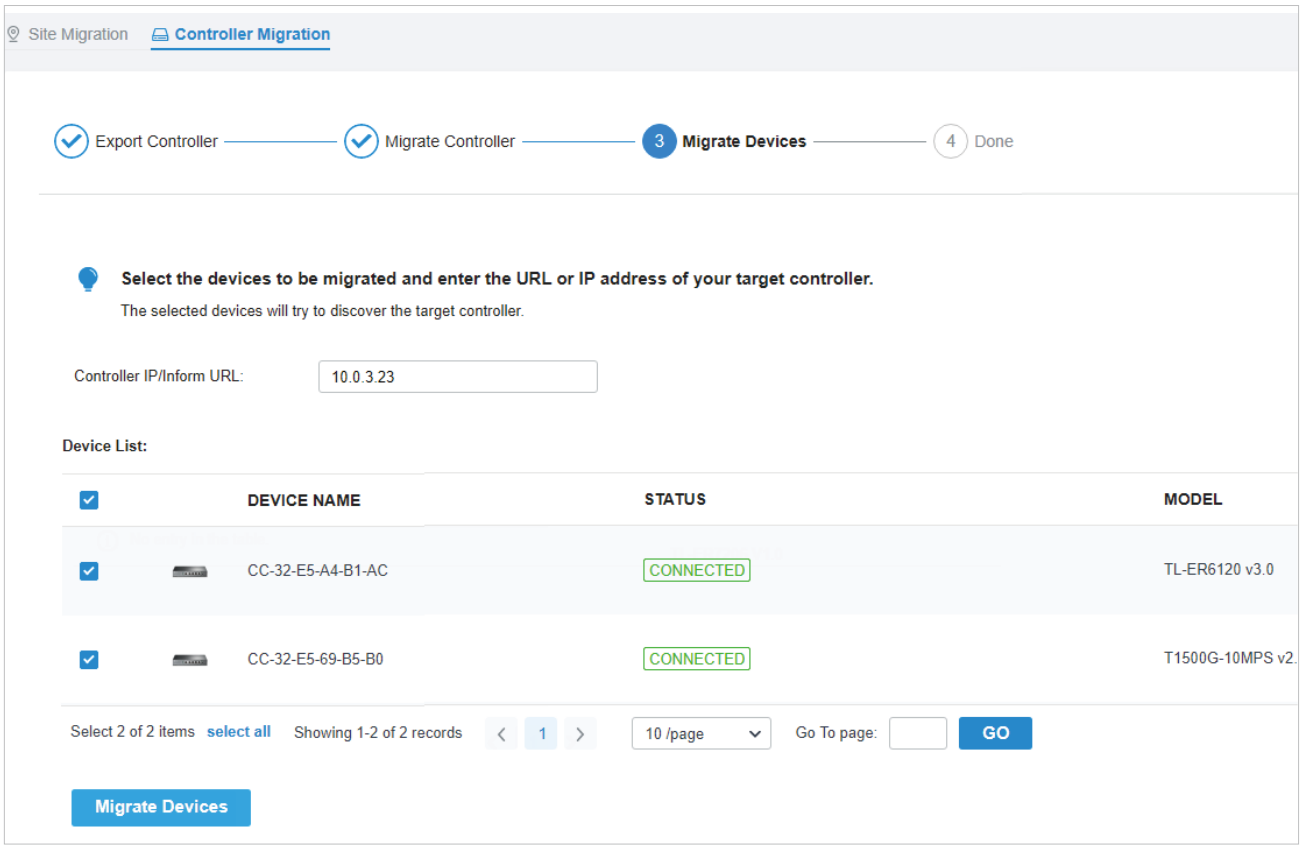
1. Enter the IP address or URL of your target controller into Controller IP/Inform URL input filed. In this case, the IP address of the target controller is 10.0.3.23.



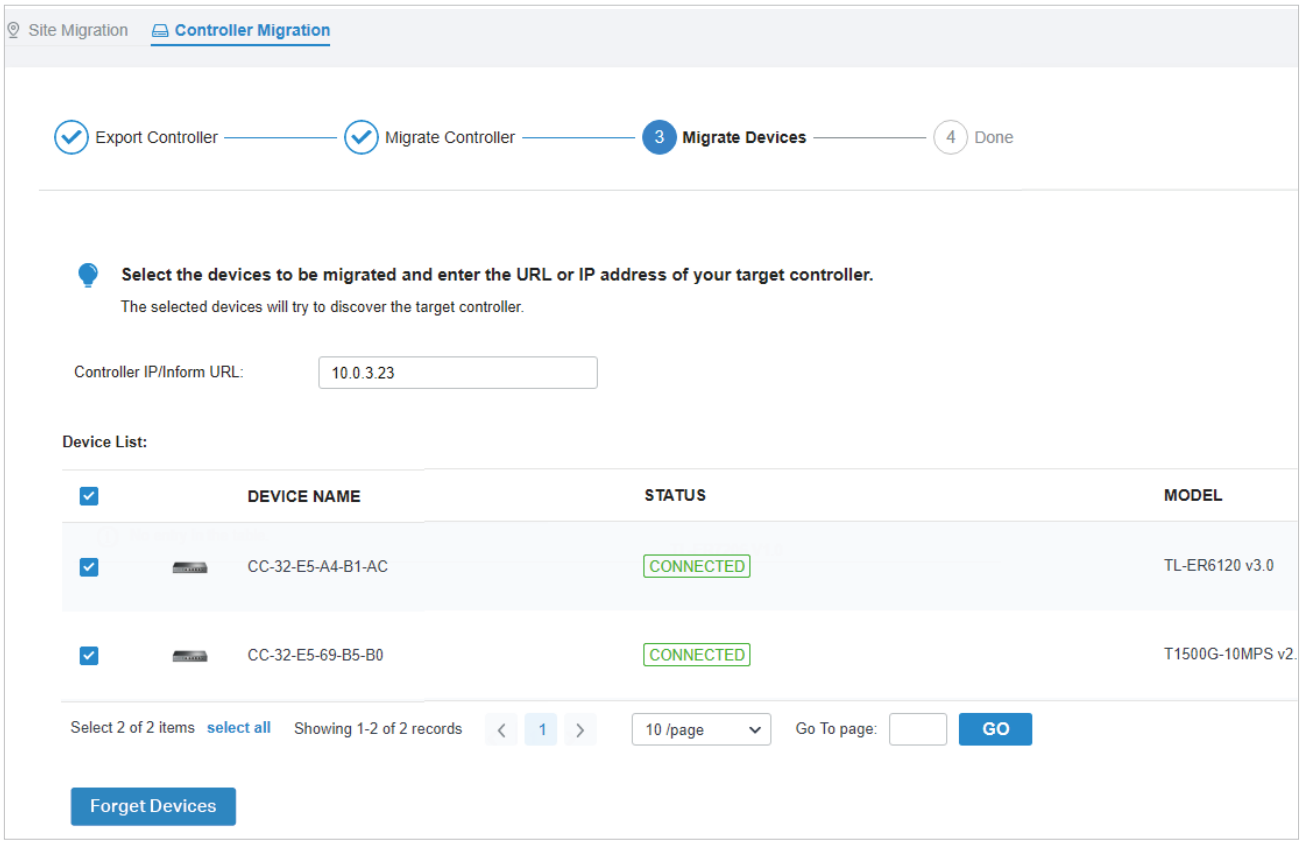
Note:

Make sure that you enter the correct IP address or URL of the target controller to establish the communication between Omada managed devices and your target controller. Otherwise Omada managed devices cannot be adopted by the target controller.

2. Select the devices that are to be migrated by clicking the box next to each device. By default, all the devices are selected. Click Migrate Devices to migrate the selected devices to the target controller.



3. Verify that all the migrated devices are visible and connected on the target controller. When all the migrated devices are in Connected status on the Device page on the target controller, click Forget Devices to finish the migration process.



4. When the migration process is completed, all the configuration and data are migrated to the target controller. You can uninstall the previous controller if necessary.

6

Configure and Monitor Omada Managed Devices

This chapter guides you on how to configure and monitor Omada managed devices, including gateways, switches and EAPs. You can configure the devices individually or in batches to modify the configurations of certain devices. The chapter includes the following sections:

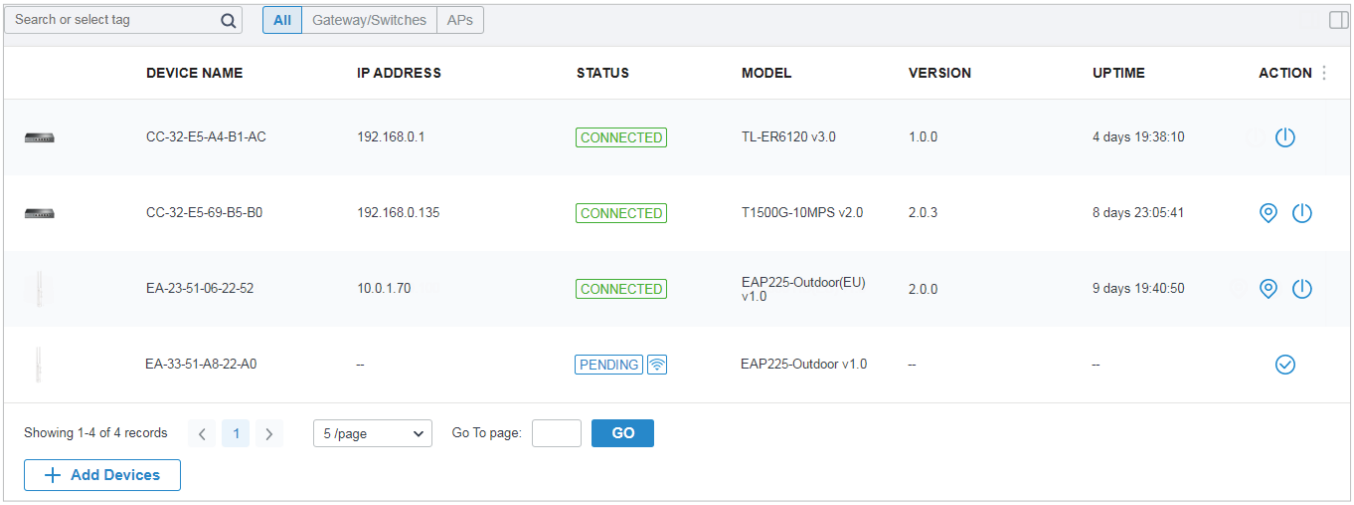
- Introduction to the Devices Page
- Configure and Monitor the Gateway
- Configure and Monitor Switches
- Configure and Monitor EAPs

6. 1 Introduction to the Devices Page

Overview

The Devices page displays all TP-Link devices discovered by the controller and their general information.

For an easy monitoring of the devices, you can customize the column and filter the devices for a better overview of device information. Also, quick operations and Batch Edit are available for configurations.



According the connection status, the devices have the following status: Pending, Isolated, Connected, Managed by Others, Heartbeat Missed,and Disconnected. The icons in the Status column are explained as follows:

PENDING	The device is in Standalone Mode or with factory settings, and has not been adopted by the controller. To adopt the device, click ✓, and the controller will use the default username and password to adopt it. When adopting, its status will change from Adopting, Provisioning, Configuring, to Connected eventually.
ISOLATED	(For APs in the mesh network) The AP once managed by the controller via a wireless connection now cannot reach the gateway. You can rebuild the mesh network by connecting it to an AP in the Connected status, then the isolated AP will turn into a connected one. For detailed configuration, refer to Mesh.
CONNECTED	The device has been adopted by the controller and you can manage it centrally. A connected device will turn into a pending one after you forget it.
MANAGED BY OTHERS	The device has already been managed by another controller. You can reset the device or provide the username and password to unbind it from another controller and adopt it in the current controller.
HEARTBEAT MISSED	A transition status between Connected and Disconnected. Once connected to the controller, the device will send inform packets to the controller in a regular interval to maintain the connection. If the controller does not receive its inform packets in 30 seconds, the device will turn into the Heartbeat Missed status. For a heartbeat-missed device, if the controller receives an inform packet from the device in 5 minutes, its status will become Connected again; otherwise, its status will become Disconnected.

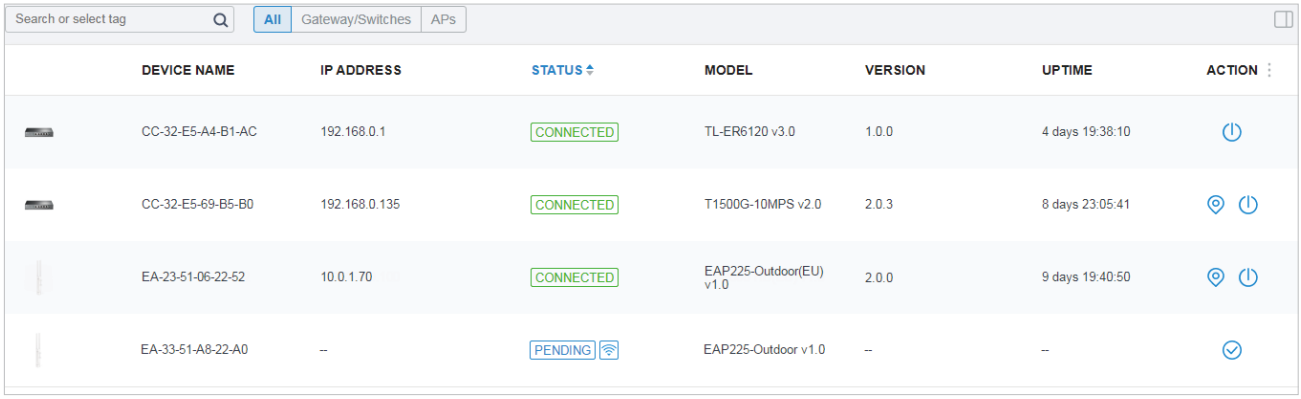
DISCONNECTED	The connected device has lost connection with the controller for more than 5 minutes.
	(For APs in the mesh network) When this icon appears with a status icon, it indicates the EAP with mesh function and no wired connection is detected by the controller. You can connect it to an uplink AP through Mesh.
	When this icon appears with a status icon, it indicates the device in the Connected, Heartbeat Missed, Isolated, or Disconnected status is migrating. For more information about Migration, refer to Migration.

Configuration

Customize the Column

To customize the columns, click ⋮ next to Action and check the boxes of information type.

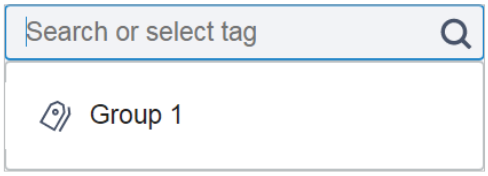
To change the list order, click the column head and ⇕ will appear to indicate the ascending or descending order.

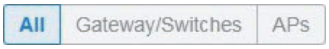


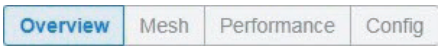
Filter the Devices

Use the search box and tab bar above the table to filter the devices.

To search the devices, enter the text in the search box or select a tag from the drop-down list. As for the device tag, refer to the general configuration of switches and EAPs.



To filter the devices, a tab bar  is above the table to filter the devices by device type.

If you select the APs tab, another tab bar  will be available to change the column quickly.

Overview	Displays the device name, IP address, status, model, firmware version, uptime, channel, and Tx power by default.

Mesh	Displays the information of devices in the mesh network, including the device name, IP address, status, model, uplink device, channel, Tx power, and the number of downlink devices, clients and hops by default.
Performance	Displays the device name, IP address, status, uptime, channel, Tx power, the number of 2.4 GHz and 5 GHz clients, Rx rate, and Tx rate by default.
Config	Displays the device name, status, version, WLAN group, and the radio settings for 2.4 GHz and 5 GHz by default.

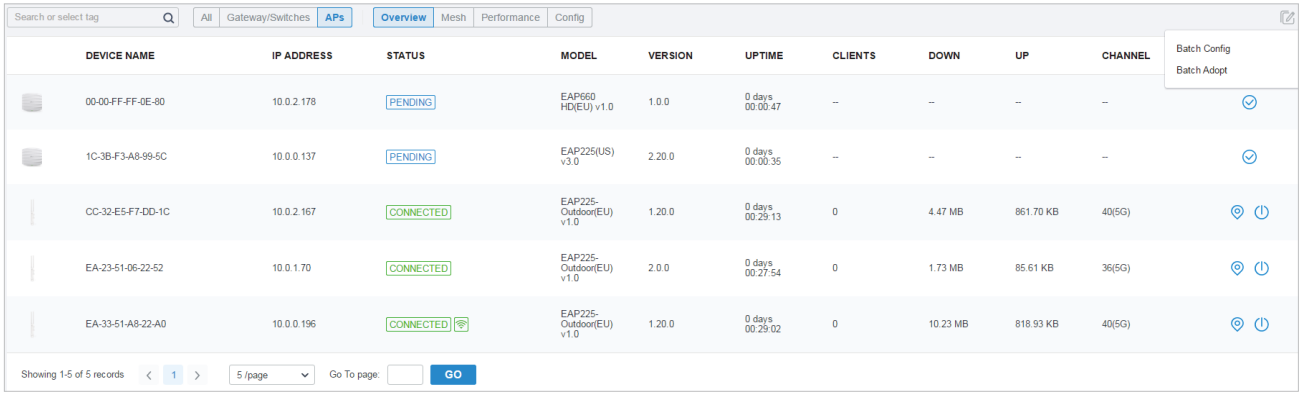
Quick Operations

Click the icons in the Action column to quickly adopt, locate, upgrade, or reboot the device.

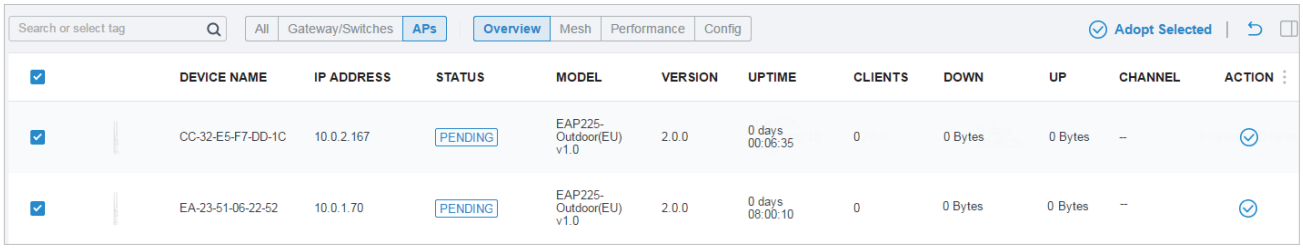
	(For pending devices) Click to adopt the device.
	(For connected switches and APs) Click this icon and the LEDs of the device will flash to indicate the device's location. The LEDs will keep flashing for 10 minutes, or you can click the icon to stop the flashing.
	(For connected devices) Click to reboot the device.
	Click to upgrade the device's firmware version. This icon appears when the device has a new firmware version. For Automatic Upgrades, refer to Services.

Batch Edit (for Switches and EAPs)

After selecting the Gateway/Switches or APs tab, you can adopt or configure the switches or EAPs in batches. Batch Config is available only for the devices in Connected/Disconnected/Heartbeat Missed/Isolated status, while Batch Adopt is available for the devices in the Pending/Managed By Others status.



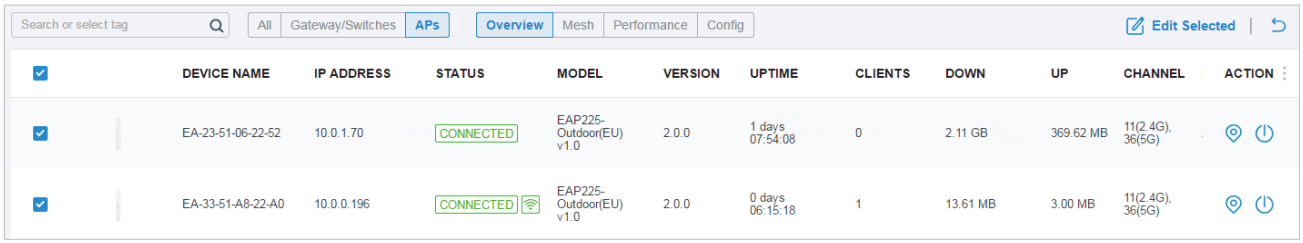
Click , select Batch Adopt, click the checkboxes of devices, and click Adopt Selected. If the selected devices are all in the Pending status, the controller will adopt then with the default username and password. If not, enter the username and password manually to adopt the devices.



Click , select Batch Config, click the checkboxes of devices, and click Edit Selected. Then the Properties window appears. There are two tabs in the window: Devices and Config.

In Devices, you can click to remove the device from the current batch configuration.

In Config, all settings are Keep Existing by default. For detailed configurations, refer to the configuration of switches and EAPs.

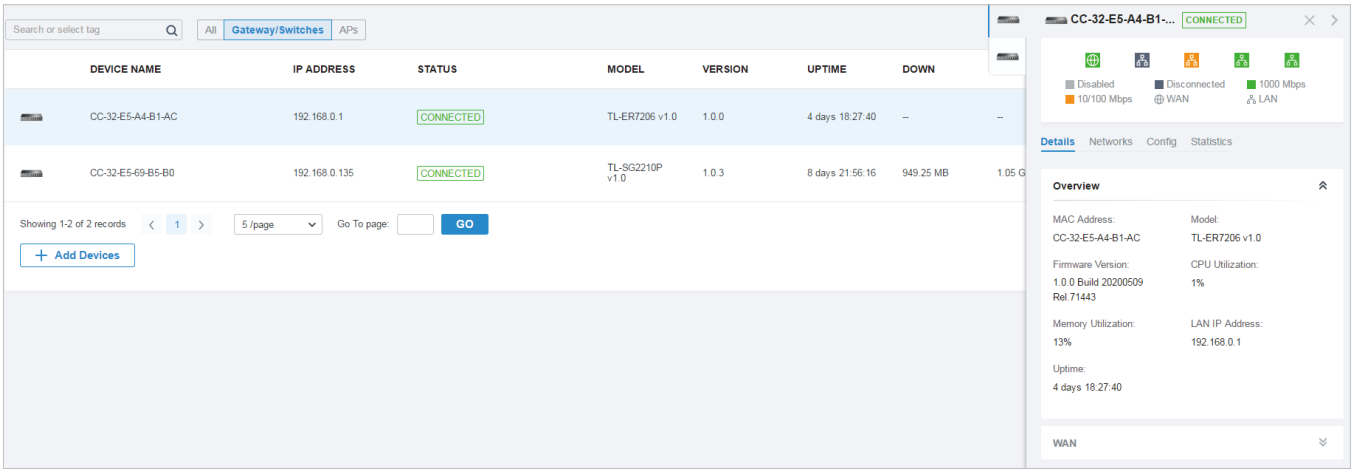


	Click to select multiple devices and add them to the Properties window for batch monitoring and management.
	Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click .
	Click to maximize the Properties window. You can also use the icon on pages other than the Devices page.
	Click to close the Properties window of the chosen device(s). Note that the unsaved configuration will be lost.
	The number on the lower-right shows the number of devices in the batch configuration.

6. 2 Configure and Monitor the Gateway

In the Properties window, you can configure the gateway managed by the controller and monitor the performance and statistics. By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of a router. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Config tab, such as IP, SNMP, IPTV, and Hardware Offload, while other tabs are mainly used to monitor the devices.



Note:

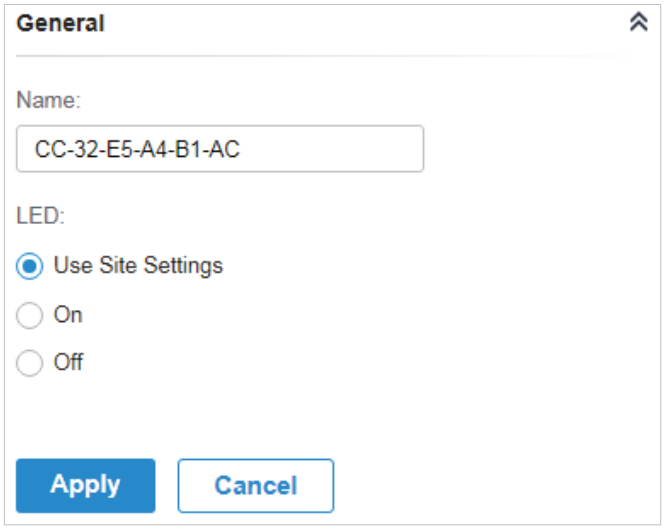
- You can adopt only one router in one site.
- The available functions in the window vary due to the model and status of the device.

6. 2. 1 Configure the Gateway

In the Properties window, click Config and then click the sections to configure the features applied to the router, including general settings, SNMP, IPTV, and advanced functions.

General

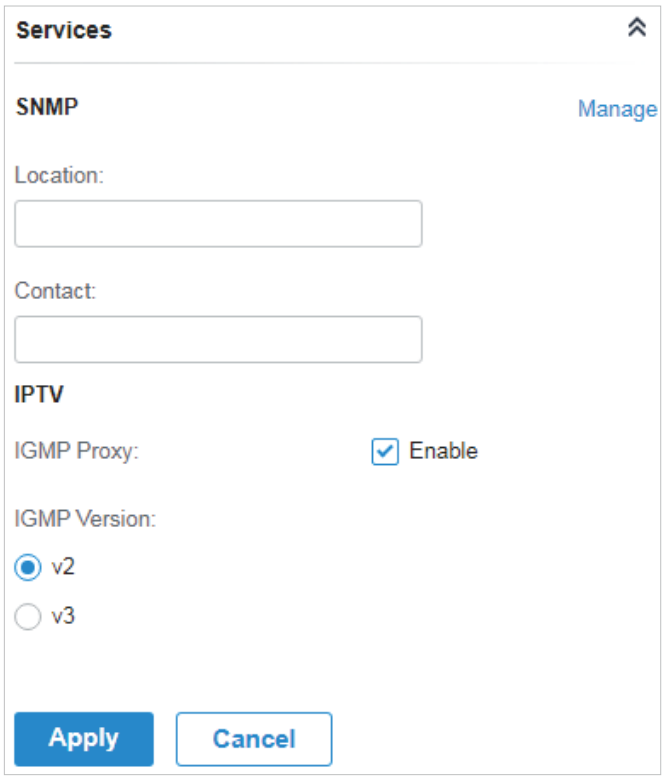
In General, you can specify the device name and LED settings of the router.



Name	Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to Services. On/Off: The device's LED will keep on/off.

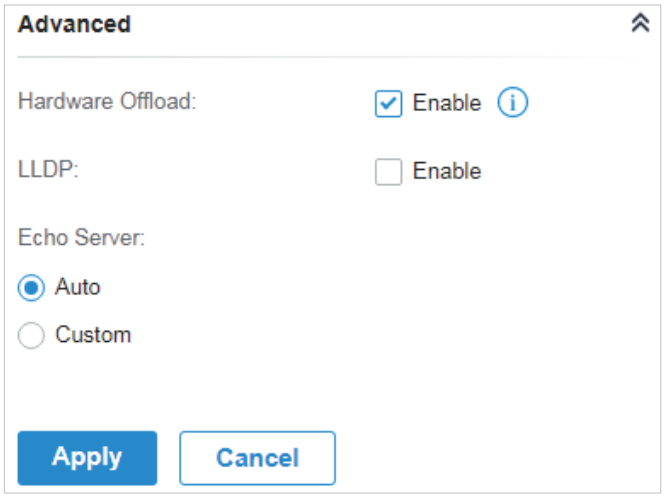
- **Services**

  In Services, you can configure SNMP to write down the location and contact detail, and enable IGMP Proxy to detect multicast number group memberships. You can also click Manage to jump to Settings > Services > SNMP, and for detailed configuration of SNMP service, refer to SNMP.



Advanced

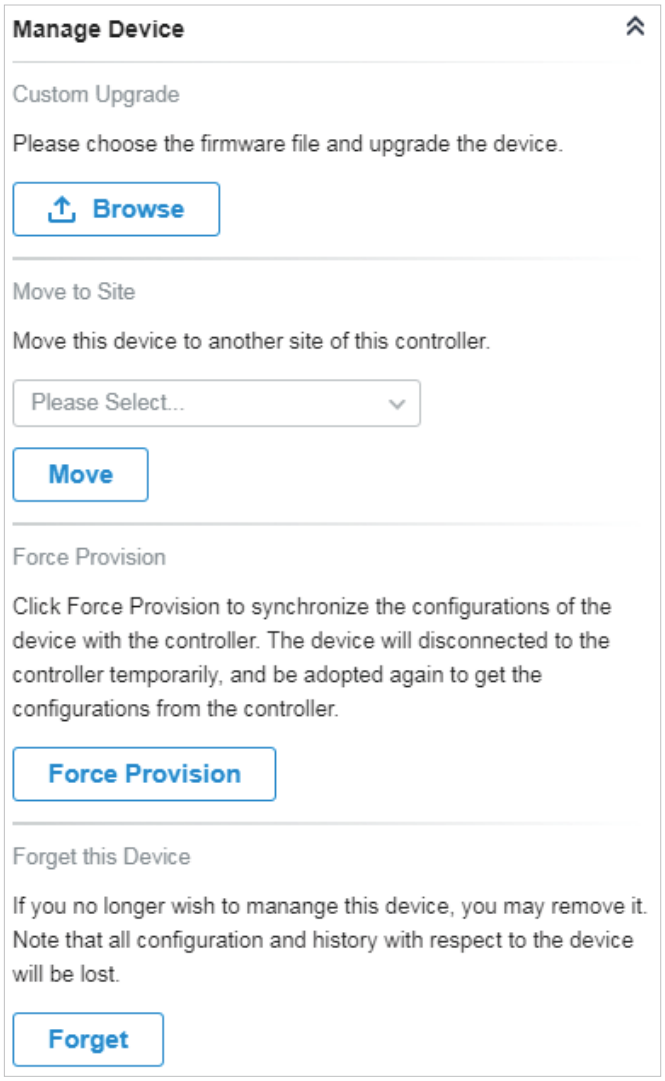
In Advanced, you can configure Hardware Offload, LLDP (Link Layer Discovery Protocol) and Echo Server to make better use of network resources.



Hardware Offload	Hardware Offload can improve performance and reduce CPU utilization by using the hardware to offload packet processing. Note that this feature cannot take effect if QoS, Bandwidth Control, or Session Limit is enabled. To configure Bandwidth Control and Session Limit for the router, refer to Transmission.
LLDP	LLDP can help discover devices.
Echo Server	Echo Server is used to test the connectivity and monitor the latency of the network automatically or manually. If you click Custom, enter the IP address or hostname of your custom server.

Manage Device

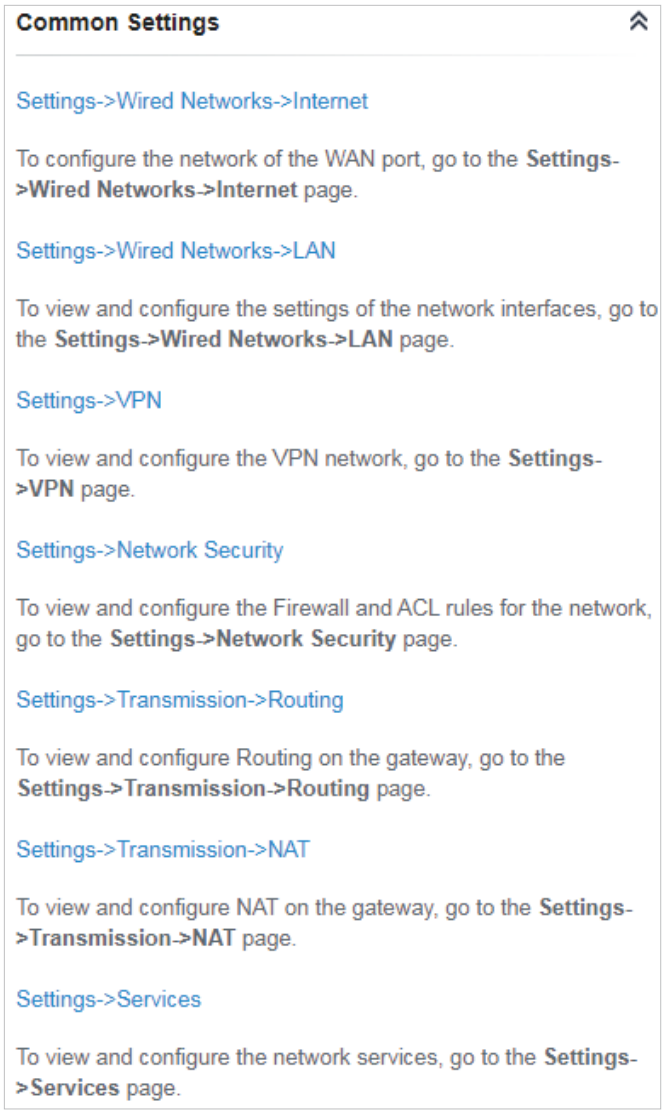
In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller, and forget the router.



Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.

- **Common Settings**

  In Common Settings, you can click the path to jump to corresponding modules quickly.

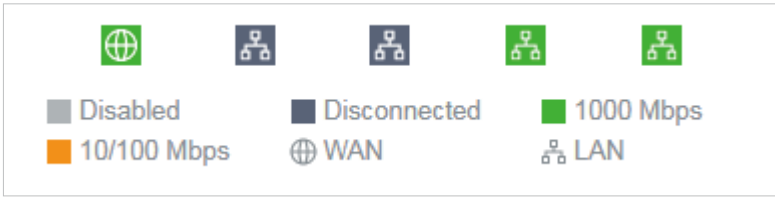


6. 2. 2 Monitor the Gateway

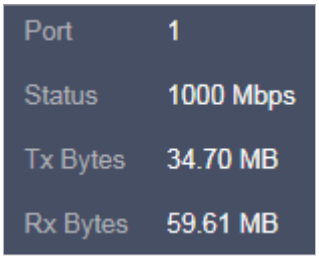
One panel and three tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Networks, and Statistics.

Monitor Panel

The monitor panel displays the router's ports, and it uses colors and icons to indicate different connection status and port types. When the router is pending or disconnected, all ports are disabled.



You can hover the cursor over the port icon for more details.

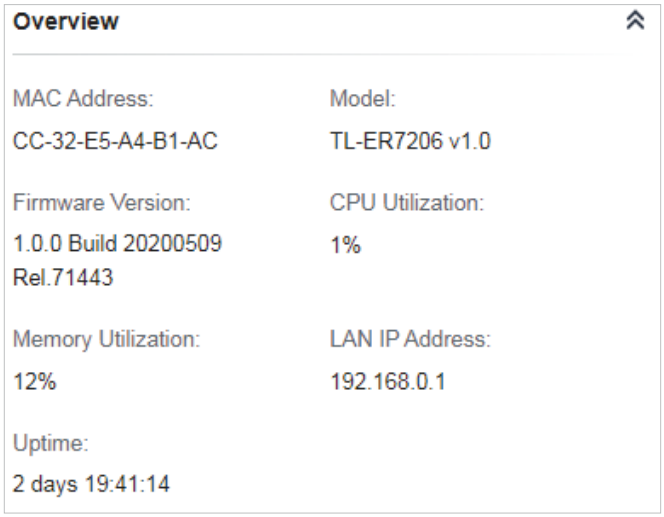


Details

In Details, you can view the basic information of the router and statistics of WAN ports to know the device's running status briefly.

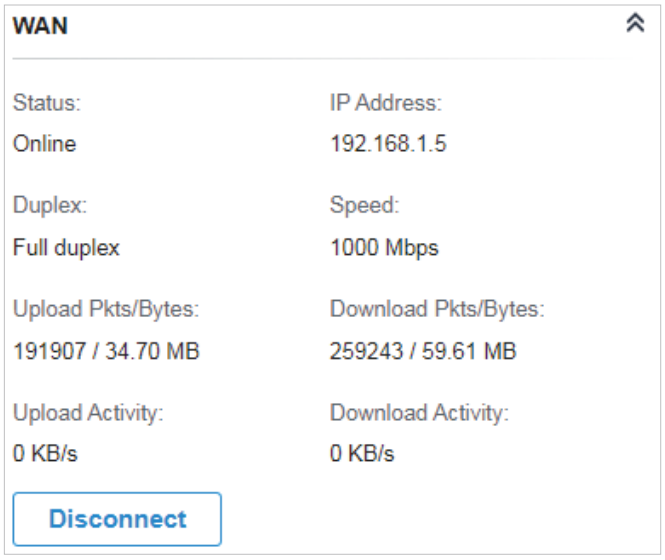
- **Overview**

  In Overview, you can view the basic information of the device. The listed information varies due to the device's status.



- **WAN**

  In WAN, you can view the basic information and statistics of the WAN port, such as the IP address, speed, duplex, and upload and download traffic.



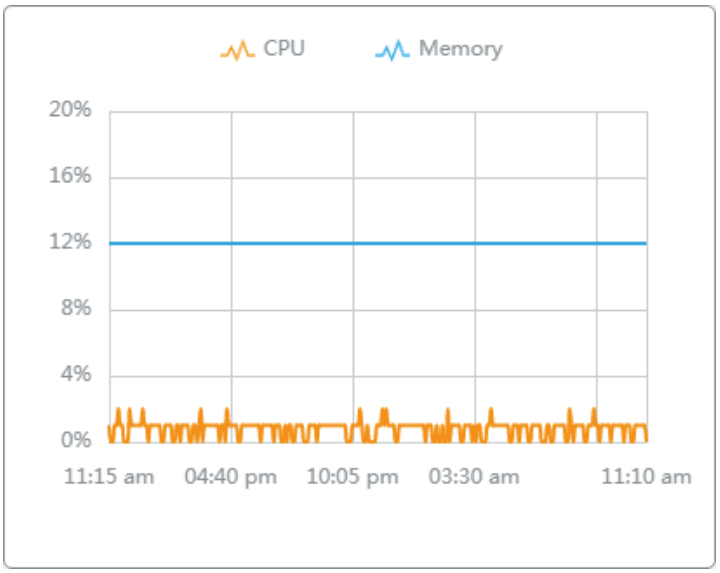
Network

In Network, you can view the network information of the router, including the Network name, IP address, transmitted and received traffics of LAN interfaces in the network, and number of clients.

Network	IP Address	Tx Bytes	Rx Bytes	Clients
LAN	192.168.0.1	596.1 MB	1.0 GB	0

Statistics

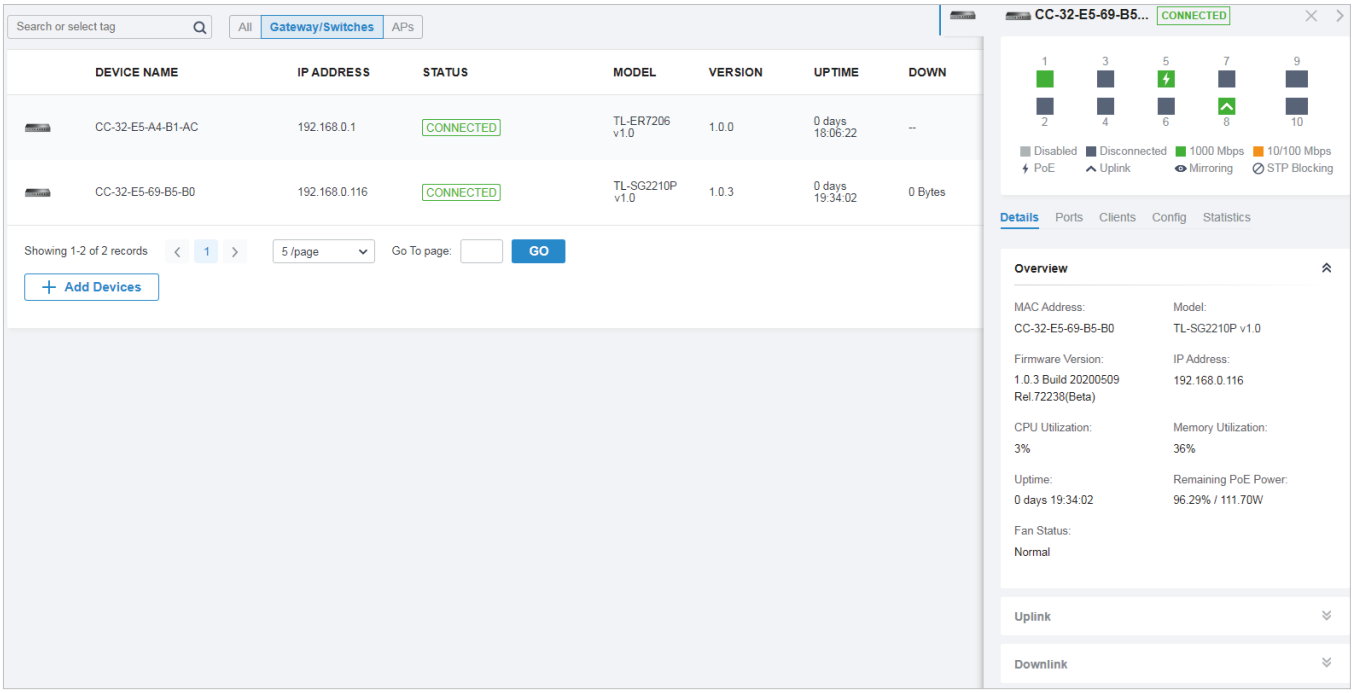
In Statistics, you can monitor the CPU and memory of the device in last 24 hours via charts. To view statistics of the device in a certain period, click the chart to jump to View the Statistics of the Network.



6. 3 Configure and Monitor Switches

In the Properties window, you can configure one or some switches connected to the controller and monitor the performance and statistics. Configurations changed in the Properties window will be applied only to the selected switch(es). By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of a switch, or click the icon to select switches for batch configuration. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Ports and Config tab, such as the port mirroring, IP address, and Management VLAN, while other tabs are mainly used to monitor the devices.



Note:

- The available functions in the window vary due to the model and status of the device.
- In Batch Config, you can only configure the selected devices, and the unaltered configurations will keep the current settings.

6. 3. 1 Configure Switches

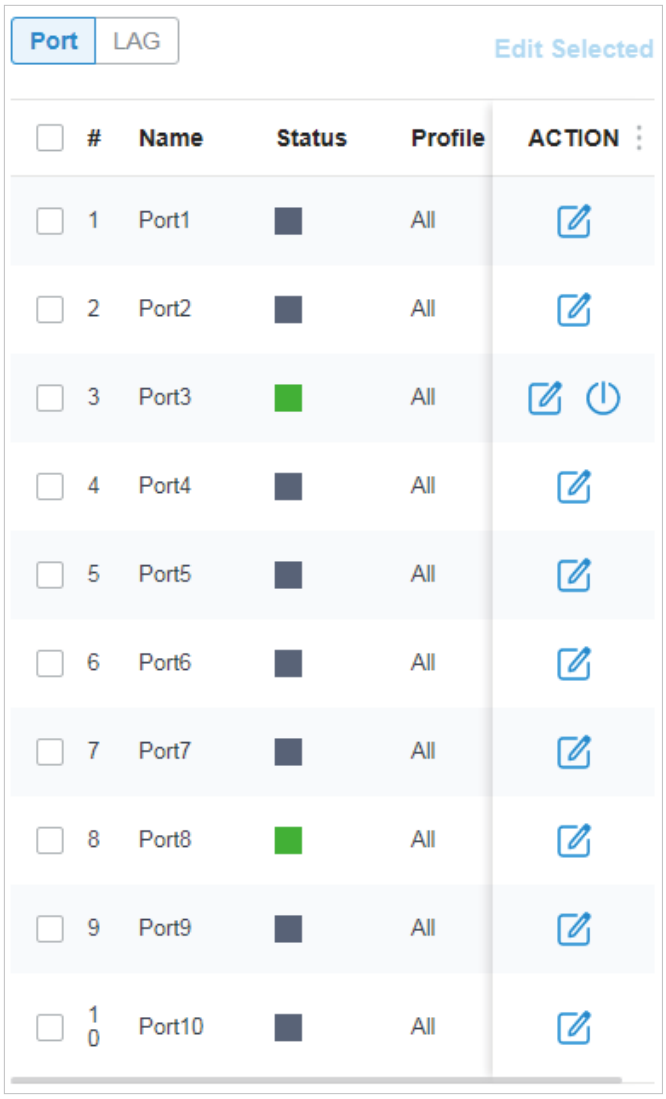
In the Properties window, you can view and configure the profiles applied to ports in Ports, and in Config, you can configure the switch features.

Ports

Port and LAG are two tabs designed for physical ports and LAGs (Link Aggregation Groups), respectively. Under the Port tag, all ports are listed but you can configure physical ports only, including overriding the applied profiles, configuring Port Mirroring, and specifying ports as LAGs. Under the LAG tag, all LAGs are listed and you can view and modify the configurations of existing LAGs.

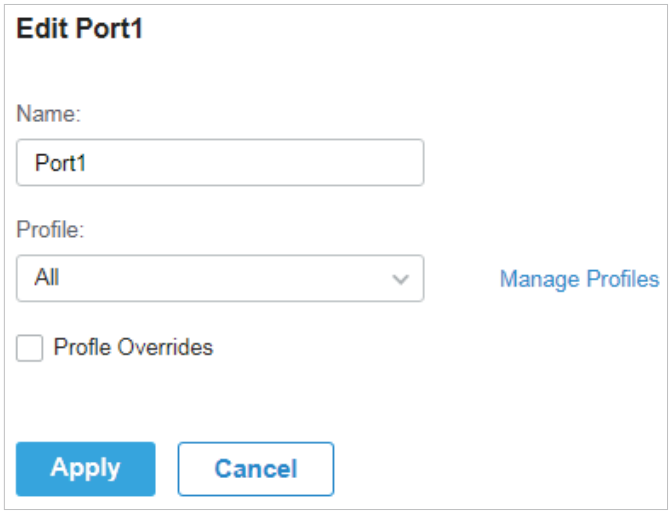
Port

In Port, you can view and configure all ports' names and applied profiles.



Status	Displays the port status in different colors. : The port profile is Disabled. To enable it, click to change the profile. : The port is enabled, but no device or client is connected to it. : The port is running at 1000 Mbps. : The port is running at 10/100 Mbps.
Profile	Displays the profile applied to the port.
Action	: Click to edit the port name and configure the profile applied to the port. : (For PoE ports) Click to reboot the connected powered devices (PDs).

To configure a single port, click in the table. To configure ports in batches, click the checkboxes and then click Edit Selected. Then you can configure the port name and profile. By default, all settings are Keep Existing for batch configuration.

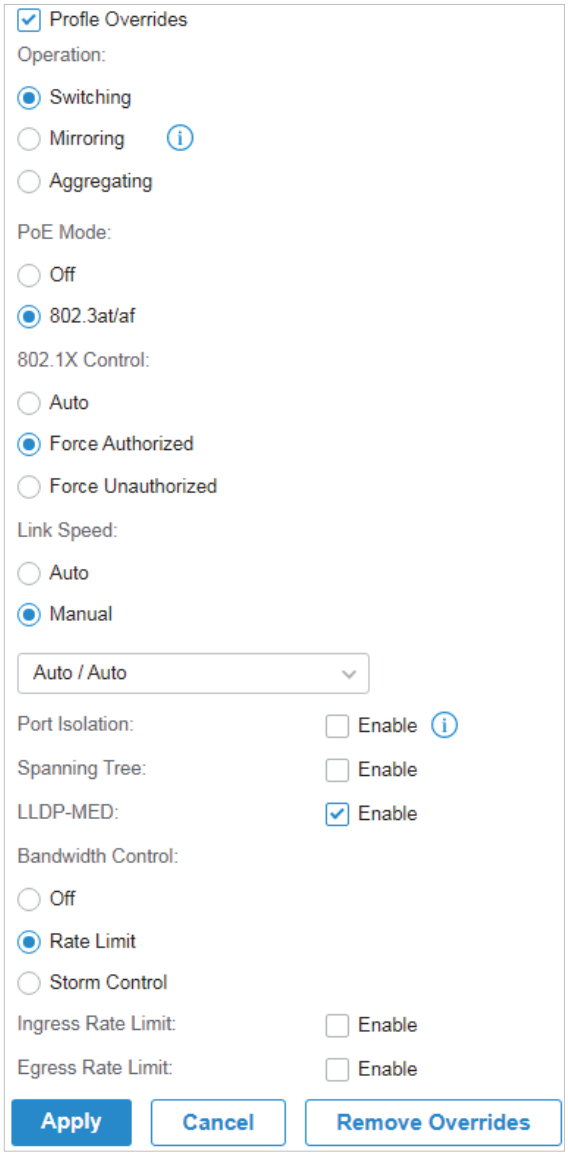


Name	Enter the port name.
Profile	Select the profile applied to the port from the drop-down list. Click Manage Profiles to jump to view and manage profiles. For details, refer to Configure Wired Networks.
Profile Overrides	Click the checkbox to override the applied profile. The parameters to be configured vary in Operation modes,

With Profile Overrides enabled, select an operation mode and configure the following parameters to override the applied profile, configure a mirroring port, or configure a LAG.

- Override the Applied Profile

  If you select Switching for Operation, configure the following parameters and click Apply to override the applied profile. To discard the modifications, click Remove Overrides and all profile configurations will become the same as the applied profile.



PoE Mode	(Only for PoE ports) Select the PoE (Power over Ethernet) mode for the port. Off: Disable PoE function on the PoE port. 802.3at/af: Enable PoE function on the PoE port.

802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to Settings > Authentication > 802.1X. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, and the client connected to the port cannot authenticate with any means. The switch cannot provide authentication services to the client through the port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Spanning Tree	Click the checkbox to enable Spanning Tree. It helps to ensure that you do not create loops when you have redundant paths in the network. To make sure Spanning Tree takes effect on the port, go to the Config tab and enable Spanning Tree on the switch.
LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP (Voice over Internet Protocol) devices.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and specify traffic threshold on each port to make good use of network bandwidth. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the specified rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Broadcast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.

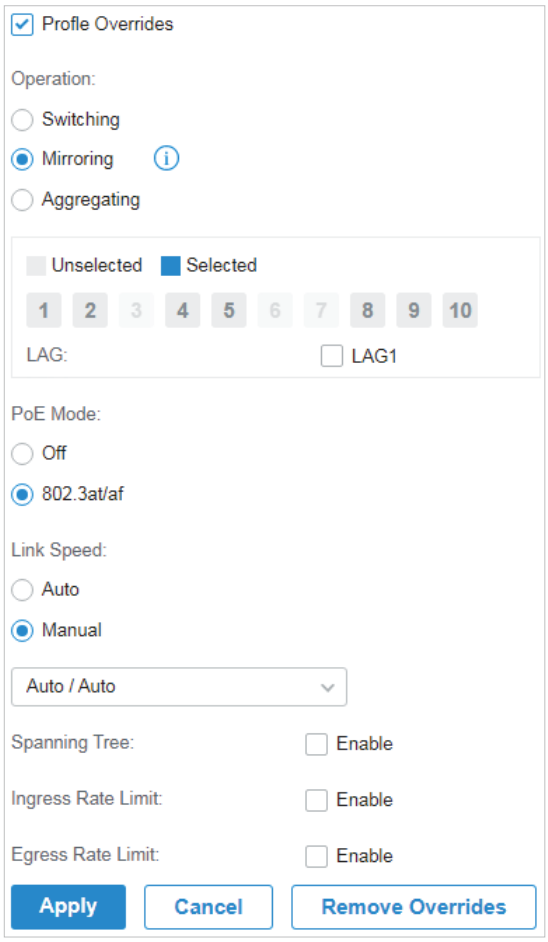
Multicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
UL-Frame Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
Action	When Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.

- Configure a Mirroring Port

  If you select Mirroring as Operation, the edited port can be configured as a mirroring port. Specify other ports as the mirrored port, and the switch sends a copy of traffics passing through the mirrored port to the mirroring port. You can use mirroring to analyze network traffic and troubleshoot network problems.

  To configure Mirroring, select the mirrored port or LAG, specify the following parameters, and click Apply. To discard the modifications, click Remove Overrides and all profile configurations become the same as the applied profile.

Note that the mirroring ports and the member ports of LAG cannot be selected as mirrored ports.



PoE Mode	(Only for PoE ports) Select the PoE mode for the port. Off: Disable PoE on the PoE port. 802.3at/af: Enable PoE on the PoE port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Spanning Tree	Click the checkbox to enable Spanning Tree. It helps to ensure that you do not create loops when you have redundant paths in the network. To make sure Spanning Tree takes effect on the port, go to the Config tab and enable Spanning Tree on the switch.
Ingress Rate Limit	Click the checkbox and specify the upper rate limit for receiving packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized.

Egress Rate Limit	Click the checkbox and specify the upper rate limit for sending packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized.

- Configure a LAG

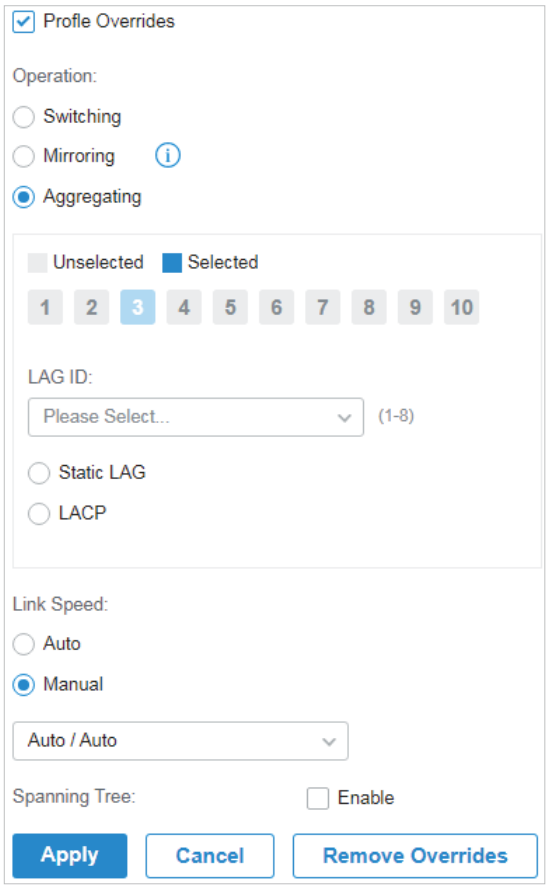
  If you select Aggregating as Operation, you can aggregate multiple physical ports into a logical interface, which can increase link bandwidth and enhance the connection reliability.

  Configuration Guidelines:

  - Ensure that both ends of the aggregation link work in the same LAG mode. For example, if the local end works in LACP mode, the peer end should also be set as LACP mode.
  - Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed, duplex, jumbo and flow control mode.
  - A port cannot be added to more than one LAG at the same time.
  - LACP does not support half-duplex links.
  - One static LAG supports up to eight member ports. All the member ports share the bandwidth evenly. If an active link fails, the other active links share the bandwidth evenly.
  - One LACP LAG supports multiple member ports, but at most eight of them can work simultaneously, and the other member ports are backups. Using LACP protocol, the switches negotiate parameters and determine the working ports. When a working port fails, the backup port with the highest priority will replace the faulty port and start to forward data.
  - The member port of an LAG follows the configuration of the LAG but not its own. Once removed, the LAG member will be configured as the default All profile and Switching operation.
  - The port enabled with Port Security, Port Mirror, MAC Address Filtering or 802.1X cannot be added to an LAG, and the member port of an LAG cannot be enabled with these functions.

  To configure a new LAG, select other ports to be added to the LAG, specify the LAG ID, and choose a LAG type. Click Apply. To discard the modifications, click Remove Overrides and all

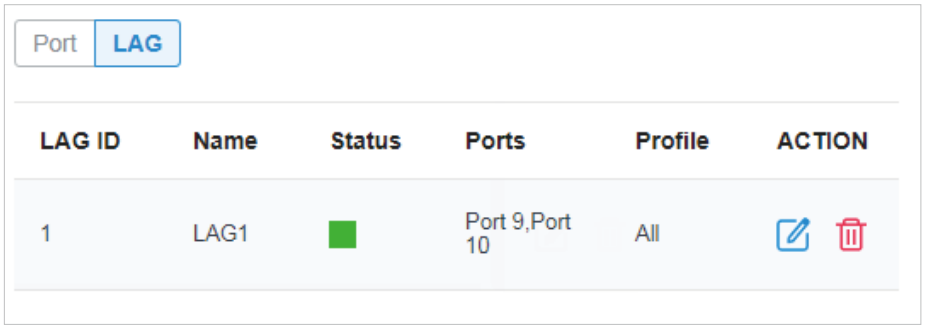
profile configurations become the same as the applied profile. For other parameters, configure them under the LAG tab.



LAG ID	Specify the LAG ID of the LAG. Note that the LAG ID should be unique. The valid value of the LAG ID is determined by the maximum number of LAGs supported by your switch. For example, if your switch supports up to 14 LAGs, the valid value ranges from 1 to 14.
Static LAG	Select the LAG type as Static LAG, and the member ports are added to the LAG manually.
LACP	Select the LAG type as LACP (Link Aggregation Control Protocol), and the switch use LACP to implement dynamic link aggregation and disaggregation. LACP extends the flexibility of the LAG configurations.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Spanning Tree	Click the checkbox to enable Spanning Tree. It helps to ensure that you do not create loops when you have redundant paths in the network. To make sure Spanning Tree takes effect on the LAG, go to the Config tab and enable Spanning Tree on the switch.

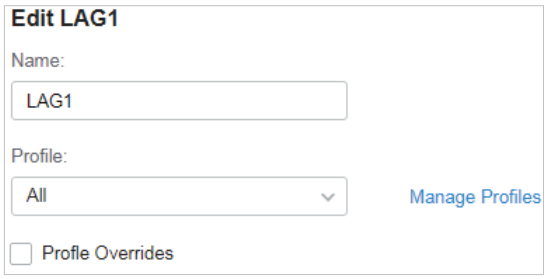
LAG

LAGs (Link Aggregation Groups) are logical interfaces aggregated, which can increase link bandwidth and enhance the connection reliability. You can view and edit the LAGs under the LAG tab. To configure physical ports as a LAG, refer to Configure a LAG.



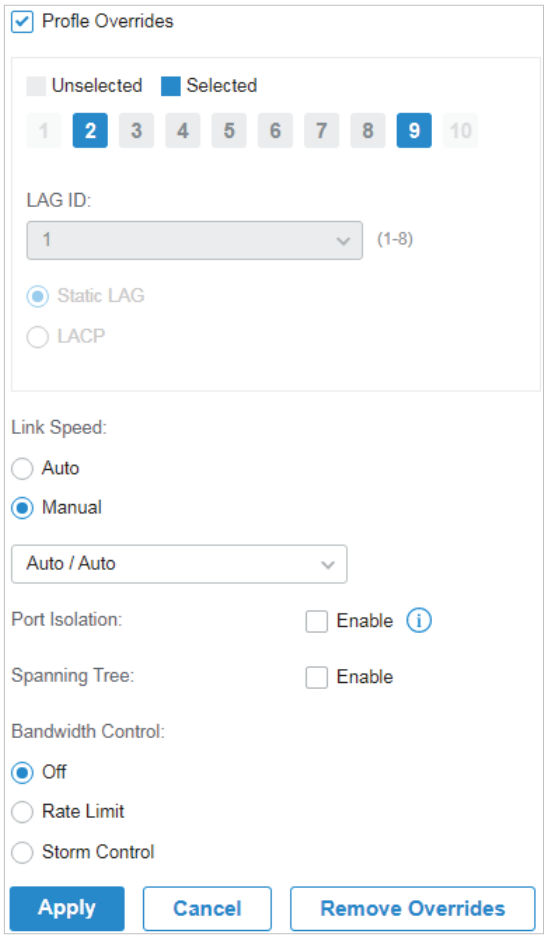
Status	Displays the status in different colors. : The LAG profile is Disable. To enable it, click to change the profile. : The port is enabled, but no device or client is connected to it. : The LAG ports are running at 1000 Mbps. : The LAG port are running at 10/100 Mbps.
Ports	Displays the port number of LAG ports.
Profile	Displays the profile applied to the port.
Action	: Click to edit the port name and configure the profile applied to the port. : Click to delete the LAG. Once deleted, the ports will be configured as the default All profile and Switching operation. You can configure the ports under the Port tab.

Click to configure the LAG name and the applied profile.



Name	Enter the port name.
Profile	Select the profile applied to the port from the drop-down list. Click Manage Profiles to jump to view and manage profiles. For details, refer to Configure Wired Networks.
Profile Overrides	Click the checbox to override the applied profile. The parameters to be configured vary in Operation modes.

With Profile Overrides enabled, you can reselect the LAG members and configure the following parameters.



Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Spanning Tree	Click the checkbox to enable Spanning Tree. It helps to ensure that you do not create loops when you have redundant paths in the network. To make sure Spanning Tree takes effect on the LAG, go to the Config tab and enable Spanning Tree on the switch.

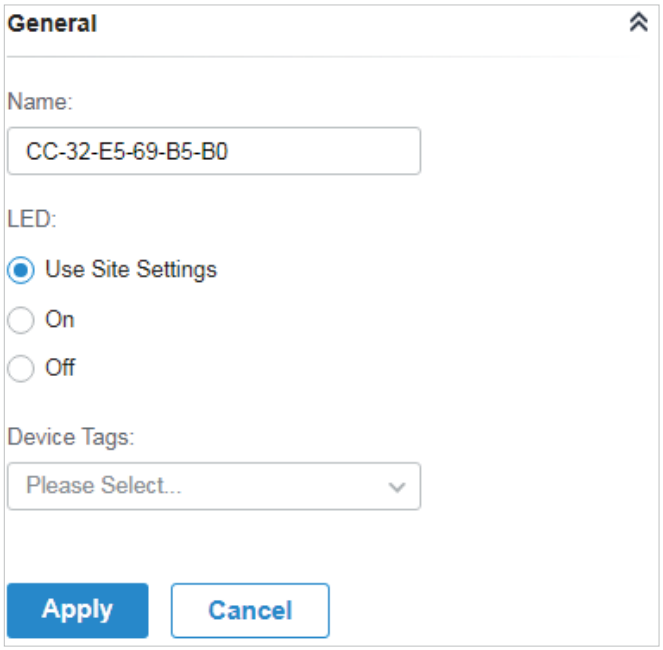
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the specified rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Broadcast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
UL-Frame Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
Action	With Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.

Config

In Config, click the sections to configure the features applied to the selected switch(es), including the general settings, services, and networks.

General

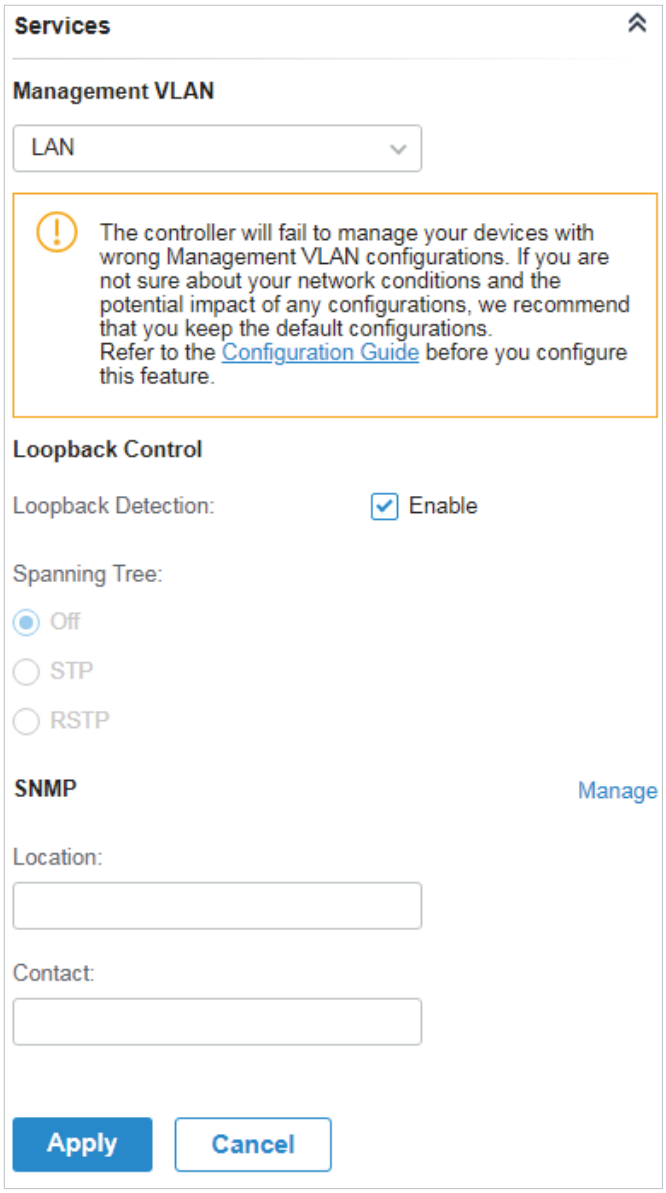
In General, you can specify the device name and LED settings of the switch, and categorize it via device tags.



Name	(Only for configuring a single device) Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to Services. On/Off: The device's LED will keep on/off.
Device Tags	Select a tag from the drop-down list or create a new tag to categorize the device.

Services

In Services, you can configure Management VLAN, Loopback Control and SNMP.



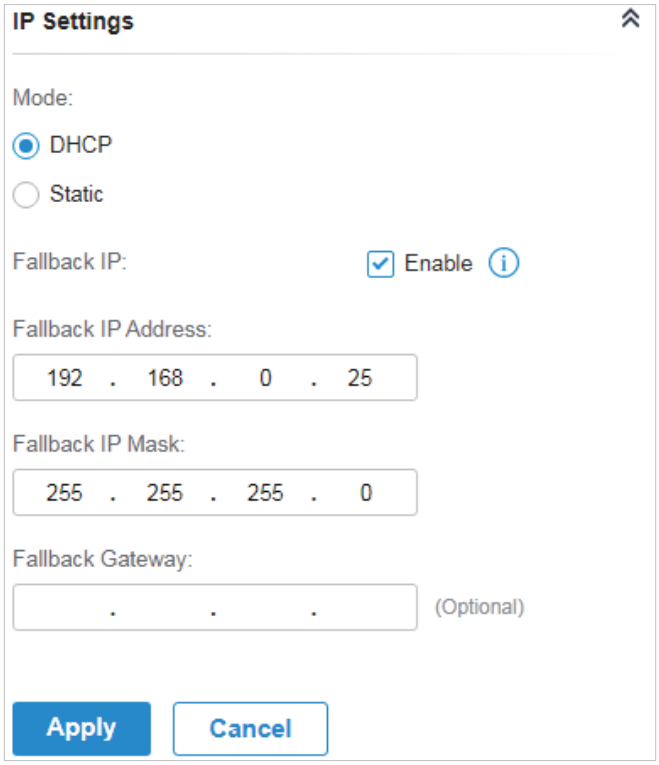
Management VLAN	To configure Management VLAN, create a network in LAN first, and then select it as the management VLAN on this page. For details, refer to Configure Wired Networks. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
Loopback Detection	When enabled, the switch checks the network regularly to detect the loopback. Note that Lopback Detection and Spanning Tree are not availiable at the same time.

Spanning Tree	Select a mode for Spanning tree. This feature is avaliable only when Loopback Detection is disabled. Off: Disable Spanning Tree on the switch. STP: Enable STP (Spanning Tree Protocal) to prevent loops in the network. STP helps to block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. RSTP: Enable RSTP (Rapid Spanning Tree Protocal) to prevent loops in the network. RSTP provides the same features as STP with faster spanning ree convergence. Priority: When STP/RSTP enabled, specify the priority for the swith in Spanning Tree. In STP/RSTP, the switch with the highest priority will be selected as the root of the spanning tree. The switch with the lower value has the higher priority.
SNMP	(Only for configuring a single device) Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP, and for detailed configuration of SNMP service, refer to SNMP.

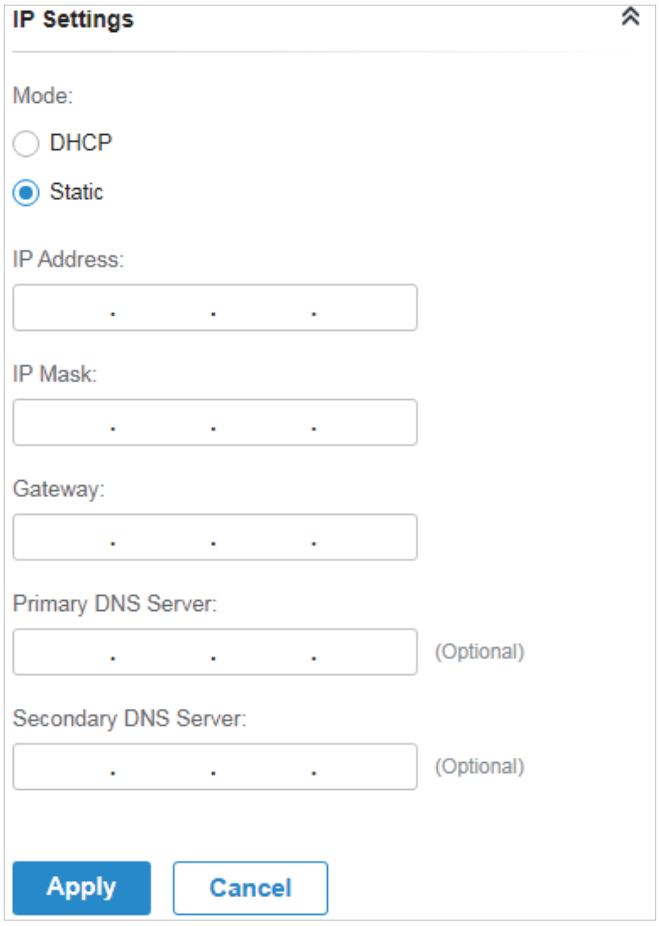
- **IP Settings (Only for configuring a single device)**

  In IP Settings, select an IP mode and configure the parameters for the device.

  If you select DHCP as the mode, make sure there is a DHCP server in the network and then the device will obtain dynamic IP address from the DHCP server automatically. You can set a fallback IP address to hold an IP address in reserve for the situation in which the device fails to get a dynamic IP address. Enable Fallback IP and then set the IP address, IP mask and gateway.

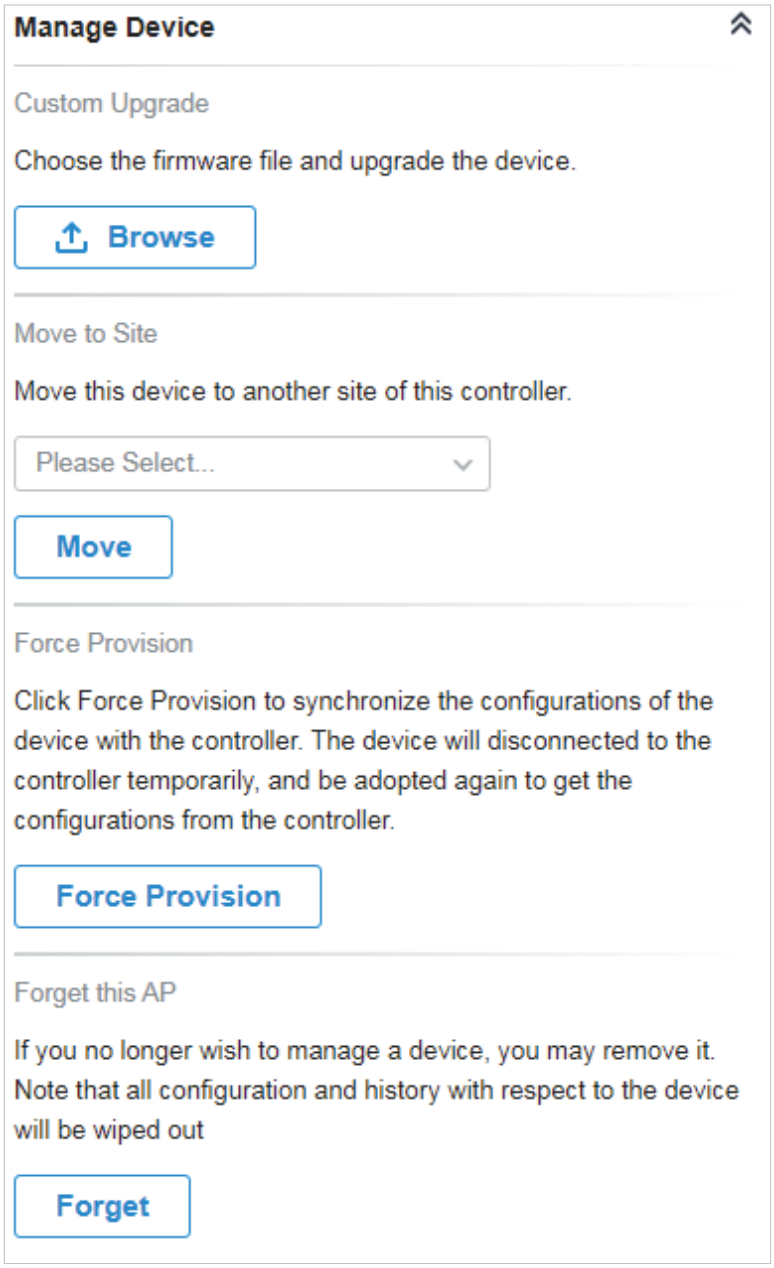


If you select Static as the mode, set the IP address, IP mask, gateway, and DNS server for the static address.



Manage Device

In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller and forget the switch.



Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	(Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.

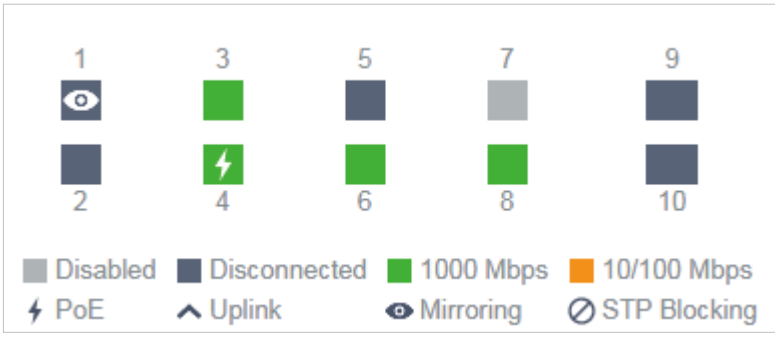
Forget	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.

6. 3. 2 Monitor Switches

One panel and four tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Clients, and Statistics.

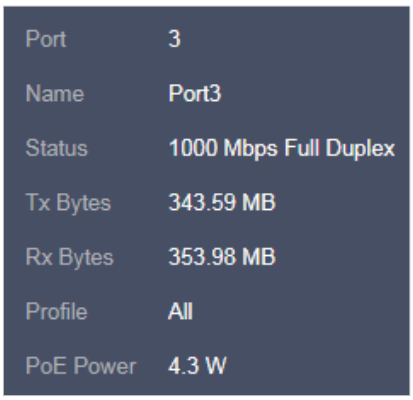
Monitor Panel

The monitor panel displays the switch's ports and uses colors and icons to indicate the connection status and port type. When the switch is pending or disconnected, all ports are disabled.



PoE	A PoE port connected to a powered device (PD).
Uplink	An uplink port connected to WAN.
Mirroring	A mirroring port that is mirroring another switch port.
STP Blocking	A port in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.

You can hover the cursor over the port icon (except disabled ports) for more details. The displayed information varies due to connection status and port type.



Status	Displays the negotiation speed of the port.

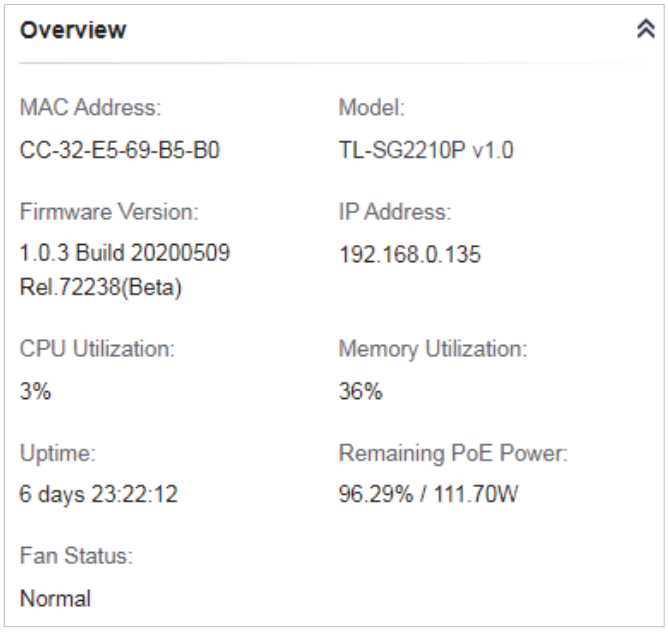
Tx Bytes	Displays the amount of data transmitted as bytes.
Rx Bytes	Displays the amount of data received as bytes.
Profile	Displays the name of profile applied to the port, which defines how the packets in both ingress and egress directions are handled. For detailed configuration, refer to Create Profiles.
PoE Power	Displays the percentage of received packets that have errors and the percentage of packets that were dropped.
Uplink	Displays the name of device connected to the uplink port.
Mirroring From	Displays the name of port that is mirrorred.
LAG ID	Displays the name of ports that are aggregated into a logical interface.

Details

In Details, you can view the basic information, traffic information, and radio information of the device to know the device's running status.

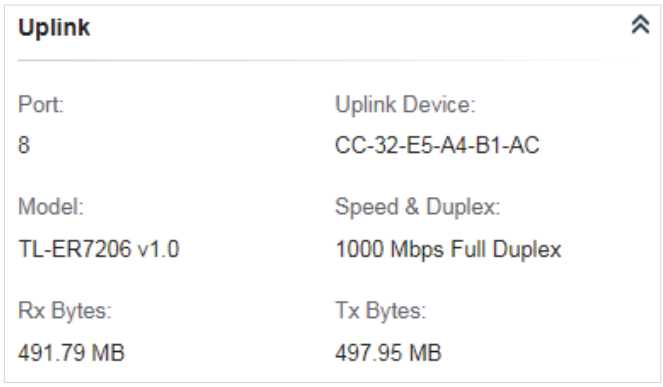
- **Overview**

  In Overview, you can view the basic information of the device. The listed information will be varied due to the device's model and status.



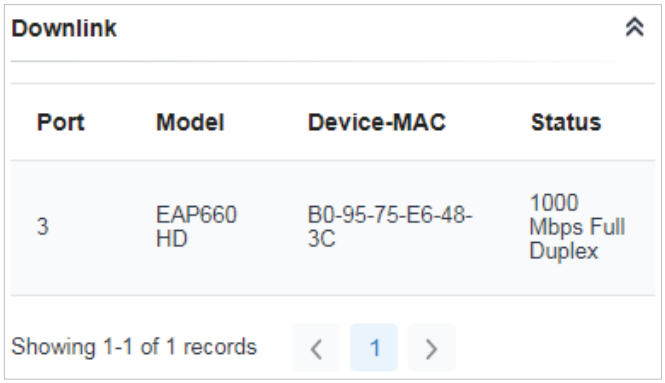
- **Uplink (Only for the switch connected to an Omada-managed router/switch in Connected status)**

  Click Uplink to view the uplink information, including the uplink port, the uplink device, the negotiation speed, and transmission rate.



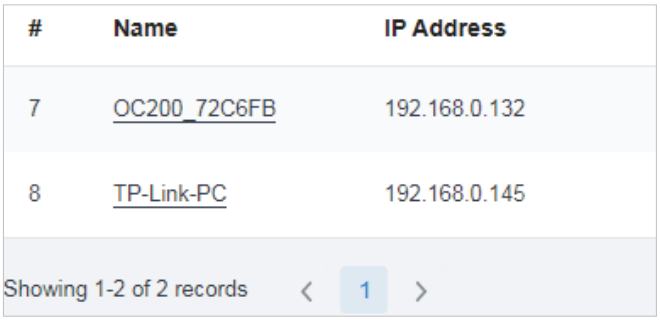
- **Downlink (Only for the switch connected to Omada-managed devices in Connected status)**

  Click Downlink to view the downlink information, including the downlink ports, devices name and model as well as negotiation speed.



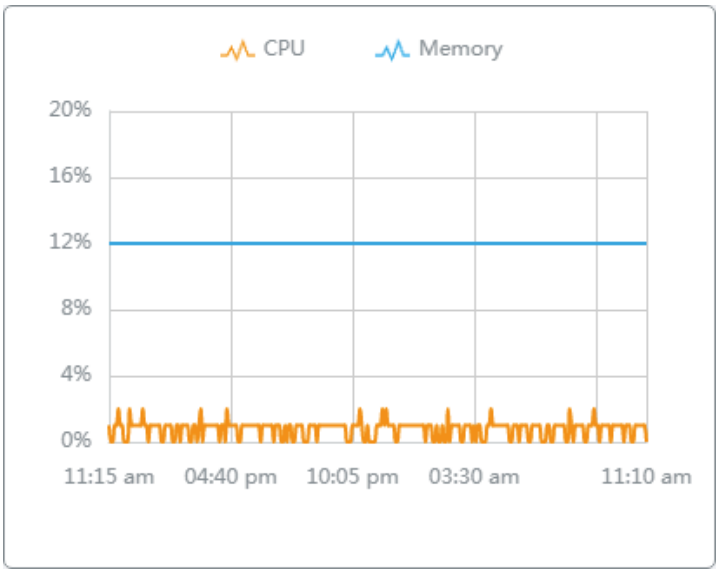
Clients

In Clients, you can view the information of clients connected to the switch, including the client name, IP address and the connected port. You can click the client name to open its Properties window.



Statistics

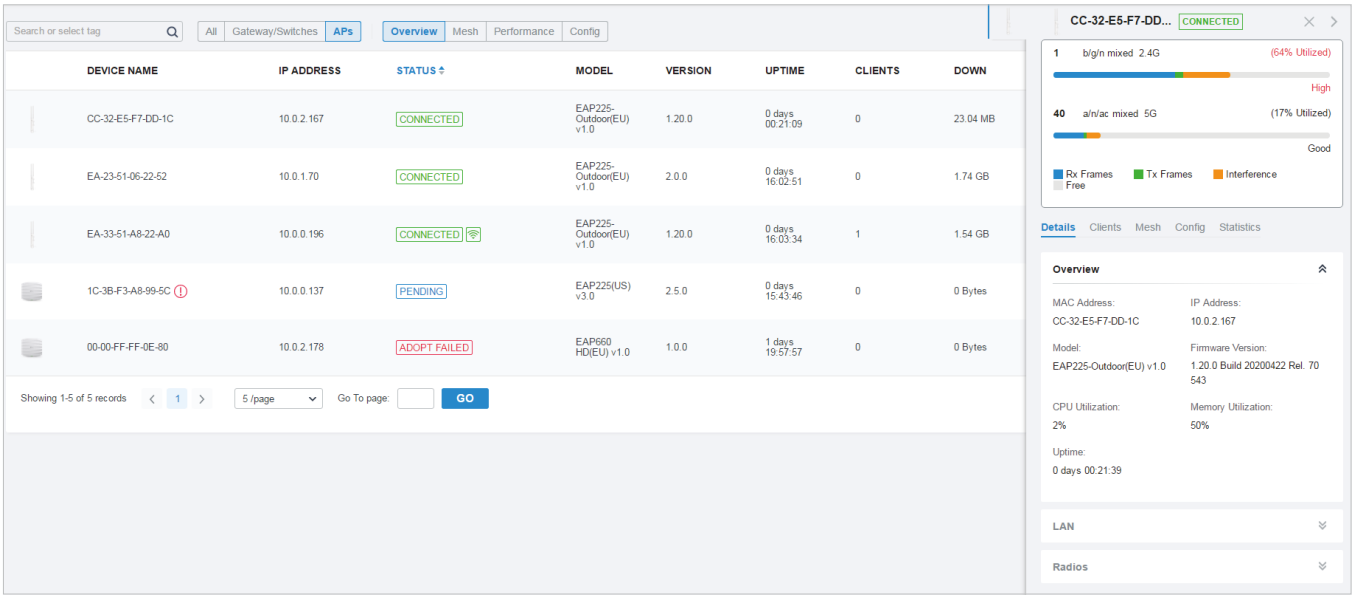
In Statistics, you can monitor the CPU and memory of the device in last 24 hours via charts. To view statistics of the device in certain period, click the chart to jump to View the Statistics of the Network.



6. 4 Configure and Monitor EAPs

In the Properties window, you can configure one or some EAPs connected to the controller and monitor the performance and statistics. Configurations changed in the Properties window will be applied only to the selected AP(s). By default, all configurations are synchronized with the current site.

To open the Properties window, click the entry of an AP, or click the icon to select APs for batch configuration. A monitor panel and several tabs are listed in the Properties window. Most features to be configured are gathered in the Config tab, such as IP, radios, SSID, and VLAN, while other tabs are mainly used to monitor the device.



Note:

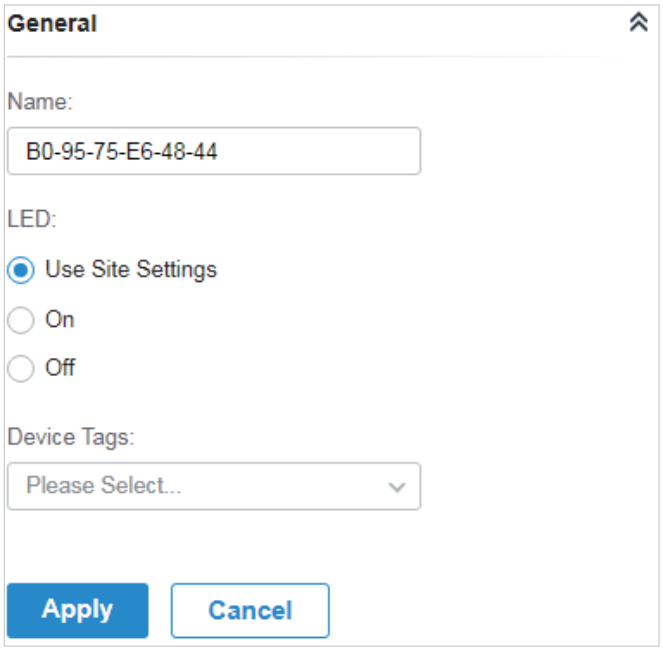
- The available functions in the window vary due to the model and status of the device.
- In Batch Config, you can only configure the selected devices, and the unaltered configurations will keep the current settings.
- In Batch Config, if some functions, such as the 5 GHz band, are available only on some selected EAPs, the corresponding configurations will not take effect. To configure them successfully, check the model of selected devices first.

6. 4. 1 Configure EAPs

In the Properties window, click Config and then click the sections to configure the features applied to the selected AP(s), including the general settings, IP settings, Radios, SSIDs, VLAN, SNMP, and advanced functions.

- **General**

  In General, you can specify the device name and LED settings of the AP, and categorize it via device tags.



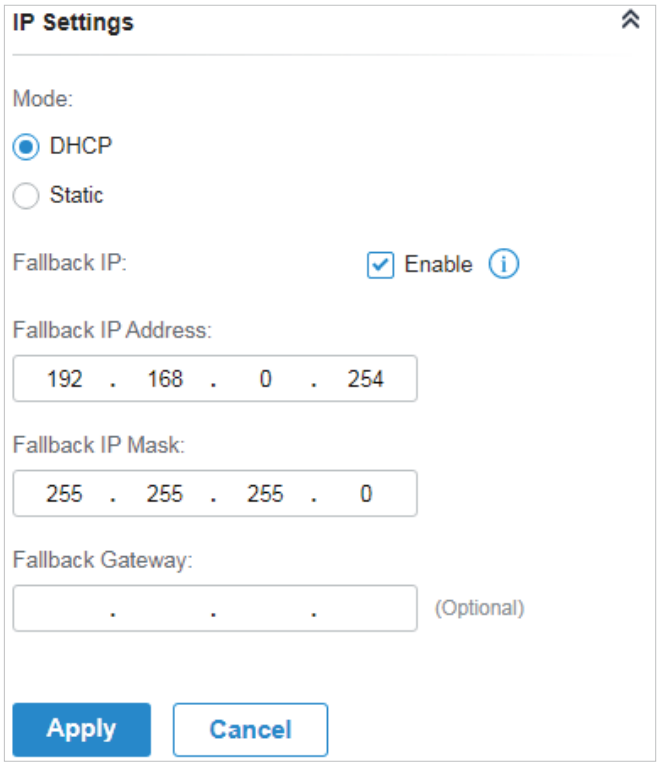
Name	(Only for configuring a single device) Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to Services. On/Off: The device's LED will keep on/off.
Device Tags	Select a tag from the drop-down list or create a new tag to categorize the device.

- **IP Settings (Only for configuring a single device)**

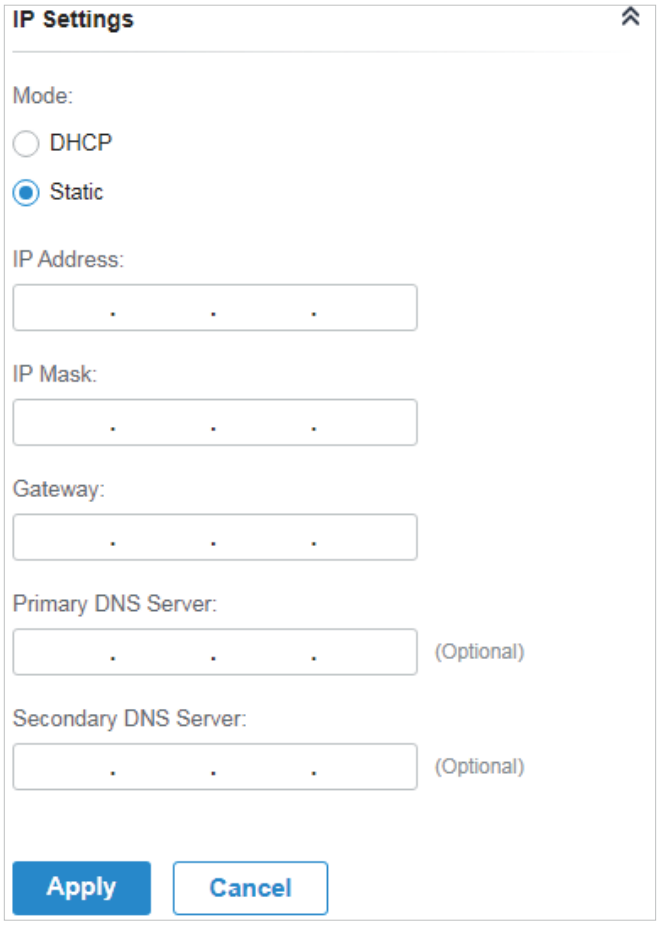
  In IP Settings, select an IP mode and configure the parameters for the device.

  If you select DHCP as the mode, make sure there is a DHCP server in the network and then the device will obtain dynamic IP address from the DHCP server automatically. You can set a fallback IP

address to hold an IP address in reserve for the situation in which the device fails to get a dynamic IP address. Enable Fallback IP and then set the IP address, IP mask and gateway.

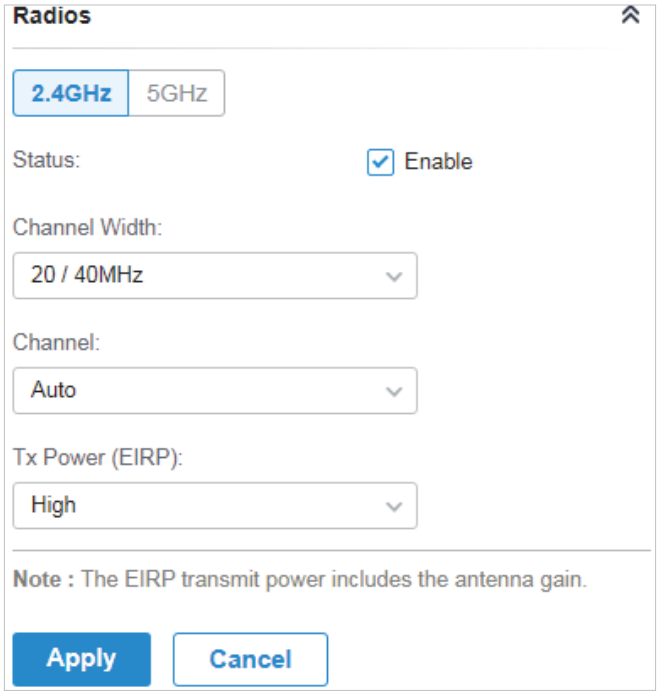


If you select Static as the mode, set the IP address, IP mask, gateway, and DNS server for the static address.



Radios

In Radios, you can control how and what type of radio signals the EAP emits. Select the frequency band 2.4GHz 5GHz and configure the following parameters.

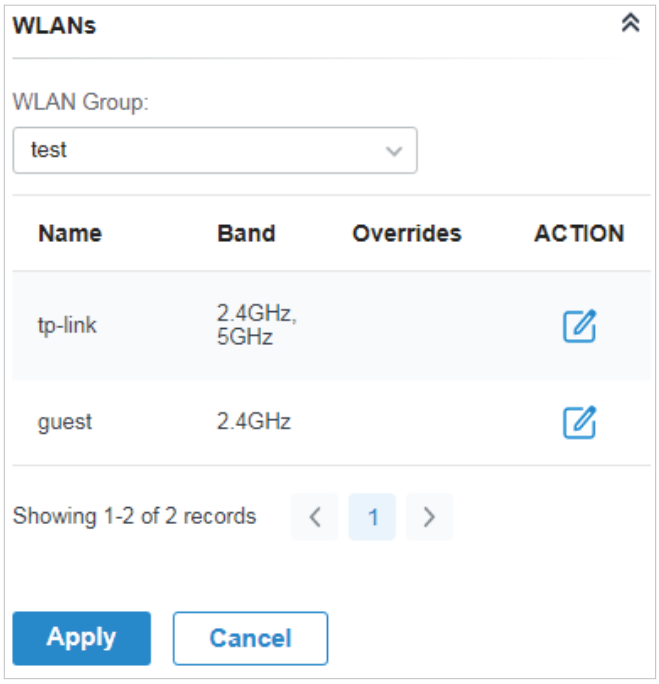


Status	If you disable the frequency band, the radio on it will turn off.
Channel Width	Specify the channel width of the band. Two bands have different available options: 20 MHz, 40 MHz and 20/40 MHz for 2.4 GHz, and 20 MHz, 40 MHz, 80 MHz and 20/40/80 MHz for 5 GHz. Note that the option 20/40 MHz and 20/40/80 MHz channels enable higher data rates but leave fewer available channels for other 2.4 GHz and 5 GHz devices.
Channel	Specify the operation channel of the EAP to improve wireless performance. If you select Auto for the channel setting, the EAP scans available channels and selects the channel where the least amount of traffic is detected.
Tx Power	Specify the Tx Power (Transmit Power) in the 4 options: Low, Medium, High and Custom. The actual power of Low, Medium and High are based on the minimum transmit power (Min. Txpower) and maximum transmit power (Max. TxPower), which may vary in different countries and regions. Low: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (round off the value) Medium: Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (round off the value) High: Max. TxPower Custom: Specify the value manually.

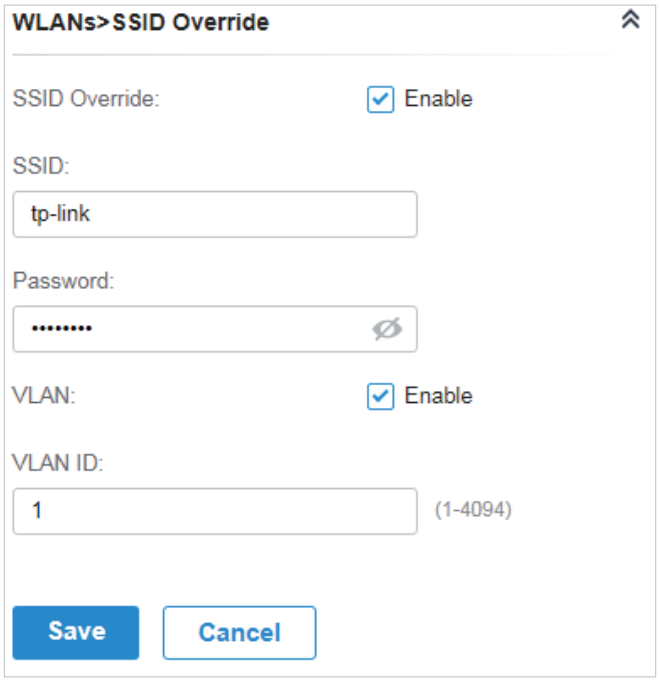
WLANs

In WLANs, you can apply the WLAN group to the EAP and specify a different SSID name and password to override the SSID in the WLAN group. After that, clients can only see the new SSID and

use the new password to access the network. To create or edit WLAN groups, refer to Configure Wireless Networks.



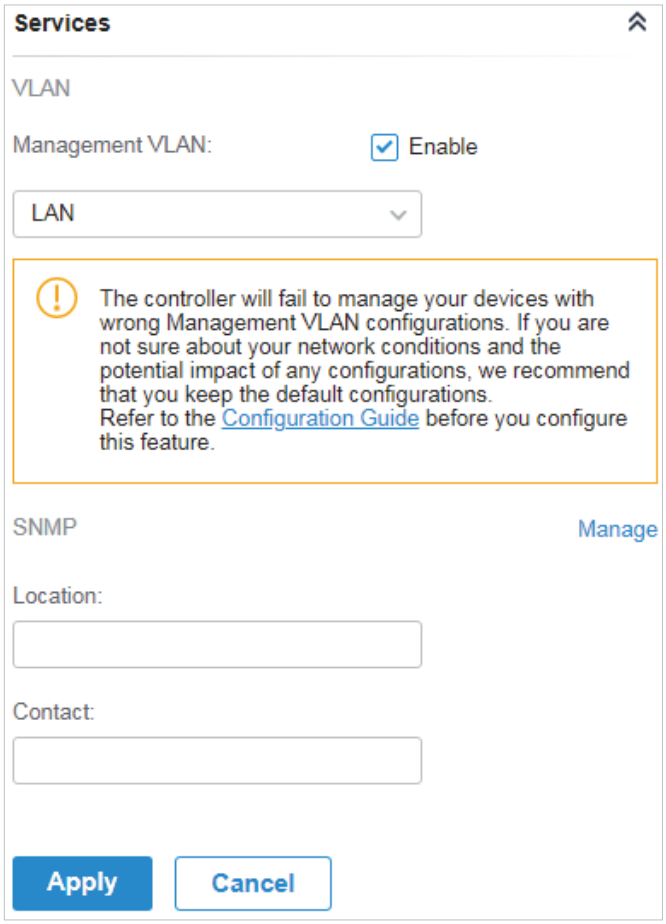
(Only for configuring a single device) To override the SSID, select a WLAN group, click in the entry and then the following page appears.



SSID Override	Enable or disable SSID Override on the EAP. If SSID Override enabled, specify the new SSID and password to override the current one.
VLAN	Enable or disable VLAN. If VLAN enabled, enter a VLAN ID to add the new SSID to the VLAN.

Services

In Services, you can configure Management VLAN to protect your network and SNMP to write down the location and contact detail.

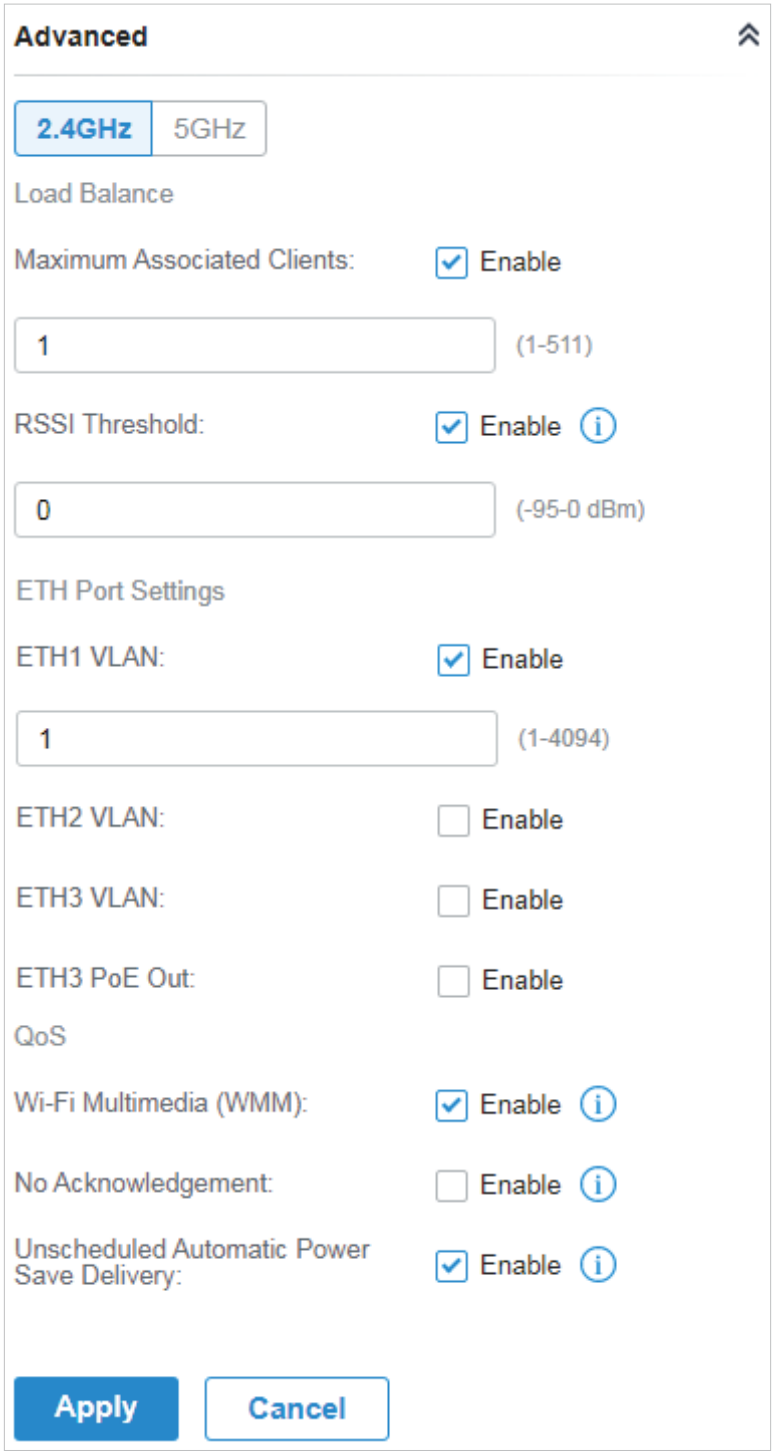


Management VLAN	To configure Management VLAN, create a network in LAN first, and then select it as the management VLAN on this page. For details, refer to Configure Wired Networks. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
SNMP	(Only for configuring a single device) Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP, and for detailed configuration of SNMP service, refer to SNMP.

Advanced

In Advanced, configure Load Balance and QoS to make better use of network resources. Load Balance can control the client number associated to the EAP, while QoS can optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media.

Select the frequency band 2.4GHz 5GHz and configure the following parameters and features.

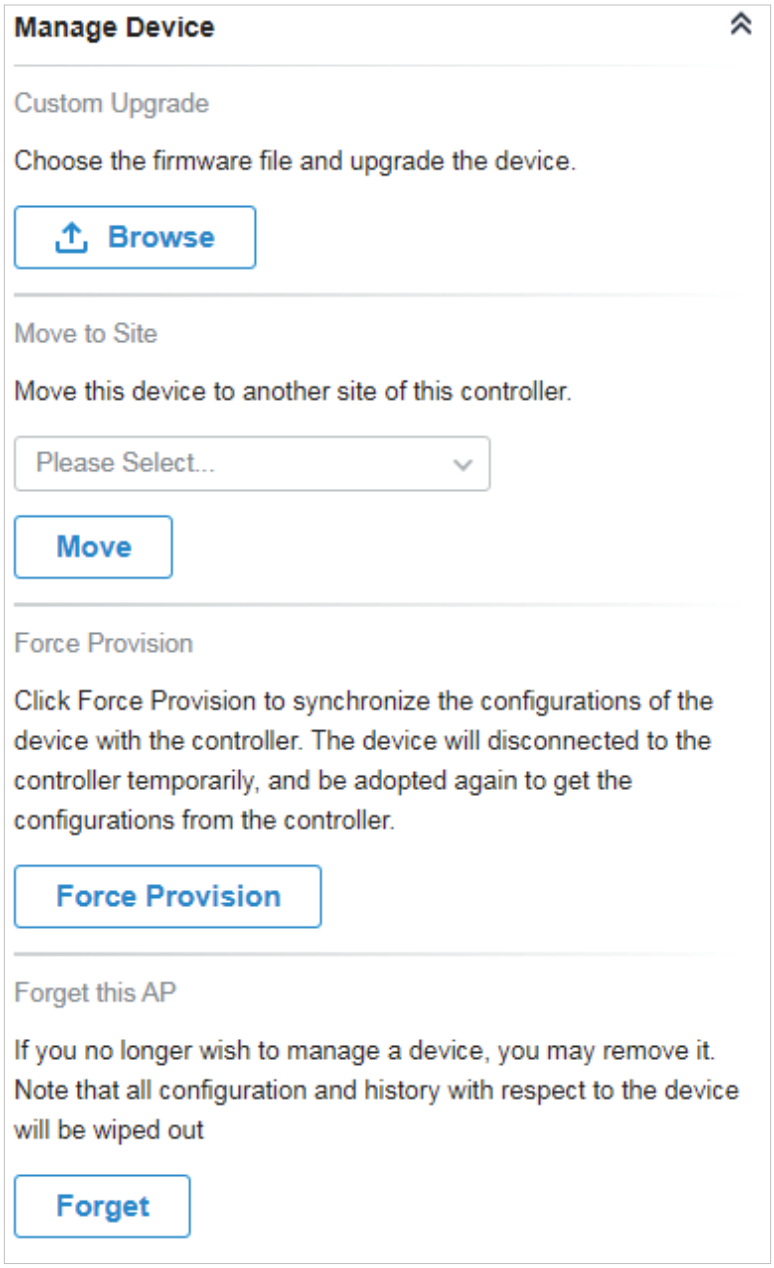


Max Associated Clients	Enable this function and specify the maximum number of connected clients. If the connected client reaches the maximum number, the EAP will disconnect those with weaker signals to make room for other clients requesting connections.
RSSI Threshold	Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If the client's signal strength is weaker than the threshold, the client will lose connection with the EAP.

ETH VLAN/ETH2 VLAN/ ETH3 VLAN	(Only for Wall Plate AP) Enable this function and add the corresponding AP's LAN port to the VLAN specified here. Then the hosts connected to this EAP can only communicate with the devices in this VLAN.
ETH3 PoE Out	(Only for Wall Plate AP with the PoE out port) Enable this function to supply power to the connected device on this port.
Wi-Fi Multimedia (WMM)	With WMM enabled, the EAP maintains the priority of audio and video packets for better media performance.
No Acknowledgment	Enable this function to specify that the EAPs will not acknowledge frames with QoS No Ack. Enabling No Acknowledgment can bring more efficient throughput, but it may increase error rates in a noisy Radio Frequency (RF) environment.
Unscheduled Automatic Power Save Delivery	When enabled, this function can greatly improve the energy-saving capacity of clients.

Manage Device

In Manage Device, you can upgrade the device's firmware version manually, move it to another site, synchronize the configurations with the controller and forget the AP.



Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	(Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.

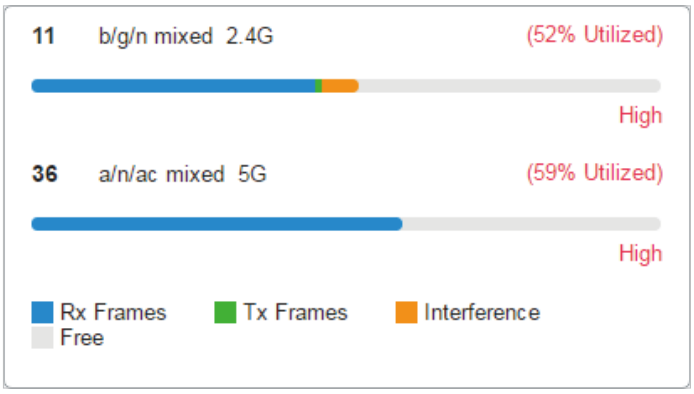
Forget this AP	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.

6. 4. 2 Monitor EAPs

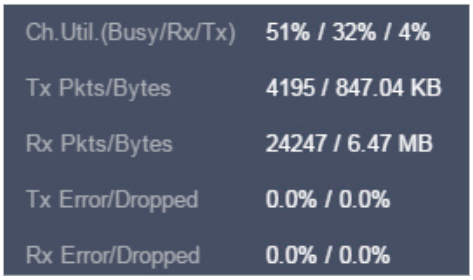
One panel and four tabs are provided to monitor the device in the Properties window: Monitor Panel, Details, Clients, Mesh, and Statistics.

Monitor Panel

The monitor panel illustrates the active channel information on each radio band, including the EAP's operation channel, radio mode and channel utilization. Four colors are used to indicate the percentage of Rx Frames (blue), Tx Frames (green), Interference (orange), and Free bandwidth (gray).



You can hover the cursor over the channel bar for more details.



Ch.Util.(Busy/Rx/Tx)	Displays channel utilization statistics. **Busy**: Displays the sum of Tx, Rx, and also non-WiFi interference, which indicates how busy the channel is. **Rx**: Indicates how often the radio is in active receive mode. **Tx**: Indicates how often the radio is in active transmit mode.
Tx Pkts/Bytes	Displays the amount of data transmitted as packets and bytes.
Rx Pkts/Bytes	Displays the amount of data received as packets and bytes.

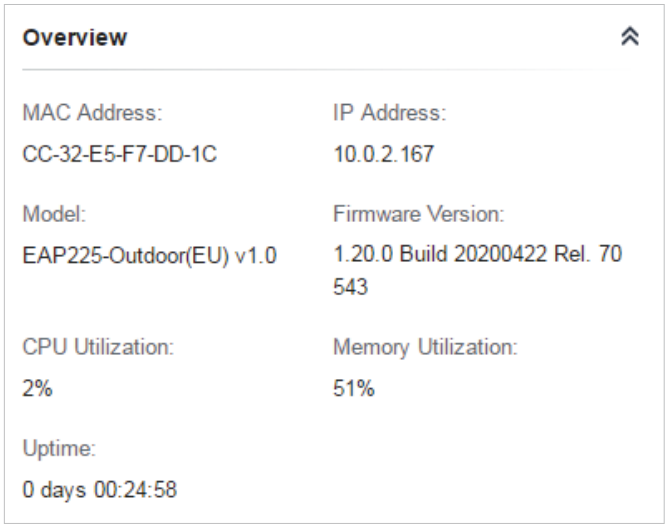
Tx Error/Dropped	Displays the percentage of transmit packets that have errors and the percentage of packets that were dropped.
Rx Error/Dropped	Displays the percentage of receive packets that have errors and the percentage of packets that were dropped.

Details

In Details, you can view the basic information, traffic information, and radio information of the device to know the device's running status.

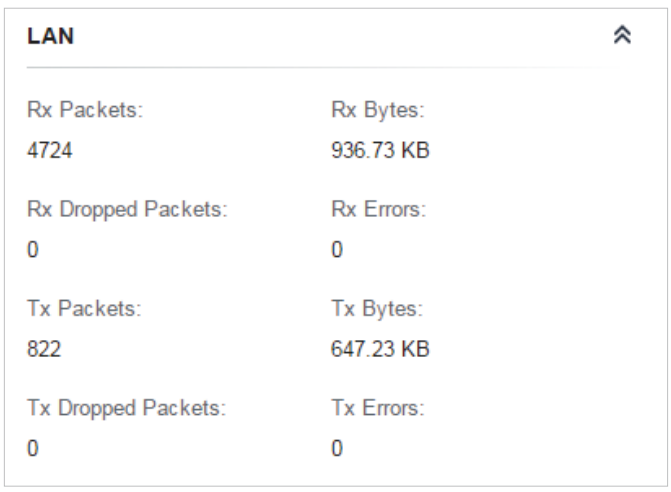
- **Overview**

  In Overview, you can view the basic information of the device. The listed information varies due to the device's status.



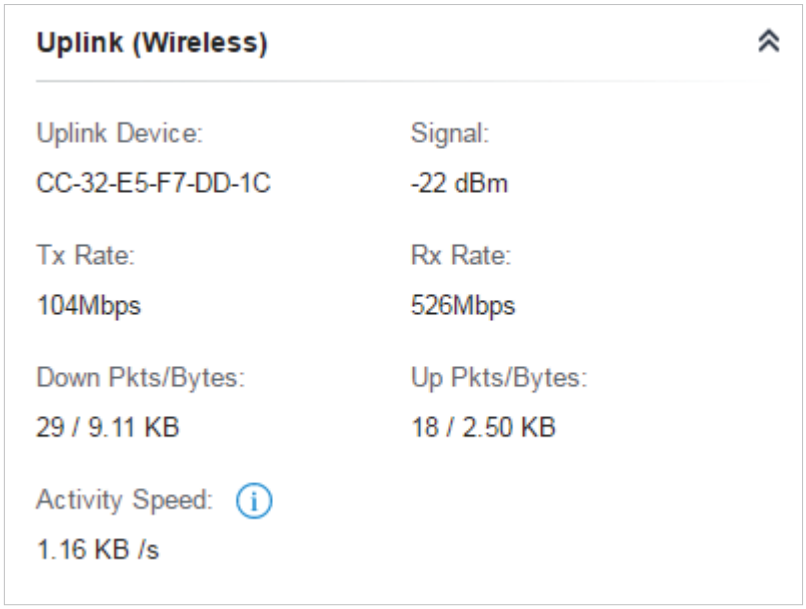
- **LAN (Only for devices in the Connected status)**

  Click LAN to view the traffic information of the LAN port, including the total number of packets, the total size of data, the total number of packets loss, and the total size of error data in the process of receiving and transmitting data.



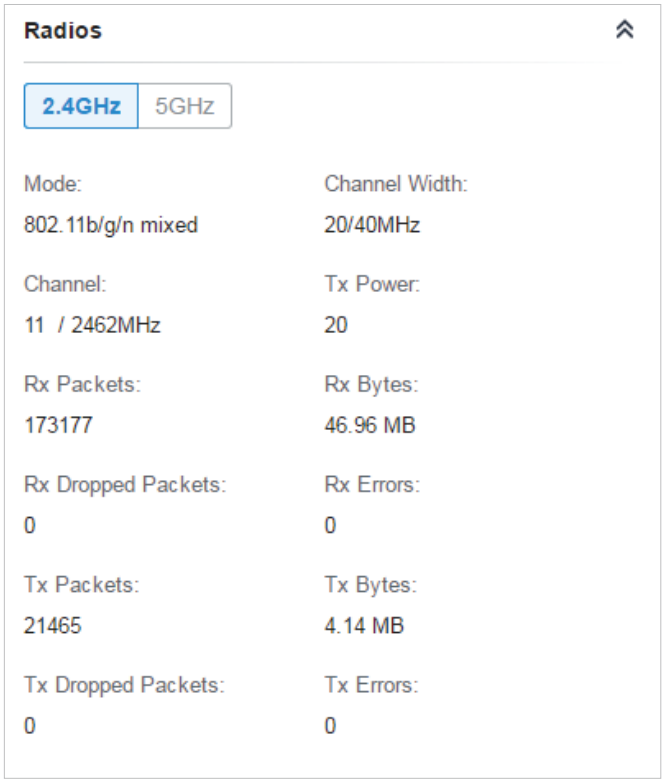
- **Uplink (Wireless) (Only for devices in the Connected status)**

  Click Uplink (Wireless) to view the traffic information related to the uplink AP, including the signal strength, transmission rate, ratio of packets number and size, and dynamic downstream rate.



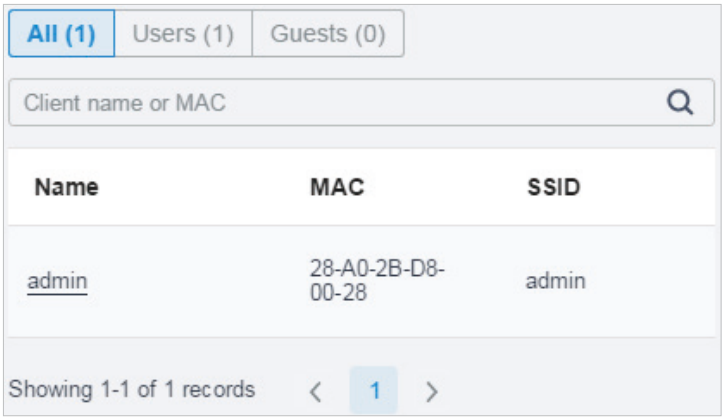
- **Radios (Only for devices in the Connected status)**

  Click Radio to view the radio information including the frequency band, the wireless mode, the channel width, the channel, and the transmitting power. You can also view parameters of receiving/transmitting data on each radio band.



Clients

In Clients, you can view the information of users and guests connecting to the AP, including client name, MAC address and the connected SSID. Users are clients connected to the AP's SSID with Guest Network disabled, while Guests are clients connected to that with Guest Network enabled. You can click the client name to open its Properties window.



Mesh (Only for pending/connected/isolated devices supporting Mesh)

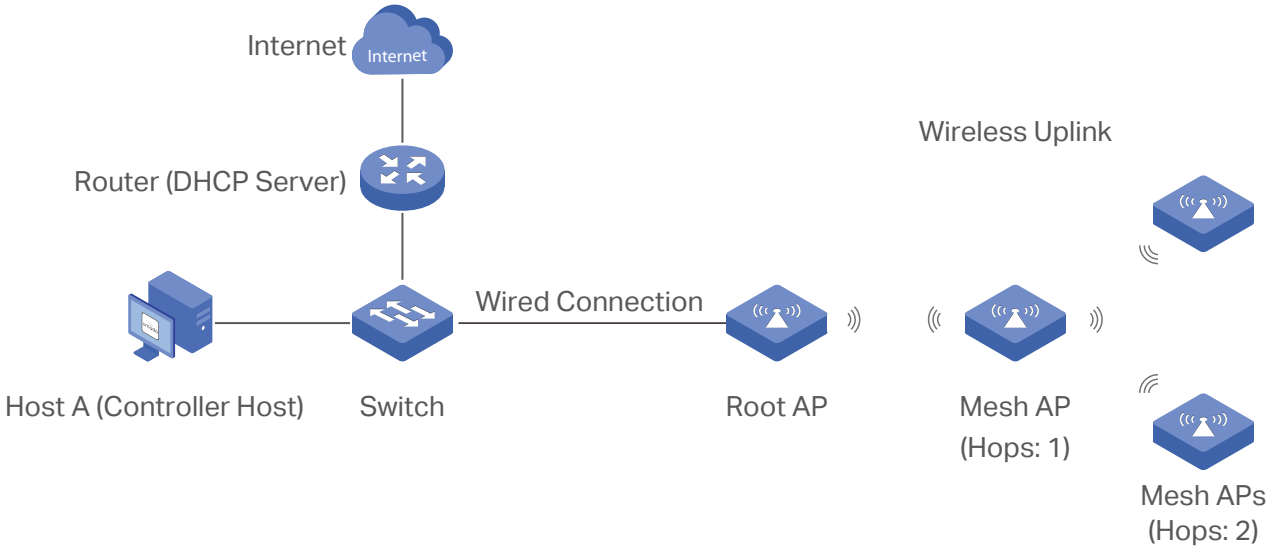
Mesh is used to establish a wireless network or expand a wired network through wireless connection on 5 GHz radio band. In practical application, it can help users to conveniently deploy APs without requiring Ethernet cable. After mesh network establishes, the EAPs can be configured and managed in Omada controller in the same way as wired EAPs. Meanwhile, because of the ability to self-organize and self-configure, mesh also can efficiently reduce the configuration.

Note that only certain EAP models support Mesh, and the EAPs should be in the same site to establish a Mesh network.

To understand how mesh can be used, the following terms used in Omada Controller will be introduced:

Root AP	The AP is managed by Omada Controller with a wired data connection that can be configured to relay data to and from mesh APs (downlink AP).
Isolated AP	When the EAP which has been managed by Omada Controller before connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state.
Mesh AP	An isolated AP will become a mesh AP after establishing a wireless connection to the AP with network access.
Uplink AP/Downlink AP	Among mesh APs, the AP that offers the wireless connection for other APs is called uplink AP. A Root AP or an intermediate AP can be the uplink AP. And the AP that connects to the uplink AP is called downlink AP. An uplink AP can offer direct wireless connection for 4 downlink APs at most.
Wireless Uplink	The action that a downlink AP connects to the uplink AP.
Hops	In a deployment that uses a root AP and more than one level of wireless uplink with intermediate APs, the uplink tiers can be referred to by root, first hop, second hop and so on. The hops should be no more than 3.

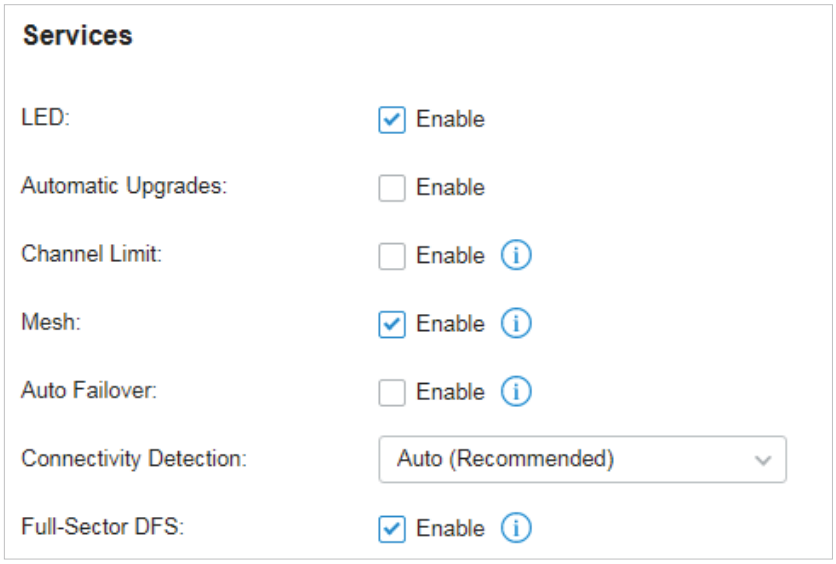
A common mesh network is shown as below. Only the root AP is connected by an Ethernet cable, while other APs have no wired data connection. Mesh allows the isolated APs to communicate with pre-configured root AP on the network. Once powered up, factory default or unadopted EAPs can detect the EAP in range and make itself available for adoption in the controller.



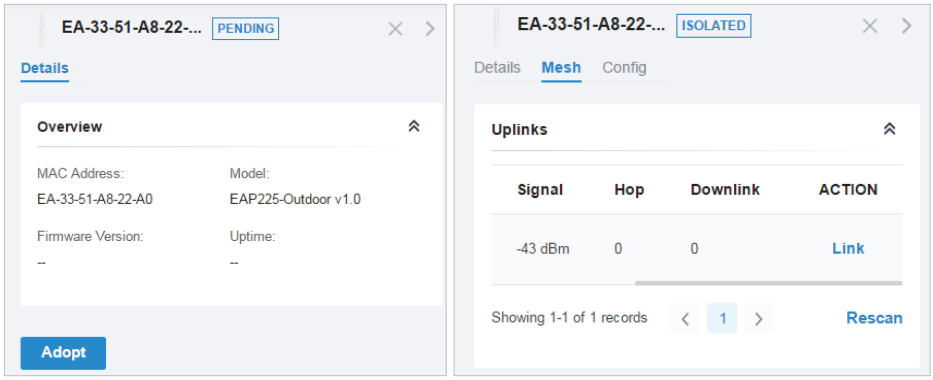
After all the EAPs are adopted, a mesh network is established. The EAPs connected to the network via wireless connection also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

To build a mesh network, follow the steps below:

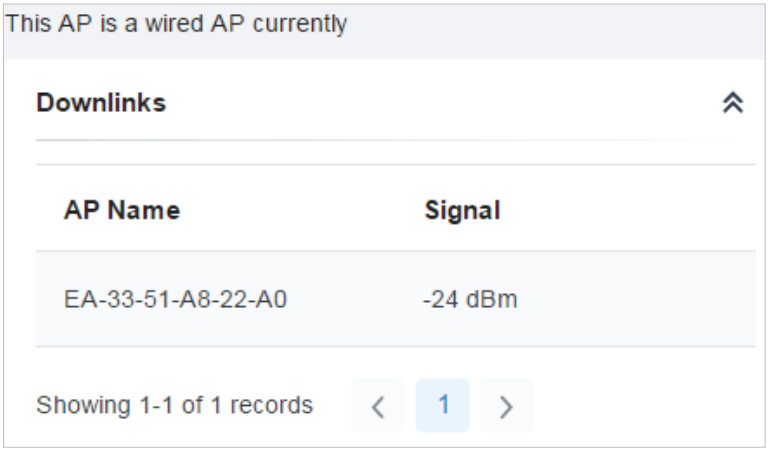
1. Go to Settings > Site to make sure Mesh is enabled.



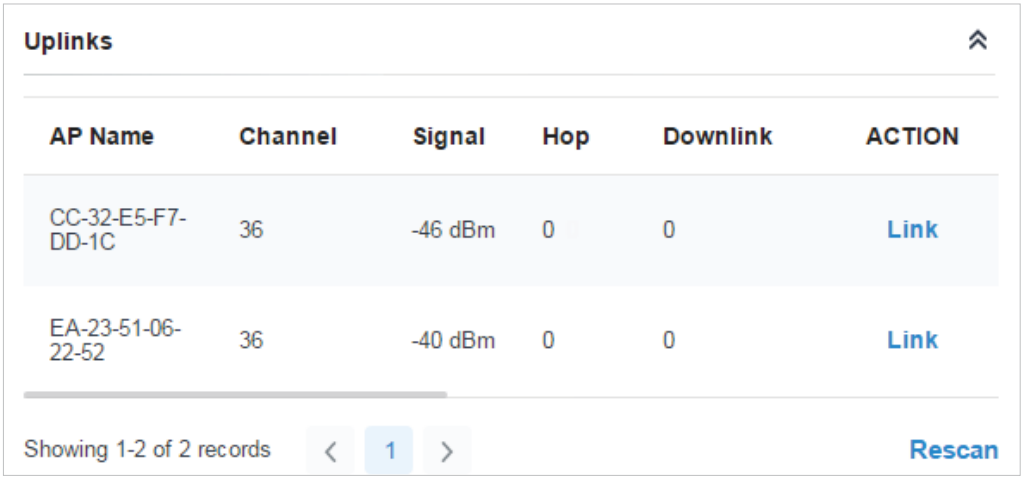
2. Go to Devices to adopt a pending AP or link an isolated AP.



In Mesh, if the selected AP is an uplink AP, this page lists all downlink APs connected to the AP.

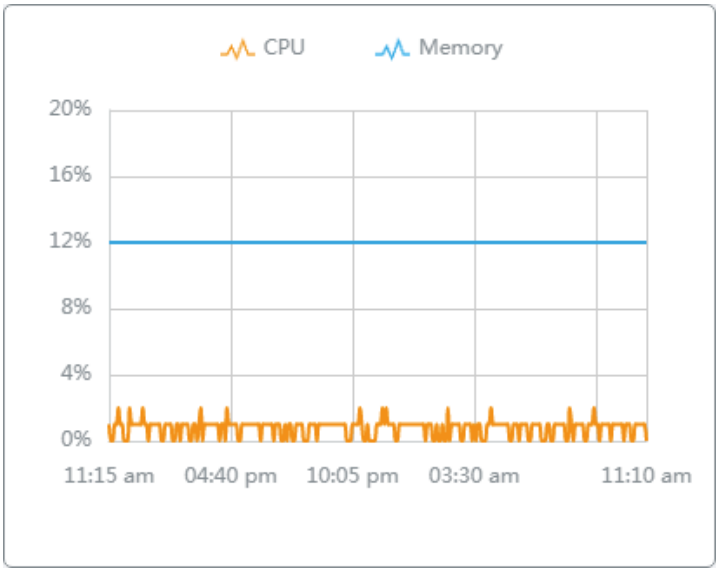


If the selected AP is a downlink AP, this page lists all available uplink APs and their channel, signal strength, hop, and the number of downlink APs. You can click Rescan to search the available uplink APs and refresh the list, and click Link to connect the uplink AP and build up a mesh network.



Statistics

In Statistics, you can monitor the utilization of the device in last 24 hours via charts, including CPU/Memory Monitor, Channel Utilization, Dropped Packets, and Retried Packets. To view statistics of the device in certain period, click the chart to jump to View the Statistics of the Network.





Monitor and Manage the Clients

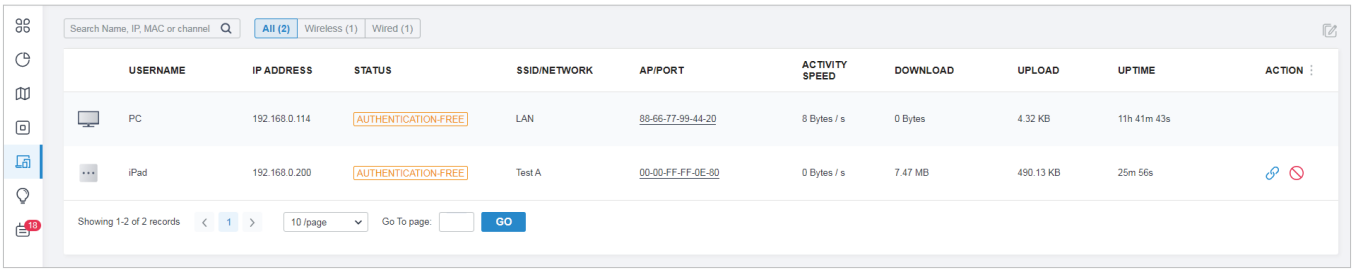
This chapter guides you on how to monitor and manage the clients through the Clients page using the clients table and the properties window and the Hotspot Manager system. To view clients that have connected to the network in the past, refer to View the Statistics During the Specified Period with Insight. This chapter includes the following sections:

- Manage Wired and Wireless Clients in Clients Page
- Manage Client Authentication in Hotspot Manager

7. 1 Manage Wired and Wireless Clients in Clients Page

7. 1. 1 Introduction to Clients Page

The Clients page offers a straight-forward way to manage and monitor clients. It displays all connected wired and wireless clients in the chosen site and their general information. You can also open the Properties window for detailed information and configurations.



PENDING	The client has not passed the portal authentication and it is not connected to the internet.
AUTHORIZED	The client has been authorized and is connected to the internet.
CONNECTED	The client is connected to internet via non-portal network.
AUTHENTICATION-FREE	The client does not need to be authorized and it is connected to the internet.

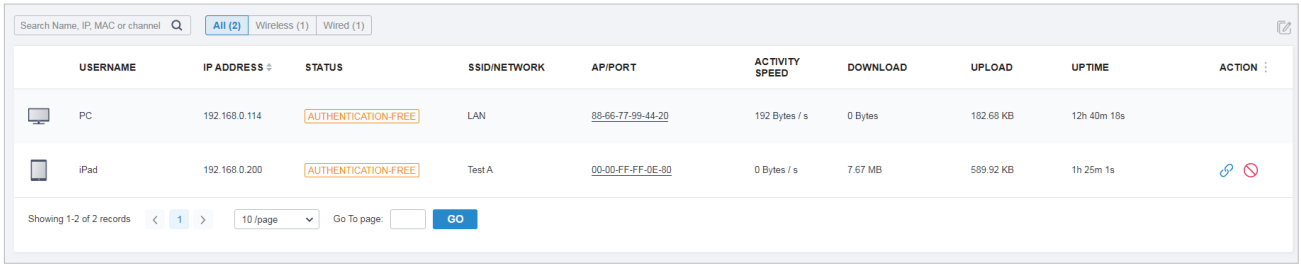
7. 1. 2 Using the Clients Table to Monitor and Manage the Clients

To quickly monitor and manage the clients, you can customize the columns and filter the clients for a better overview of their information. Also, quick operations and batch configuration are available.

- **Customize the Information Columns**

  Click ⋮ next to the Action column and you have three choices: Default Columns, All Columns, and Customize Columns. To customize the information shown in the table, click the checkboxes of information type.

  To change the list order, click the column head and the icon appears for you to choose the ascending or descending order.



Filter the Clients

To search specific client(s), use the search box above the table. To filter the clients by their connection type, use the tab bars above the table. For wireless clients, you can further filter them by the frequency band and the type of connected wireless network.

Search Name, IP, MAC or channel	Filter clients using the search box based on username, IP address, MAC address or channel.
All (2) Wireless (1) Wired (1)	Filter clients based on their connection type.
All (2) 2.4 GHz (0) 5 GHz (2)	(For wireless clients) Filter wireless clients based on the frequency band they are using.
All (2) Users (0) Guests (2)	(For wireless clients) Filter wireless clients based on the type of connected wireless network. Guests are clients connected to the guest network, which you can set during the Quick Setup, creating wireless networks, etc.

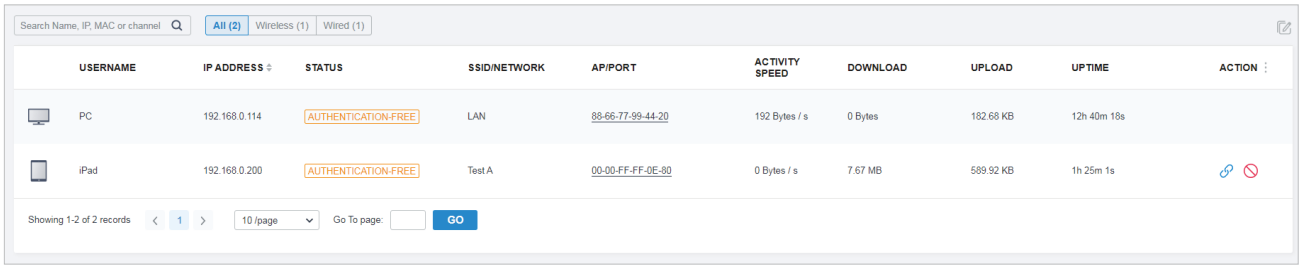
Quick Operations

For quick operations on a single client, click the icons in the Action column. The available icons vary according to the client status and connection type.

	Click to block the client in the chosen site. You can view blocked clients in Known Clients.
	(With portal authentication enabled) Click to manually authorize the client that has not passed the portal authentication.
	(With portal authentication enabled) Click to unauthorize the client that has passed the portal authentication.
	(For wireless clients) Click to reconnect the wireless client to the wireless network.

Multiple Select for Batch Configuration

To select multiple clients and add them to the Properties window, click on the upper-right and then check the boxes. When you finish choosing the clients, click Edit Selected and the chosen client(s) will be added to the Properties window for batch client configuration.



7. 1. 3 Using the Properties Window to Monitor and Manage the Clients

In Properties window, you can view more detailed information about the connected client(s) and manage them. To open the Properties window, click the entry of a single client, or click the icon to select multiple clients for batch configuration. Use the following icons for the Properties window.

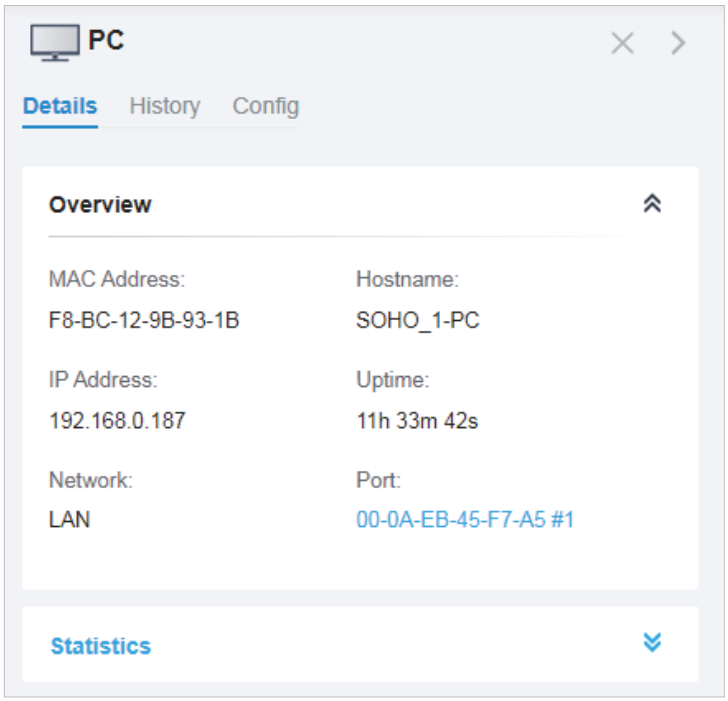
	Click to select multiple clients and add them to the Properties window for batch monitoring and management.
	Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click .
	Click to maximize the Properties window. You can also use the icon on pages other than the Clients page.
	Click to close the Properties window of the chosen client(s). Note that the unsaved configuration for the client(s) will be lost.
	The number on the lower-right shows the number of clients in the batch client configuration.

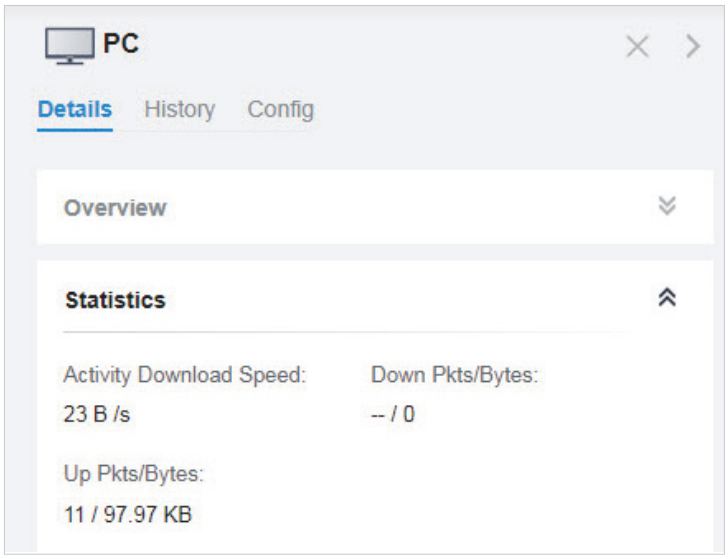
Monitor and Manage a Single Client

- **Monitor a Single Client**

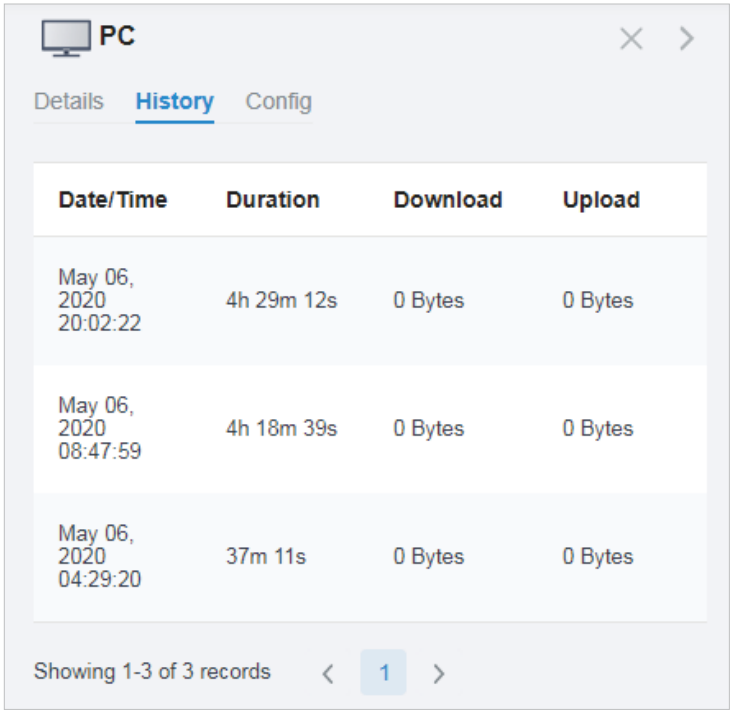
  After opening the Properties window of a single client, you can view the basic information, traffic statistics, and connection history under the Details and History tabs.

  Under the Details tab, Overview and Statistics displays the basic information and traffic statistics of the client, respectively. The listed information varies due to the client's status and connection type.



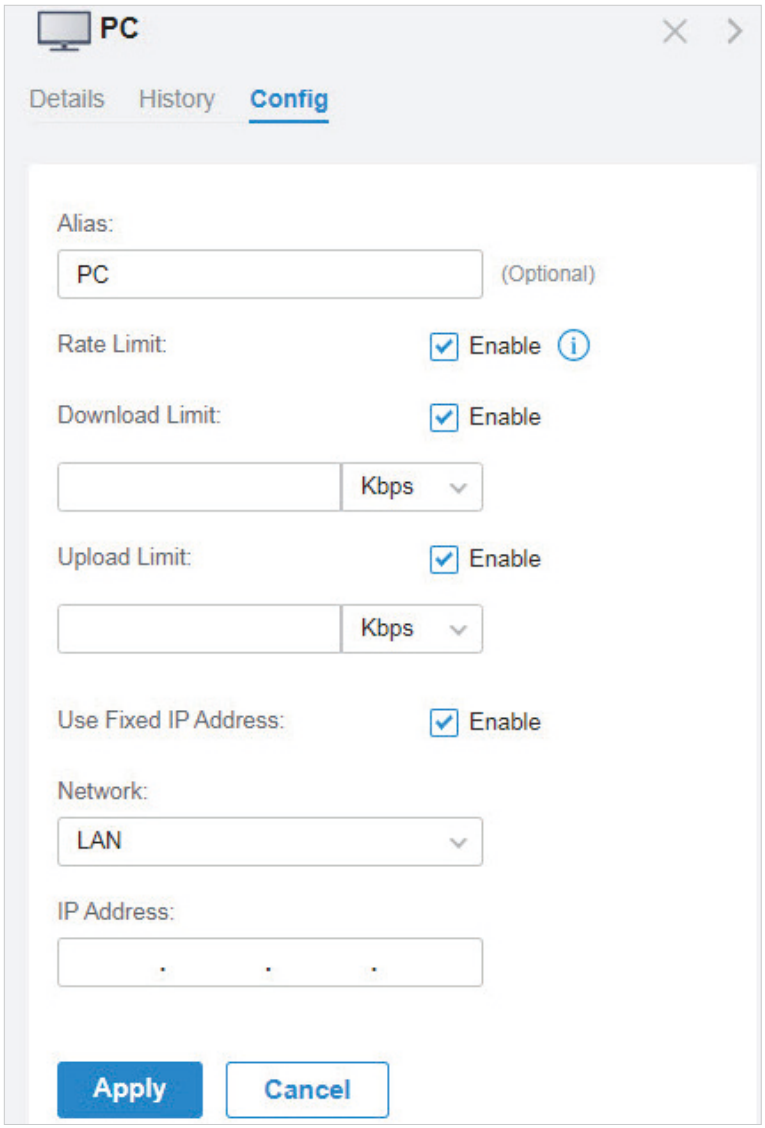


Under the History tab, you can view the connection history of the client.



Manage a Single Client

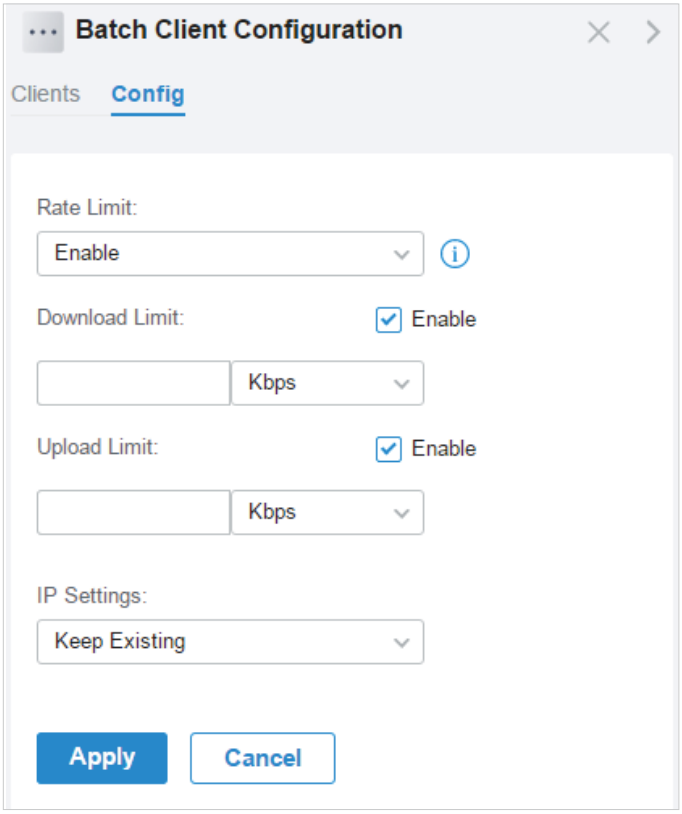
In Config, you can configure the following parameters:



Alias	Specify the client's alias to better identify different clients, and the alias is used as the client's username in the table on the Clients page.
Rate Limit	Click the chekbox to enable rate limit for the client. With the function enabled, you can further set limits for download and upload rate. If rate limit is disabled, the rate limit of the client remains its default setting. Note: Rate Limit on this page is only available for the clients connected to the EAPs. To limit the rate of the clients connected to the gateway or switch, go to Bandwidth Control page.
Use Fixed IP Address	Click the checkbox to configure a fixed IP address for the client. With this funciton enabled, select a network and specify an IP address for the client. To view and configure networks, refer to Configure Wired Networks. Note: An Omada-managed gateway is required for this function. Otherwise, you cannot set a fixed IP address for the client.

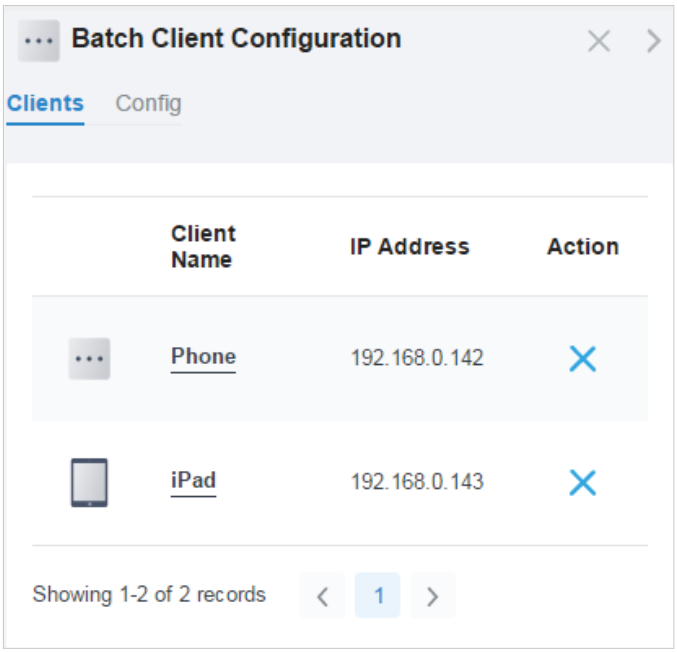
Monitor and Manage Multiple Clients

To manage multiple clients at the same time, click , select multiple clients, and click Edit Selected. Then you can configure the following parameters under the Config tab.



Rate Limit	Keeping existing: The rate limit of the chosen clients remains their current settings. Enable: With Rate Limit enabled, specify limits for download and/or upload rate for all the chosen clients. Disable: With Rate Limit disabled, there is no rate limit for the chosen clients. Note: Rate Limit on this page is only available for the clients connected to the EAPs. To limit the rate of the clients connected to the gateway or switch, go to Bandwidth Control page.
IP Setting	Keeping existing: The IP setting of the chosen clients remains their current settings. Use DHCP: The IP addresses of the clients is automatically assigned by the DHCP server, such as the Layer 3 switch and the gateway. Use Fixed IP Address: Select a network and assign fixed IP addresses to the chosen clients manually. To view and configure networks, refer to Configure Wired Networks. Note that an Omada-managed gateway is required for this function. Otherwise, you cannot set fixed IP addresses for the chosen clients.

You can view their names and IP addresses in the Clients tab and remove client(s) from Batch Client Configuration by clicking ✕ in the Action column.



7. 2 Manage Client Authentication in Hotspot Manager

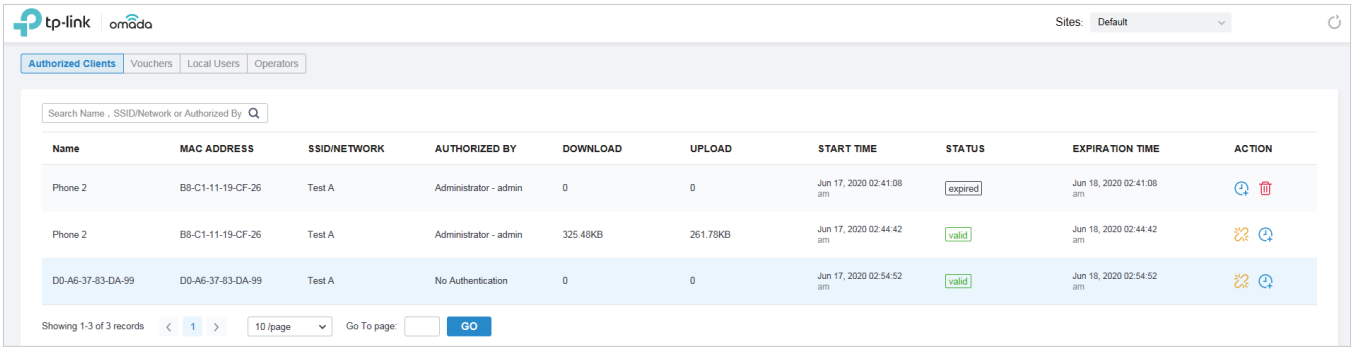
Hotspot Manager is a portal management system for centrally monitoring and managing the clients authorized by portal authentication. The following four tabs are provided in the system for a easy and direct management.

Authorized Clients	View the records of the connected and expired portal clients.
Vouchers	Create vouchers for Portal authentication, and view and manage the related information.
Local Users	Create local user accounts for Portal authentication, view their information, and manage them.
Operators	Create operator accounts for Hotspot management, view their information, and manage them.

7. 2. 1 Authorized Clients

The Authorized Clients tab is used to view and manage the clients authorized by portal system, including the expired clients and the clients within the valid period.

To open the list of Authorized Clients, click Hotspot Manager from the drop-down list of Sites and click Authorized Clients in the pop-up page. You can search certain clients using the search box, view their detailed information in the table, and manage them using the action column.



	Click to extend the valid period of the authorized client. You can choose the preset time length or set a customized period based on needs.
	Click to disconnect the authorized client(s). When you disconnect an authorized client, the client needs to be re-authenticated for the next connection.
	Click to delete the expired client from the list.

7. 2. 2 Vouchers

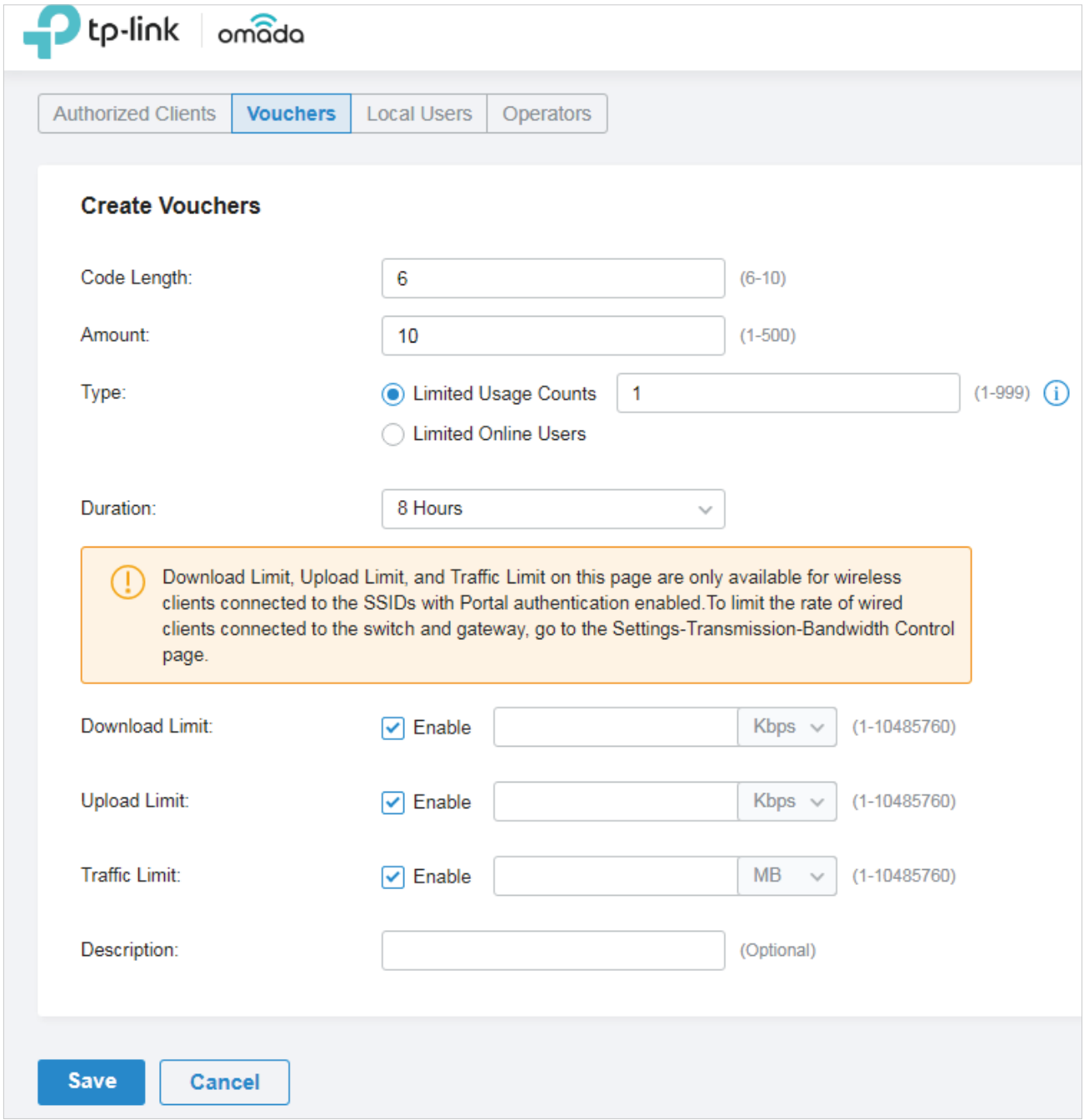
The Vouchers tab is used to create vouchers and manage unused voucher codes. With voucher configured and codes created, you can distribute the voucher codes generated by the controller to

clients for them to access the network via portal authentication. For detailed configurations, refer to Portal.

Create vouchers

Follow the steps below to create vouchers for authentication:

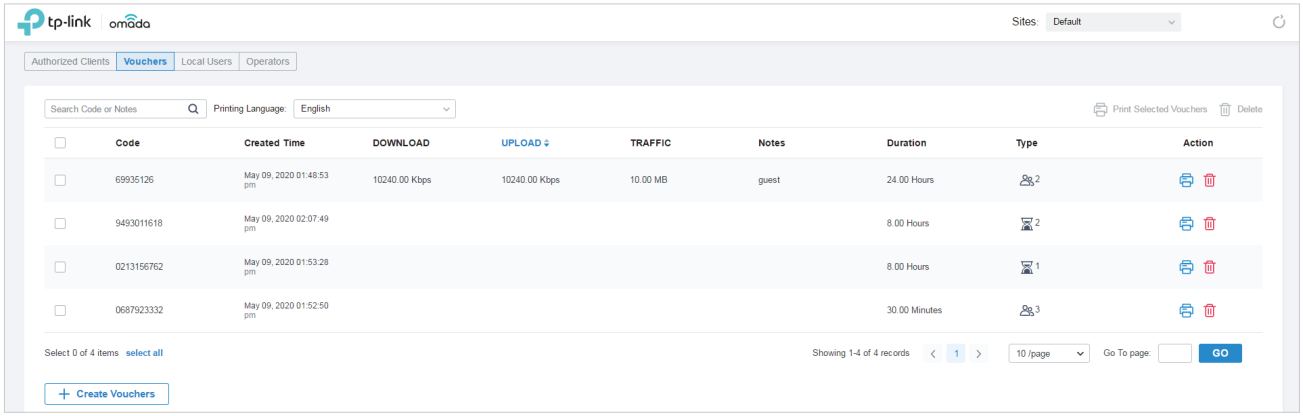
1. Click Hotspot Manager from the drop-down list of Sites and click Vouchers in the pop-up page.
2. Click +Create Vouchers on the lower-left, and the following window pops up. Configure the following parameters and click Save.



Code Length	Specify the length of the code(s) from 6 to 10 digits.

Amount	Specify the number of voucher codes you want to create.
Type	Select a type to limit the usage counts or the number of authorized users of a voucher code. Limited Usage Counts: The voucher code can only be used for a limited number of times within its valid period. Limited Online Users: The voucher code can be used for an unlimited number of times within its valid period, but only a limited number of wireless clients can access the network with this voucher code at the same time.
Duration	Select the valid period for the voucher code(s).
Download/Upload Limit	Click the checkbox and specify the rate limit for download/upload for wireless clients using the voucher code(s). The value of the download and upload rate can be set in Kbps or Mbps. Note: Download/Upload Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to the Settings >Transmission > Bandwidth Control.
Traffic Limit	Click the checkbox and specify the total traffic limit for the voucher, and the value of the traffic limit can be set in MB or GB. Once the limited is reached, the client(s) can no longer access the network using the voucher. Note: Traffic Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to the Settings > Transmission > Bandwidth Control.
Description (optional)	Enter notes for the created voucher code(s), and the input description is displayed in the voucher list under the voucher tab.

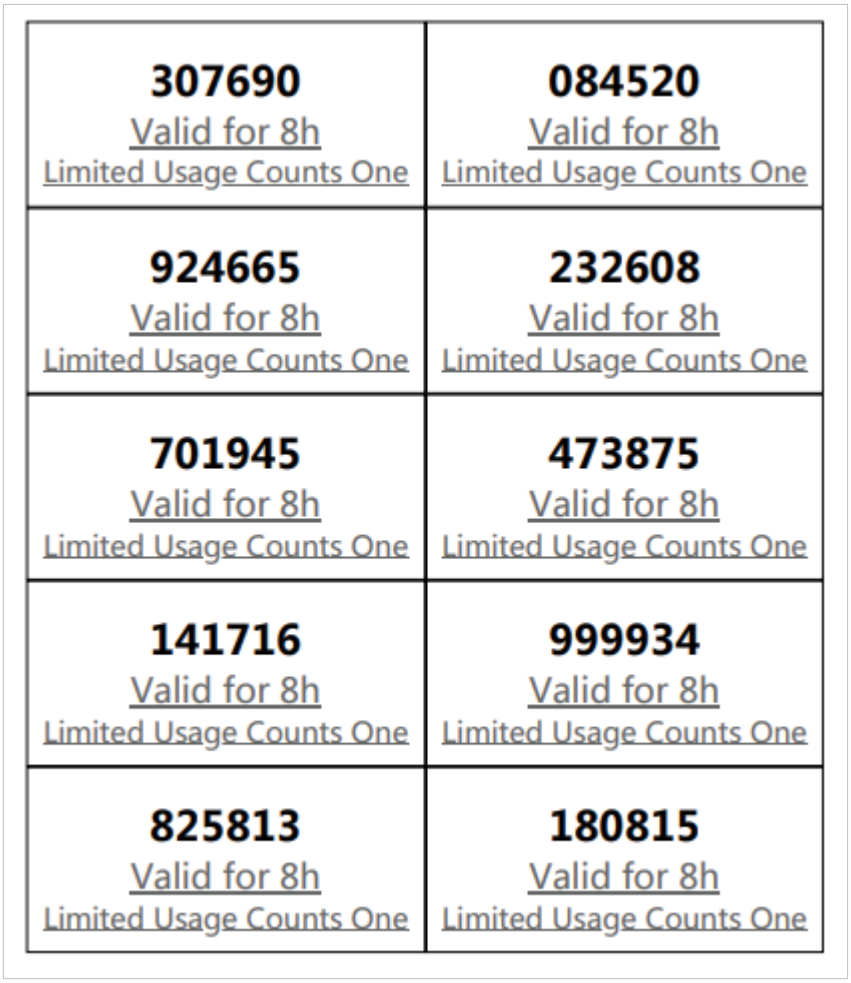
3. The voucher codes are generated and displayed in the table.



2	The voucher code can be used for an unlimited number of times within its valid period, but only a limited number of wireless clients can access the internet with this voucher code at the same time. The number on the right shows the limited number of users.

2	The voucher code can only be used for a limited number of times within its valid period. The number on the right shows the limited number of authentication times.

4. Print the vouchers. Click to print a single voucher, or click checkboxes of vouchers and click Print Selected Vouchers to print the selected vouchers.



307690 Valid for 8h Limited Usage Counts One	**084520** Valid for 8h Limited Usage Counts One
924665 Valid for 8h Limited Usage Counts One	**232608** Valid for 8h Limited Usage Counts One
701945 Valid for 8h Limited Usage Counts One	**473875** Valid for 8h Limited Usage Counts One
141716 Valid for 8h Limited Usage Counts One	**999934** Valid for 8h Limited Usage Counts One
825813 Valid for 8h Limited Usage Counts One	**180815** Valid for 8h Limited Usage Counts One

5. Distribute the vouchers to clients, and then they can use the codes to pass authentication. If a voucher code expires, it will be automatically removed from the list.
6. To delete certain vouchers manually, click to delete a single voucher, or Delete to delete multiple voucher codes at a time.

7. 2. 3 Local Users

The Local Users tab is used to create user accounts for authentication. With the Local User configured, clients are required to enter the username and password to pass the authentication. You can create multiple accounts and assign them to different users. For detailed configurations, refer to Portal.

Create Local Users

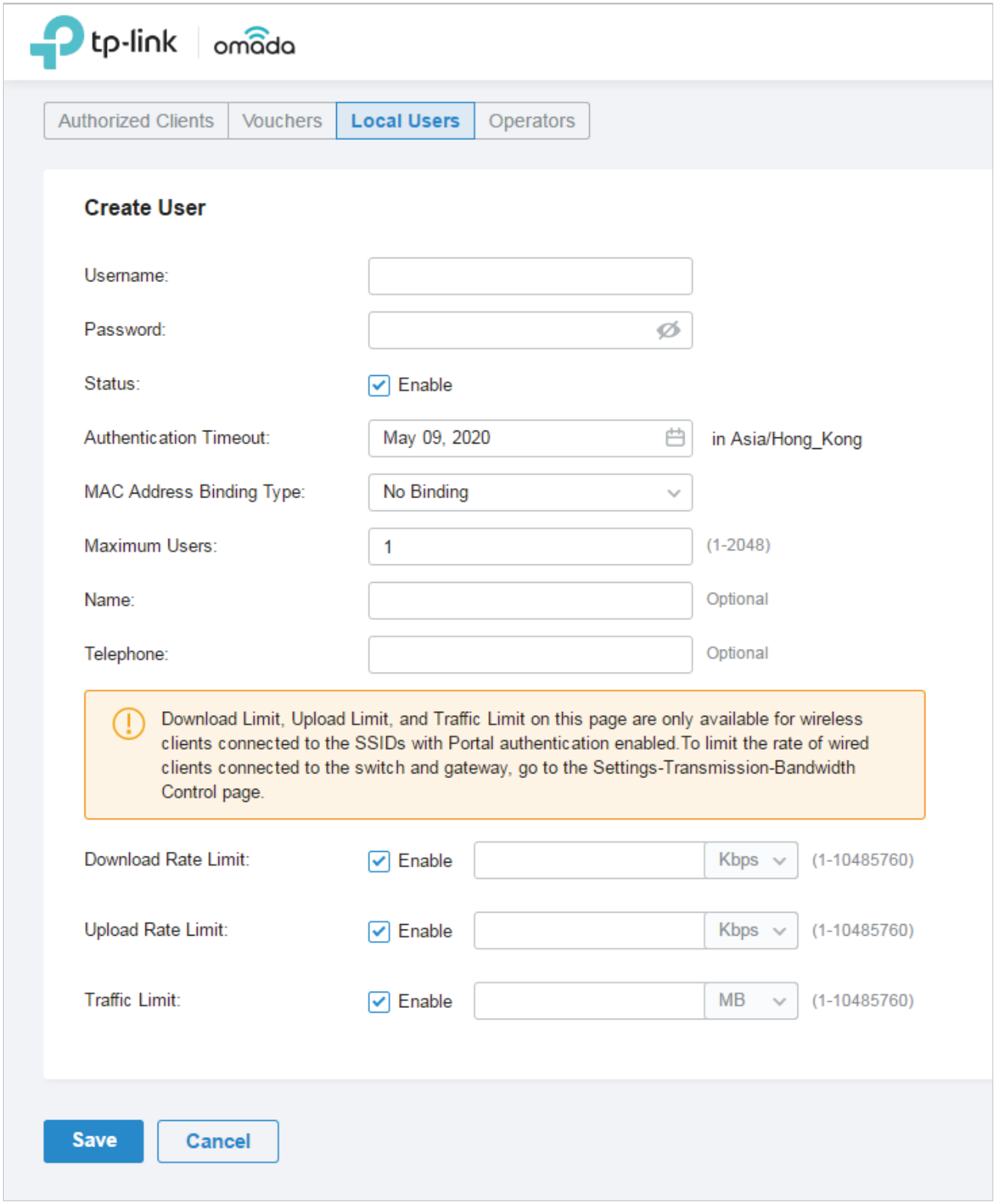
There are two ways to create local user accounts: create accounts on the page and import from a file.

To create local user accounts, follow the steps below.

1. Click Hotspot Manager from the drop-down list of Sites and click Local Users in the pop-up page.
2. Create Local User accounts through two different ways.

- **Create Local User accounts**

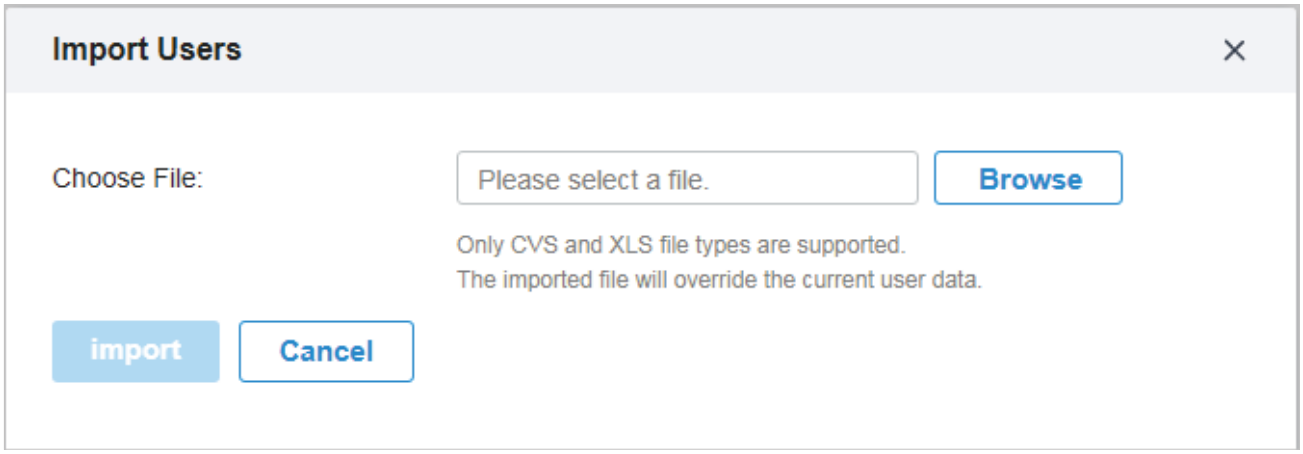
  Click +Create User on the lower-left, and the following window pops up. Configure the following parameters and click Save.



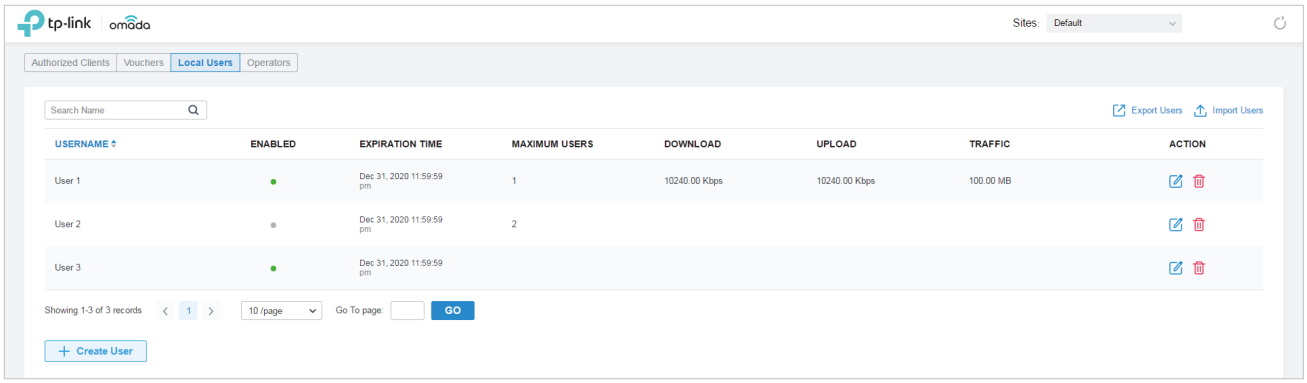
Username	Specify the username. The username should be different from the existing ones, and it is not editable once it is created.
Password	Specify the password. Local users are required to enter the username and password to pass authentication and access the network.
Status	When the status is enabled, it means the user account is valid. You can disabled the user account, and enable it later when needed.
Authentication Timeout	Specify the authentication timeout for local users. After timeout, the users need to log in again on the authentication page to access the network.
MAC Address Binding Type	There are three types of MAC binding: No Binding, Static Binding and Dynamic Binding. No Binding: No MAC address is bound to the local user account. Static Binding: Bind a MAC address to this user account manually. Then only the user with the this MAC address can use the username and password to pass the authentication. Dynamic Binding: The MAC address of the first user that passes the authentication will be bound to this account. Then only this user can use the username and password to pass the authentication.
Maximum Users	Specify the maximum number of users that can use this account to pass the authentication.
Name (optional)	Specify a name for identification.
Telephone (optional)	Specify a telephone number for identification.
Download/Upload Limit	Click the checkbox and specify the rate limit for download/upload for users of the local user account. The value of the download/upload rate can be set in Kbps or Mbps. Note: Download/Upload Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to the Settings >Transmission > Bandwidth Control.
Traffic Limit	Click the checkbox and specify the total traffic limit for the local user account, and the value of the traffic limit can be set in MB or GB. Once the limited is reached, the user(s) can no longer access the network using this account. Note: Traffic Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to the Settings > Transmission > Bandwidth Control.

- **Create Local User accounts from files.**

  Click Import Users on the upper-right, and the following window pops up. Select a file in the format of CVS or Excel, and click Import. To see required parameters and corresponding explanation, refer to Create Local User accounts. Note that the imported file will override the current user data.



3. The local user account(s) will be created and displayed in the module. You can view the information of the created local users, search certain accounts through the name, and use icons for management.



Import Users	Click to add local user(s) from files in the format of CVS or Excel. It is recommended when you need to create local users in batches. Note that the imported file will override the current user data.
Export Users	Click to export the local user(s) to files in the format of CVS or Excel.
	Click to edit the parameters for the local user.
	Click to delete the local user.

7. 2. 4 Operators

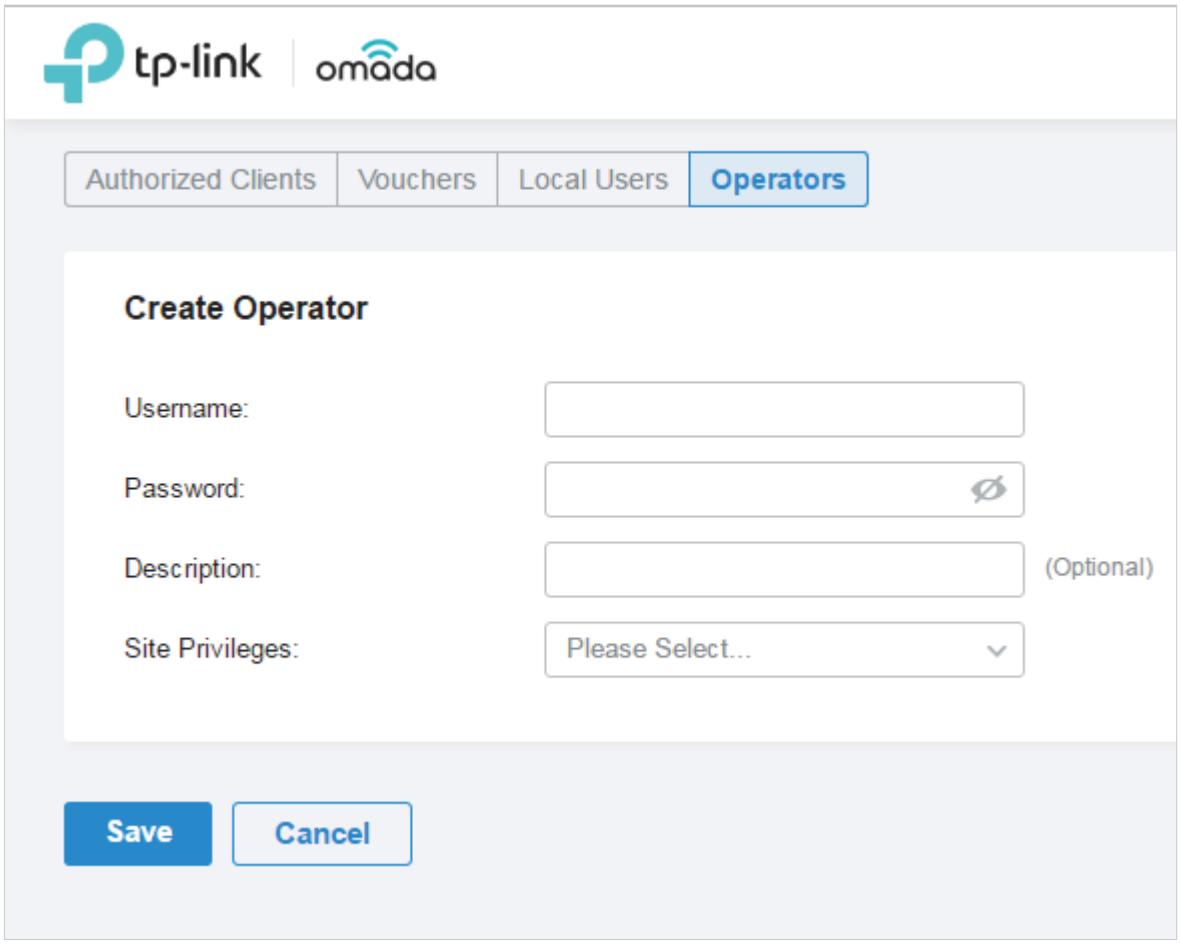
The Operators tab is used to manage and create operator accounts that can only be used to remotely log in to the Hotspot Manager system and manage vouchers and local users for specified sites. The

operators have no privileges to create operator accounts, which offers convenience and ensures security for client authentication.

Create Operators

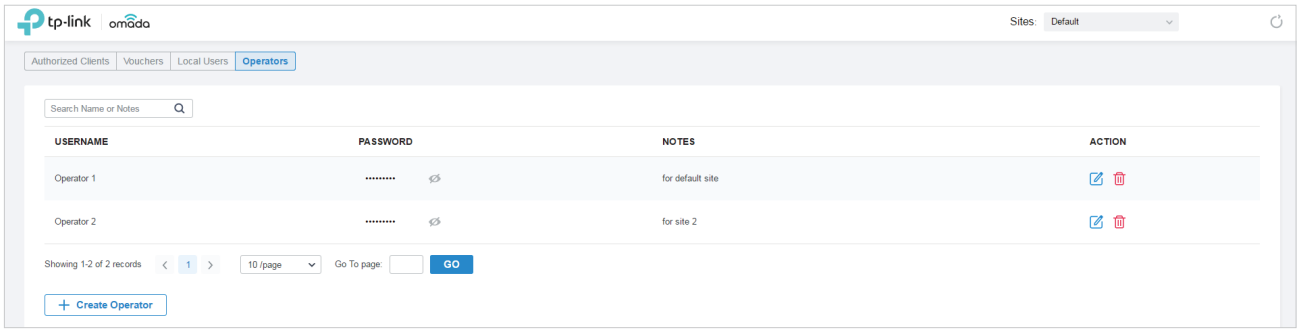
To create operator accounts, follow the steps below.

1. Click Hotspot Manager from the drop-down list of Sites and click Operators in the pop-up page.
2. Click + Create Operator on the lower-left, and the following window pops up.



3. Specify the username, password and description (optional) for the operator account. Then select sites from the drop-down list of Site Privileges. Click Save.

4. The operator accounts are created and displayed in the table. You can view the information of the create operator accounts on the page, search certain accounts through the name and notes, and use icons for management.



	Click to edit the parameters for the operator account.
	Click to delete the operator account.

5. Then you can use an operator account to log in to the Hotspot Manager system:

- **For software controller**

  Visit the URL https://Omada Controller Host's IP Address:8043/hotspot (for example: https://192.168.0.174:8043/hotspot), and use the operator account to enter the hotspot manager system.

- **For hardware controller**

  Visit the URL https://Omada Controller Host's IP Address:443/hotspot (for example: https://192.168.0.174:443/hotspot), and use the operator account to enter the hotspot manager system.

- **For cloud-based controller**

  Visit the URL https://omada.tplinkcloud.com/hotspot, and use the operator account to enter the hotspot manager system.

8

Monitor the Network

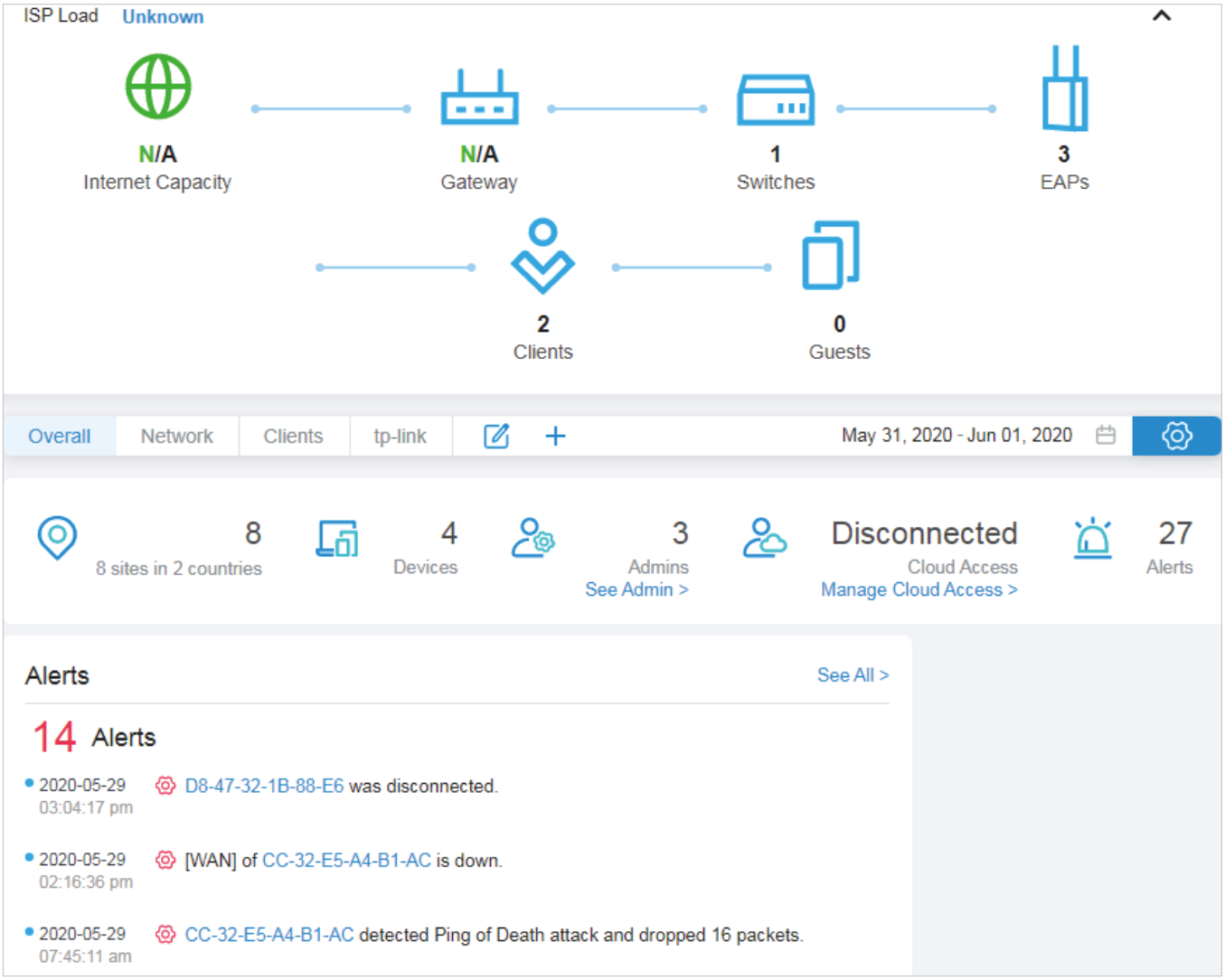
This chapter guides you on how to monitor the network devices, clients, and their statistics. Through visual and real-time presentations, Omada SDN Controller keeps you informed about the accurate status of the managed network. This chapter includes the following sections:

- View the Status of Network with Dashboard
- View the Statistics of the Network
- Monitor the Network with Map
- View the Statistics During Specified Period with Insight
- View and Manage Logs

8. 1 View the Status of Network with Dashboard

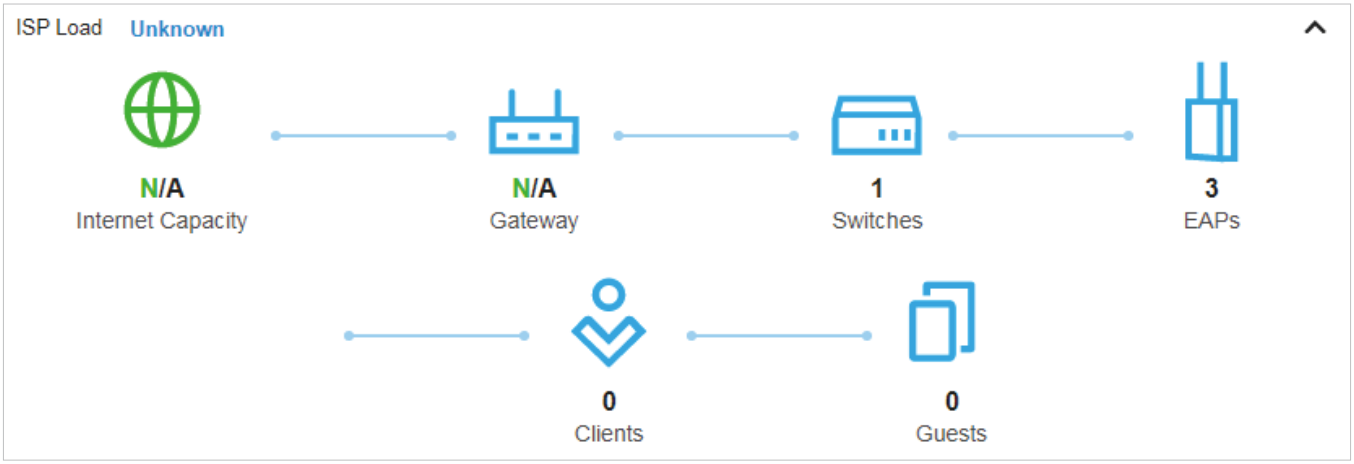
8. 1. 1 Page Layout of Dashboard

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

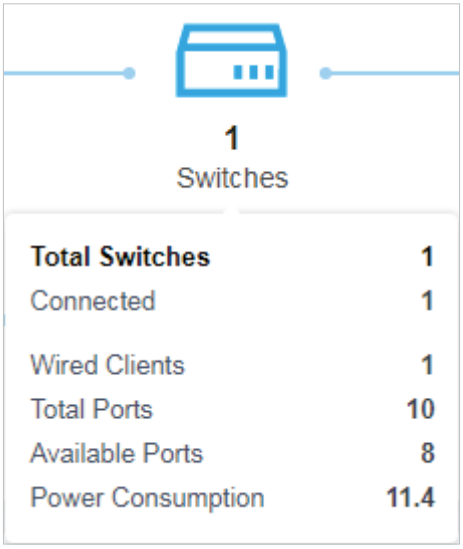


Topology Overview

Topology Overview on the top shows the status of ISP Load and numbers of devices, clients and guests. ISP Load has four statuses: Unknown, Good, Medium, Poor.



You can hover the cursor over the gateway, switch, AP, client or guest icons to check their status. For detailed information, click the icon here to jump to the Devices or Clients section.



Tab Bar

You can customize the widgets displayed on the tab for Dashboard page. Three tabs are created by default and cannot be deleted.



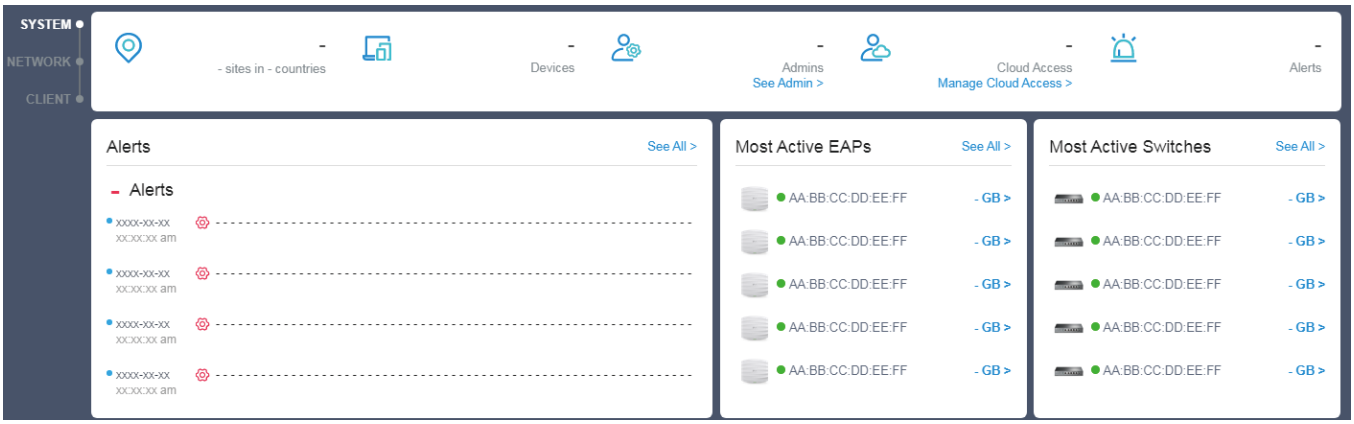
Overall	(Only for administrators) Display Controller Overview and Association Failures by default.
Network	Displays Alerts, Wi-Fi Traffic Distribution, Wi-Fi Summary and Traffic Activities by default.
Clients	Displays Most Active Clients, Clients Freq Distribution, and Client Activities by default.

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.
May 28, 2020 - May 29, 2020 	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.
	Click a tab and then click the widget in the pop-up page to add it to this tab or remove it.

8. 1. 2 Explanation of Widgets

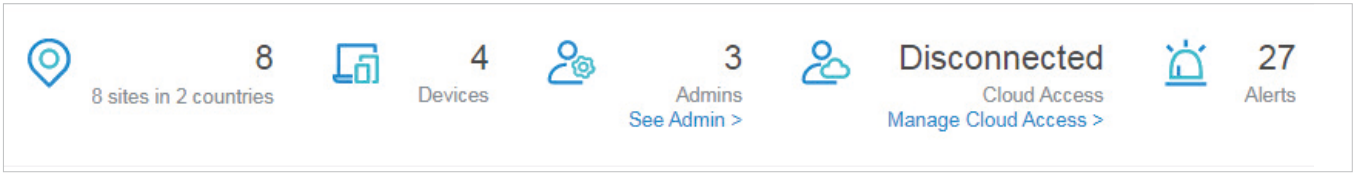
The widgets are divided into three categories: System, Network, Client. You can click the  icon to add or remove the widgets.



System	(Only for the Overall tab) Controller Overview
Network	Alerts, Most Active EAPs, Most Active Switches,Wi-Fi Traffic Distribution, Wi-Fi Summary, Traffic Distribution, Client Distribution, Traffic Activities, Retried Rate/Dropped Rate
Client	Most Active Clients, Longest Client Uptime, Clients Freq Distribution, Client Activities, Association Failures

System

Controller Overview in System can be displayed only in the Overall tab. It provides a real-time overview of the whole controller, including the total number of site, devices, admin accounts, alerts, and the status of cloud access.



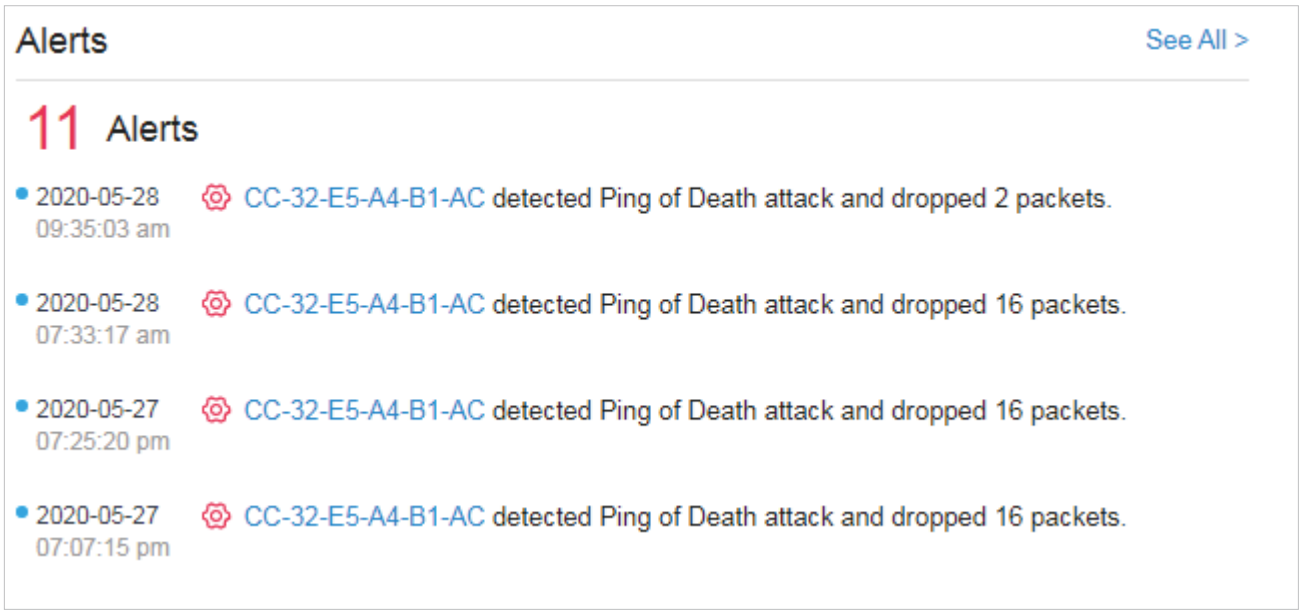
To view and edit admin accounts, click See Admin > to jump to the Admin section. To configure Cloud Access, click Manage Cloud Access > to jump to Settings > Cloud Access. For detailed configuration, refer to Manage Administrator Accounts of Omada SDN Controller and Manage Your Controller Remotely via Cloud Access in this guide.

Network

Widgets in Network use lists and charts to illustrate the traffic status of wired and wireless networks in the site, including the most active devices, traffic statistics and distribution.

- **Alerts**

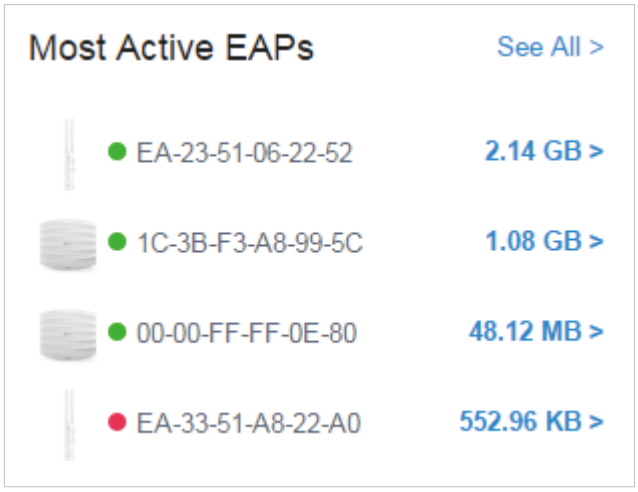
  The Alerts widget displays the total number of unarchived alerts happened in the site and details of the latest five. To view all the alerts and archive them, click Details to jump to Log > Alerts. To specify events appeared in Alerts, go to Log > Notifications and configure the events as the Alert level. For details, refer to View and Manage Logs.



- **Most Active EAPs/Most Active Switches**

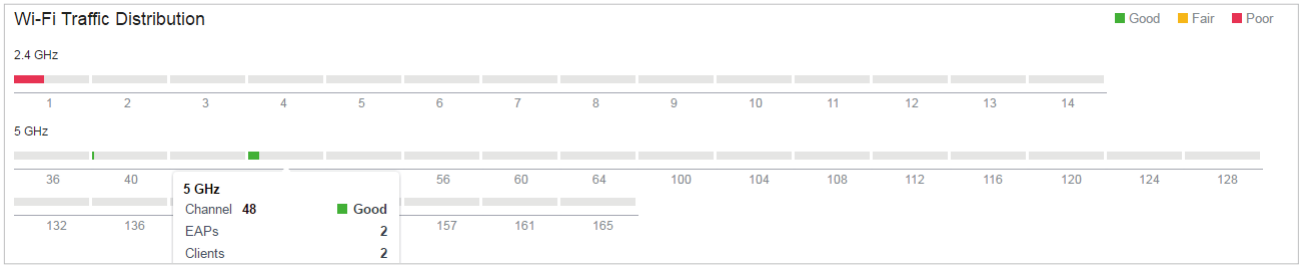
  These two widgets can display, respectively, 15 most active EAPs and switches in the site based on the total number of traffic within the time range. Only the devices that has been adopted by the controller will be displayed.

To view all the devices discovered by the controller, click Details to jump to the Devices section. You can also click the traffic number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to Configure and Monitor Omada Managed Devices.



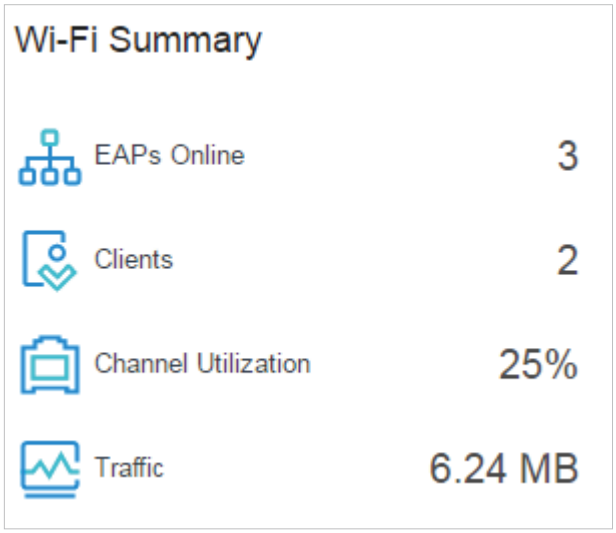
- **Wi-Fi Traffic Distribution**

The Wi-Fi Traffic Distribution widget displays channel distribution of all connected EAPs in the site. Good, Fair, and Poor are used to describe channel status which indicates channel interference from low to high. You can hover your cursor over the band to view the number of EAPs and clients on the channel.



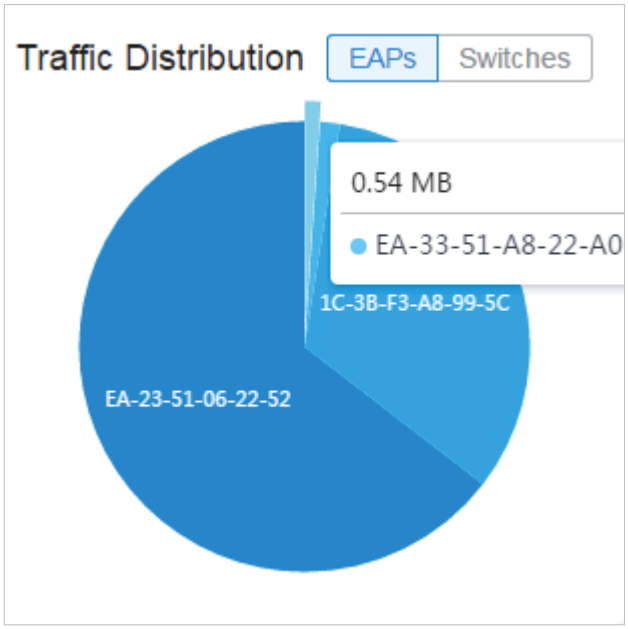
- **Wi-Fi Summary**

  The Wi-Fi Summary widget summarizes the real-time status of wireless networks in the site, including the number of connected EAPs and clients, the channel utilization, and the total number of traffic within the time range.



- **Traffic Distribution**

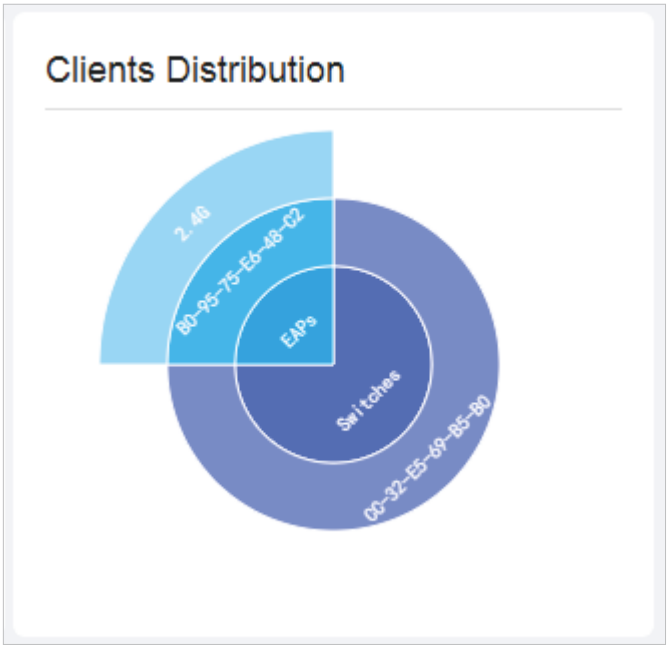
  The Traffic Distribution widget uses a pie chart to display the traffic distribution on EAPs and switches in the site within the time range. Click the tab to display the statistic of EAPs or switches, and click the slice to view the total number of traffic, its proportion, and the device name.



- **Client Distribution**

  The Client Distribution widget uses a sunburst chart to display the real-time distribution of connected clients in the site. The chart has up to three levels. The inner circle is divided by the

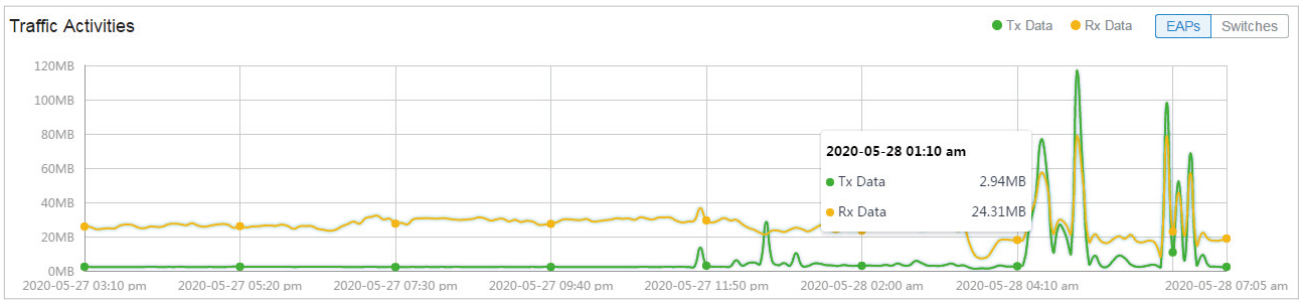
device category the clients connected to, the middle is by the device name, and the outer is by the frequency band. You can hover the cursor over the slice to view specific values.



- **Traffic Activities**

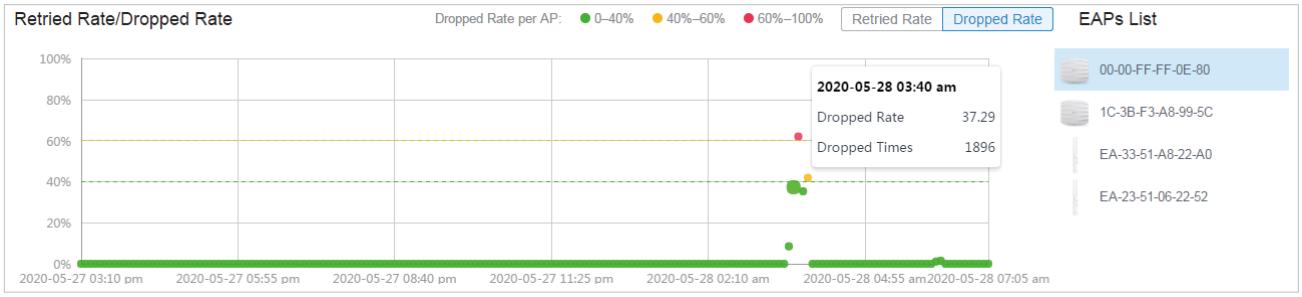
  The Traffic Activities widget displays the Tx and Rx data of EAPs and switches within the time range. Only activities of the devices in the connected status currently will be counted.

  Click the tab to display the statistic of EAPs or switches, and move the cursor on the line chart to view specific values of traffic. For detailed statistics of certain devices within a time range, refer to View the Statistics of the Network.



- **Retried Rate/Dropped Rate**

  The Retried Rate/Dropped Rate widget displays the rate of retried and dropped packets of the connected EAPs within the time range. Select an AP from the list and click the tab to display the chart of retried rate or dropped rate. You can move the cursor on the point to view specific values.



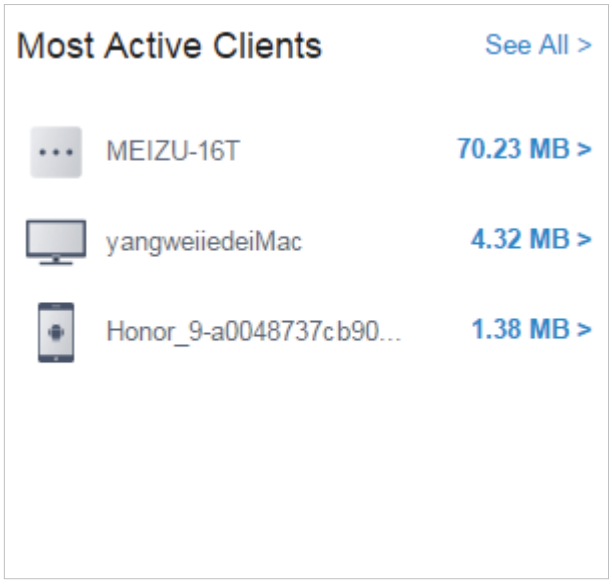
Client

Widgets in Clients use lists and charts to illustrate the traffic status of wired and wireless clients in the site, including the most active clients, activity statistics and distribution.

- **Most Active Clients**

  The Most Active Clients widget can display 15 most active clients. Only the clients in the connected status currently will be displayed.

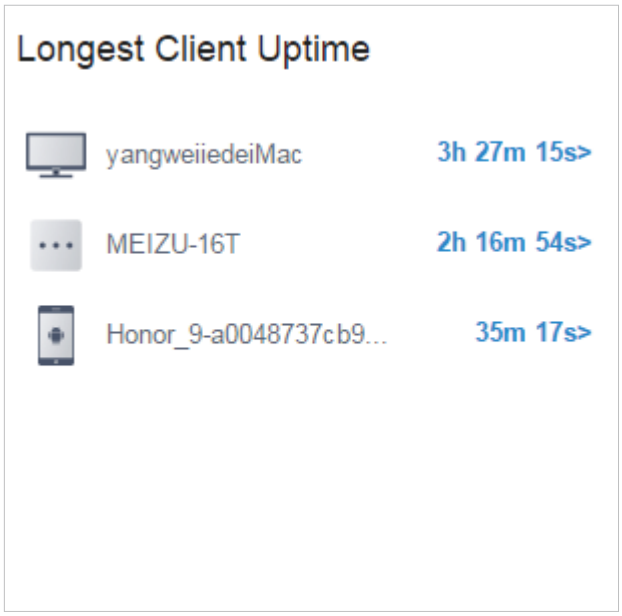
  To view all the clients connected to the network, click Details to jump to the Clients section. You can also click the traffic number in the widget to open the client's Properties window for further configurations and monitoring. For details, refer to Client.



- **Longest Client Uptime**

  The Longest Client Uptime widget can display up to15 clients sorted by the uptime. Only the clients in the connected status currently will be displayed. You can also click the uptime in the widget to

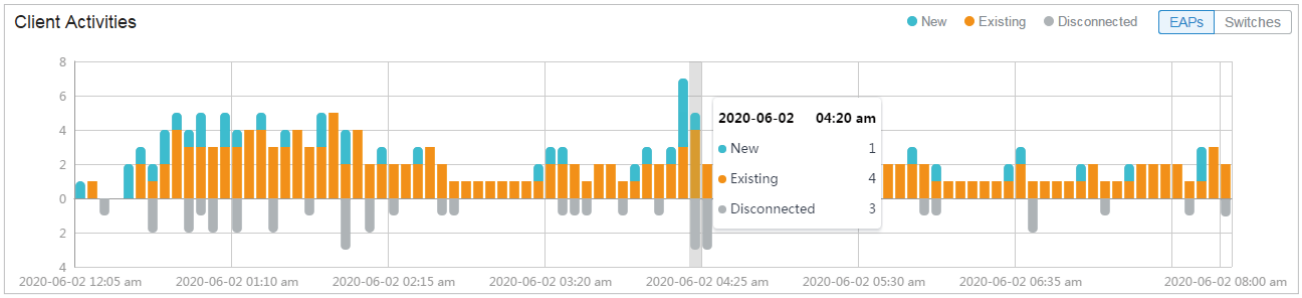
open the client's Properties window for further configurations and monitoring. For details, refer to Client.



- **Client Activities**

  The Client Activities widget displays how the number of connected client changes over time within the time range. In the stacked chart, you can easily compare the total number of clients and analyze the variation of each time period.

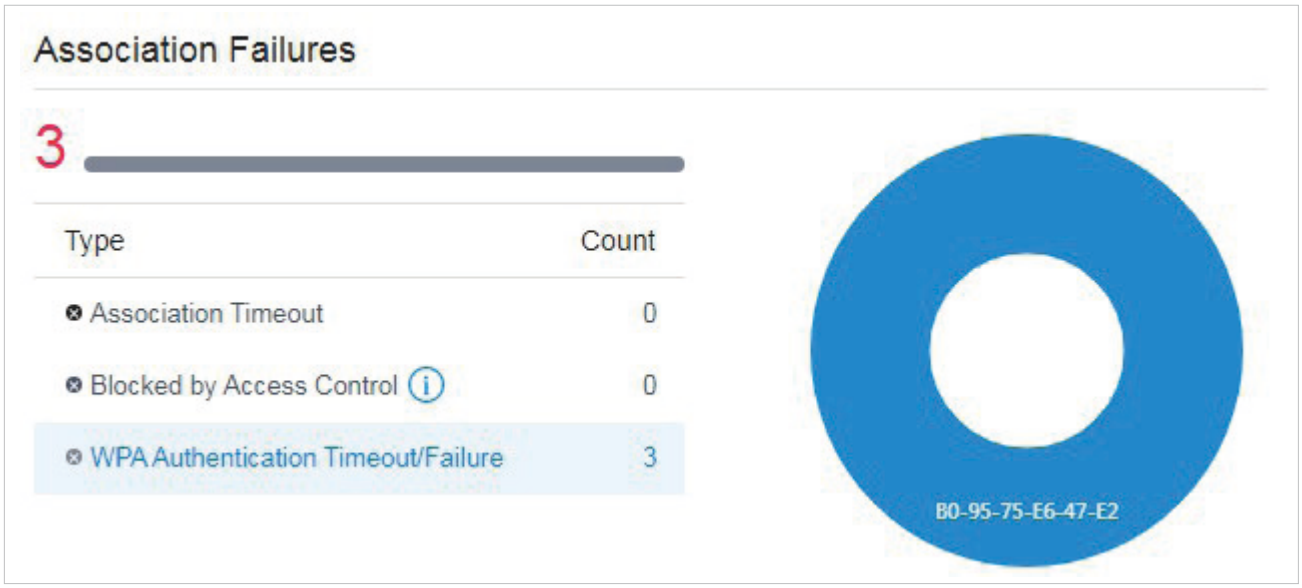
  The total value of a column shows the total number of connected clients in this time period, and the segments in three colors shows the change of client number compared with the last time period. Blue represents the newly connected clients, orange is the clients have been connected in the last period, and gray is the newly disconnected clients.



- **Association Failures**

  The Association Failures widget list three failure types and the times of clients failed to connect to the EAPs' networks in the site. A single bar is next to the count to show the proportion of the

three failure reasons using gray colors from dark to light. Click the reason in the list to view the distribution of failures on EAPs.



Association Timeout	The connection failed because of session timeout.
Blocked by Access Control	The connection failed because the client has been blocked. For details about blocked clients, refer to Known Clients.
WPA Authentication Timeout/Failure	The connection failed because the client did not pass the authentication due to authentication timeout or wrong password.

8. 2 View the Statistics of the Network

Statistics provides a visual representation of device data in Omada SDN Controller. You can easily monitor the network traffic and performance under the following tabs, Performance, Switch Statistics, and Speed Test Statistics.

8. 2. 1 Performance

In Performance, you can view the device performance in a specified period by graphs, such as user counts, CPU and memory usage, and transmitted and received packets. The graphs vary due to the device type and status.

Tab Bar

The tabs and calendar on the top are used to specify the displayed statistics, and the legends on the right account for elements in the graphs.



	Click to select a device from the drop-down list to view its statistics. The tabs vary due to the type of the selected device.
	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.
	(For gateway) Click to select the port of gateway on the tab to view the statistics.
	(For AP) Click to select the band of the AP to view the statistics.

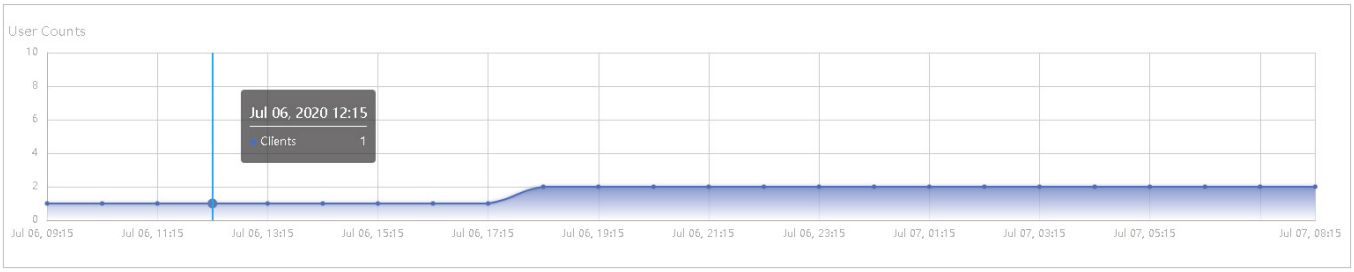
Statistical Graphs

Statistical graphs vary according to the type of devices. The chart below shows the statistical graphs which correspond to the gateway, switch, and AP.

Gateway	User Counts, Usage, Traffic, Packets
Switch	User counts, Usage
AP	User Counts, Usage, Traffic, Packets, Dropped, Errors, Retries

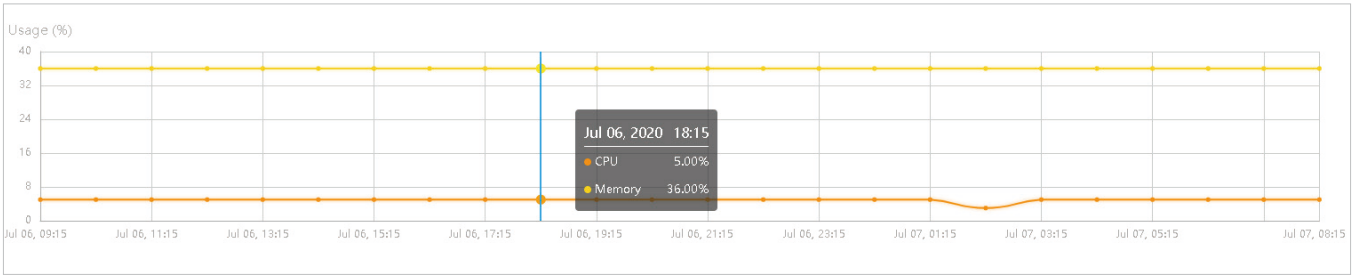
■ User Counts

The User Counts graph displays the number of users connected to the devices during the selected time range. Hover the cursor over the line to display the specific values.



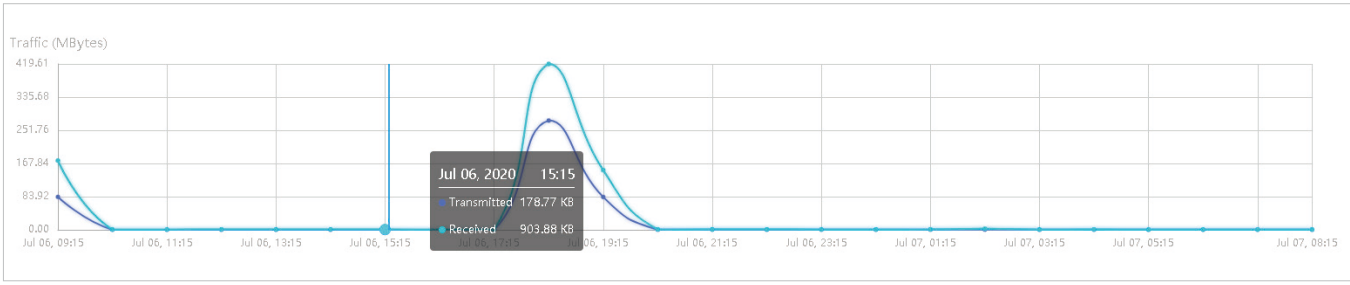
■ Usage

The Usage graph uses the orange line and yellow line 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.



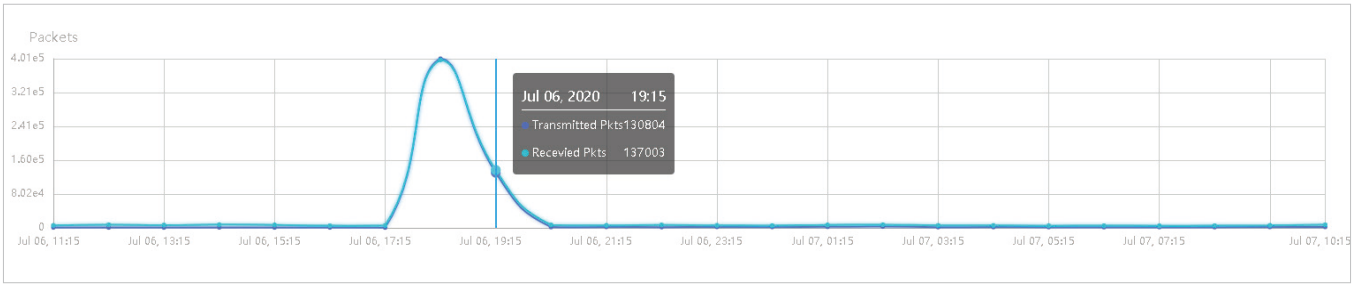
■ Traffic

The Traffic graph uses the dark blue line and light blue line to display the bytes of data transmitted and received during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



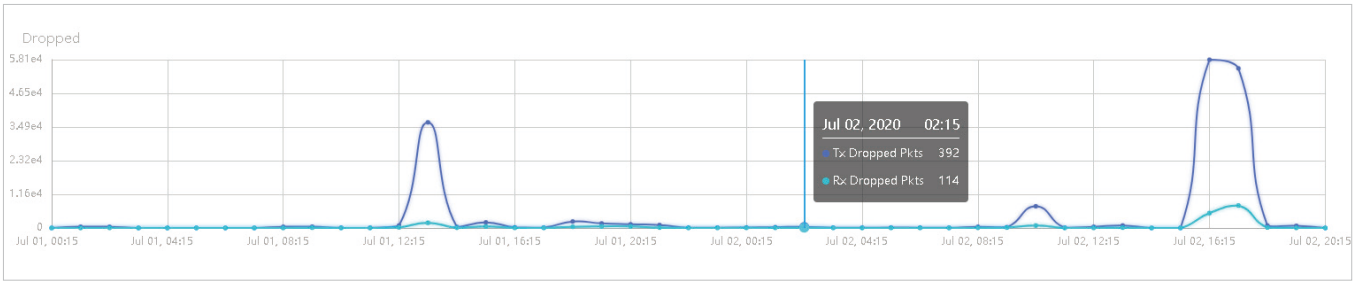
■ Packets

The Packets graph uses the dark blue line and light blue line to display the number of packets transmitted and received during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



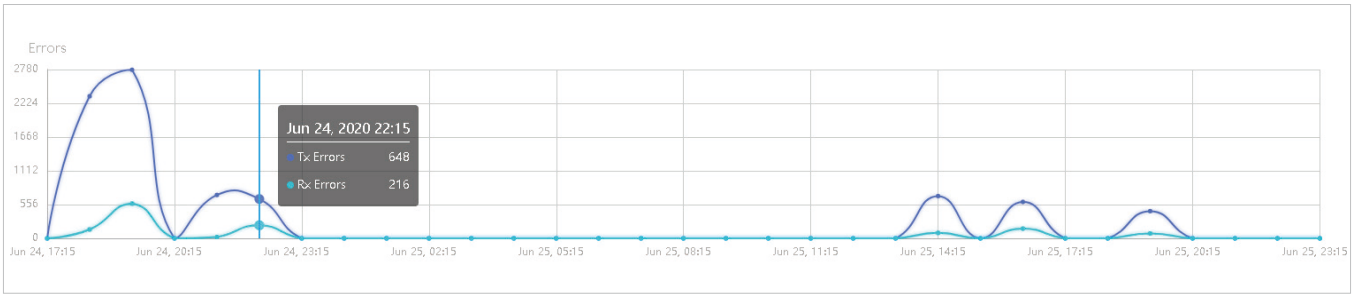
■ Dropped

The Dropped graph uses the dark blue line and light blue line to display the number of dropped Tx packets and Rx packets during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



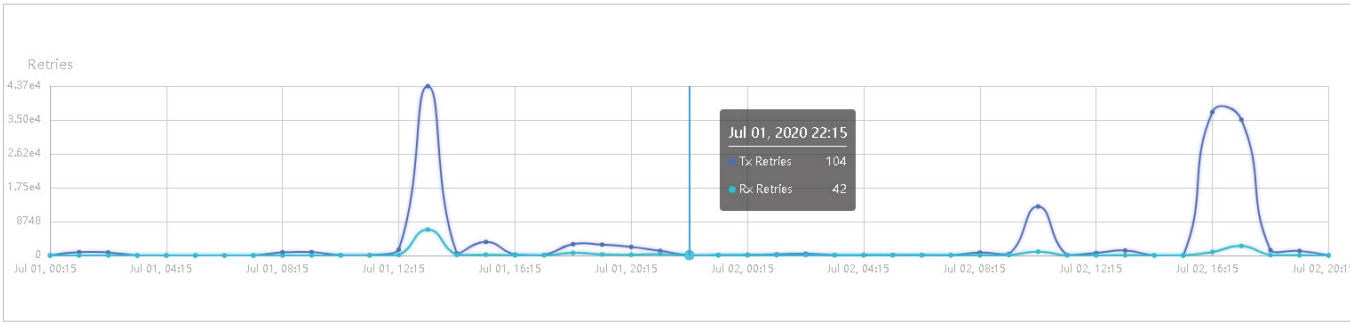
■ Errors

The Errors graph uses the dark blue line and light blue line to display the number of error packets sent to AP and received by AP during the selected time range, respectively. Hover the cursor over the line to display the specific values.



- **Retries**

The Retries graph uses the dark blue line and light blue line to display the number of times that the data packets are transmitted again and received again during the selected period, respectively. Hover the cursor over the lines to display the specific values.



8. 2. 2 Switch Statistics

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

Tab Bar

The tabs and calendar on the top are used to specify the displayed statistics, and the legends on the right account for elements in the graphs.

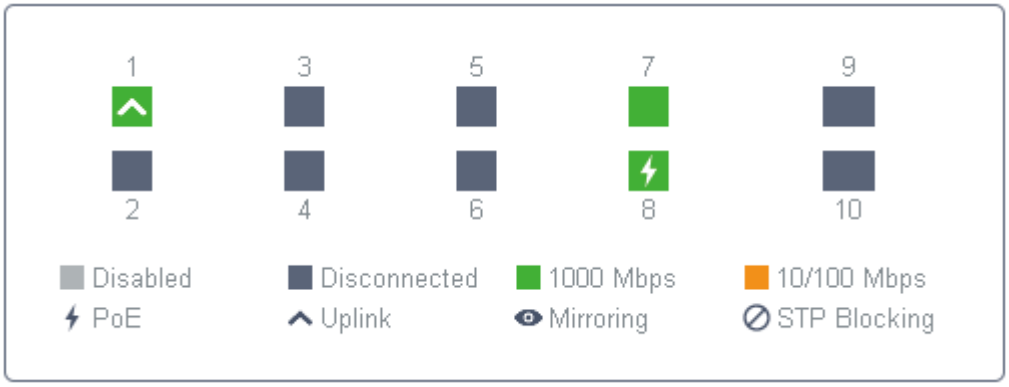


	Click to select a switch from the drop-down list to view its statistics.
	Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly 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.
	Select Natural, Transmitted, Received, or All 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. All: 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. bps: Displays the traffic rate in bps. Bytes: Displays the traffic statistics in Bytes. Packets: Displays the total number of packets.
	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.

Monitor Panel

The monitor panel below the tab bar displays the current status of the ports on the selected switch.

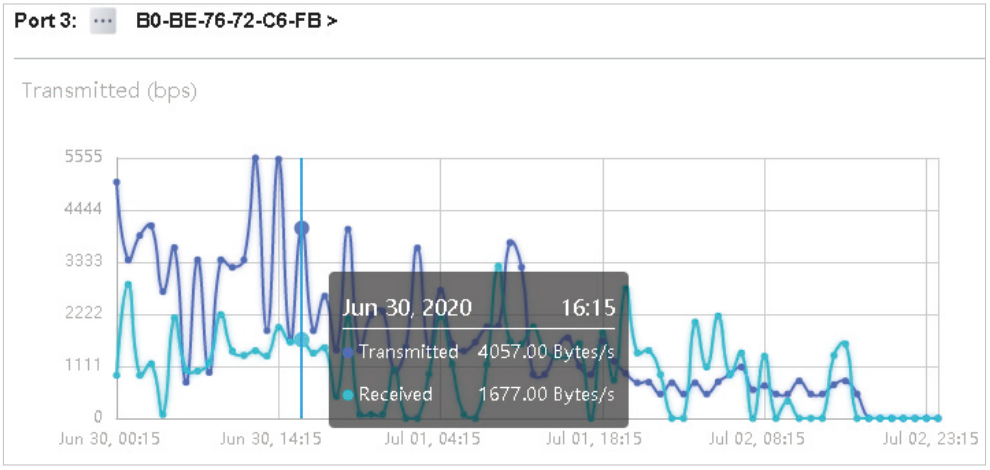


Disabled	The port profile is Disable. To enable it, refer to Configure and Monitor Switches.
Disconnected	The port is enabled but connects to no devices or clients.
1000 Mbps	The port is running at 1000 Mbps.
10/100 Mbps	The port is running at 10/100 Mbps.
PoE	A PoE port connected to a powered device (PD).
Uplink	An uplink port connected to WAN.
Mirroring	A mirroring port that is mirroring another switch port.
STP Blocking	A port in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.

Statistical Graphs

Statistical graphs below the monitor panel display the traffic statistics of active ports.

You can specify the data type and measuring unit by clicking the bps | Bytes | Packets tab. The dark blue and light blue are used to indicate the transmitted and received statistics, respectively. Hover the cursor over the lines to display the specific values. To view and configure the device connected to the port, click the device name beside the port number.



8. 2. 3 Speed Test Statistics

Speed Test Statistics displays the results of the periodic speed test running on WAN ports, including the network latency and speed. To enable the speed test, go to Settings > Sites, enable Periodic Speed Test in Service, and specify the test interval. For details, refer to Services.

Tab Bar

The tab and calendar on the top are used to specify the displayed statistics, and the legends on the right account for elements in the graphs.

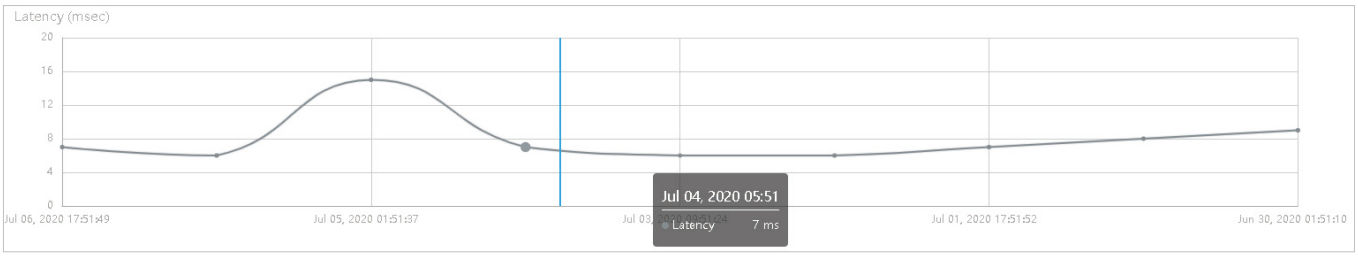
Jul 06, 2020 - Jul 07, 2020	Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right.
WAN | WAN/LAN1	Select the port you want to view the latency and speed.

Statistical Graphs

Statistical graphs below the tab bar display the network latency and speed of the WAN port.

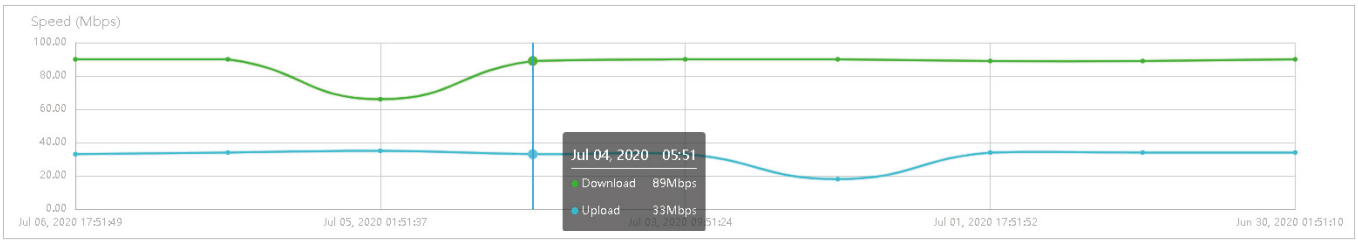
■ Latency

The Latency graph displays the time that it takes for a packet to travel from the gateway to the service provider's gateway.



■ Speed

The Speed graph uses the blue line and green line to display the upload and download speed of the WAN port, respectively.

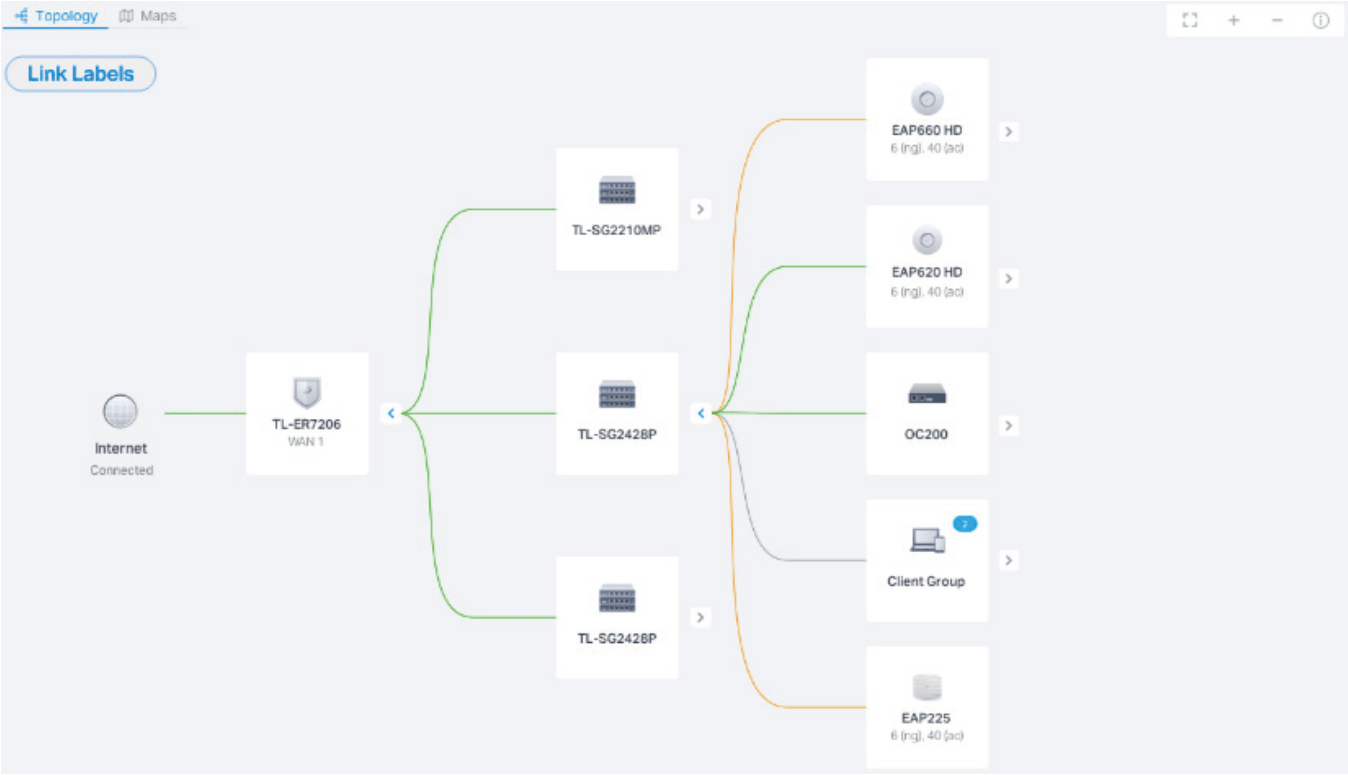


8. 3 Monitor the Network with Map

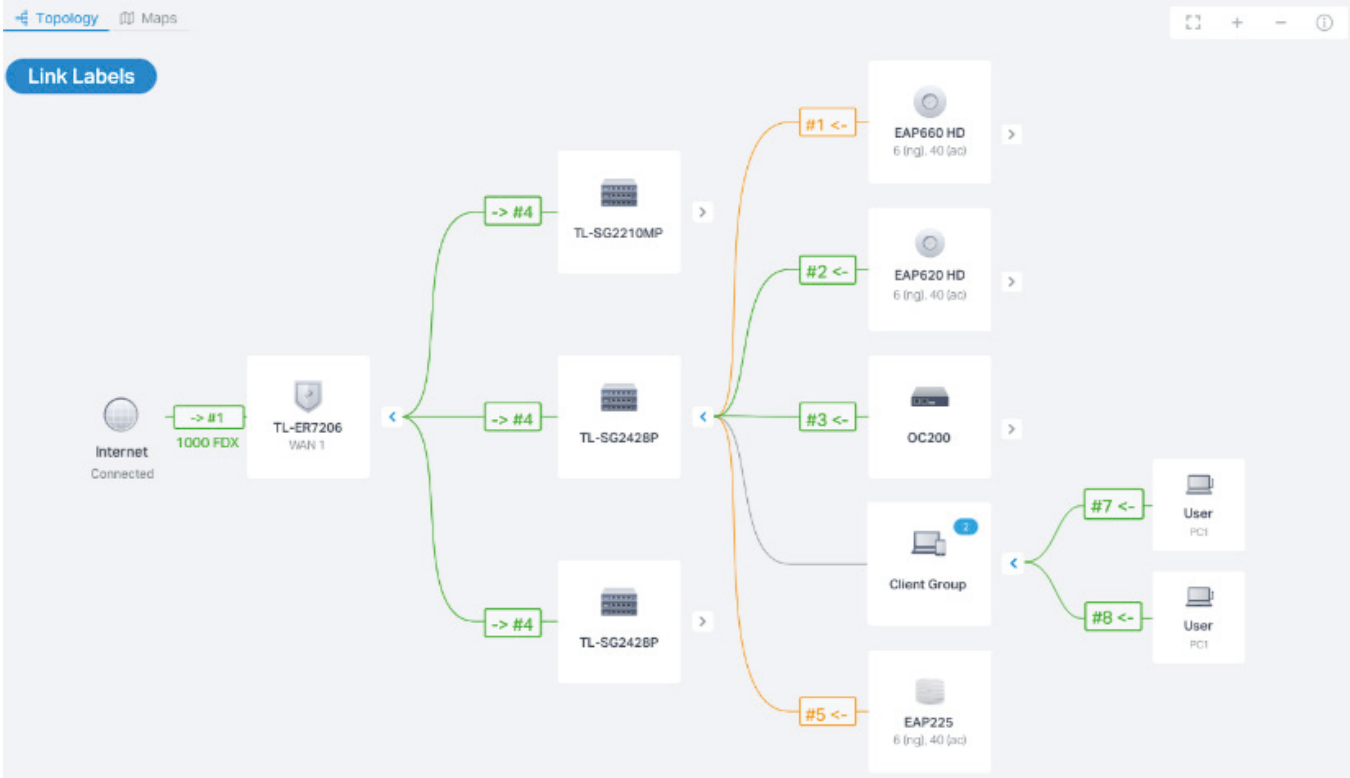
In the Map section, you can look over the topology and device provisioning of network in Topology, and customizes a visual representation of your network in Map.

8. 3. 1 Topology

Go to Map > Topology, and you can view the topology generated by the controller automatically. You can click the icon of devices to open the Properties window. For detailed configuration and monitoring in the Properties window, refer to Configure and Monitor Omada Managed Devices.



For a better overview of the network topology, you can control the display of branches, the size of the diagram, and the link labels.



- **Display of Branches**

  The default view shows the all devices connected by solid and dotted lines. Click the icon of the client group to view clients connected to the same device. Click the nods ⊕ to unfold or ⊖ to fold the branches.

- **Diagram Size**

  Click the icons at the right corner to adjust the size of the topology and view the legends.

	Click to fit the topology to the web page.
	Click to zoom in the topology.
	Click to zoom out the topology.
	Click to view the meaning of lines in the topology. Solid and dotted lines are used to indicate wired and wireless connections, respectively, and four colors are used to indicate the link speed.

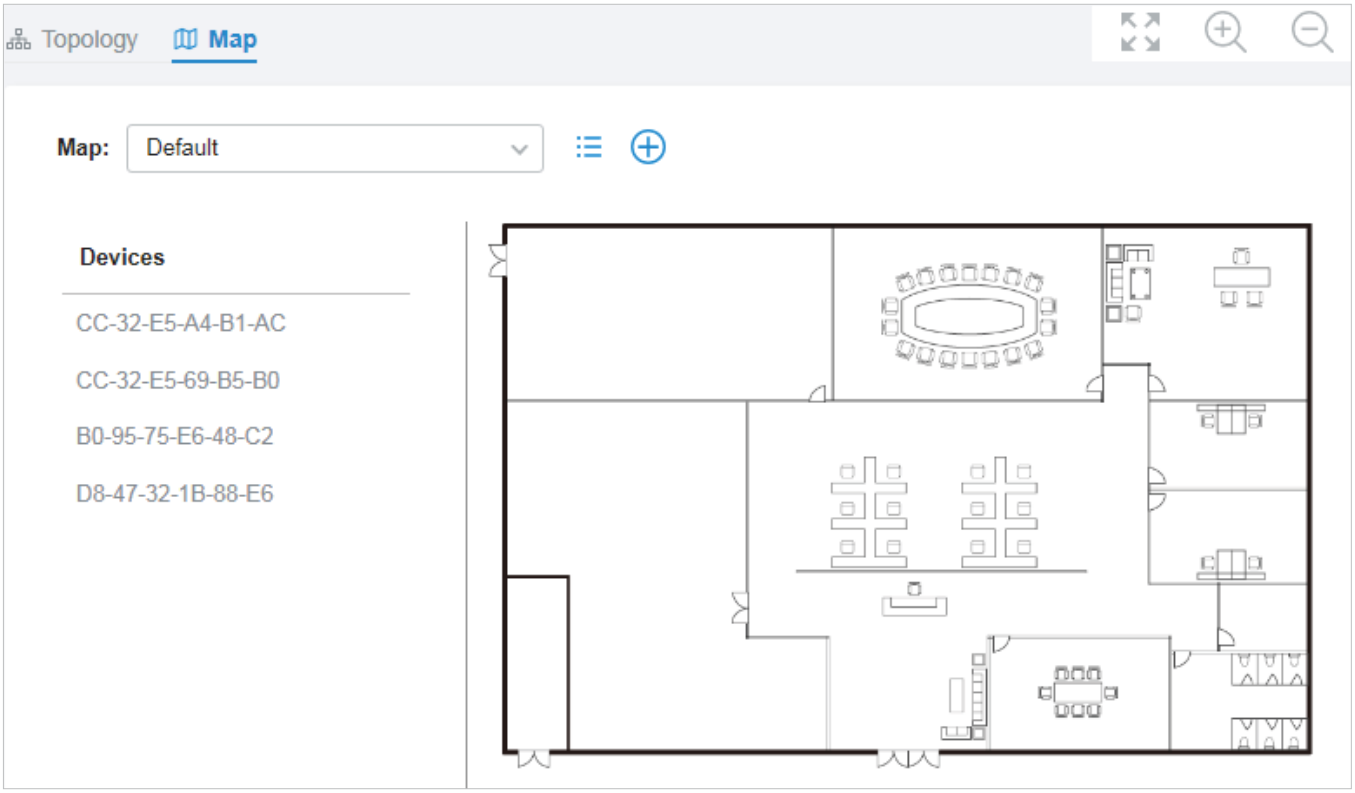
- **Link Labels**

  Click Link Labels at the left corner, and labels will appear to display the link status. Information on the labels varies due to the link connections.

-> WAN1 1000 FDX	(For the WAN port of router connected to the internet) Displays the port name, link speed and duplex type.
#7 <->#8 1000 FDX	(For simple wired connections) Displays the link speed, duplex type, and connected port number. Note that only the switch's port number can be displayed in the label.
LAG1#4,5 <->LAG2#7,8 1000 FDX	(For Link Aggregation) Displays the LAG speed, duplex type, LAG ID, and the port number of LAG members.
↑360Mbps ↓400Mbps 100% (-35dBm)	(For wireless connections between APs) Displays the RSSI (displayed in percentage and dBm) and the negotiation rate of uplink and downlink.
48 5 GHz Free Wi-Fi	(For wireless connections between APs and clients) Displays the wireless channel of AP, connected SSID, and its signal strength.

8. 3. 2 Map

Go to Map > Map, and a default map is shown as below with the unplaced devices listed on the left. You can upload your local map images and drag in the devices to customize a visual representation of your network.

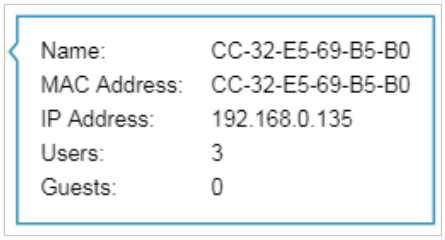


Customize Map

Click the following icons to add, edit, and select the map. After selecting a map, click and drag in the devices from the Devices list to place it on the map according to the actual locations.

	Click to add a map. In the pop-up window, enter the description and upload an image in the .jpg, .jpeg, .gif, .png, .bmp, .tiff format.
	Click to edit maps in the pop-up window. Click  to edit the description of the map. Click  to delete the map.
	Click to select a map from the drop-down list to place the devices.

Hover your cursor over the device icon to view the basic information of it, including the device name, MAC address, IP address and connected clients.



You can click the device icon to reveal additional action icons:

	Indicates that the device is unlocked and you can click it to lock the device in the current location. When unlocked, you can move the device on the map and click the action icons around it.
	Indicates that the device is locked on the map and you can only click the icon to unlock the device.
	Displays the device's Properties window. For detailed configuration and monitor in the Properties window, refer to Configure and Monitor Omada Managed Devices.
	Click to remove the selected device back into the Device list.
	(Only for connected switches and APs) Click to flash the LED of the device on the map. Then the LED will flash for 10 minutes or until the cancel button is clicked again.
	Click to stop the LED from flashing.

- **Diagram Size**

  Click the icons at the right corner to adjust the size of the topology and view the legends.

	Click to fit the map to the web page.
	Click to zoom in the map.
	Click to zoom out the map.

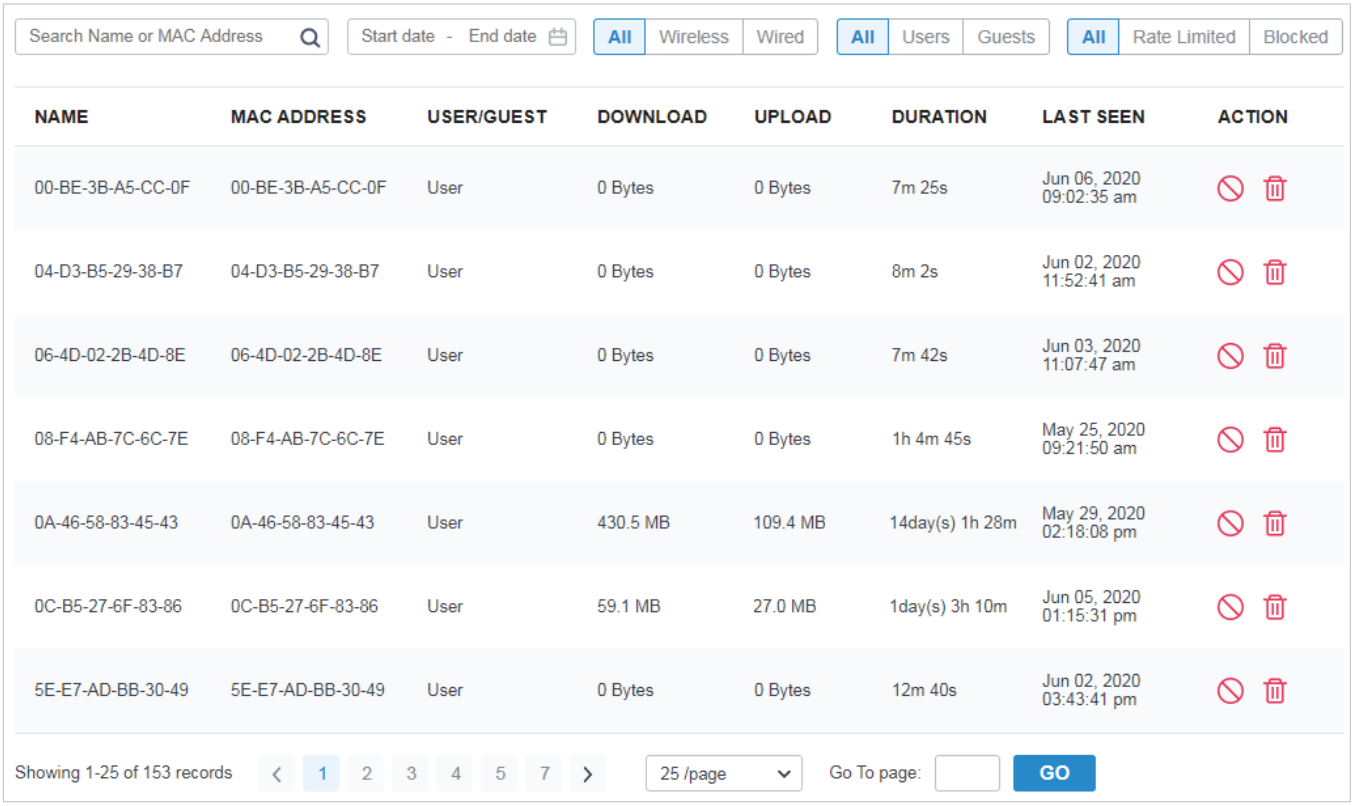
8. 4 View the Statistics During Specified Period with Insight

In the Insight page, you can monitor the site history of connected clients, portal authorizations, and rouge APs. For a better monitoring, you can specify the time period and classify the clients and APs.

8. 4. 1 Known Clients

In Known Clients, a table lists all clients that connected to the network before in the site.

In the table, you can view the client's basic information, role and connection statistics, including download and upload traffics, connection duration, and the last time it connected to the network.



A search bar, a time selector and three tabs are above the table for searching and filtering.

Search Name or MAC Address	Enter the client name or MAC address to search the clients.
Start date - End date	Filter the clients based on Last Seen. Click the selector to open the calendar. Click a specific date twice in the calendar to display the records on the day. To display the records of a time range, click the start date and end date in the calendar.

All Wireless Wired	Click the tabs to filter the clients listed in the table. The three tabs can take effect simultaneously.
All Users Guests	All/Wireless/Wired: Click All to display both wireless and wired clients. Click Wireless or Wired to display wireless or wired clients only.
All Rate Limited Blocked	All/Users/Guests: Click All to display both users and guests. Click Users or Gusets to display users or guests only. Guests are users connected to the wireless guest network. To configure guest network, refer to Configure Wireless Networks. All/Rate Limitted/Blocked: Click All to display both rate limited and blocked clients. Click Rate Limitted or Blocked to display rate limited or blocked clients only. To configure Rate Limit, refer to Client. To block the clients, click the ⊘ icon in the table.

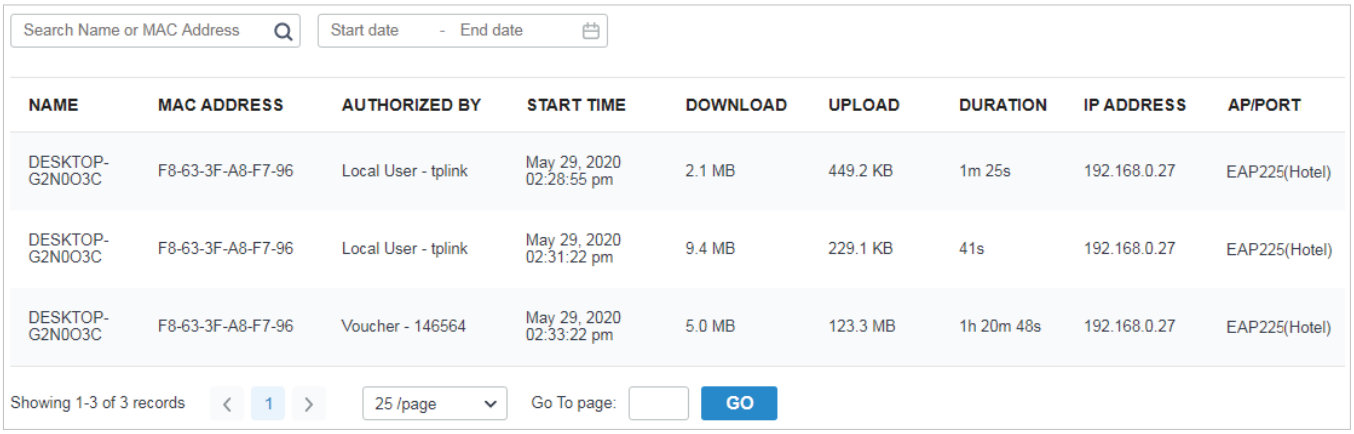
You can also take actions to block or forget the client. For detailed monitor and management, click the entry in the table to open the Properties window of the client. For more details, refer to Using the Clients Table to Monitor and Manage the Clients.

⊘	(For unblocked clients) Click to block the client in the site. Once blocked, the client is banned from connecting to the network in the site.
🔗	(For blocked clients) Click to unblock the client in the site.
🗑	Click to forget the client. Once forget, all statistics and history of the client in the site are dropped.

8. 4. 2 Past Portal Authorizations

In Past Portal Authorization, a table lists all clients that passed the portal authorization before.

In the table, you can view the client's name, MAC address, authorization credential, uplink and downlink traffics, authorization time and duration, IP address, and the network/port it connected to. For detailed monitoring and management, refer to Manage Client Authentication in Hotspot Manager.

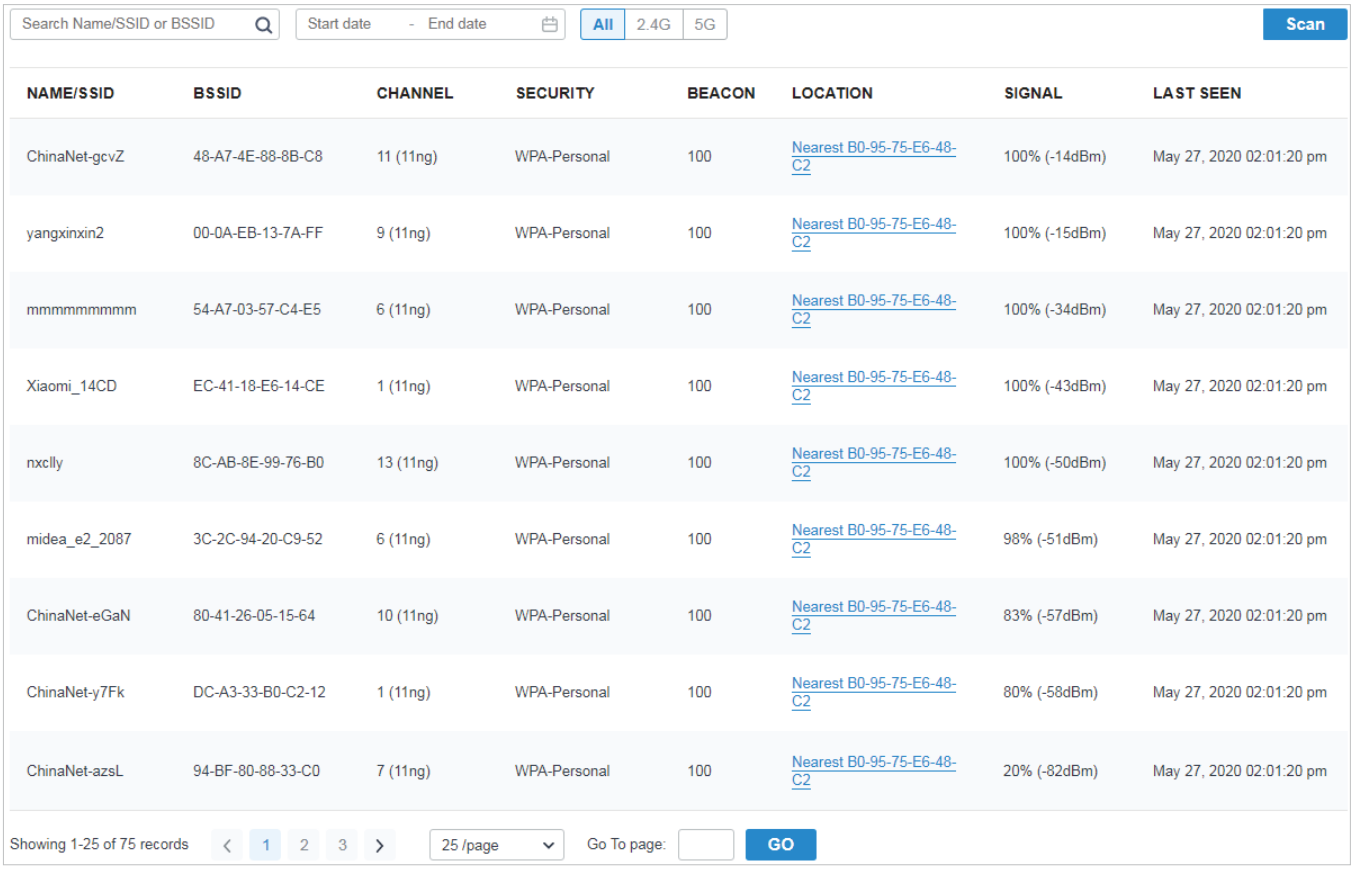


A search bar and a time selector are above the table for searching and filtering.

Search Name or MAC Address	Enter the client name or MAC address to search the clients.
Start date - End date	Filter the clients based on Start Time. Click the selector to open the calendar. Click a specific date twice in the calendar to display the clients authorized on the day. To display the clients authorized during a time range, click the start date and end date in the calendar.

8. 4. 3 Rogue APs

A rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. In Rogue APs, you can scan rogue APs and view the rogue APs scanned before.



Search Name or MAC Address	Enter the client name or MAC address to search the clients.
Start date - End date	Filter the rogue APs based on Last Seen. Click the selector to open the calendar. Click a specific date twice in the calendar to display the rogue APs scanned on the day. To display the scanned AP during a time range, click the start date and end date in the calendar.
All 2.4G 5G	Click the tab to filter the rogue APs listed in the table based on the frequency band.

Scan	Click to scan rogue APs. It may take several minutes, and the wireless service may be influenced during scanning.
BSSID	A string with a similar form as MAC address to recognize access points.
Channel	Displays the operation channel and standard of the rogue AP.
Security	Displays the security strategy of the rogue AP.
Beacon	Displays the beacon interval of the rogue AP. Beacons are transmitted periodically by the EAP to announce the presence of a wireless network for the clients, and the interval means how often the AP send a beacon to clients.
Location	Displays the managed AP nearest to the rogue AP. You can click the nearest AP to open its Properties window.
Signal	Displays the signal strength in percentage and dBm).
Last Seen	Display the last time that the rogue AP was scanned by the controller.

8. 5 View and Manage Logs

The controller 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 Alerts and Events, and configure their notification levels in Notifications.

All logs can be classified from the following four aspects.

- **Occurred Hierarchies**

  Two categories in occurred hierarchies are Controller and Site, which indicate the log activities happened, respectively, at the controller level and in the certain site. Only Master Administrators can view the logs happened at the controller level.

- **Notifications**

  Two categories in notifications are Event and Alert, and you can classify the logs into them by yourself.

- **Severities**

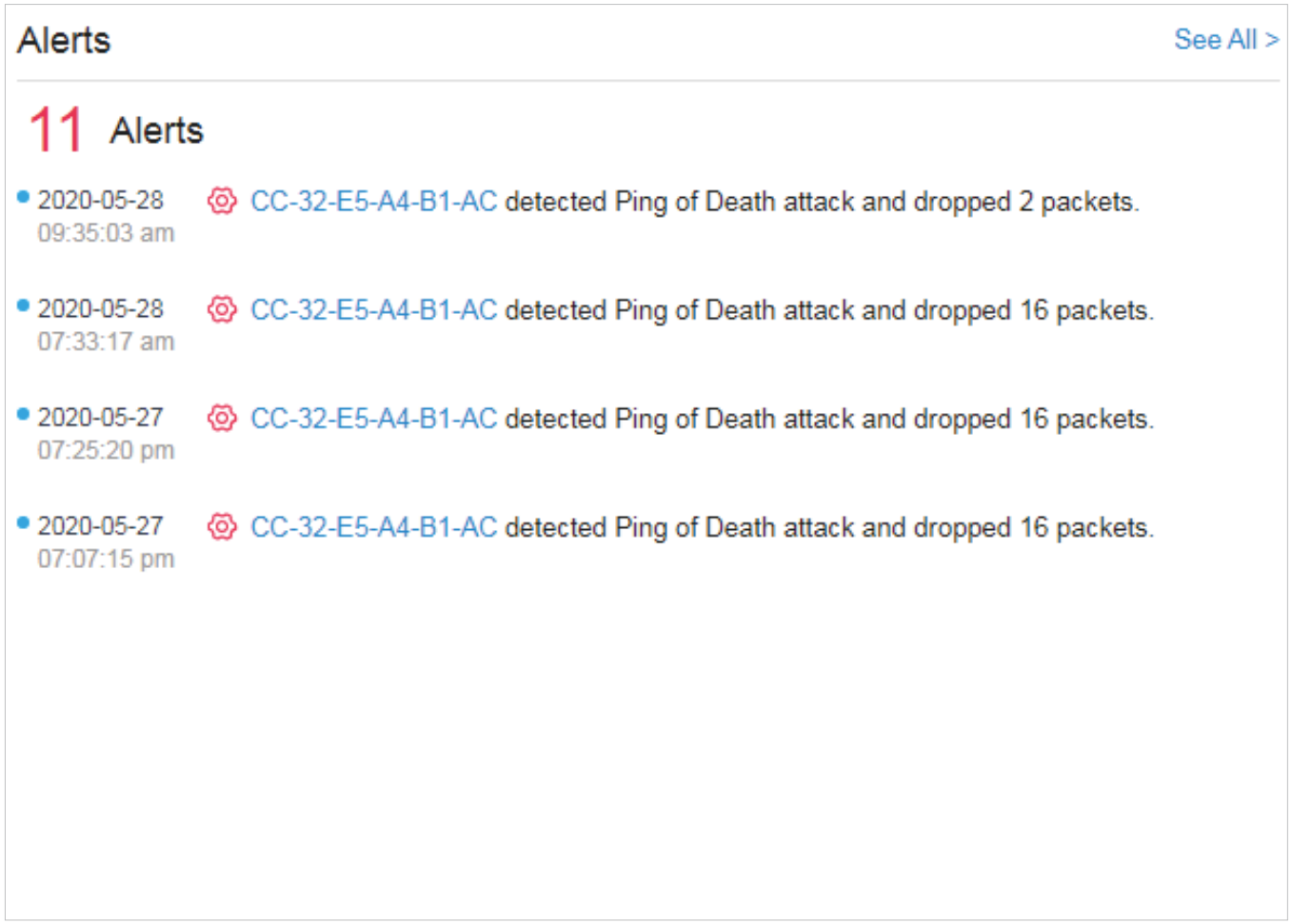
  Three levels in severities are Error, Warning, and Info, whose influences are ranked from high to low.

- **Contents**

  Four types in contents are Operation, System, Device, and Client, which indicate the log contents relating to.

8. 5. 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.

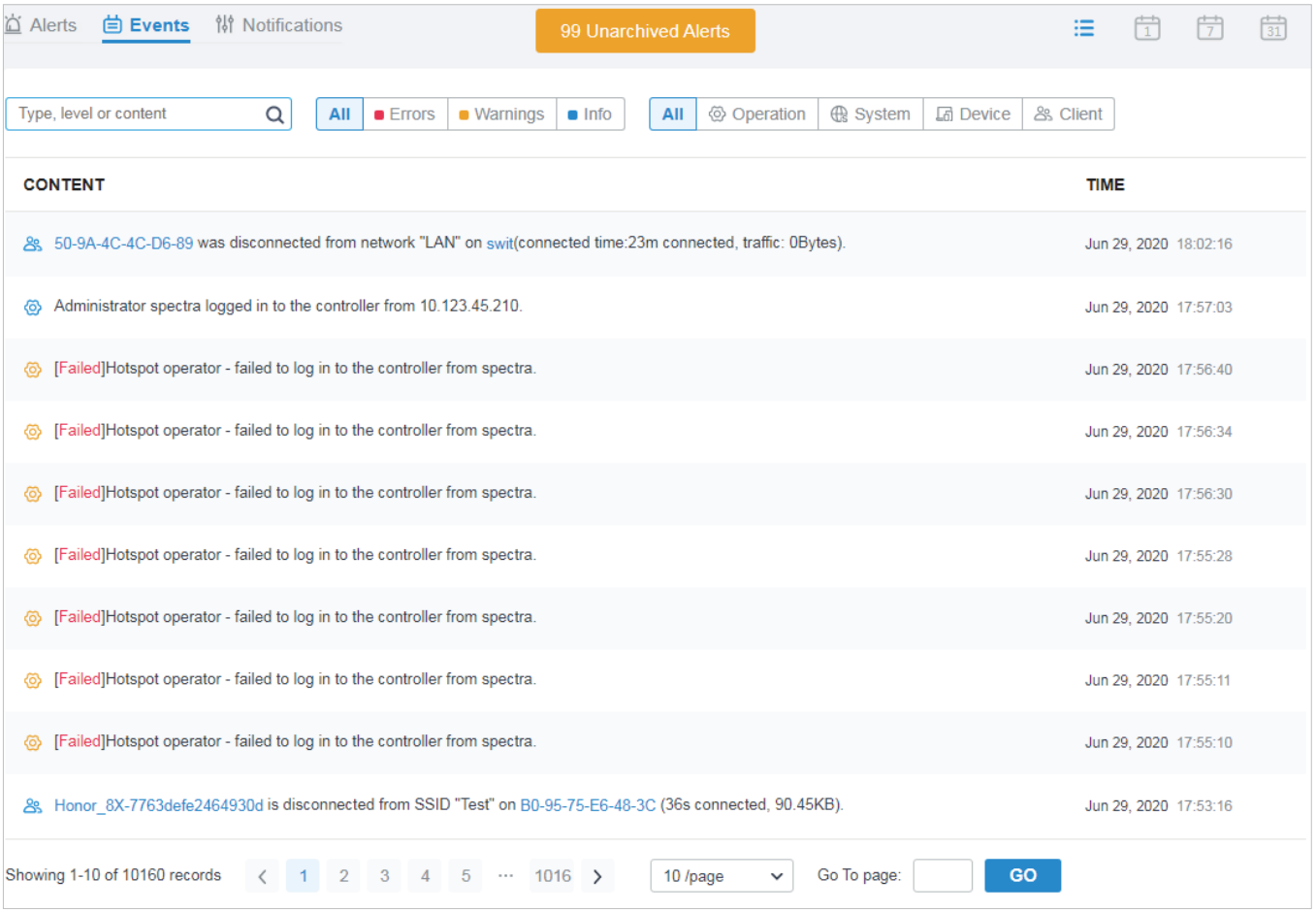


	Click to change the view mode for a better overview. : Displays the logs in a table. / / : Displays the logs in a day/week/month. To change the time, click or . To jump back to the current one, click Today/This Week/This Month.
Type, level or content	Enter the content types, severity levels, or key words to search the logs.
Unarchived Archived	Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously.
All Errors Warnings	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: Click All to display logs in both Error, Warning, and Info levels. Click Errors or Warnings to display logs in Error or Warning levels only.

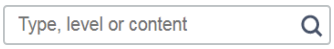
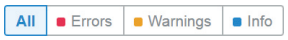
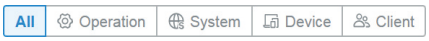
Content	Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.
Time	Displays when the activity happened.
Archive All	Click to archive all unarchived logs.
	Click to archive the log entry.

8. 5. 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.

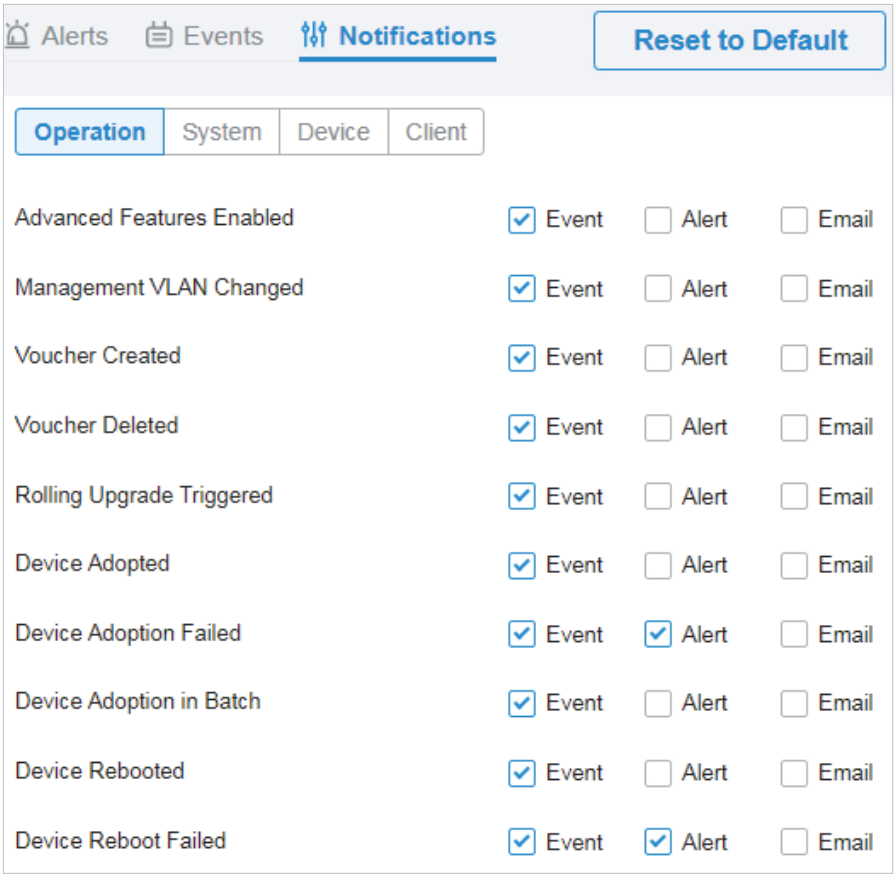


	Click to change the view mode. : Displays the logs in a table. / / : Displays the logs in a day/week/month. To change the time, click or . To jump back to the current one, click Today/This Week/This Month.

	Enter the content types, severity levels, or key words to search the logs.
 	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 logs in both Error and Warning levels. Click Errors, Warnings or Info to display logs in the corresponding level only. All/Operation/System/Device/Client: Click All to display all types of logs. Click Operation or System or Device or Client to display the corresponding type of logs only.
Content	Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.
Time	Displays when the activity happened.

8. 5. 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 for the current site. Also, you can enable Email for the logs. With proper configurations, the controller 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 in the current site to the default.
Operation | System | Device | Client	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, the controller will not record the activity logs.
Email	Enable the checkboxes to specify the activity logs as alert logs. With proper settings in Site and Admin, the controller can send emails to notify the administrators and viewers of the site's alert logs once generated.
	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 default.

The Email checkboxes are used to enable Alert Emails for the logs. To make sure the administrators and viewers can receive alert emails of the site, follow the following steps:

1) Enable Mail Server

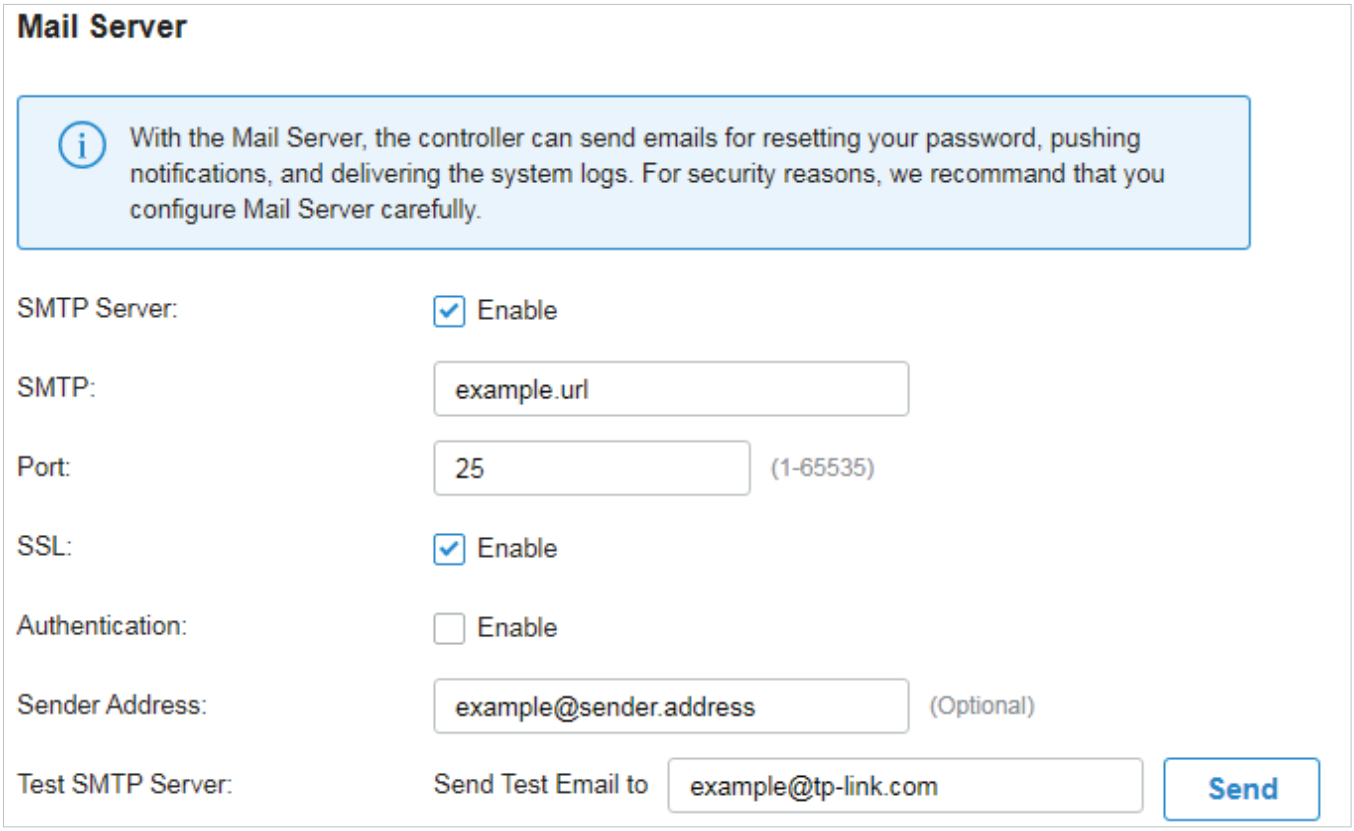
2) Enable Alert Emails in Site

3) Enable Alert Emails in Admin

4) Enable Alert Emails in Logs

Enable Mail Server > Enable Alert Emails in Site > Enable Alert Emails in Admin

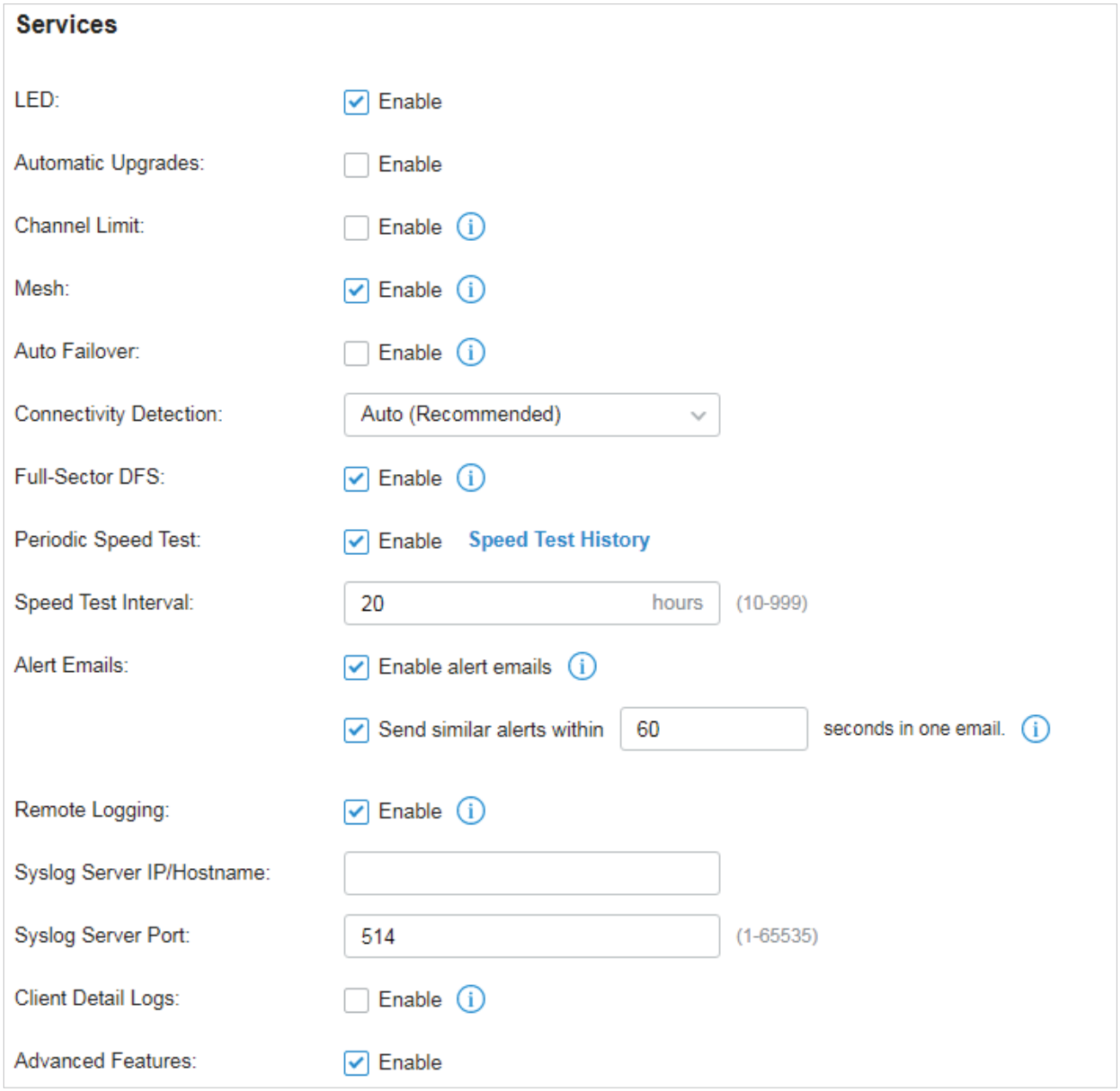
Go to Settings > Controller. In the Mail Server section, enable SMTP Server and configure the parameters. Then click Save.



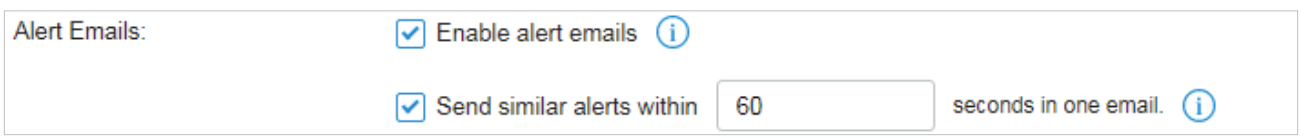
SMTP	Enter the URL or IP address of the SMTP server according to the instructions of the email service provider.
Port	Configure the port used by the SMTP server according to the instructions of the email service provider.
SSL	Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between the controller 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	Enter the username for your email account if Authentication is enabled.
Password	Enter the password for your email account if Authentication is enabled.
Sender Address	(Optional) Specify the sender address of the email.
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 Site** > Enable Alert Emails in Admin

1. Go to Settings > Site and enable Alert Emails in the Services section.



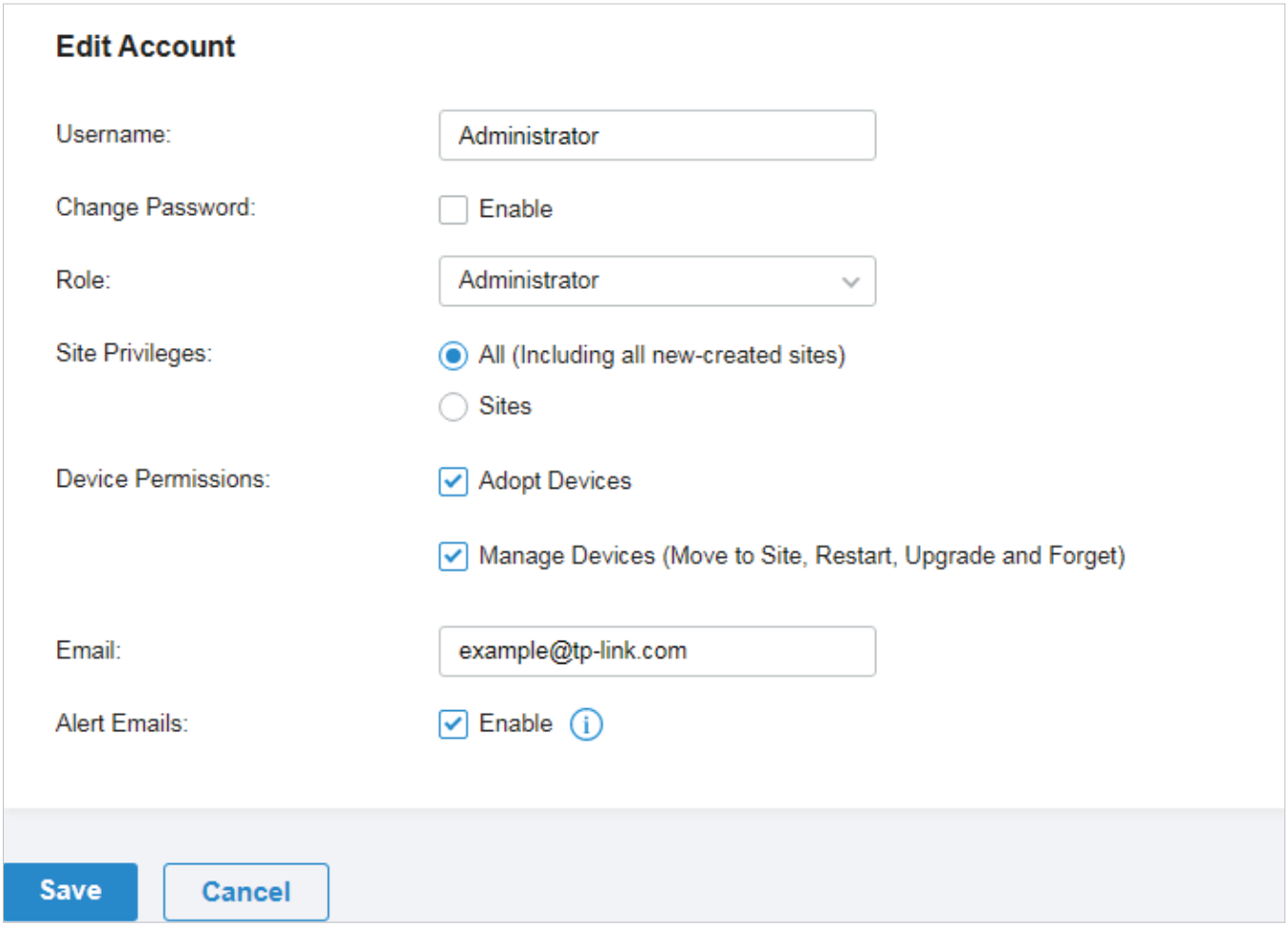
2. (Optional) On the same page, enable Send similar alerts within seconds in one email and specify the time interval. When enabled, the similar alerts generated in each time period are collected and sent to administrators and viewers in one email.



3. Click Apply.

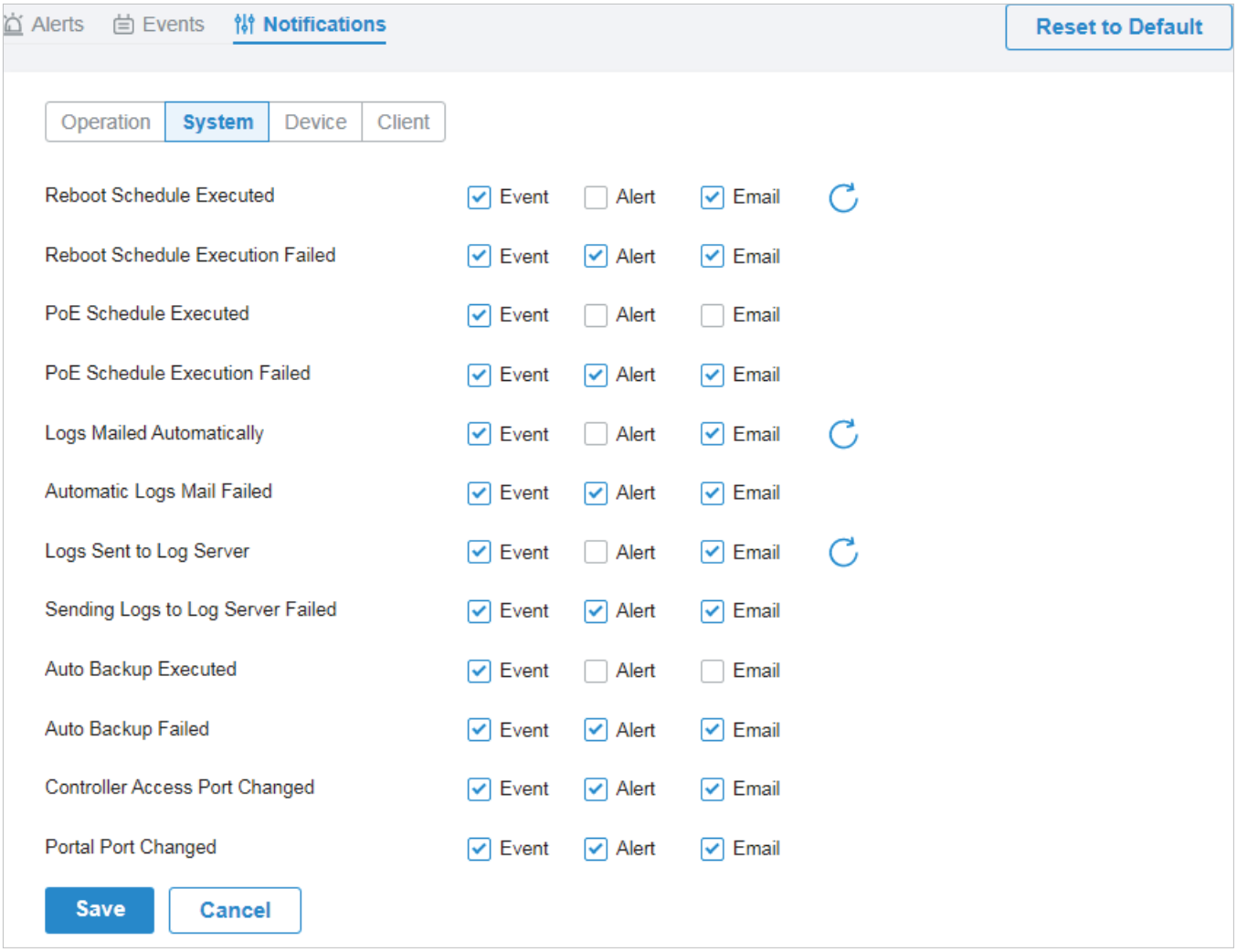
Enable Alert Emails in Site > Enable Alert Emails in Admin > Enable Alert Emails in Logs

Go to Admin and configure Alert Emails for the administrators and viewers to receive the emails. Click + Add New Admin Account to create an account or click to edit an account. Enter the email address in Email and enable Alert Emails. Click Create or Apply.



Enable Alert Emails in Site > Enable Alert Emails in Admin > 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 the controller emails administrators. Click Save.



9

Manage Administrator Accounts of Omada SDN Controller

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:

- Introduction to User Accounts
- Manage and Create Local User Accounts
- Manage and Create Cloud User Accounts

9. 1 Introduction to User Accounts

Omada SDN Controller offers three levels of access available for users: master administrator, administrator, and viewer. Because the controller 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 the controller as required. This approach ensures security and gives convenience for management.

- **Master Administrator**

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

- **Administrator**

Administrators can create and delete viewers in the Admin page, but they can be created and deleted only by master administrator. In the Settings page, administrators have no permission to some modules, including cloud access, migration, 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 master administrator and administrator.

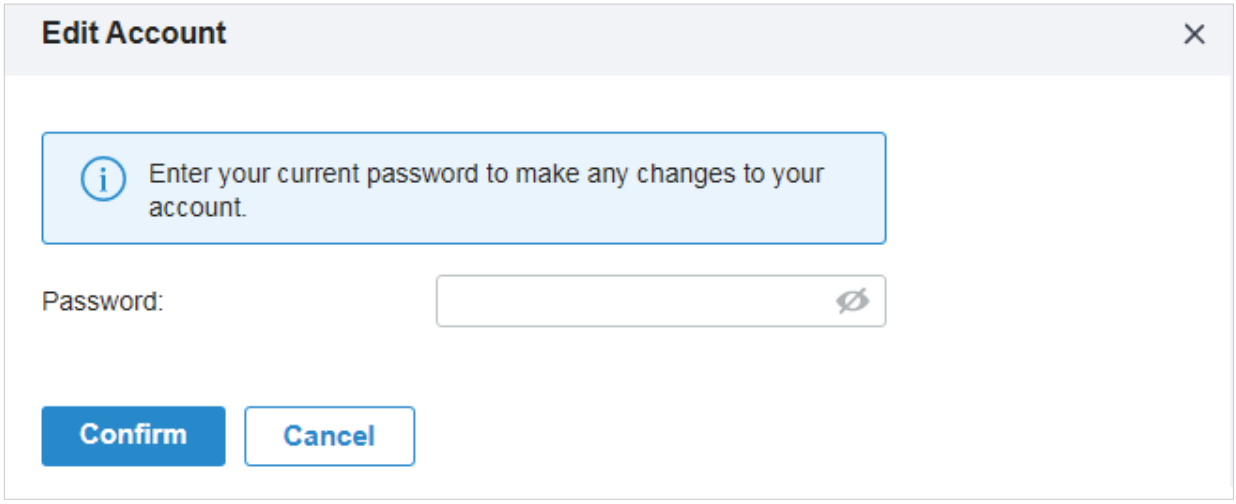
9. 2 Manage and Create Local User Accounts

By default, Omada SDN Controller automatically sets up a local user with the role called master administrator as the primary administrator. The username and password of the master administrator are the same as that of the controller account by default. The master administrator cannot be deleted, and it can create, edit, and delete other levels of user accounts.

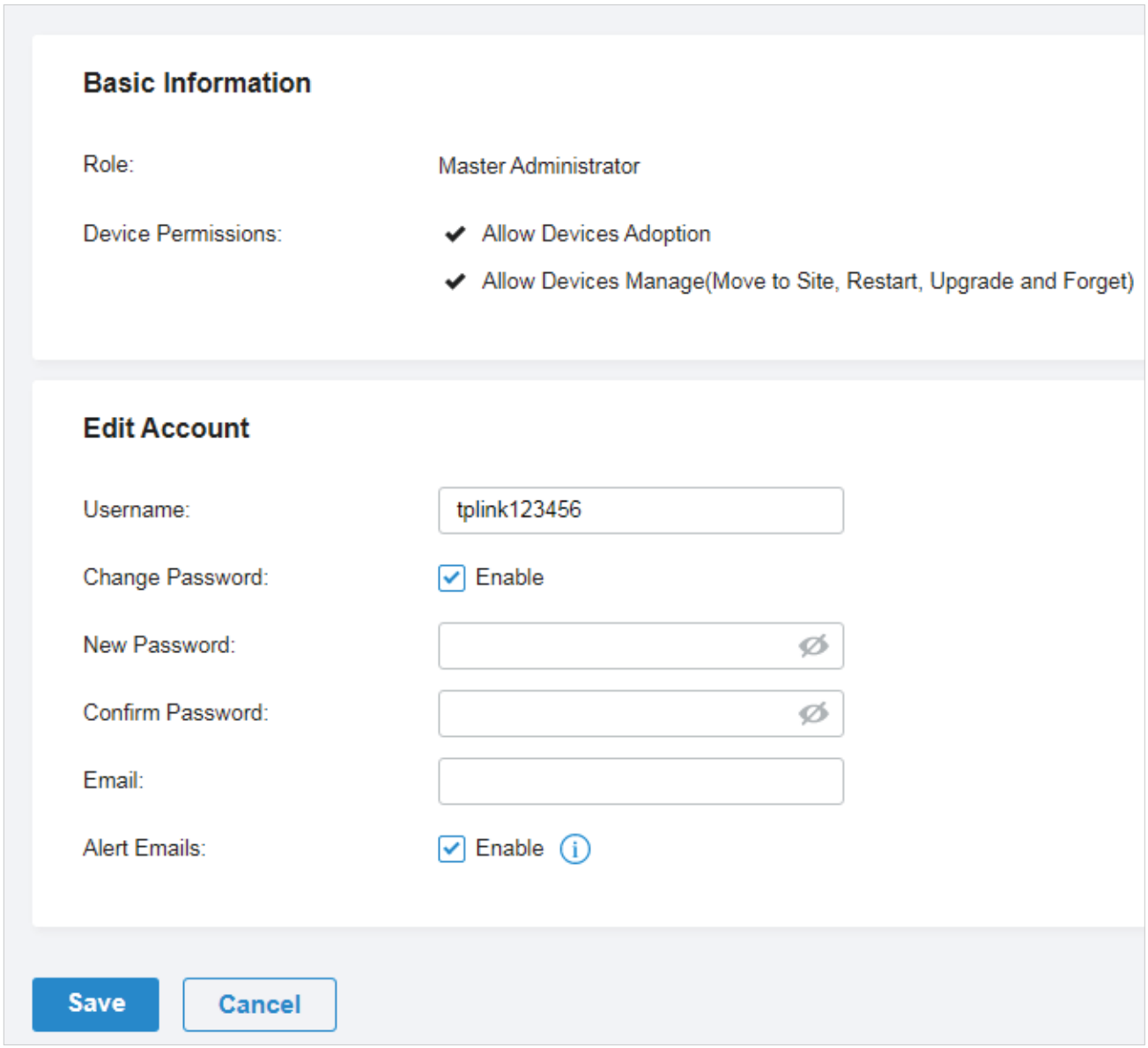
9. 2. 1 Edit the Master Administrator Account

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

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



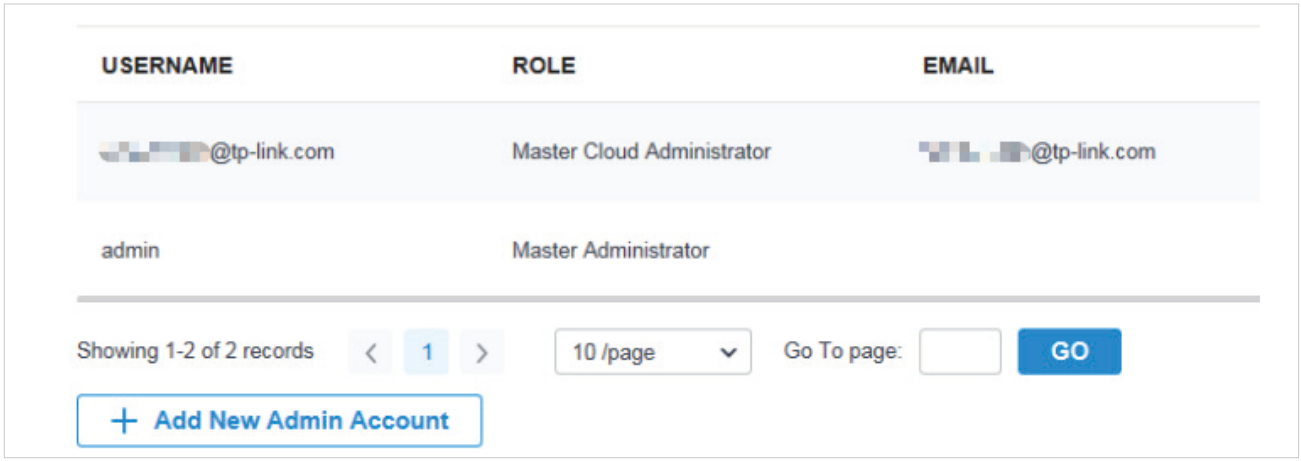
2. Basic information including role and device permissions is shown. You can change the password and enable alert emails by checking the box. Click Save.



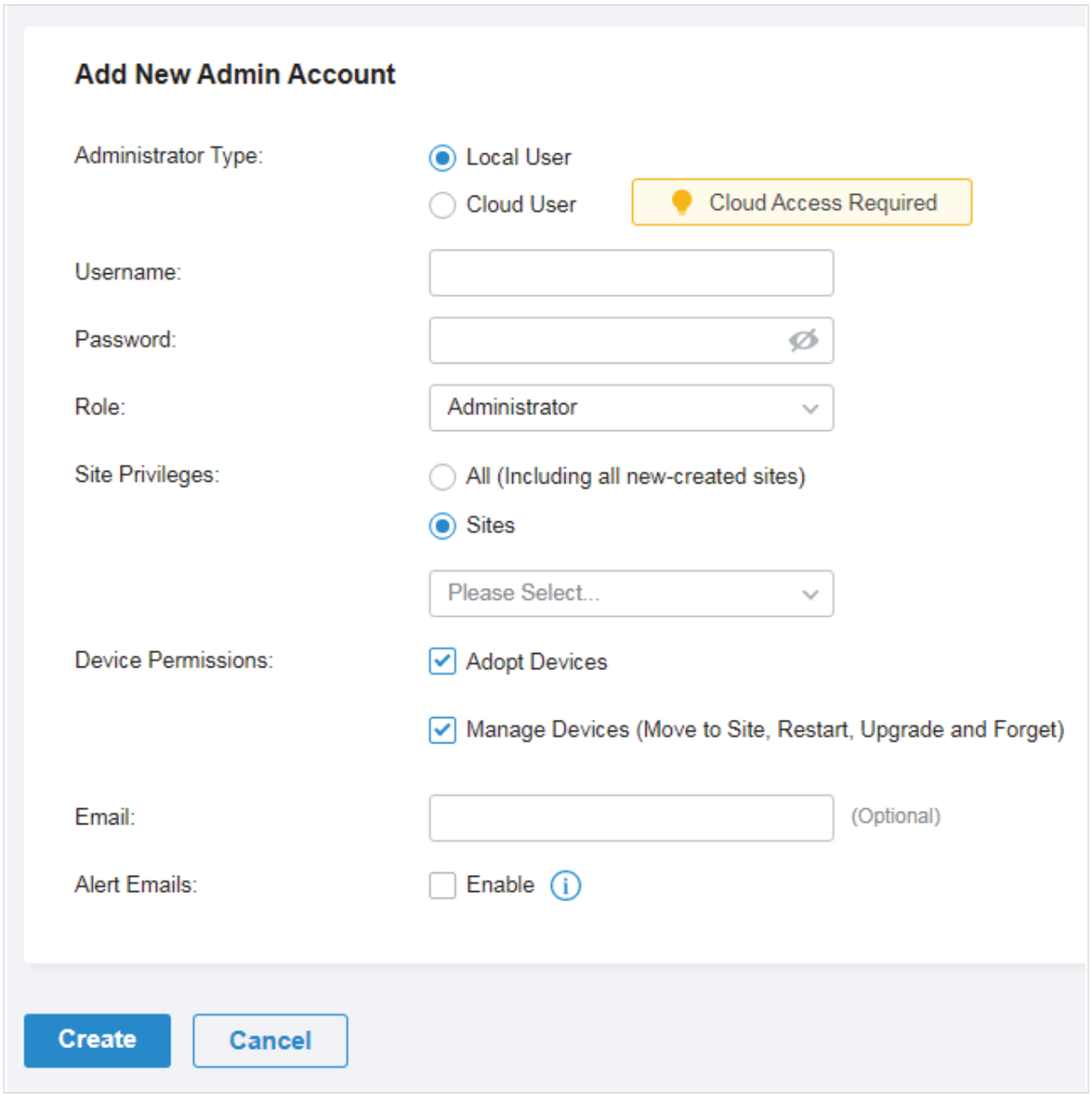
9. 2. 2 Create and Manage Administrator and Viewer

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

1. Click + Add New Admin Account.



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



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. Administrator: 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 master administrator and other administrator accounts. 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. All: The created user has device permissions in all sites, including all new-created sites. Sites: The created user has device permission in the sites that are selected. Select the sites by checking the box before them.
Device Permissions (when creating a local administrator)	Grant following permission to the created user in the role of administrator by checking the box(es). Adopt Devices: the created administrator account can view the devices in status of pending in the privileged sites, and the administrator account has permissions to adopt the devices. Device Manage: the created administrator account can manage the devices in the privileged sites.
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. For detailed configurations, refer to notification.

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

	To edit the parameters for the user. Master administrator can edit all user accounts, Administrator can edit itself and viewer accounts of its privileged sites, and viewer can only edit itself.
	To delete the account. Master administrator can delete all user accounts apart from itself, administrator can delete viewer accounts of its privileged sites, and viewer cannot delete any accounts.

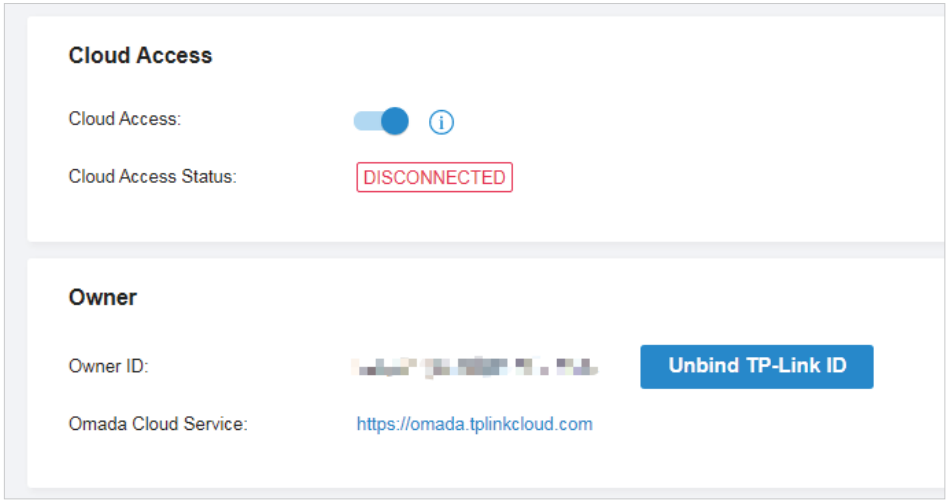
9. 3 Manage and Create Cloud User Accounts

For cloud-based controller, the cloud access is enabled by default, and the controller automatically sets up the cloud master administrator. Software and hardware controller automatically sets up the cloud master administrator if you have enabled cloud access and bound the controller 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 master administrator is cannot be deleted, and it can create, edit, and delete other levels of user accounts.

9. 3. 1 Set Up the Cloud Master Administrator

For software and hardware controller, if you have not enabled the cloud access and bound the controller with a TP-Link ID in quick setup, to set up the cloud master administrator, follow these steps:

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

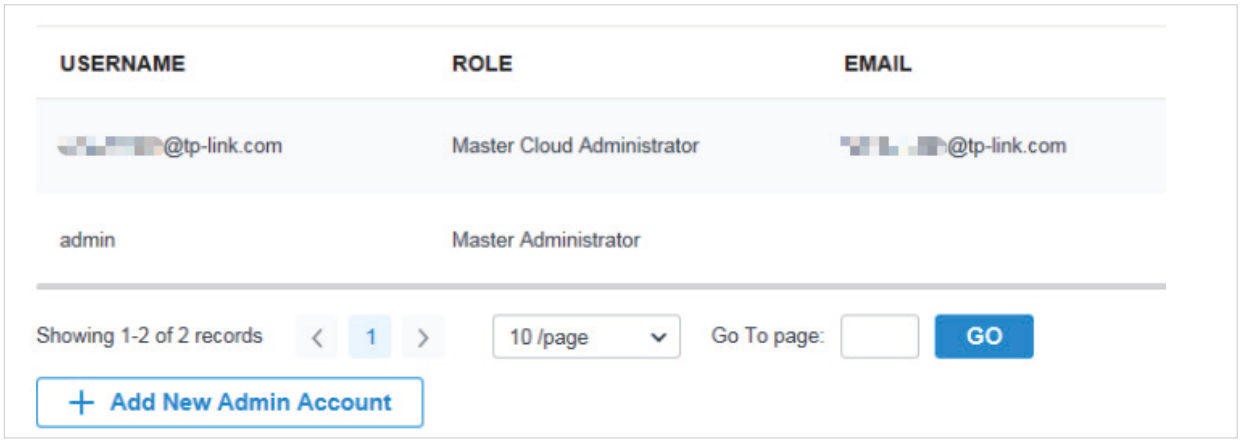


2. In Admin, a cloud master administrator with the same username as the TP-Link ID will be automatically created. The Cloud Master Administrator cannot be deleted. You can log in with the cloud master administrator when the cloud access is enabled.

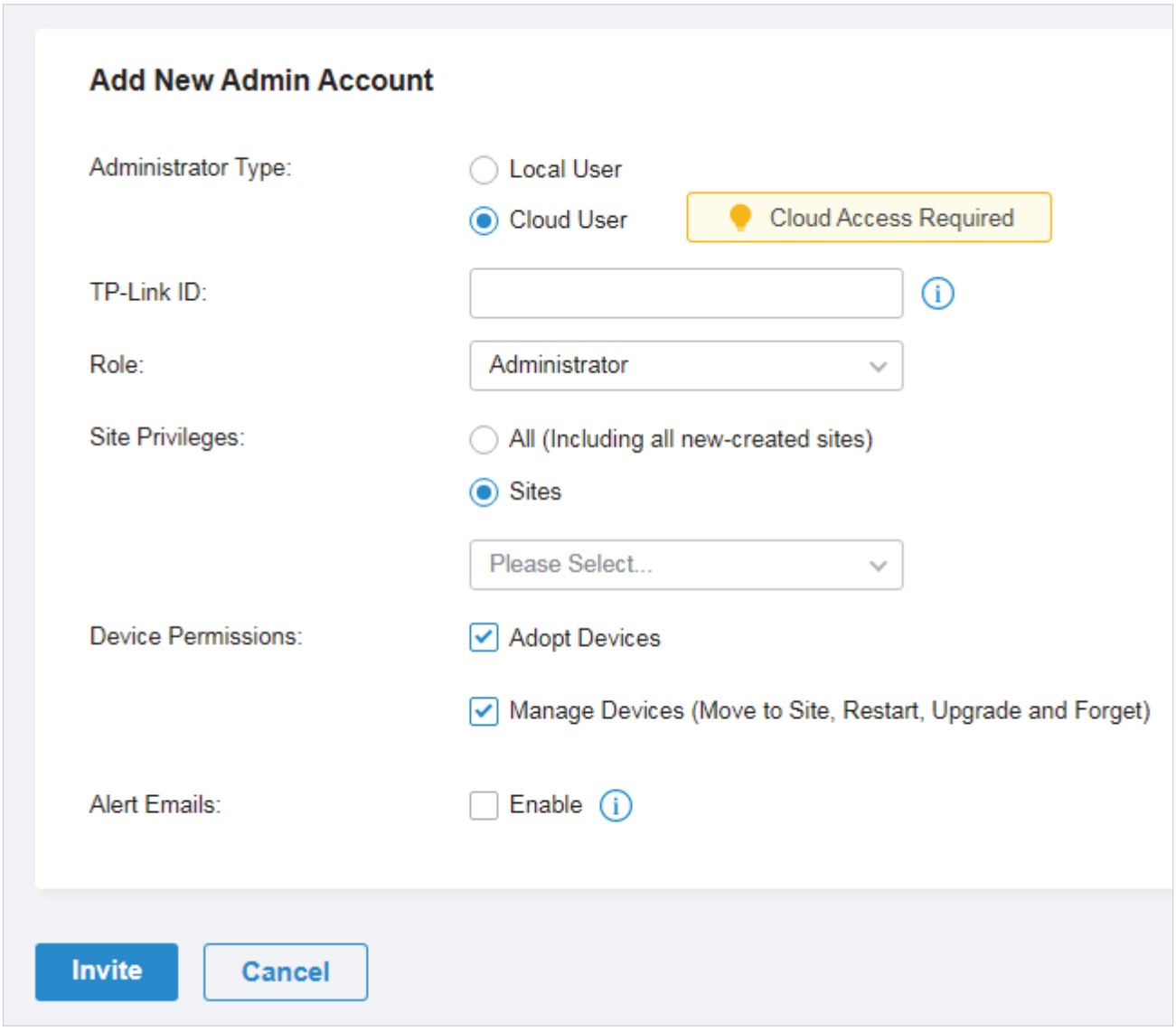
9. 3. 2 Create and Manage Cloud Administrator and Cloud Viewer

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

1. Click + Add New Admin Account.



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



TP-Link ID	Enter an email address of the created cloud user, and then an invitation email will be sent to the email address. If the email address has already been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation. 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. Administrator: 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 master administrator and other administrator accounts. 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. All: The created user has permission in all sites, including all new-created sites. Sites: The created user has permission in the sites that are selected. Select the sites by checking the box before them.
Device Permissions (when creating a cloud administrator)	Grant following permission to the created user in the role of cloud administrator by checking the box(es). Adopt Devices: The created administrator account can view the devices in status of pending in the privileged sites, and the administrator account has permission to adopt the devices. Device Manage: The created administrator account has privileges to manage the devices in the privileged sites.
Alert Emails	Check the box if you want the created user to receive emails about alerts of the privileged sites. For detailed configurations, refer to notification.

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

	To edit the parameters for the user. Cloud master administrator can edit all user accounts, administrator can edit itself and viewer accounts of its privileged sites, viewer can only edit itself.
	To delete the account. Cloud master administrator can delete all user accounts apart from master administrator and itself, administrator can delete viewer accounts of its privileged sites, viewer cannot delete any accounts.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2020 TP-Link Technologies Co., Ltd.. All rights reserved.