Configure the Network with Omada SDN Controller

Full version of Omada SDN Controller User Guide is available at **https://www.tp-link.com/support/download/omada-software-controller**

CONTENTS

1.Configure the Network with Omada SDN Controller

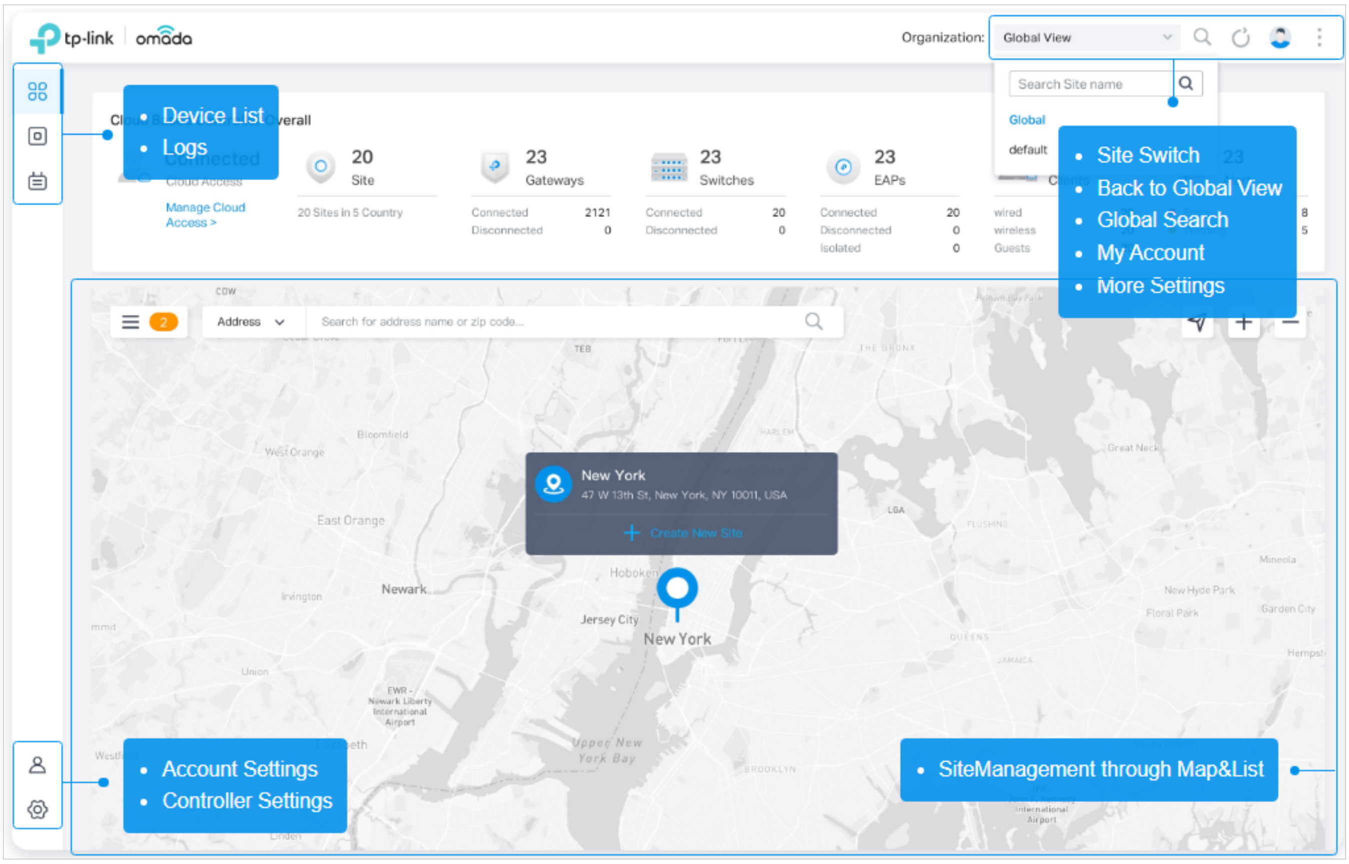
1. 1 Navigate the UI

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 Controller UI.

- **Global Overview**

  Know the status of your sites at a glance, and manage sites in the Omada platform.

  - Site Monitoring—Keep you informed of accurate, real-time status of every site.
  - Site Management—Manage all sites to deploy the whole network.
  - Account Settings—Manage all administrative accounts.

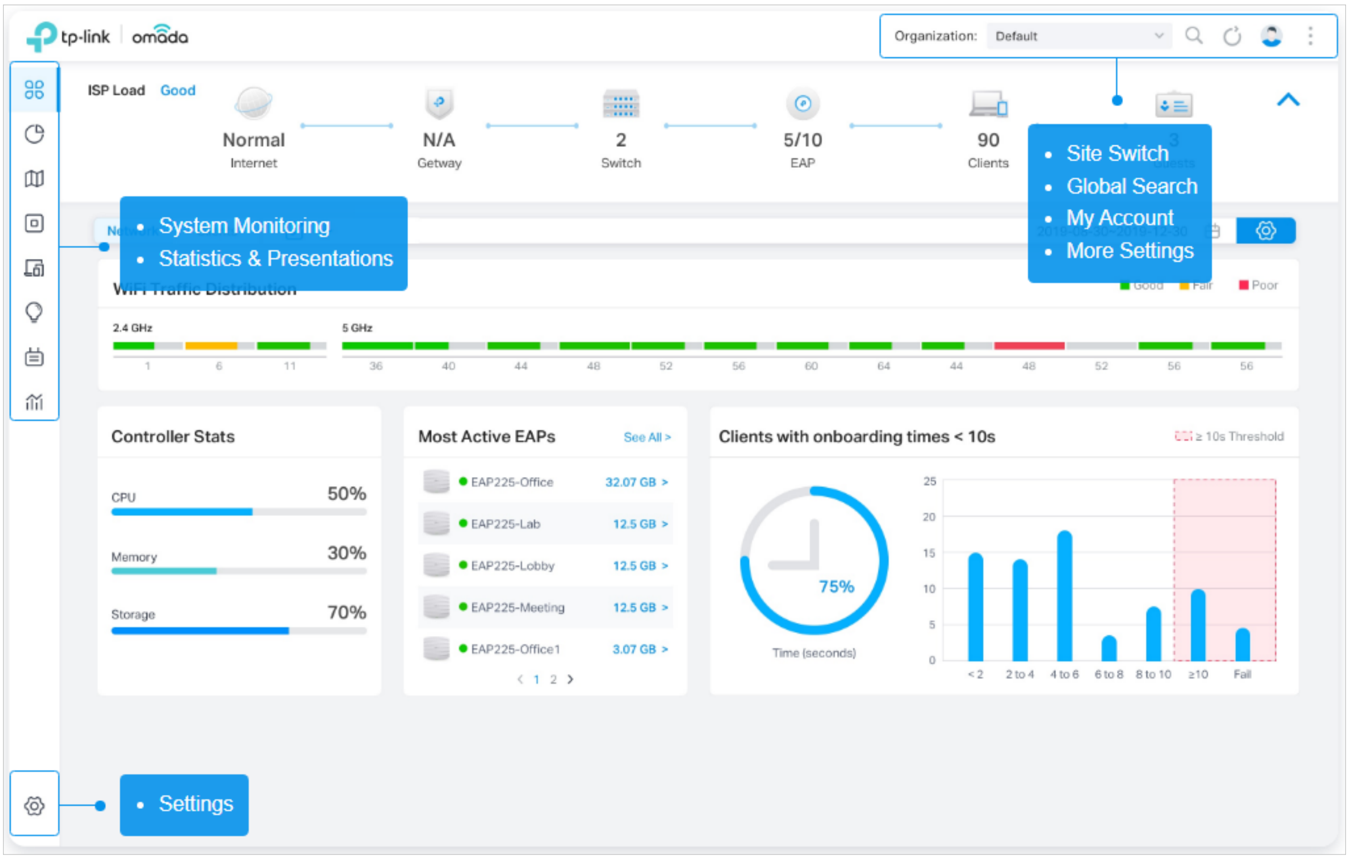


- **Site Overview**

  Know the status of your network at a glance, gain insights, and manage network devices all in the Omada platform.

  - Statistics & Monitoring—Keep you informed of accurate, real-time status of every network device and client.

- Settings—Configure all your network devices centrally.

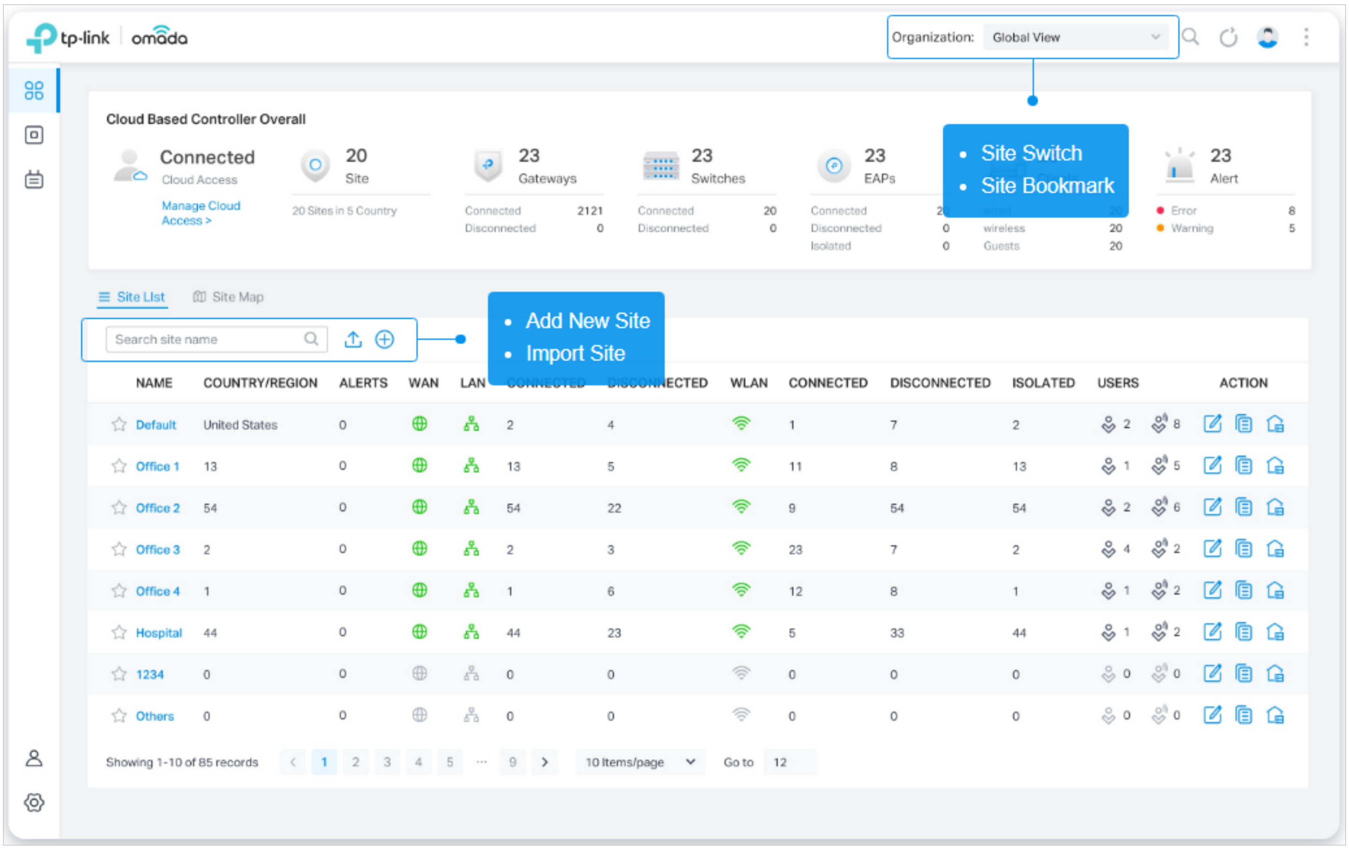


- **Site Overview**

  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.

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

- Import Site — Click Import Site to import the site from another controller.
- Site Bookmark – Click Bookmark to place frequently-used sites on the top of the list.



Cloud Based Controller Overall

Connected
Cloud Access
Manage Cloud Access >

20 Site
20 Sites in 5 Country

23 Gateways
Connected 2121
Disconnected 0

23 Switches
Connected 20
Disconnected 0

23 EAPs
Connected 20
Disconnected 0
Isolated 0

wired 20
wireless 20
Guests 20

23 Alert
Error 8
Warning 5

NAME	COUNTRY/REGION	ALERTS	WAN	LAN	CONNECTED	DISCONNECTED	WLAN	CONNECTED	DISCONNECTED	ISOLATED	USERS		ACTION
☆ Default	United States	0	●	●	2	4	●	1	7	2	2	8	✎
☆ Office 1	13	0	●	●	13	5	●	11	8	13	1	5	✎
☆ Office 2	54	0	●	●	54	22	●	9	54	54	2	6	✎
☆ Office 3	2	0	●	●	2	3	●	23	7	2	4	2	✎
☆ Office 4	1	0	●	●	1	6	●	12	8	1	1	2	✎
☆ Hospital	44	0	●	●	44	23	●	5	33	44	1	2	✎
☆ 1234	0	0	○	○	0	0	○	0	0	0	0	0	✎
☆ Others	0	0	○	○	0	0	○	0	0	0	0	0	✎

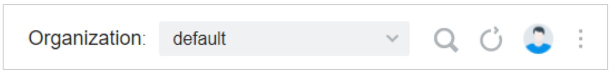
Showing 1-10 of 85 records < 1 2 3 4 5 ··· 9 > 10 Items/page Go to 12

■ **Network Monitoring**

Visual data keeps the network administrator informed about accurate status of every network device and client on the wired and wireless network.

The Controller UI is grouped into task-oriented menus. These menus 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:



Organization: default

Organization Management

Global View — Know the status of your Site at a glance, and manage sites in the Omada platform.

Site View — Know the status of your network at a glance, gain insights, and manage network devices all in the Omada platform.

Hotspot Manager — Centrally monitor and manage the clients authorized by portal authentication.

Global Search Feature

Click 🔍 and enter the keywords to quickly look up the functions or devices that you want to configure. And you can search for the devices by their MAC addresses and device names.

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, Tutorial and Feedback.

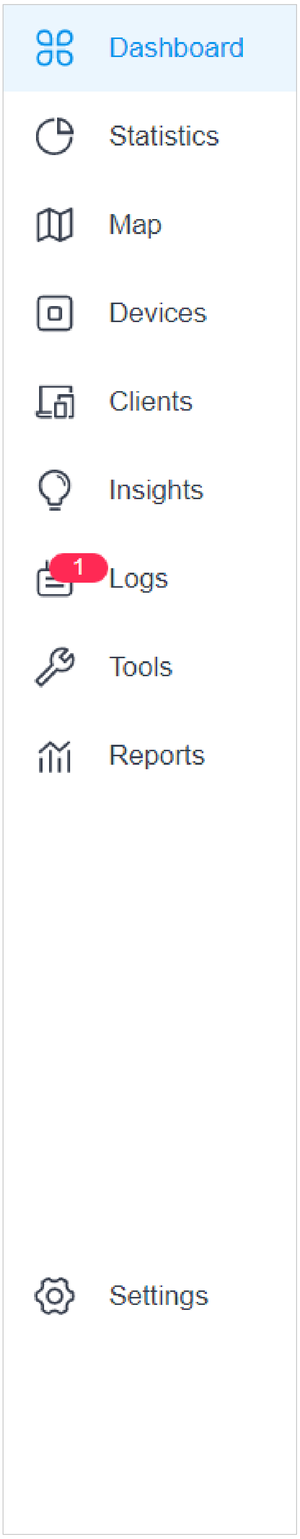
Preferences: Click to jump to Maintenance and customize the Controller UI depending on your needs. For details, refer to 5. 3 Maintenance

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.

Feedback: Click to send your feedback to us.

The left-hand navigation bar provides access to:



Dashboard displays a summarized view of the network status through different visualizations. The customizable and widget-driven dashboard is a powerful tool that arms you with real-time data for monitoring the network. With the drag and drop feature, you can modify your dashboard and re-arrange it to let you track all the important metrics.

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.

Device displays all TP-Link devices discovered on the site and their general information. This list view can change depending on your monitoring need 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.

Insights 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 shows log lines about varied activities of users, devices, and systems events, such as administrative actions and abnormal device behaviors. Comprehensive logs make historical information more accurate, readily accessible, and usable, which allows for proactive troubleshooting. And you can determine alert-level events and enable pushing notifications.

Tools provides various network tools for you to test the device connectivity, capture packets for troubleshooting, and open Terminal to execute CLI or Shell commands.

Reports provides intuitive charts and detailed statistics concerning your network situation, managed devices, and connected clients.

Settings allows you to provision and configure all your network devices on the same site in minutes and maintain the controller system for best performance.

1. 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.

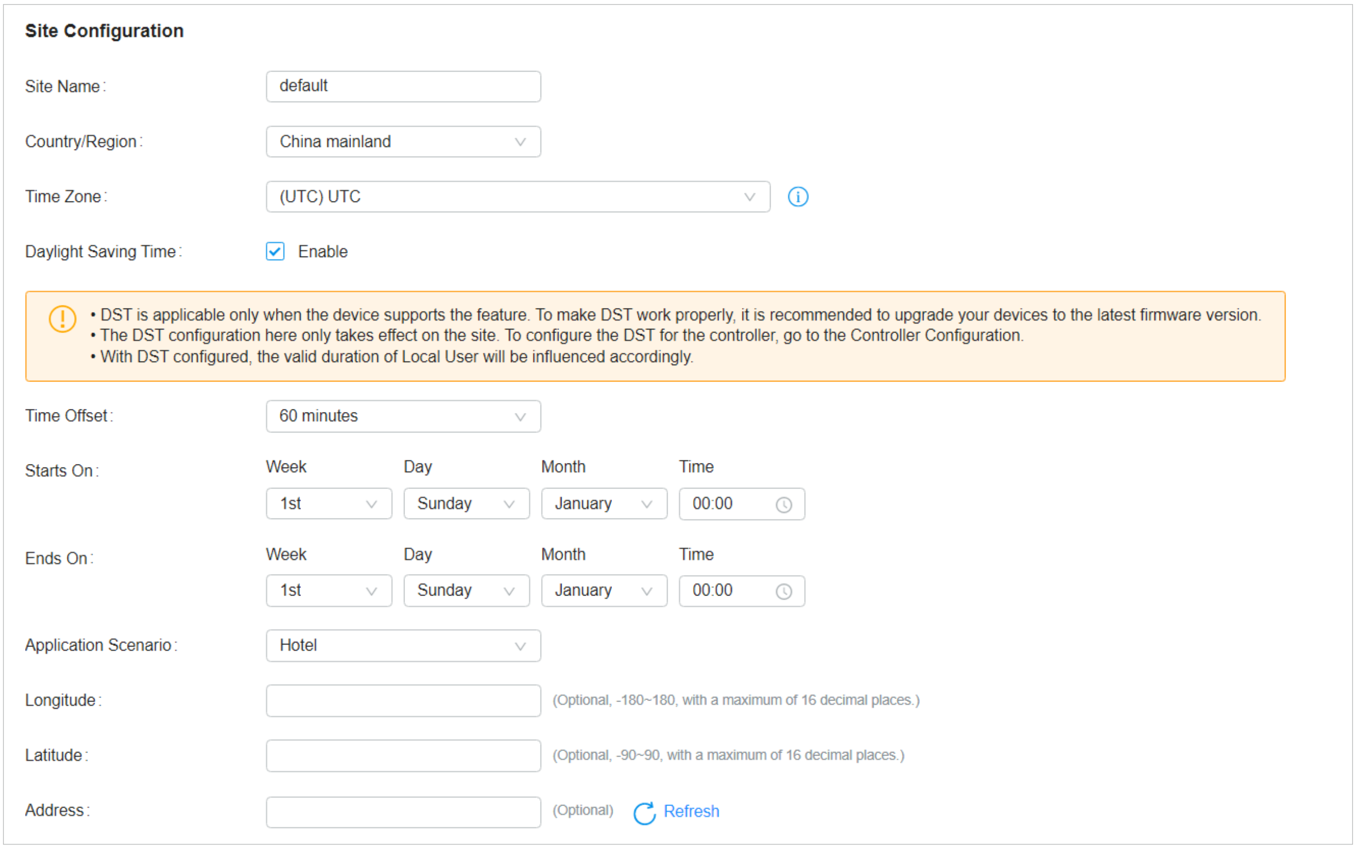
1. 2. 1 Site Configuration

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 Organization in the top-right corner, go to Settings > Site, and configure the following information of the site in Site Configuration. Click Save.



Site Configuration

Site Name: default

Country/Region: China mainland

Time Zone: (UTC) UTC

Daylight Saving Time: ☑ Enable

- DST is applicable only when the device supports the feature. To make DST work properly, it is recommended to upgrade your devices to the latest firmware version.
- The DST configuration here only takes effect on the site. To configure the DST for the controller, go to the Controller Configuration.
- With DST configured, the valid duration of Local User will be influenced accordingly.

Time Offset: 60 minutes

	Week	Day	Month	Time
Starts On:	1st	Sunday	January	00:00
Ends On:	1st	Sunday	January	00:00

Application Scenario: Hotel

Longitude: (Optional, -180~180, with a maximum of 16 decimal places.)

Latitude: (Optional, -90~90, with a maximum of 16 decimal places.)

Address: (Optional)

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.

Daylight Saving Time	Enable the feature if your country/region implements DST. When it is enabled, the icon DST will appear on the upper right, showing the DST settings and status.
Time Offset	Select the time added in minutes when Daylight Saving Time starts.
Starts On	Specify the time when the DST starts. The clock will be set forward by the time offset you specify.
Ends On	Specify the time when the DST ends.The clock will be set back by the time offset you specify.
Application Scenario	Specify the application scenario of the site. To customize your scenario, click Create New Scenario in the drop-down list.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.

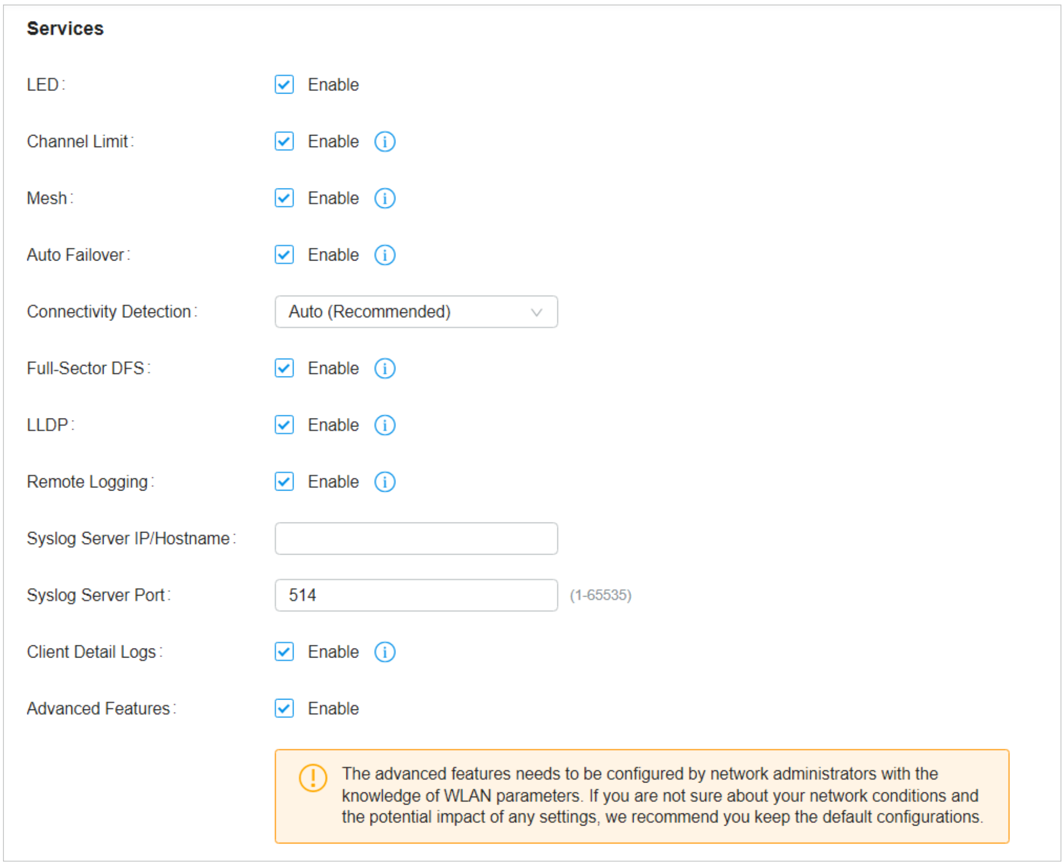
1. 2. 2 Services

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 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.



Services

LED:	☑ Enable
Channel Limit:	☑ Enable ⓘ
Mesh:	☑ Enable ⓘ
Auto Failover:	☑ Enable ⓘ
Connectivity Detection:	Auto (Recommended) ⌄
Full-Sector DFS:	☑ Enable ⓘ
LLDP:	☑ Enable ⓘ
Remote Logging:	☑ Enable ⓘ
Syslog Server IP/Hostname:	
Syslog Server Port:	514 (1-65535)
Client Detail Logs:	☑ Enable ⓘ
Advanced Features:	☑ Enable

ⓘ The advanced features needs to be configured by network administrators with the knowledge of WLAN parameters. If you are not sure about your network conditions and the potential impact of any settings, we recommend you keep the default configurations.

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 Chapter 6. Configure and Monitor Omada Managed Devices.
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	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.
LLDP	Click the checkbox to enable LLDP (Link Layer Discovery Protocol) for device discovery and auto-configuration of VoIP devices.
Remote Logging	With this feature configured, the controller will send generated site logs to the log server. When enabled, the following items are required: Syslog Server IP/Hostname: Enter the IP address or hostname of the log server. Syslog Server Port: Enter the port of the server. Client Detail Logs: With this feature enabled, the logs of clients will be sent to the syslog 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 4. 2. 3 Advanced Features.

1. 2. 3 Advanced Features

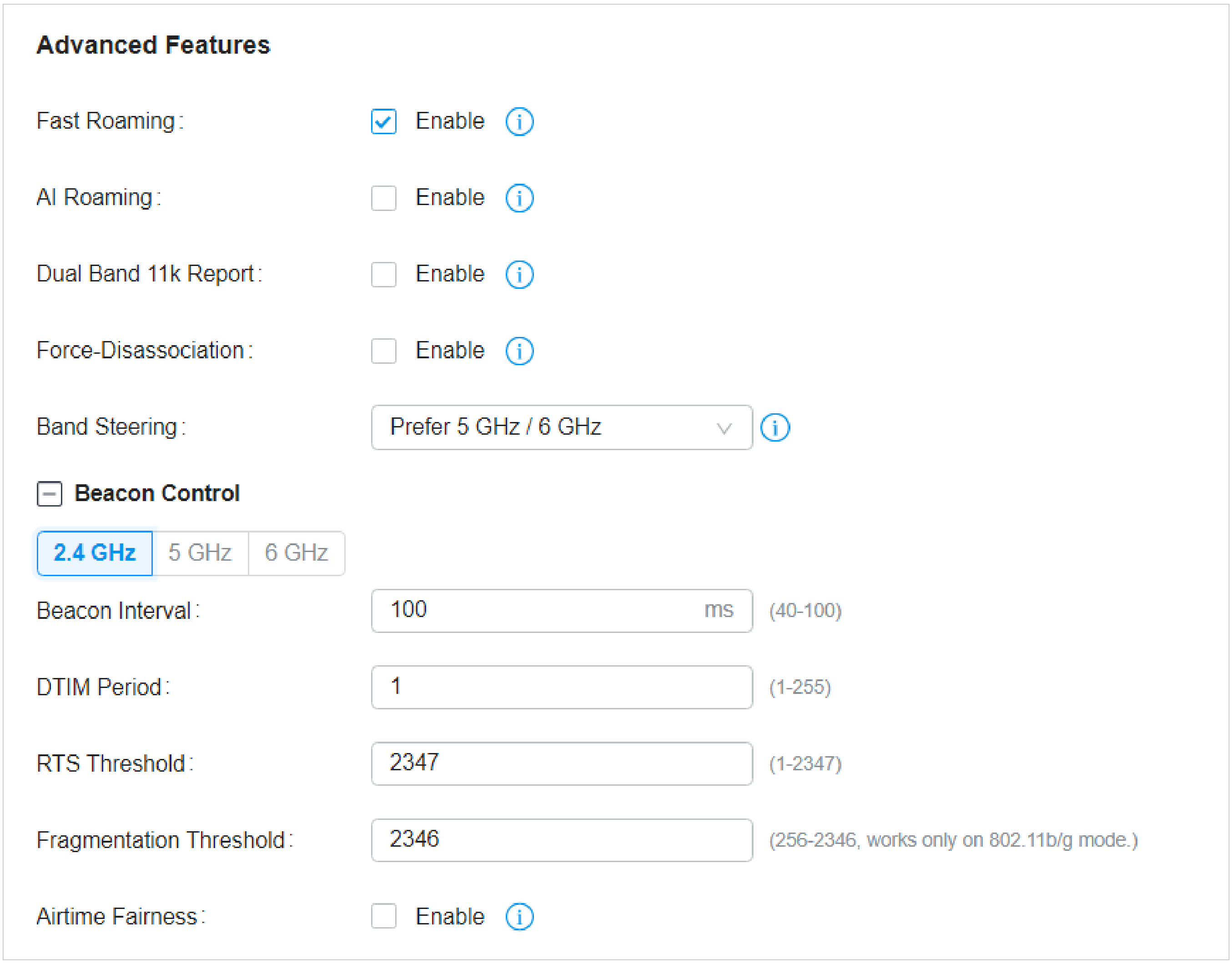
Overview

Advanced features include Fast Roaming, Band Steering, and Beacon Control. They 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 Organization 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.



Advanced Features

Fast Roaming: ☑ Enable ⓘ

AI Roaming: □ Enable ⓘ

Dual Band 11k Report: □ Enable ⓘ

Force-Disassociation: □ Enable ⓘ

Band Steering: Prefer 5 GHz / 6 GHz ⓘ

⊟ **Beacon Control**

Beacon Interval: 100 ms (40-100)

DTIM Period: 1 (1-255)

RTS Threshold: 2347 (1-2347)

Fragmentation Threshold: 2346 (256-2346, works only on 802.11b/g mode.)

Airtime Fairness: □ Enable ⓘ

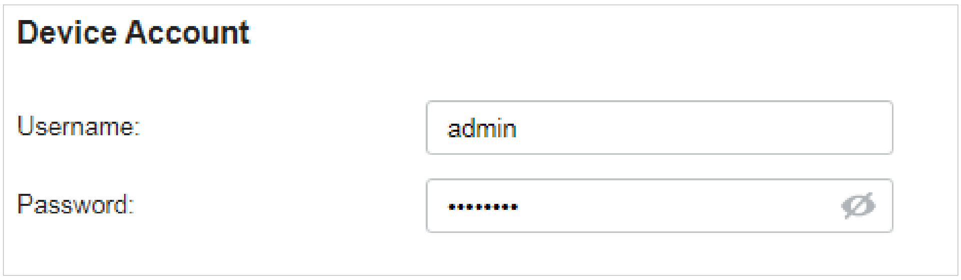
Fast Roaming	With this feature enabled, wireless clients that support 802.11k/v can improve fast roaming experience when moving among different APs. By default, it is disabled. This feature is available for some certain devices.
AI Roaming	With Fast Roaming enabled, you can enable AI Roaming to facilitate Fast Roaming, which improves roaming experience of the wireless clients that support 802.11k/v. This feature is available for some certain devices.
Dual Band 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 in 2.4 GHz, 5 GHz and 6 GHz bands to provide better wireless experience. When enabled, multi-band clients will be steered to the 5 GHz and 6 GHz band according to the configured parameters. This function can improve the network performance because the 5 GHz and 6 GHz band supports a larger number of non-overlapping channels and is less noisy.
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.

1. 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.

Select a site from the drop-down list of Organization. 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.



Device Account

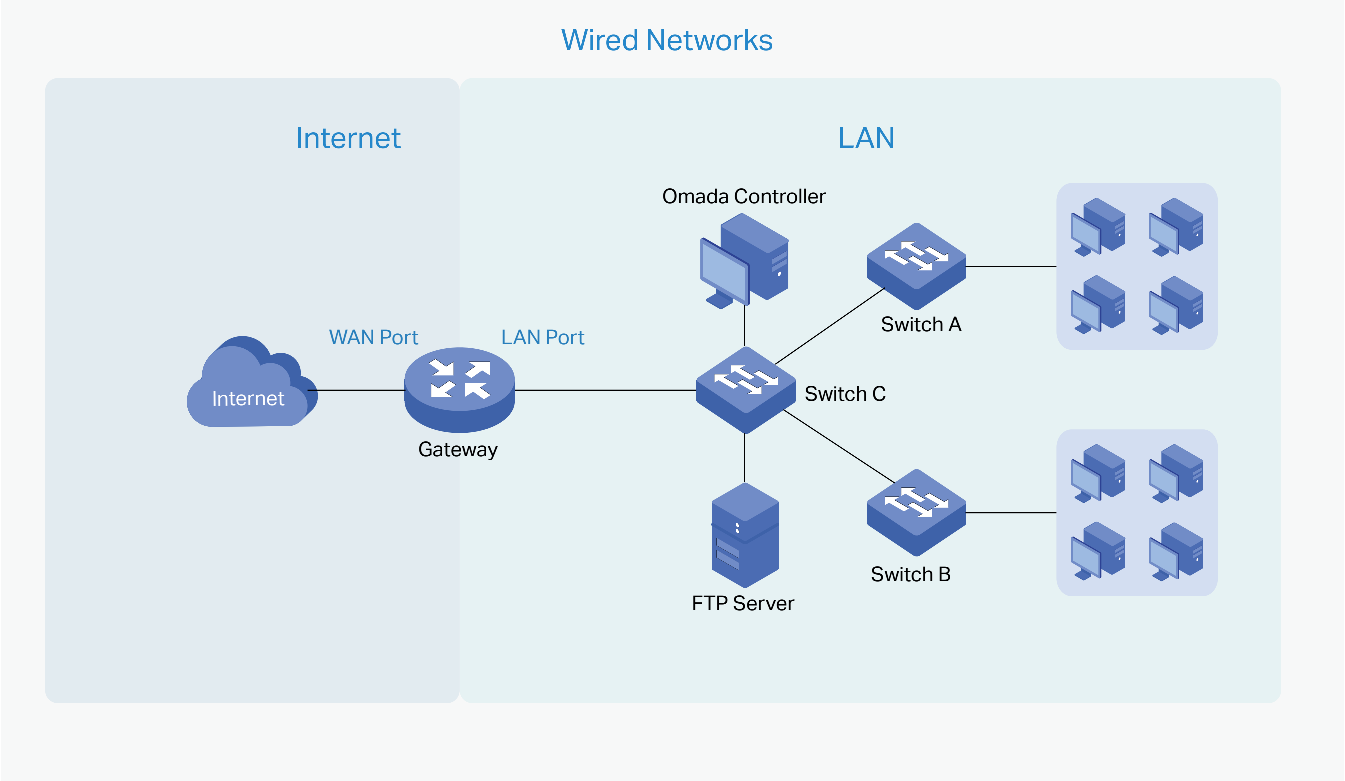
Username: admin

Password: ••••••••

1. 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 on the gateway and how they connect to the internet. You can set up an IPv4 connection and IPv6 connection to your internet service provider (ISP) according to your needs. The parameters of the internet connection for the gateway depend on which connection types you use. For an IPv4 connection, the following internet connection types are available: Dynamic IP, Static IP, PPPoE, L2TP, and PPTP. For an IPv6 connection, the following internet connection types are available: Dynamic IP (SLAAC/ DHCPv6), Static IP, PPPoE, 6to4 Tunnel, and Pass-Through (Bridge). And, when more than one WAN port is configured, you can configure Load Balancing to optimize the resource utilization if needed.

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.

1. 3. 1 Set Up an Internet Connection

Configuration

To set up an internet connection, follow these steps:

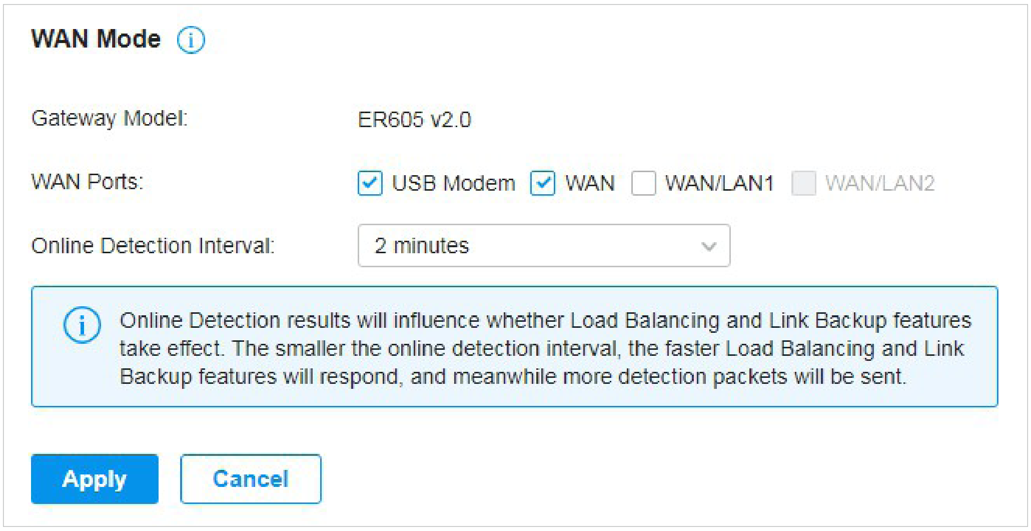
1) Configure the number of WAN ports on the gateway based on needs.

2) Configure WAN Connections. You can set up the IPv4 connection, IPv6 connection, or both.

3) (Optional) Configure Load Balancing if more than one WAN port is configured.

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

Select a site from the drop-down list of Organization. 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 Mode

Gateway Model: ER605 v2.0

WAN Ports: ☑ USB Modem ☑ WAN □ WAN/LAN1 □ WAN/LAN2

Online Detection Interval: 2 minutes

Online Detection results will influence whether Load Balancing and Link Backup features take effect. The smaller the online detection interval, the faster Load Balancing and Link Backup features will respond, and meanwhile more detection packets will be sent.

Apply Cancel

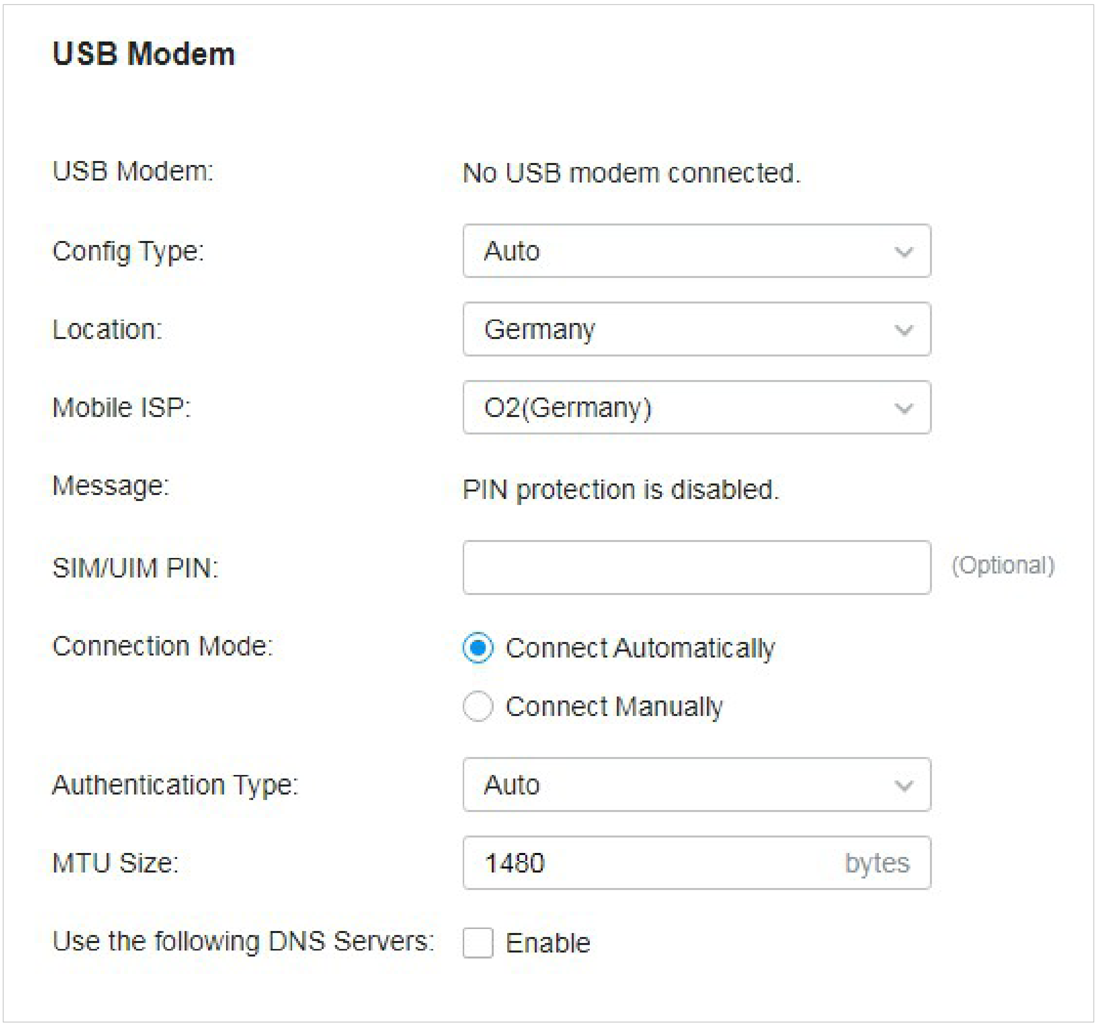
Gateway Model	Display the gateway model and version.
WAN Ports	Click the check box to enable the port as a WAN port. To configure multiple WAN ports, enable the ports one by one. Note that modification of WAN ports will automatically delete the current configurations associated with the ports, and the gateway will reboot.
Online Detection Interval	Select how often the WAN ports detect WAN connection status. If you don’t want to enable online detection, select Disable. Note that Load Balancing and Link Backup will take effects based on the results of online detection. Configure a proper online detection interval to make sure that Load Balancing and Link Backup works.

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

Note:

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

- Set Up USB Modem Connection



USB Modem

USB Modem: No USB modem connected.

Config Type: Auto

Location: Germany

Mobile ISP: O2(Germany)

Message: PIN protection is disabled.

SIM/UIM PIN: (Optional)

Connection Mode: ● Connect Automatically ○ Connect Manually

Authentication Type: Auto

MTU Size: 1480 bytes

Use the following DNS Servers: □ Enable

USB Modem	Display whether a USB modem is connected to the device and the name of the connected USB modem.
Config Type	Select a configuration type for the USB modem. Auto: Use the Location and Mobile ISP information below for configuration. Manually: Enter the Dial Number, APN, Username, and password provided by your Mobile ISP.
Location	Select your location.
Mobile ISP	Select your mobile ISP.
Message	Display the current status of the SIM card.
SIM/UIM PIN	(Optional) Enter the PIN of your SIM card. The field is required when the following information appears in the Message: PIN protection is enabled and the PIN is invalid.

Connection Mode	Select the connection mode. Connect Automatically: The router will use the USB modem to connect to the internet automatically. Connect Manually: You need to turn on/off the internet manually on the device page, refer to 6. 2. 2 Monitor the Gateway.
Authentication Mode	Select the Authentication mode for the USB modem. The default value is Auto, and it is recommended to keep the default value.
MTU Size	Specify the MTU (Maximum Transmission Unit) of the USB WAN port. The default value is 1480, and it is recommended to keep the default value. MTU is the maximum data unit transmitted in the physical network.
Use the following DNS Servers	Enable the feature if you want to specify the Primary and Secondary DNS servers manually.

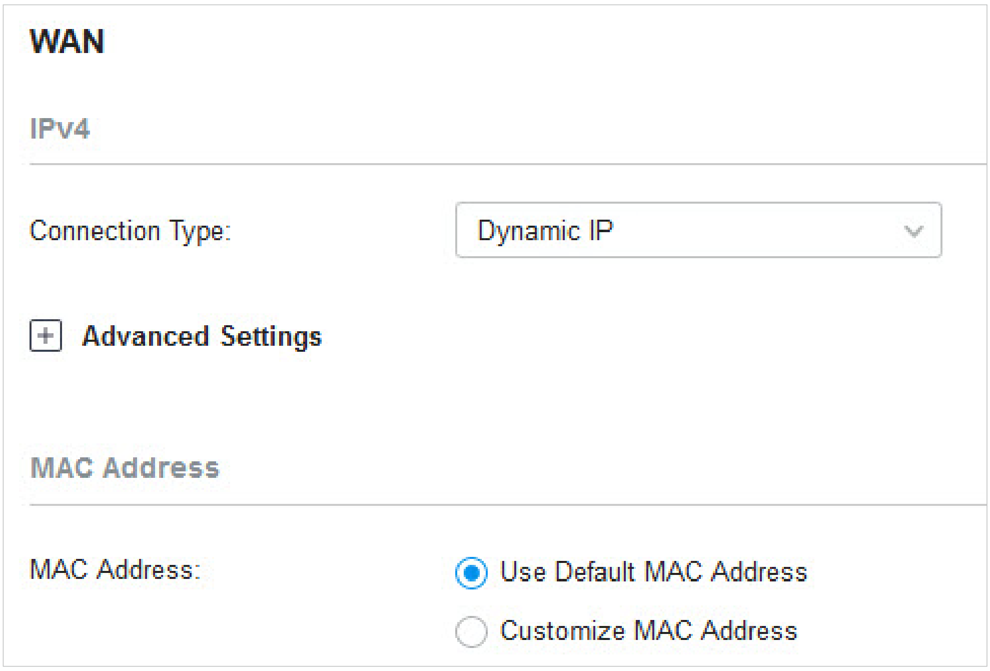
- Set Up IPv4 Connection

Select a site from the drop-down list of Organization. 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.



WAN

IPv4

Connection Type: Dynamic IP

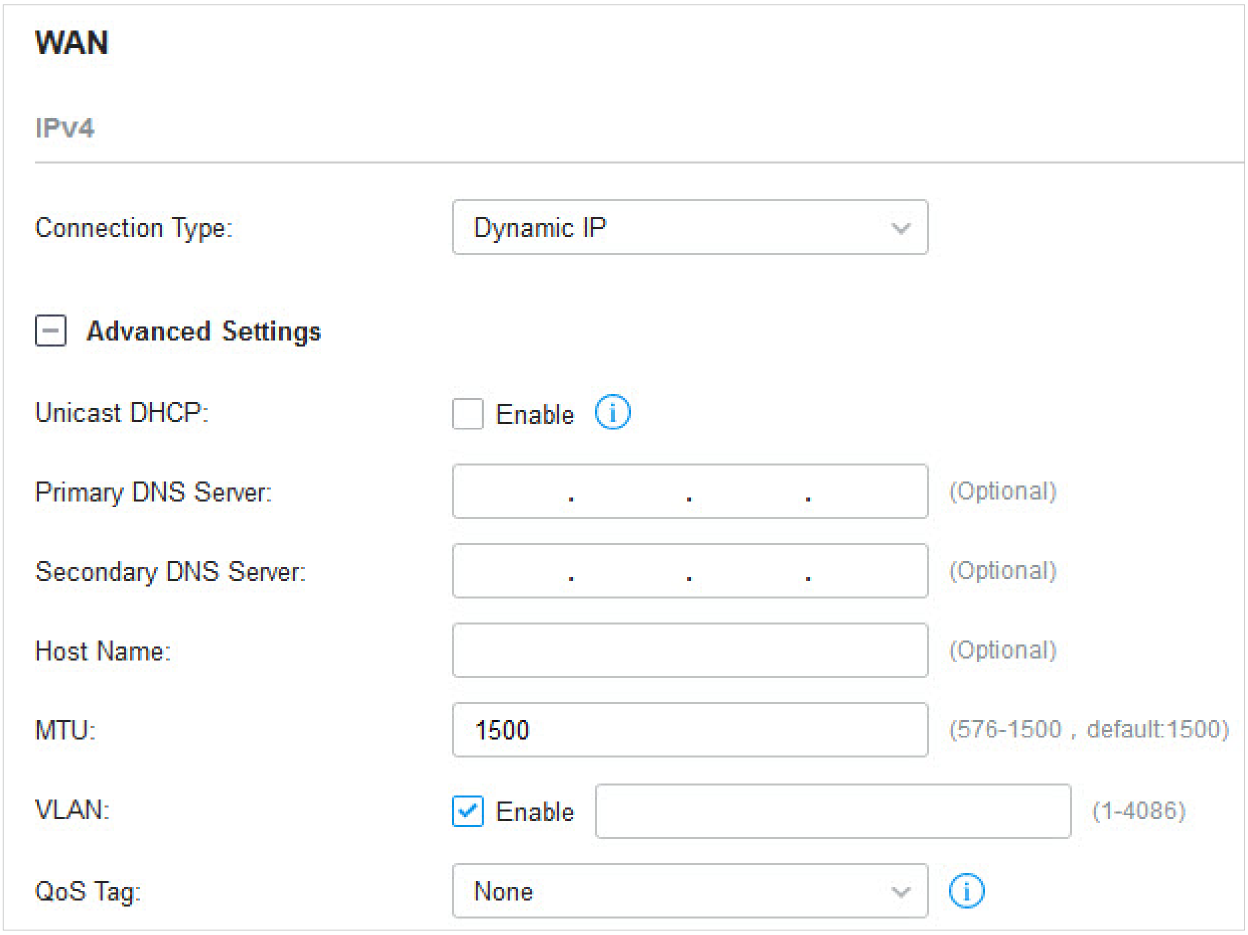
⊞ Advanced Settings

MAC Address

MAC Address: ● Use Default MAC Address ○ Customize MAC Address

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.



WAN

IPv4

Connection Type: Dynamic IP

⊟ Advanced Settings

Unicast DHCP: □ Enable ⓘ

Primary DNS Server: . . . (Optional)

Secondary DNS Server: . . . (Optional)

Host Name: (Optional)

MTU: 1500 (576-1500，default:1500)

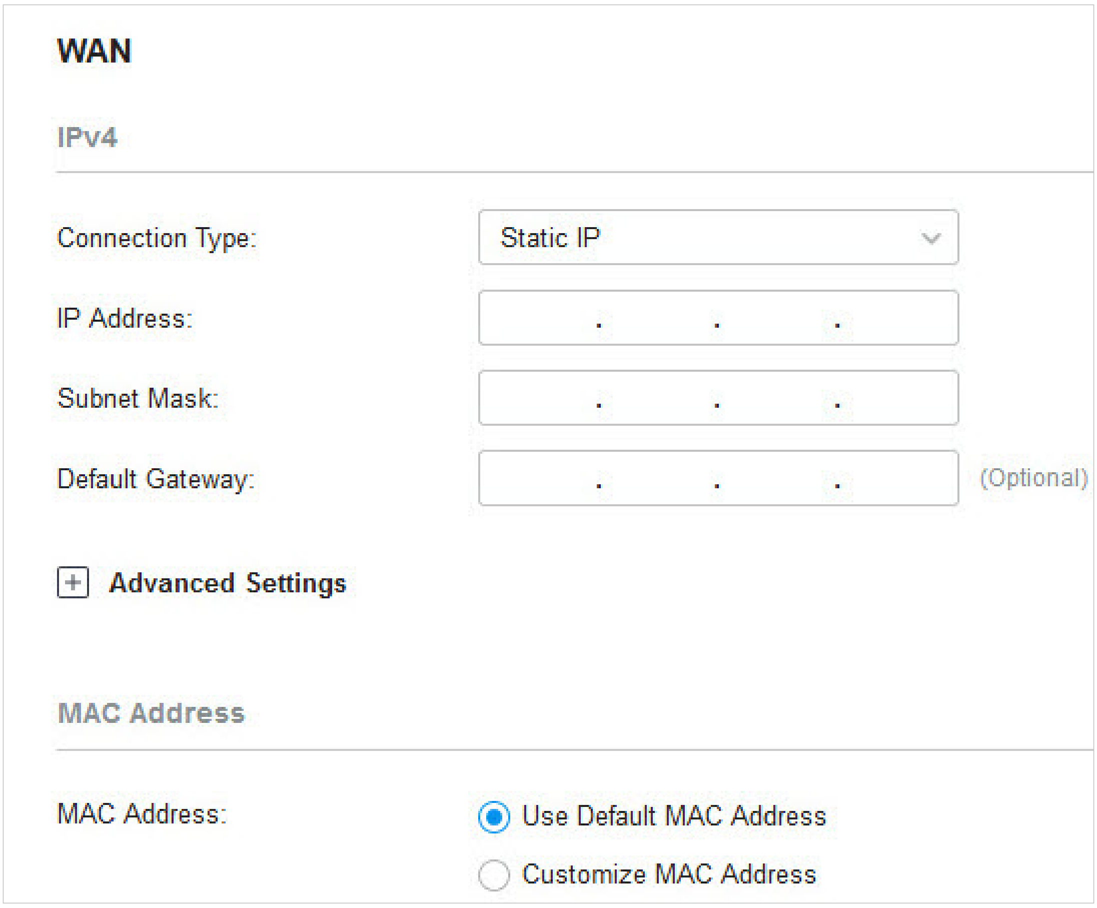
VLAN: ☑ Enable (1-4086)

QoS Tag: None ⓘ

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.



WAN

IPv4

Connection Type: Static IP

IP Address: . . .

Subnet Mask: . . .

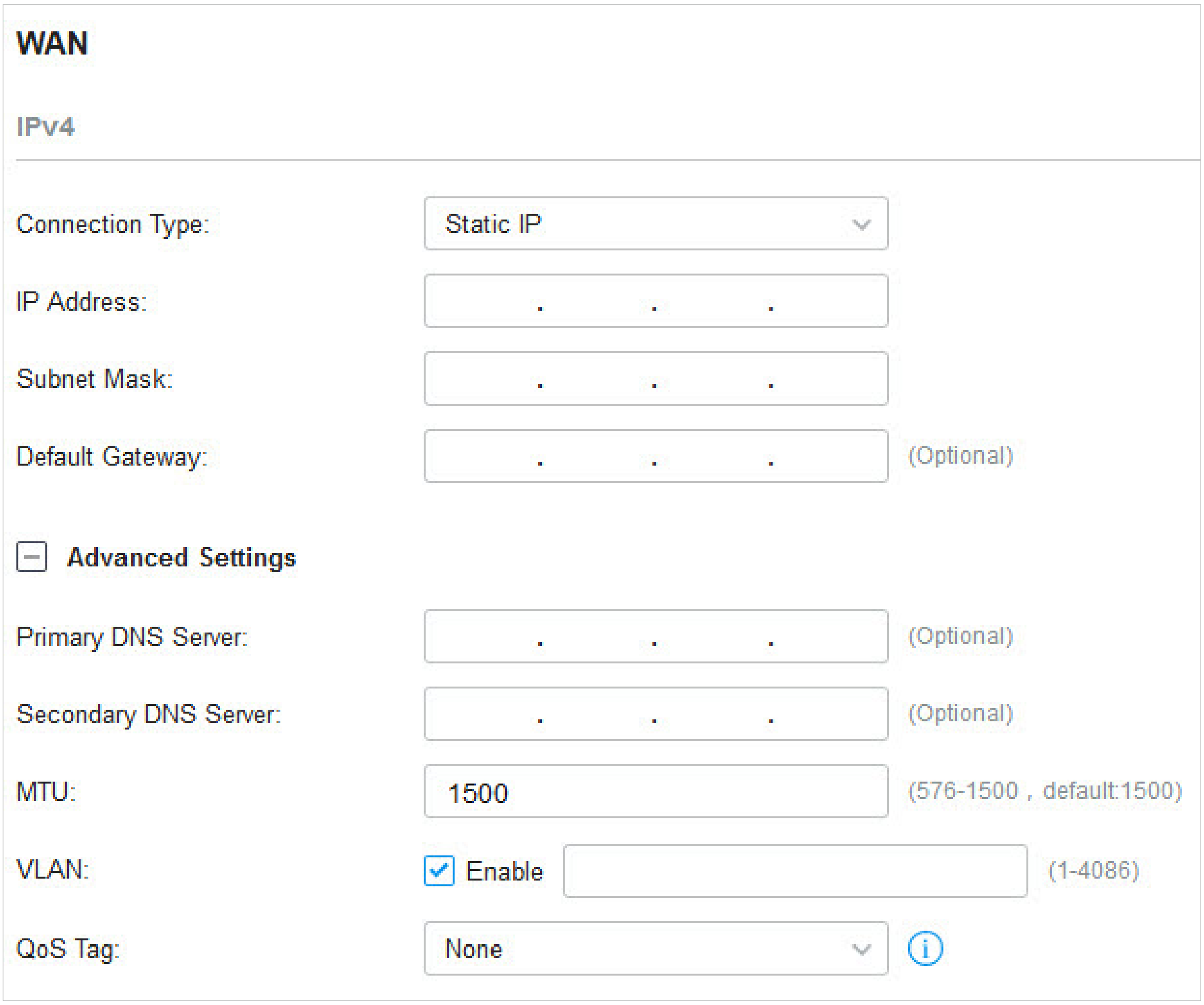
Default Gateway: . . . (Optional)

MAC Address

MAC Address: ● Use Default MAC Address ○ Customize MAC Address

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.



WAN

IPv4

Connection Type:	Static IP	
IP Address:	. . .	
Subnet Mask:	. . .	
Default Gateway:	. . .	(Optional)

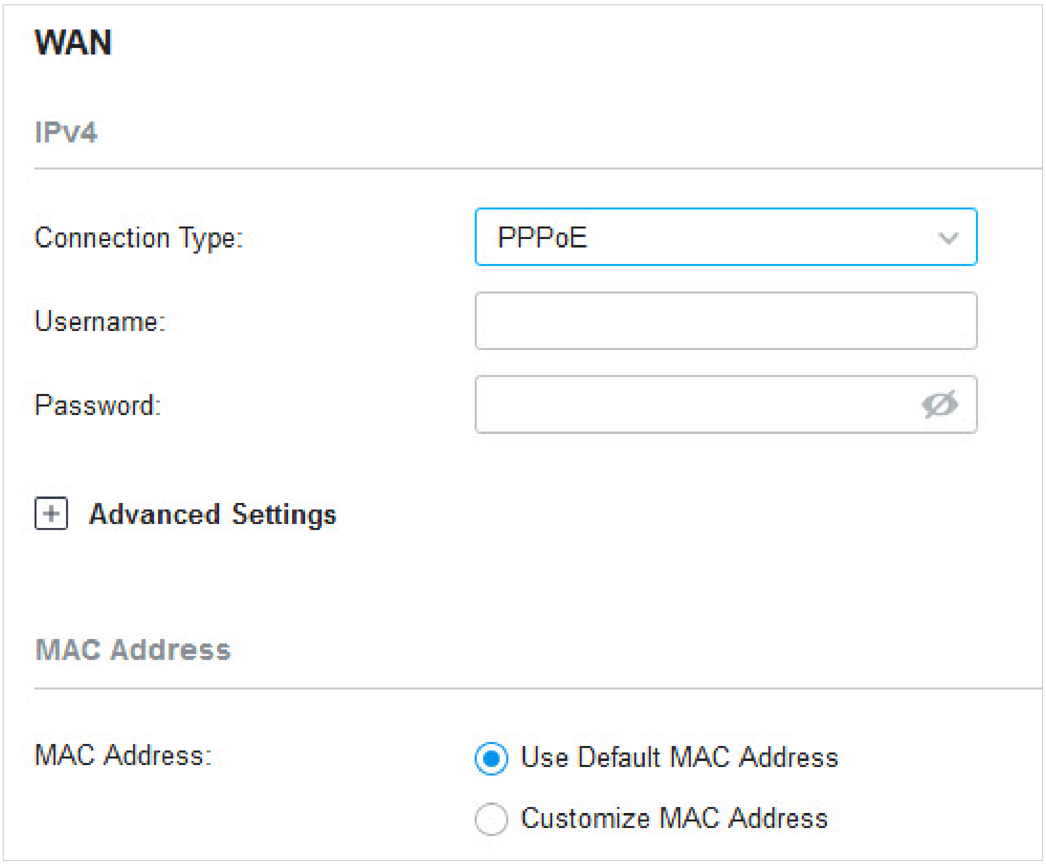
⊟ **Advanced Settings**

Primary DNS Server:	. . .	(Optional)
Secondary DNS Server:	. . .	(Optional)
MTU:	1500	(576-1500，default:1500)
VLAN:	☑ Enable	(1-4086)
QoS Tag:	None	ⓘ

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 PPPoE and configure the following parameters.



WAN

IPv4

Connection Type:	PPPoE
Username:	
Password:	

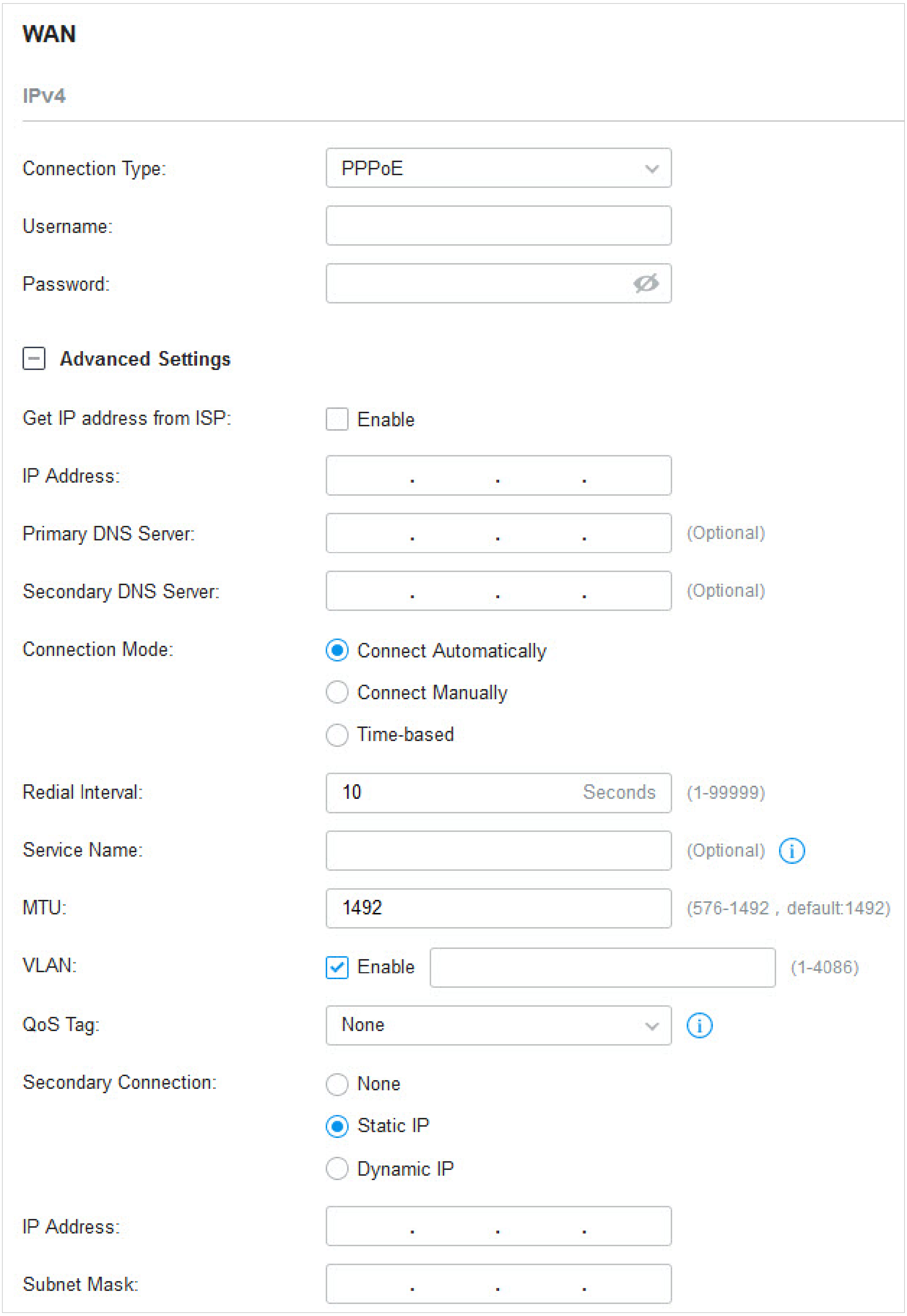
⊞ **Advanced Settings**

MAC Address

MAC Address: ● Use Default MAC Address ○ Customize MAC Address

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.



WAN

IPv4

Connection Type: PPPoE

Username:

Password:

⊟ **Advanced Settings**

Get IP address from ISP: □ Enable

IP Address: . . .

Primary DNS Server: . . . (Optional)

Secondary DNS Server: . . . (Optional)

Connection Mode: ● Connect Automatically ○ Connect Manually ○ Time-based

Redial Interval: 10 Seconds (1-99999)

Service Name: (Optional)

MTU: 1492 (576-1492，default:1492)

VLAN: ☑ Enable (1-4086)

QoS Tag: None

Secondary Connection: ○ None ● Static IP ○ Dynamic IP

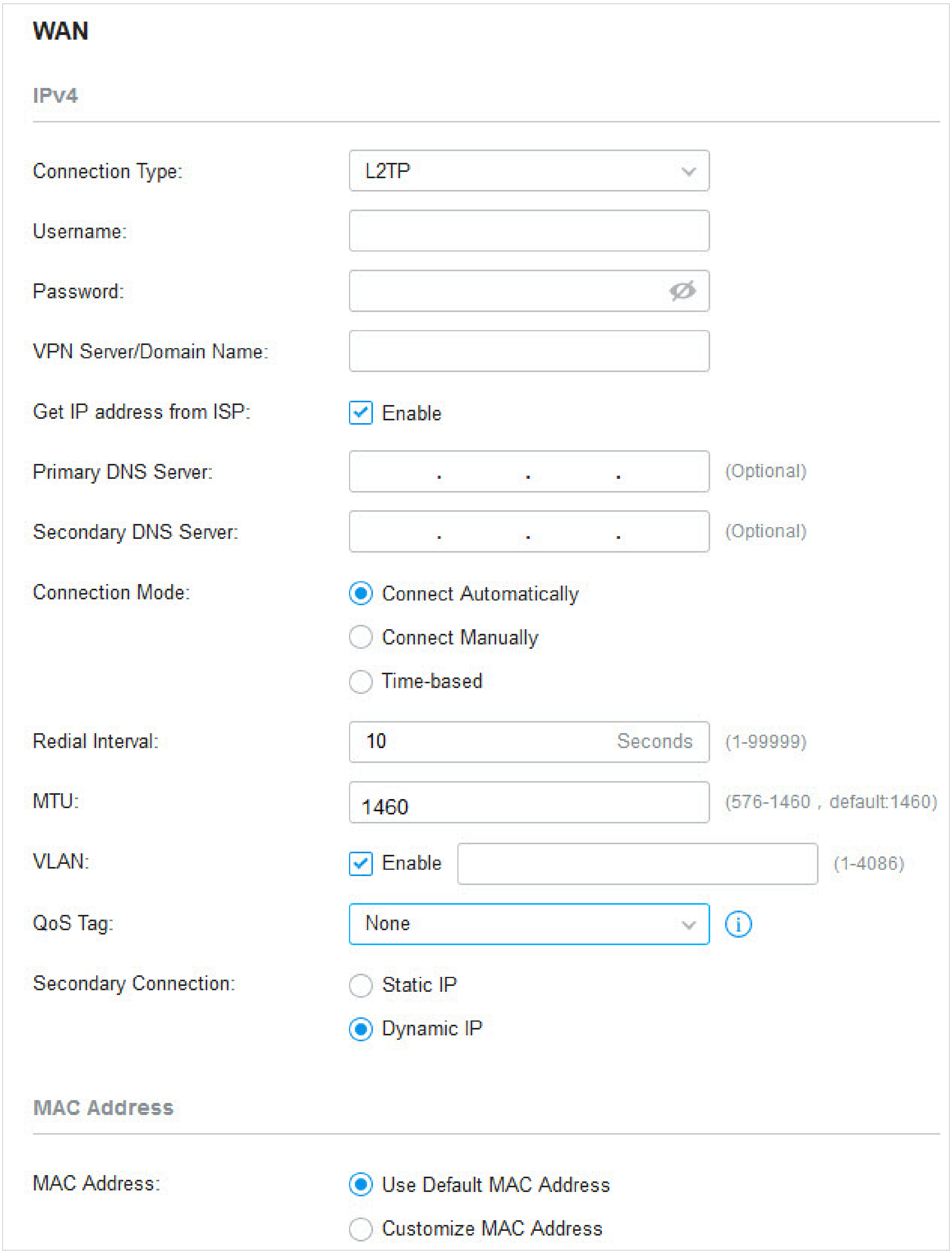
IP Address: . . .

Subnet Mask: . . .

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.



WAN

IPv4

Connection Type:	L2TP
Username:	
Password:	
VPN Server/Domain Name:	
Get IP address from ISP:	☑ Enable
Primary DNS Server:	. . . (Optional)
Secondary DNS Server:	. . . (Optional)
Connection Mode:	● Connect Automatically ○ Connect Manually ○ Time-based
Redial Interval:	10 Seconds (1-99999)
MTU:	1460 (576-1460，default:1460)
VLAN:	☑ Enable (1-4086)
QoS Tag:	None
Secondary Connection:	○ Static IP ● Dynamic IP

MAC Address

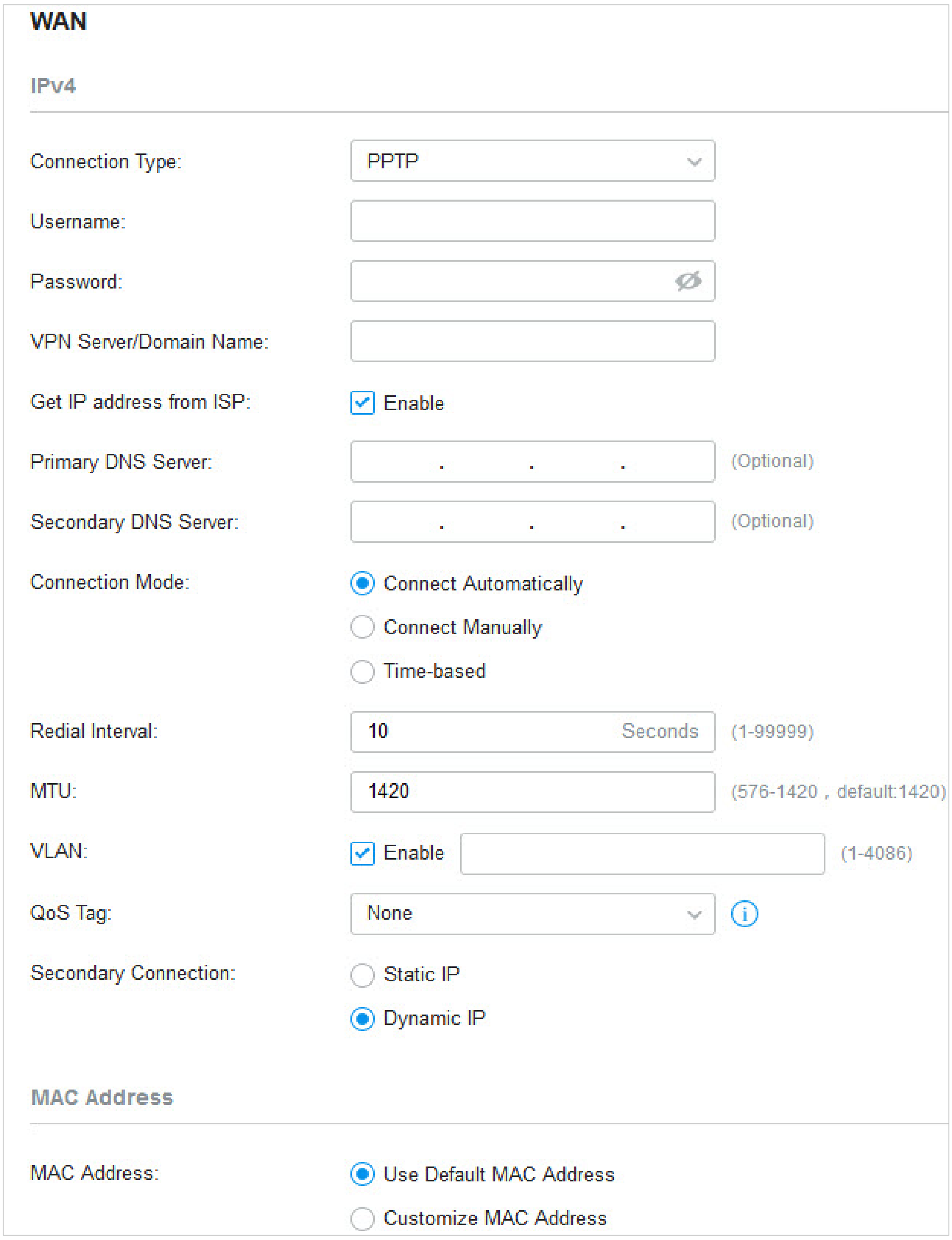
MAC Address:	● Use Default MAC Address ○ Customize MAC Address

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.



WAN

IPv4

Connection Type: PPTP

Username:

Password:

VPN Server/Domain Name:

Get IP address from ISP: ☑ Enable

Primary DNS Server: . . . (Optional)

Secondary DNS Server: . . . (Optional)

Connection Mode: ● Connect Automatically ○ Connect Manually ○ Time-based

Redial Interval: 10 Seconds (1-99999)

MTU: 1420 (576-1420，default:1420)

VLAN: ☑ Enable (1-4086)

QoS Tag: None

Secondary Connection: ○ Static IP ● Dynamic IP

MAC Address

MAC Address: ● Use Default MAC Address ○ Customize MAC Address

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.

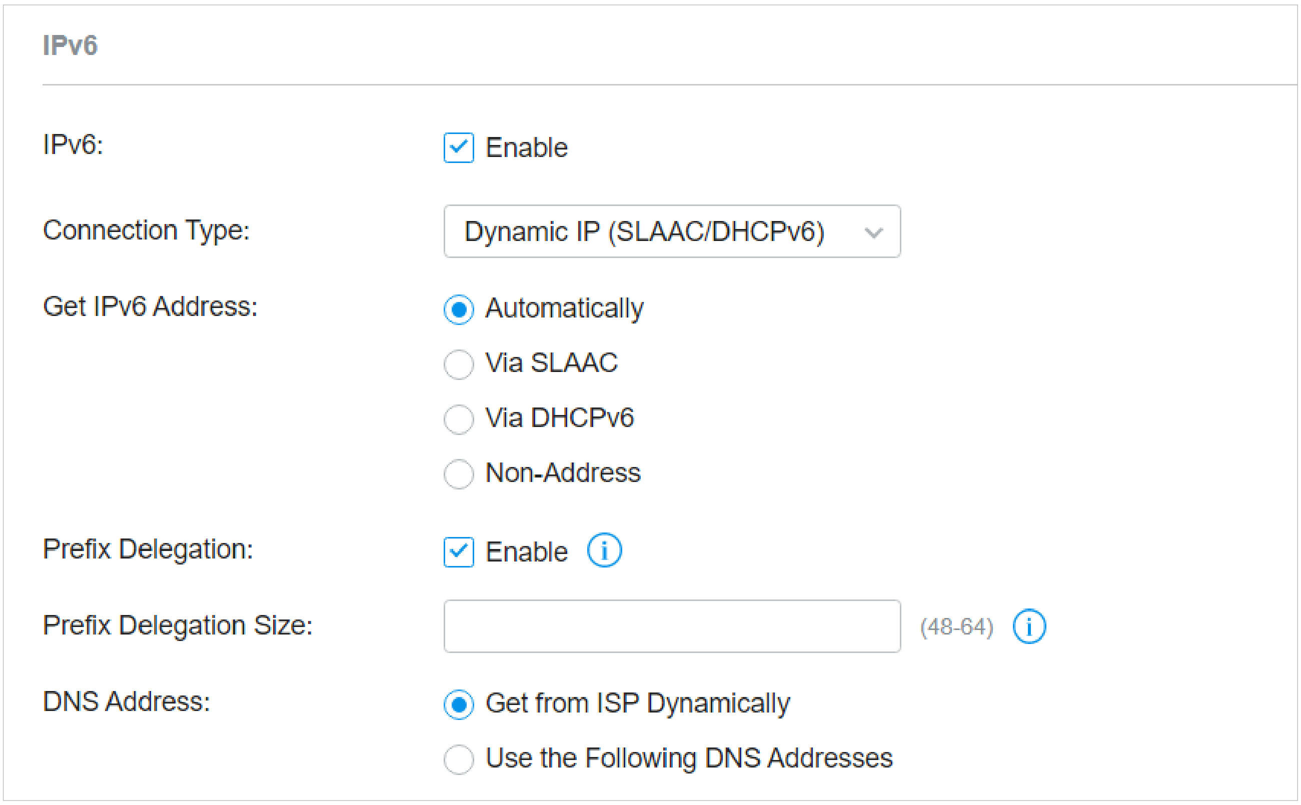
- Set Up IPv6 Connection

For IPv6 connections, check the box to enable the IPv6 connection, select the internet connection type according to the requirements of your ISP.

Connection Type	Dynamic IP (SLAAC/DHCPv6): If your ISP uses Dynamic IPv6 address assignment, either DHCPv6 or SLAAC+Stateless DHCP, select Dynamic IP (SLAAC/DHCPv6). Static IP: If your ISP provides you with a fixed IPv6 address, select Static IP. PPPoE: If your ISP uses PPPoEv6, and provides a username and password, select PPPoE. 6to4 Tunnel: If your ISP uses 6to4 deployment for assigning IPv6 address, select 6to4 Tunnel. 6to4 is an internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network. The IPv6 packet will be encapsulated in the IPv4 packet and transmitted to the IPv6 destination through IPv4 network. Pass-Through (Bridge): In Pass-Through (Bridge) mode, the gateway works as a transparent bridge. The IPv6 packets received from the WAN port will be transparently forwarded to the LAN port and vice versa. No extra parameter is required.

- **Dynamic IP (SLAAC/DHCPv6)**

Choose Connection Type as Dynamic IP (SLAAC/DHCPv6) and configure the following parameters. Then click Apply.



IPv6

IPv6: ☑ Enable

Connection Type: Dynamic IP (SLAAC/DHCPv6)

Get IPv6 Address: ● Automatically ○ Via SLAAC ○ Via DHCPv6 ○ Non-Address

Prefix Delegation: ☑ Enable

Prefix Delegation Size: (48-64)

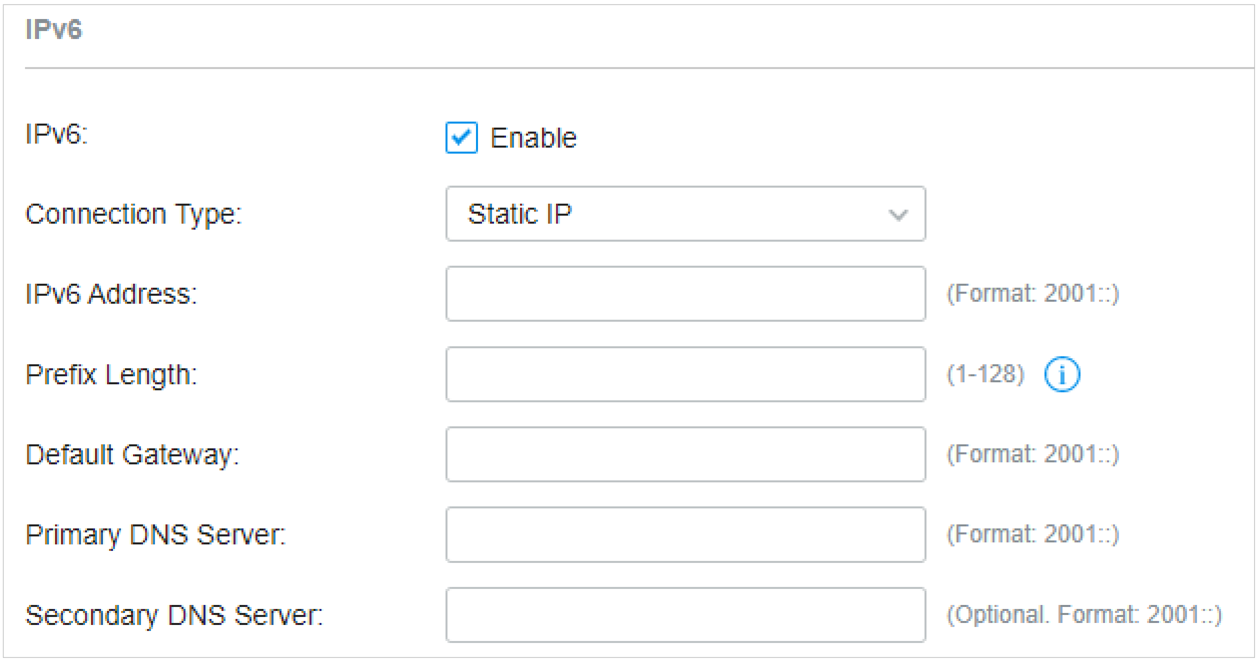
DNS Address: ● Get from ISP Dynamically ○ Use the Following DNS Addresses

Get IPv6 Address	Select the proper method whereby your ISP assigns IPv6 address to your gateway. Automatically: With this option selected, the gateway will automatically select SLAAC or DHCPv6 to get IPv6 addresses. Via SLAAC: With SLAAC (Stateless Address Auto-Configuration) selected, your ISP assigns the IPv6 address prefix to the gateway and the gateway automatically generates its own IPv6 address. Also, your ISP assigns other parameters including the DNS server address to the gateway. Via DHCPv6: With DHCPv6 selected, your ISP assigns an IPv6 address and other parameters including the DNS server address to the gateway using DHCPv6. Non-Address: With this option selected, the gateway will not get an IPv6 address.
Prefix Delegation	Select Enable to get an address prefix by DHCPv6 server from your ISP, or Disable to designate an address prefix for your LAN port manually. Clients in LAN will get an IPv6 address with this prefix.
Prefix Delegation Size	With Prefix Delegation enabled, enter the Prefix Delegation Size to determine the length of the address prefix. If you are not sure about the value, you can ask your ISP.

DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually. Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP. Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

- **Static IP**

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



IPv6

IPv6: ☑ Enable

Connection Type: Static IP

IPv6 Address: (Format: 2001::)

Prefix Length: (1-128)

Default Gateway: (Format: 2001::)

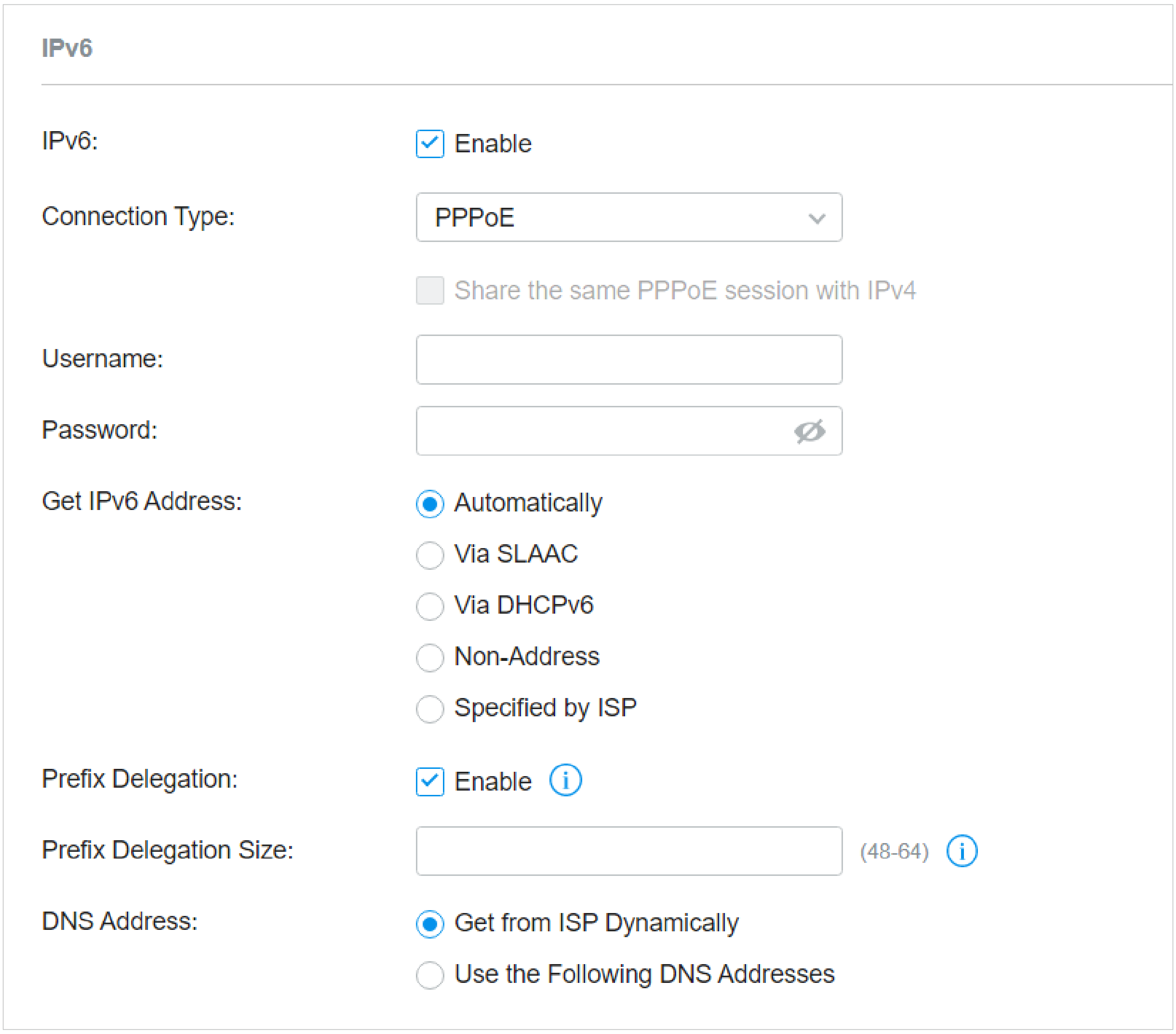
Primary DNS Server: (Format: 2001::)

Secondary DNS Server: (Optional. Format: 2001::)

IPv6 Address	Enter the static IPv6 address information received from your ISP.
Prefix Length	Enter the prefix length of the IPv6 address received from your ISP.
Default Gateway	Enter the default gateway provided by your ISP.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

- **PPPoE**

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



IPv6

IPv6: ☑ Enable

Connection Type: PPPoE

□ Share the same PPPoE session with IPv4

Username:

Password:

Get IPv6 Address: ● Automatically ○ Via SLAAC ○ Via DHCPv6 ○ Non-Address ○ Specified by ISP

Prefix Delegation: ☑ Enable

Prefix Delegation Size: (48-64)

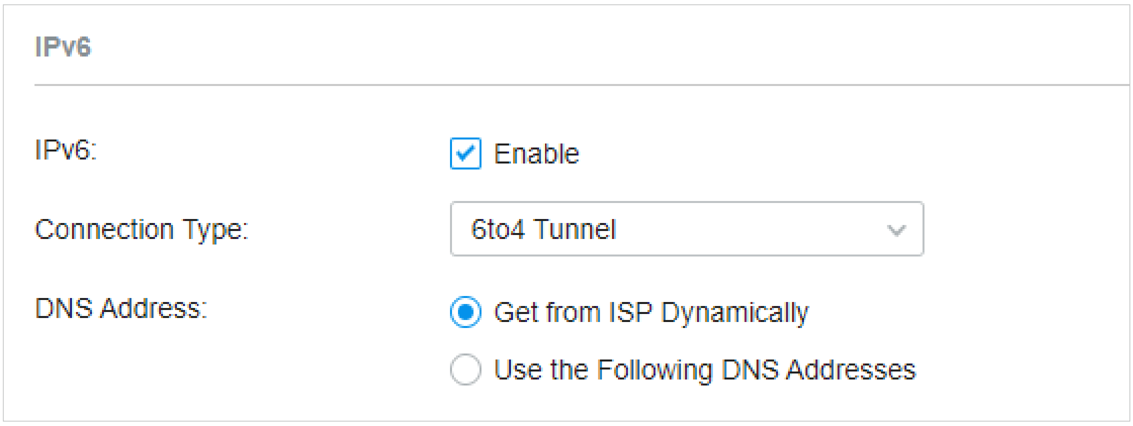
DNS Address: ● Get from ISP Dynamically ○ Use the Following DNS Addresses

Share the same PPPoE session with IPv4	If your ISP provides only one PPPoE account for both IPv4 and IPv6 connections, and you have already established an IPv4 connection on this WAN port, you can check the box, then the WAN port will use the PPP session of IPv4 PPPoE connection to get the IPv6 address. In this case, you do not need to enter the username and password of the PPPoE account. If your ISP provides two separate PPPoE accounts for the IPv4 and IPv6 connections, or the IPv4 connection of this WAN port is not based on PPPoE, do not check the box and manually enter the username and password for the IPv6 connection.
Username	Enter the username of your PPPoE account provided by your ISP.
Password	Enter the password of your PPPoE account provided by your ISP.

Get IPv6 Address	Select the proper method whereby your ISP assigns IPv6 address to your gateway. Automatically: With this option selected, the gateway will automatically select the method to get IPv6 addresses between SLAAC and DHCPv6. Via SLAAC: With SLAAC (Stateless Address Auto-Configuration) selected, your ISP assigns the IPv6 address prefix to the gateway and the gateway automatically generates its own IPv6 address. Also, your ISP assigns other parameters including the DNS server address to the gateway. Via DHCPv6: With DHCPv6 selected, your ISP assigns an IPv6 address and other parameters including the DNS server address to the gateway using DHCPv6. Non-Address: With this option selected, the gateway will not get an IPv6 address. Specified by ISP: With this option selected, enter the IPv6 address you get from your ISP.
Prefix Delegation	Select Enable to get an address prefix by DHCPv6 server from your ISP, or Disable to designate an address prefix for your LAN port manually. Clients in LAN will get an IPv6 address with this prefix.
Prefix Delegation Size	With Prefix Delegation enabled, enter the Prefix Delegation Size to determine the length of the address prefix. If you are not sure about the value, you can ask your ISP.
DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually. Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP. Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

- **6to4 Tunnel**

Choose Connection Type as 6to4 Tunnel and configure the following parameters. Then click Apply.



IPv6

IPv6: ☑ Enable

Connection Type: 6to4 Tunnel

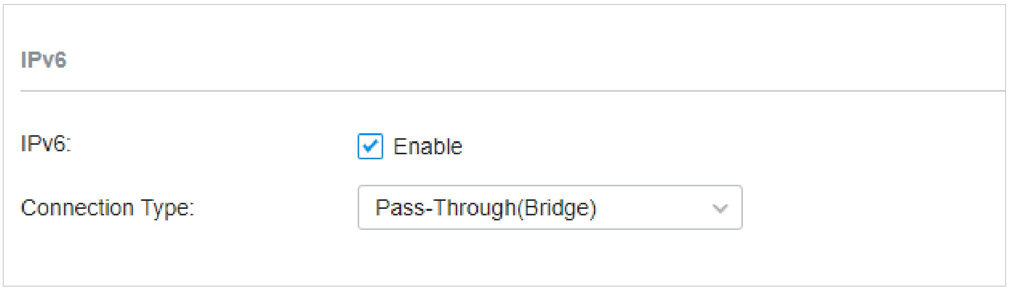
DNS Address: ● Get from ISP Dynamically

○ Use the Following DNS Addresses

DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually. Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP. Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

- **Pass-Through (Bridge)**

Choose Connection Type as Pass-Through (Bridge) and no configuration is required for this type of connection Then click Apply.



IPv6

IPv6: ☑ Enable

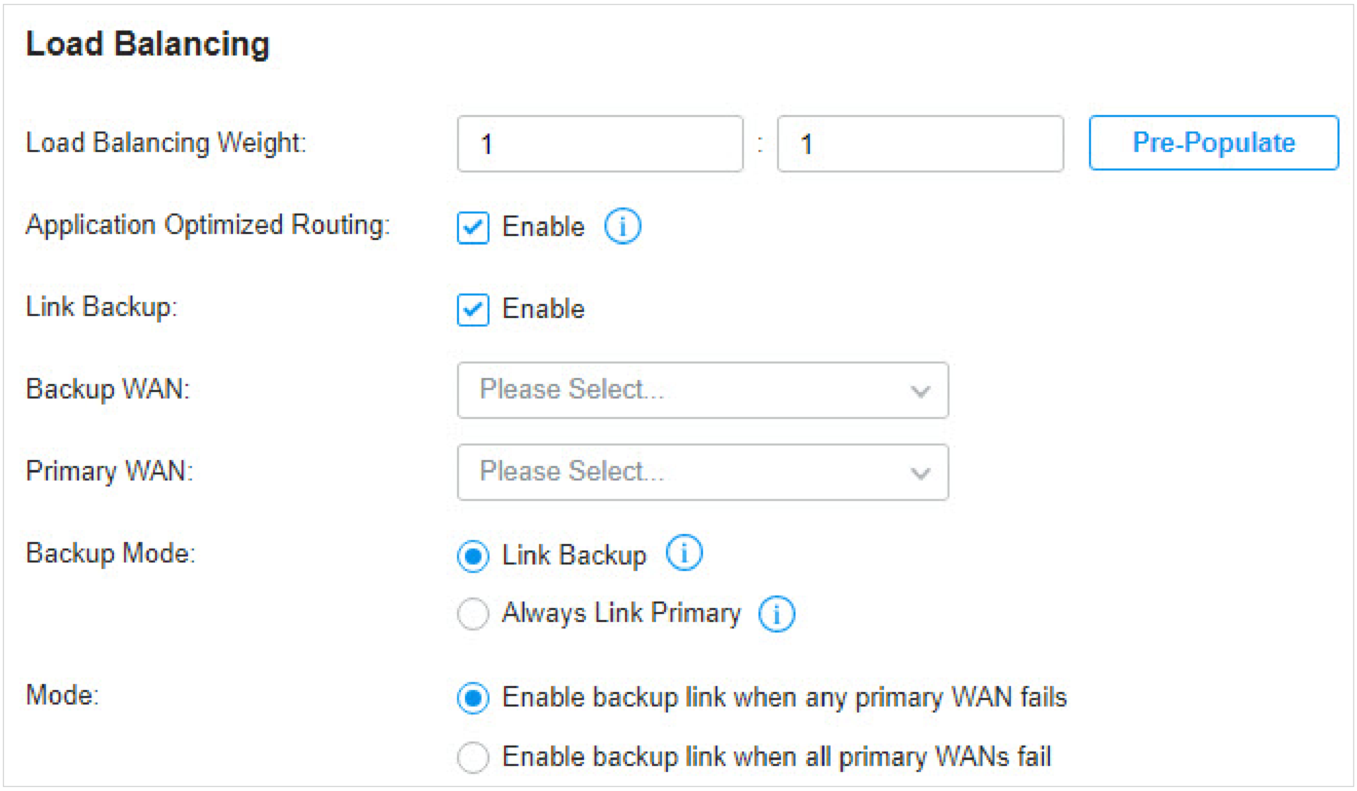
Connection Type: Pass-Through(Bridge)

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

ⓘ Note:

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

Select a site from the drop-down list of Organization. Go to Settings > Wired Networks > Internet to load the following page. In Load Balancing, configure the following parameters and click Apply.



Load Balancing

Load Balancing Weight: 1 : 1 Pre-Populate

Application Optimized Routing: ☑ Enable

Link Backup: ☑ Enable

Backup WAN: Please Select...

Primary WAN: Please Select...

Backup Mode: ● Link Backup ○ Always Link Primary

Mode: ● Enable backup link when any primary WAN fails ○ Enable backup link when all primary WANs fail

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.

1. 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.

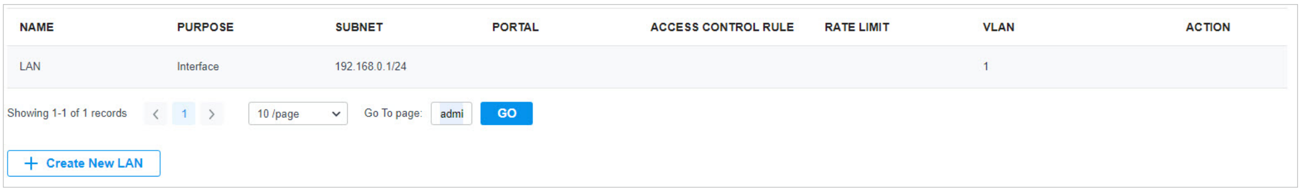
3) Assign the port profile to the desired ports of the switch to activate the LAN.

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

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. Select a site from the drop-down list of Organization. Go to Settings > Wired Networks > LAN > Networks to load the following page.

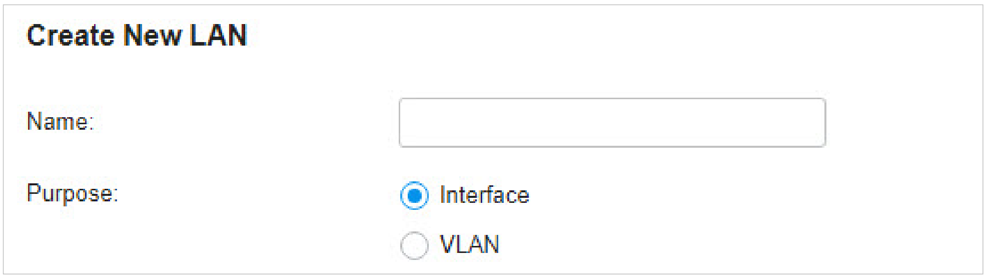


NAME	PURPOSE	SUBNET	PORTAL	ACCESS CONTROL RULE	RATE LIMIT	VLAN	ACTION
LAN	Interface	192.168.0.1/24				1	

Showing 1-1 of 1 records < 1 > 10 /page Go To page: admi GO

+ Create New LAN

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



Create New LAN

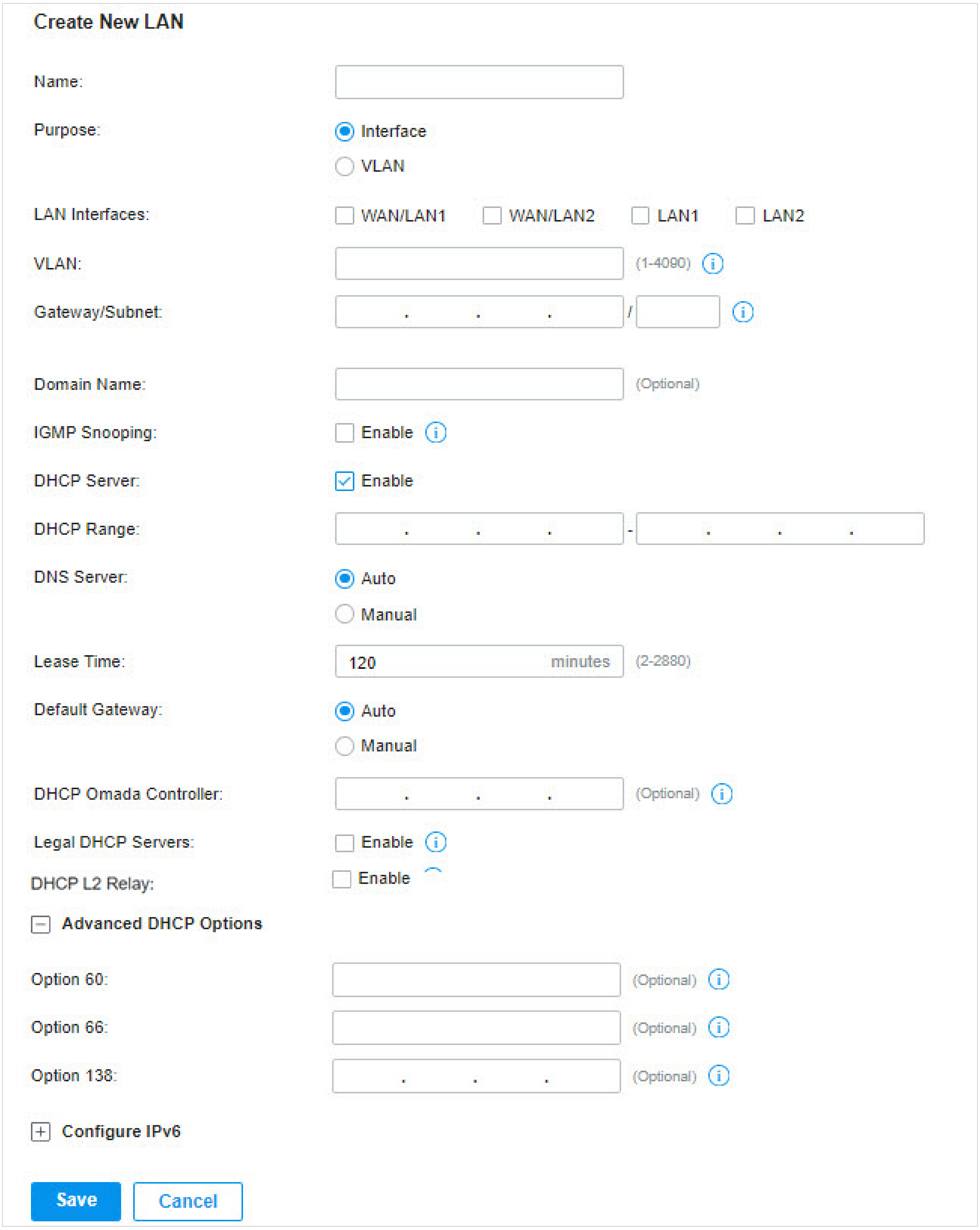
Name:

Purpose: ● Interface ○ VLAN

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



Create New LAN

Name:

Purpose: ● Interface ○ VLAN

LAN Interfaces: □ WAN/LAN1 □ WAN/LAN2 □ LAN1 □ LAN2

VLAN: (1-4090)

Gateway/Subnet: . . . /

Domain Name: (Optional)

IGMP Snooping: □ Enable

DHCP Server: ☑ Enable

DHCP Range: . . . - . . .

DNS Server: ● Auto ○ Manual

Lease Time: 120 minutes (2-2880)

Default Gateway: ● Auto ○ Manual

DHCP Omada Controller: . . . (Optional)

Legal DHCP Servers: □ Enable

DHCP L2 Relay: □ Enable

⊟ Advanced DHCP Options

Option 60: (Optional)

Option 66: (Optional)

Option 138: . . . (Optional)

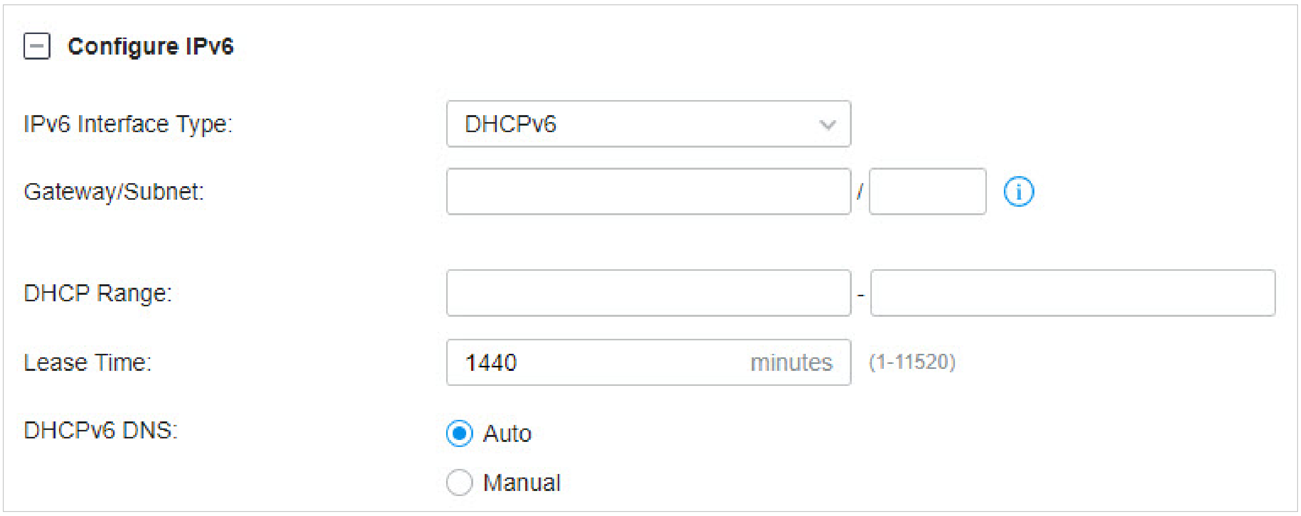
⊞ Configure IPv6

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 real time.
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. Deselect 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.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.
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.

You can configure IPv6 connections for the LAN clients based on you needs. First, determine the method whereby the gateway assigns IPv6 addresses to the clients in the local network. Some clients may support only a few of these connection types, so you should choose it according to the compatibility of clients in the local network.



⊟ **Configure IPv6**

IPv6 Interface Type: DHCPv6

Gateway/Subnet: /

DHCP Range: -

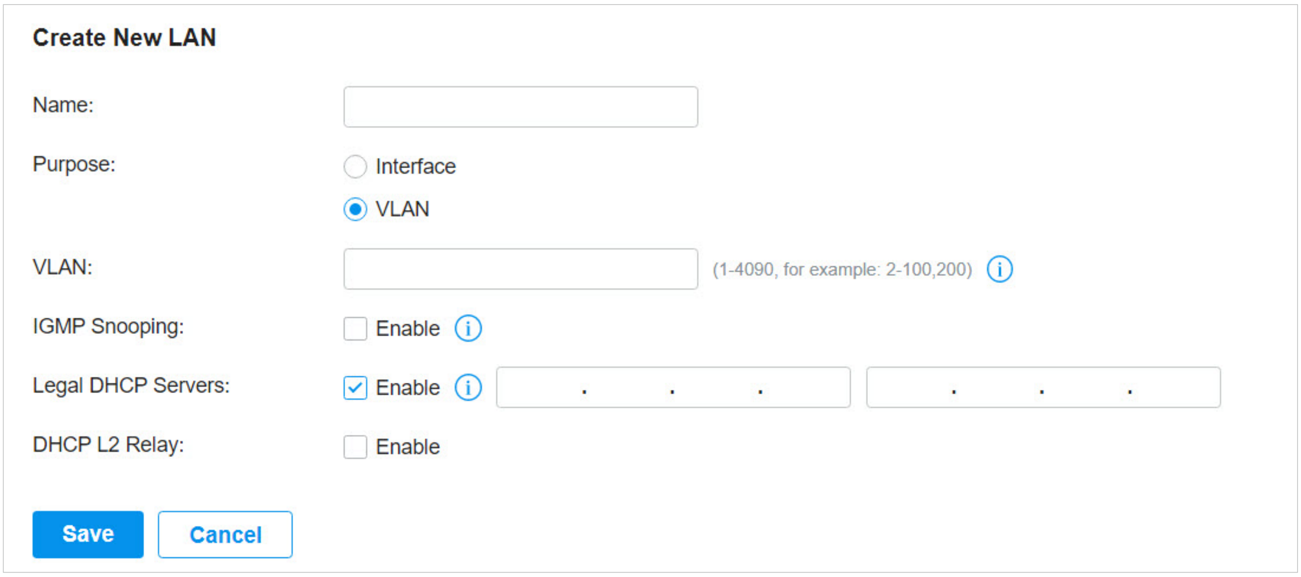
Lease Time: 1440 minutes (1-11520)

DHCPv6 DNS: ● Auto ○ Manual

IPv6 Interface Type	Configure the type of assigning IPv6 address to the clients in the local network. None: IPv6 connection is not enabled for the clients in the local network. DHCPv6: The gateway assigns an IPv6 address and other parameters including the DNS server address to each client using DHCPv6. SLAAC+Stateless DHCP: The gateway assigns the IPv6 address prefix to each client and the client automatically generates its own IPv6 address. Also, the gateway assigns other parameters including the DNS server address to each client using DHCPv6. SLAAC+RDNSS: The gateway assigns the IPv6 address prefix to each client and the client automatically generates its own IPv6 address. Also, the gateway assigns other parameters including the DNS server address to each client using the RDNSS option in RA (Router Advertisement). Pass-Through: Select this type if the WAN ports of the gateway use the Pass-Through for IPv6 connections.
With DHCPv6 selected, configure the following parameters.	
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 real time.

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.
Lease Time	This entry determines how long the assigned IPv6 address remains valid. Either keep the default 1440 minutes or change it if required by your ISP.
DHCPv6 DNS	Select a method to configure the DNS server for the network. With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. With Manual selected, enter the IP address of a server in each DNS server field.
With SLAAC+Stateless DHCP selected, configure the following parameters.	
Prefix	Configure the IPv6 address prefix for each client in the local network. Manual Prefix: With Manual Prefix selected, enter the prefix in the Address Prefix field. Get from Prefix Delegation: With Get from Prefix Delegation selected, select the WAN port with Prefix Delegation configured, and the clients will get the address prefix from the Prefix Delegation.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be added to the prefix to obtain a /64 subnet. The range of IPv6 Prefix ID is determined by the larger value of Prefix Delegation Size and Prefix Delegation Length (obtained from the ISP). Note that if the Prefix Delegation Length is larger than 64, the IPv6 Prefix ID cannot be obtained from Prefix Delegation, please select another method. In site view, go to Settings > Wired Network > Internet to configure Prefix Delegation Size.
DNS Server	Select a method to configure the DNS server for the network. Auto: With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. Manual: With Manual selected, enter the IP address of a server in each DNS server field.
With SLAAC+RDNSS selected, configure the following parameters.	
Prefix	Configure the IPv6 address prefix for each client in the local network. Manual Prefix: With Manual Prefix selected, enter the prefix in the Address Prefix field. Get from Prefix Delegation: With Get from Prefix Delegation selected, select the WAN port with Prefix Delegation configured, and the clients will get the address prefix from the Prefix Delegation.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be added to the prefix to obtain a /64 subnet.

DNS Server	Select a method to configure the DNS server for the network. Auto: With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. Manual: With Manual selected, enter the IP address of a server in each DNS server field.
With Pass-Through selected, configure the following parameters.	
IPv6 Prefix Delegation Interface	Select the WAN port using Pass-Through (Bridge) for the IPv6 connection.



Create New LAN

Name:

Purpose: ○ Interface ● VLAN

VLAN: (1-4090, for example: 2-100,200)

IGMP Snooping: □ Enable

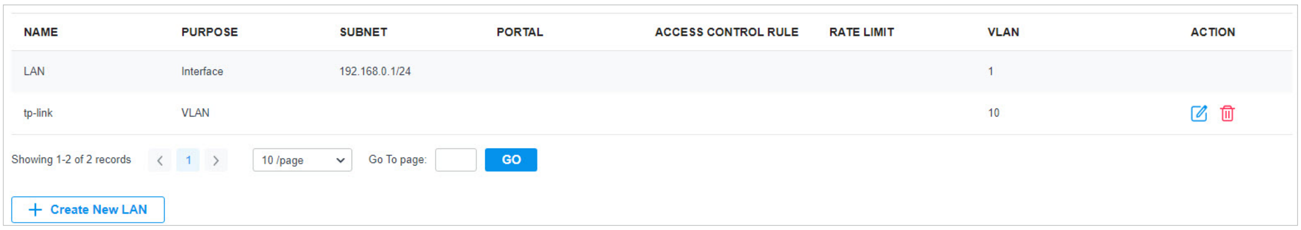
Legal DHCP Servers: ☑ Enable . . . . . .

DHCP L2 Relay: □ Enable

Save Cancel

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.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.

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.



NAME	PURPOSE	SUBNET	PORTAL	ACCESS CONTROL RULE	RATE LIMIT	VLAN	ACTION
LAN	Interface	192.168.0.1/24				1	
tp-link	VLAN					10	✎ 🗑

Showing 1-2 of 2 records < 1 > 10 /page Go To page: GO

+ Create New 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.

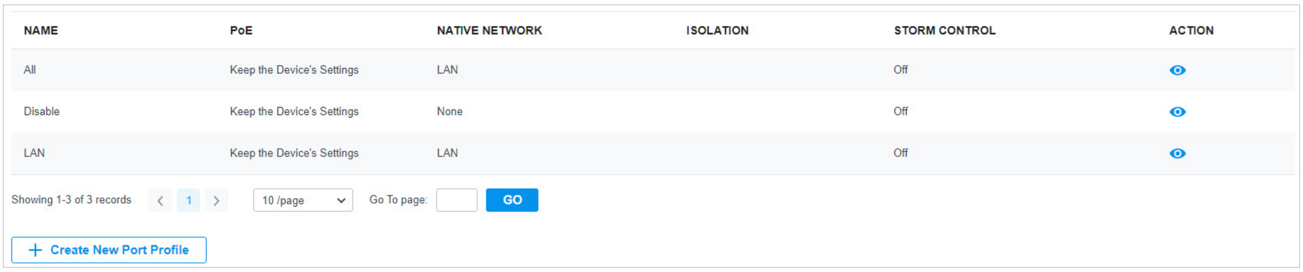
  All: In the All profile, all networks except the default network (LAN) are configured as Tagged Network, and the native network is the default network (LAN). This profile is assigned to all switch ports by default.

  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.

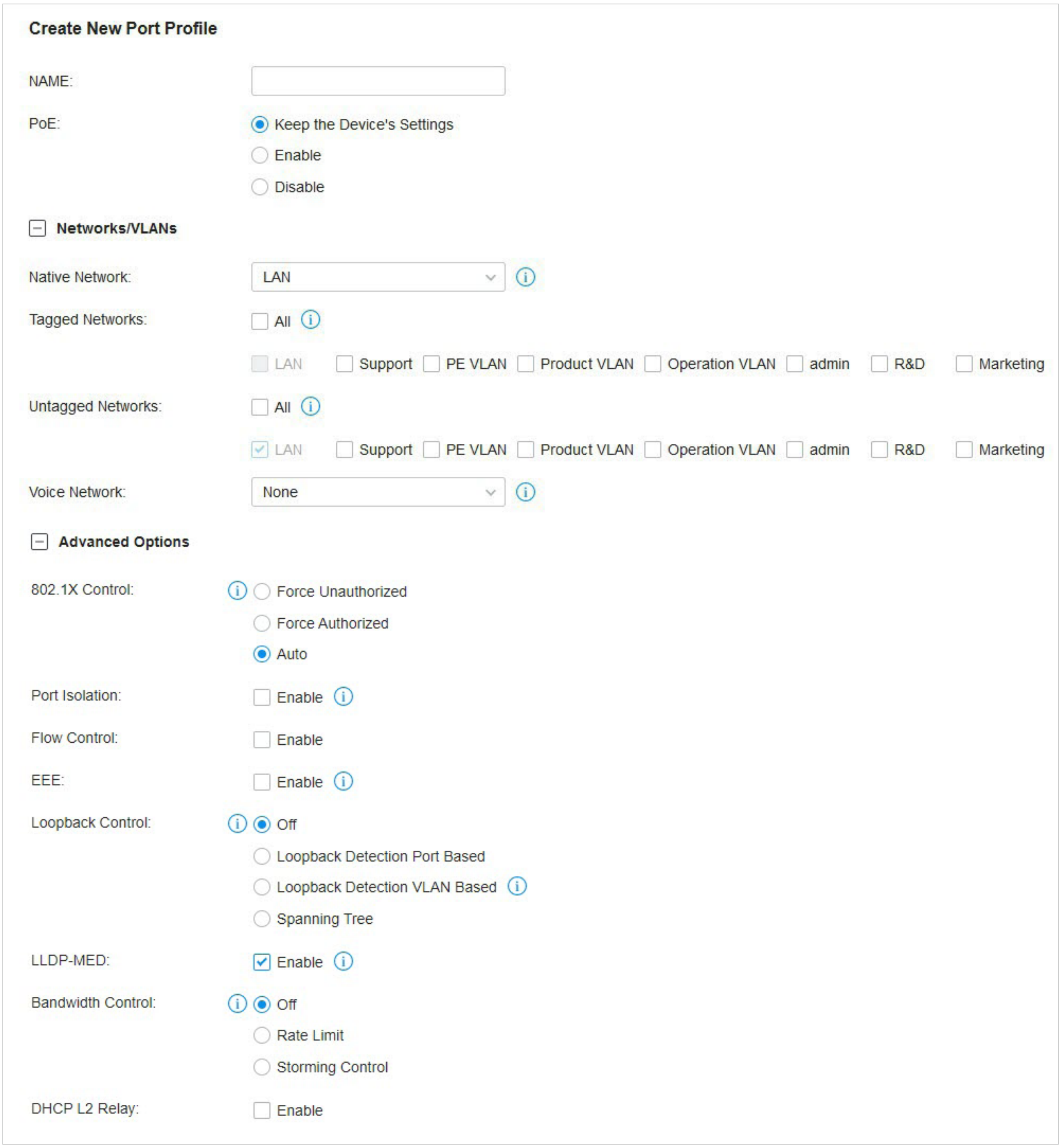
- When a network is created, the system will automatically create a profile with the same name and configure the network as the native network for the profile. In this profile, the network itself is configured as the Untagged Networks, while no networks are configured as Tagged Networks. The profile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

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



NAME	PoE	NATIVE NETWORK	ISOLATION	STORM CONTROL	ACTION
All	Keep the Device's Settings	LAN		Off	👁
Disable	Keep the Device's Settings	None		Off	👁
LAN	Keep the Device's Settings	LAN		Off	👁

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



Create New Port Profile

NAME:

PoE: ● Keep the Device's Settings ○ Enable ○ Disable

Networks/VLANs

Native Network: LAN

Tagged Networks: □ All
□ LAN □ Support □ PE VLAN □ Product VLAN □ Operation VLAN □ admin □ R&D □ Marketing

Untagged Networks: □ All
☑ LAN □ Support □ PE VLAN □ Product VLAN □ Operation VLAN □ admin □ R&D □ Marketing

Voice Network: None

Advanced Options

802.1X Control: ○ Force Unauthorized ○ Force Authorized ● Auto

Port Isolation: □ Enable

Flow Control: □ Enable

EEE: □ Enable

Loopback Control: ● Off ○ Loopback Detection Port Based ○ Loopback Detection VLAN Based ○ Spanning Tree

LLDP-MED: ☑ Enable

Bandwidth Control: ● Off ○ Rate Limit ○ Storming Control

DHCP L2 Relay: □ Enable

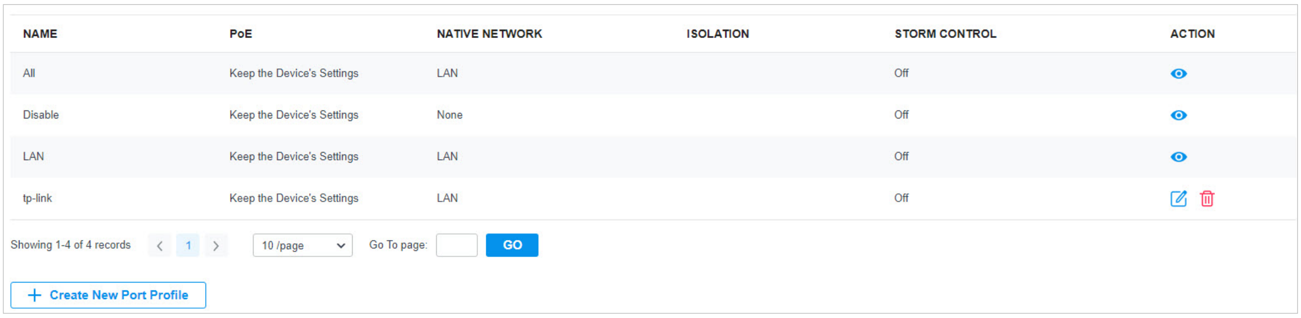
Name	Enter a name to identify the port profile.
PoE	Select the PoE mode for the ports. Keep the Device's Settings: PoE keep enabled or disabled according to the switches' settings. By default, the switches enable PoE on all PoE ports. Enable: Enable PoE on PoE ports. Disable: Disable PoE on PoE ports.

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 switches, 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, enter the site view and 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.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.

Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the VLAN will be blocked. Spanning Tree: Select STP (Spanning Tree Protocal) to prevent loops in the network. STP helps block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. 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 6. 3 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.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.
Format	Select the format of option 82 sub-option value field. Normal: The format of sub-option value field is TLV (type-length-value). Private: The format of sub-option value field is just value.

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.



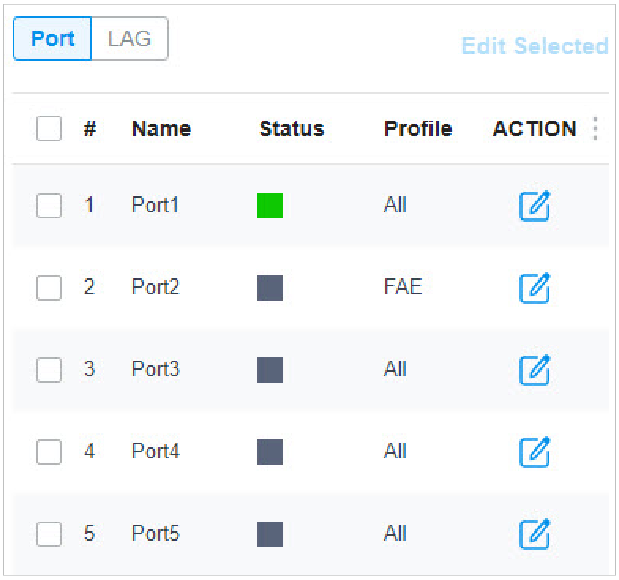
NAME	PoE	NATIVE NETWORK	ISOLATION	STORM CONTROL	ACTION
All	Keep the Device's Settings	LAN		Off	👁
Disable	Keep the Device's Settings	None		Off	👁
LAN	Keep the Device's Settings	LAN		Off	👁
tp-link	Keep the Device's Settings	LAN		Off	✎ 🗑

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

ⓘ Note:

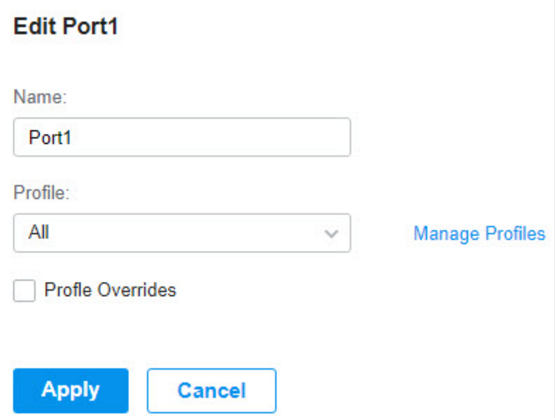
By default, there is a port profile named All, which is assigned to all switch ports by default. In the All profile, all networks except the default network (LAN) are configured as Tagged Network, and the native network is the default network (LAN).

1. Go to Devices, and click 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.



□	#	Name	Status	Profile	ACTION
□	1	Port1	🟩	All	✎
□	2	Port2	■	FAE	✎
□	3	Port3	■	All	✎
□	4	Port4	■	All	✎
□	5	Port5	■	All	✎

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 Chapter 6. Configure and Monitor Omada Managed Devices.



Edit Port1

Name: Port1

Profile: All

□ Profle Overrides

1. 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, MAC Filter, and other advanced settings.

1. 4. 1 Set Up Basic Wireless Networks

Configuration

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

1) Create a WLAN group.

2) Create Wireless Networks

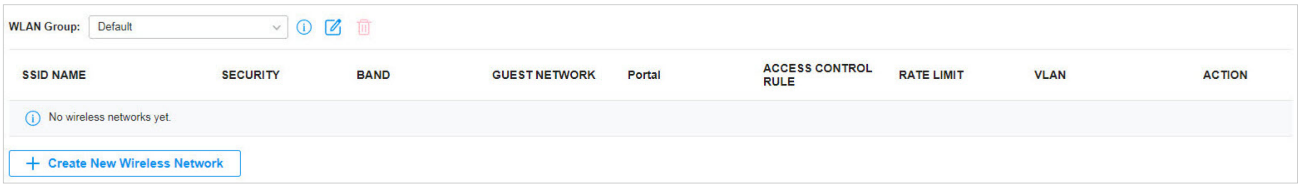
3) Apply the WLAN group to your EAPs

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

Note:

The controller provides a default WLAN group. If you simply want to configure wireless networks for the default WLAN group and apply it to all your EAPs, skip this step.

1. Select a site from the drop-down list of Organization. Go to Settings > Wireless Networks to load the following page.

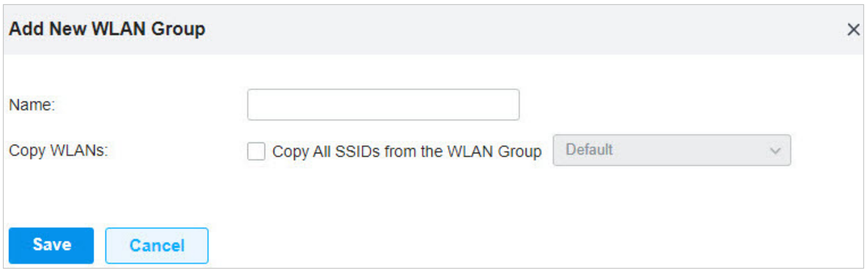


WLAN Group: Default

SSID NAME	SECURITY	BAND	GUEST NETWORK	Portal	ACCESS CONTROL RULE	RATE LIMIT	VLAN	ACTION
No wireless networks yet.								

+ Create New Wireless Network

2. 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.



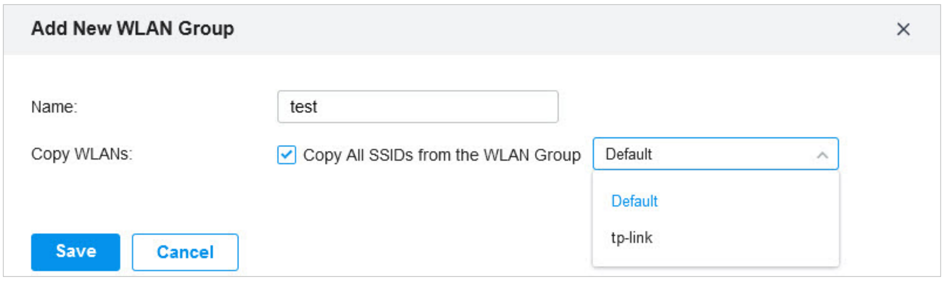
Add New WLAN Group ×

Name:

Copy WLANs: □ Copy All SSIDs from the WLAN Group Default

Save Cancel

3. (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.

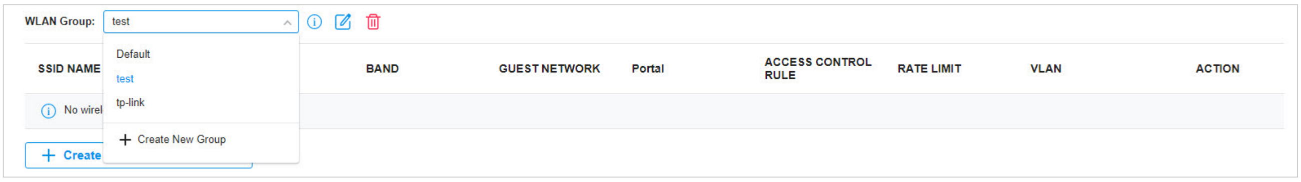


Add New WLAN Group

Name: test

Copy WLANs: ☑ Copy All SSIDs from the WLAN Group: Default

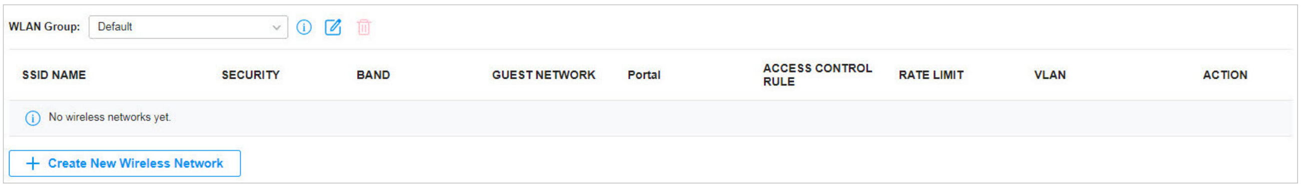
4. Click Save. The new WLAN Group is added to the WLAN Group list. You can select a WLAN Group from the list to further create and configure its wireless networks. You can click ✎ to edit the name of the WLAN Group. You can click 🗑 to delete the WLAN Group.



WLAN Group: test

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.



WLAN Group: Default

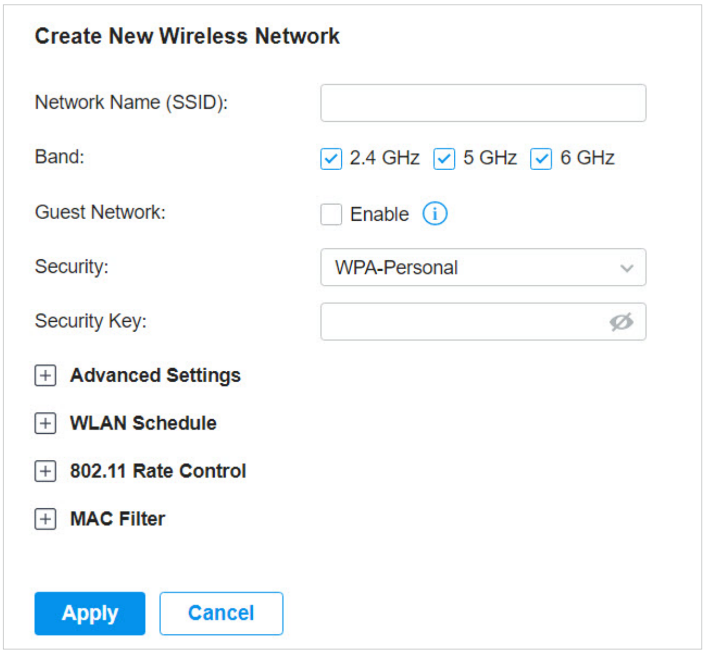
SSID NAME	SECURITY	BAND	GUEST NETWORK	Portal	ACCESS CONTROL RULE	RATE LIMIT	VLAN	ACTION

No wireless networks yet.

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

ⓘ Note:

The 6 GHz band is only available for certain devices.



Create New Wireless Network

Network Name (SSID):

Band: ☑ 2.4 GHz ☑ 5 GHz ☑ 6 GHz

Guest Network: □ Enable ⓘ

Security: WPA-Personal

Security Key:

⊞ **Advanced Settings**

⊞ **WLAN Schedule**

⊞ **802.11 Rate Control**

⊞ **MAC Filter**

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 the radio band(s) 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.

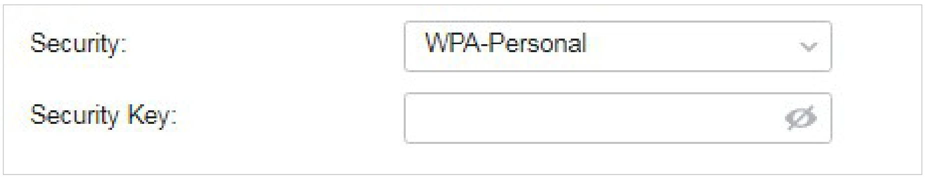
3. Select the security strategy for the wireless network.

- **None**

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

- **WPA-Personal**

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

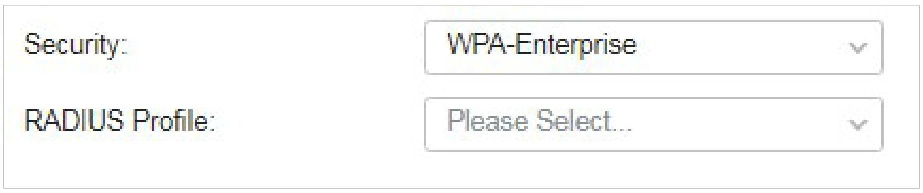


Security: WPA-Personal

Security Key:

- **WPA-Enterprise**

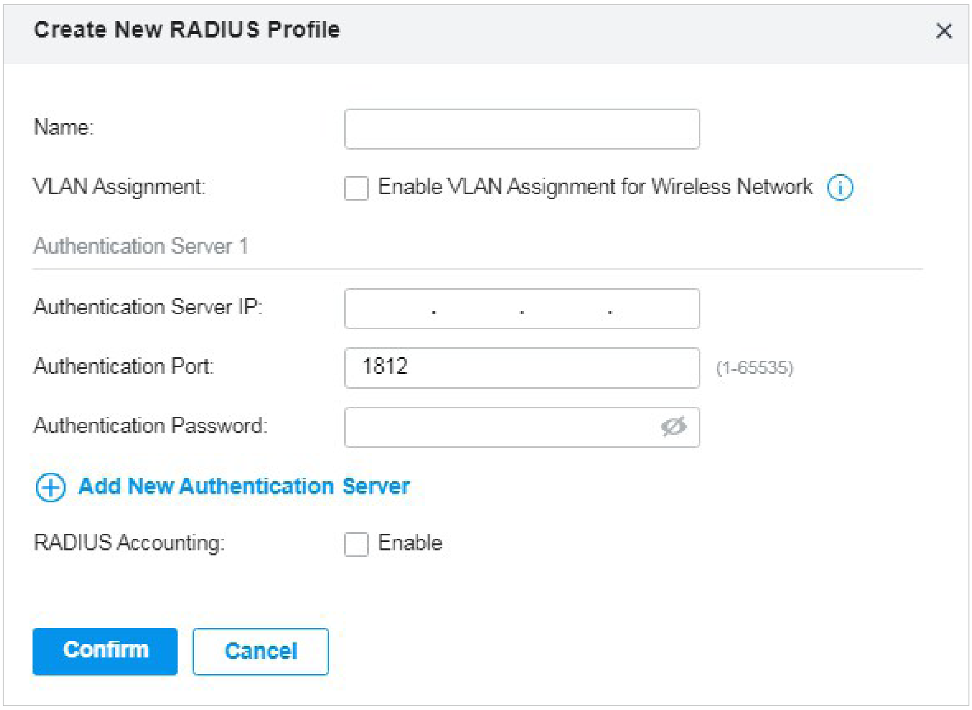
WPA-Enterprise requires an authentication server to authenticate wireless clients, and probably an accounting server to record the traffic statistics.



Security: WPA-Enterprise

RADIUS Profile: Please Select...

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 4. 9 Authentication.



Create New RADIUS Profile

Name:

VLAN Assignment: □ Enable VLAN Assignment for Wireless Network

Authentication Server 1

Authentication Server IP: . . .

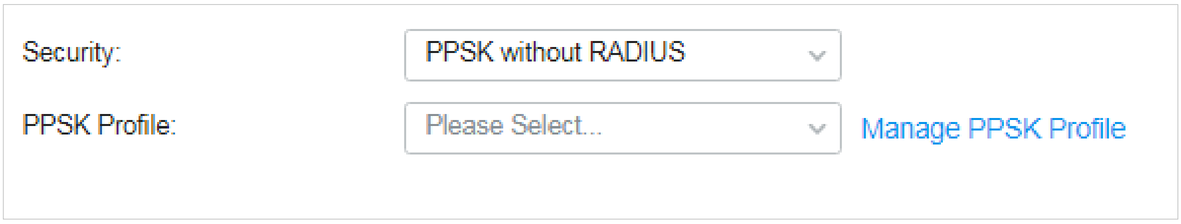
Authentication Port: 1812 (1-65535)

Authentication Password:

RADIUS Accounting: □ Enable

- **PPSK without RADIUS**

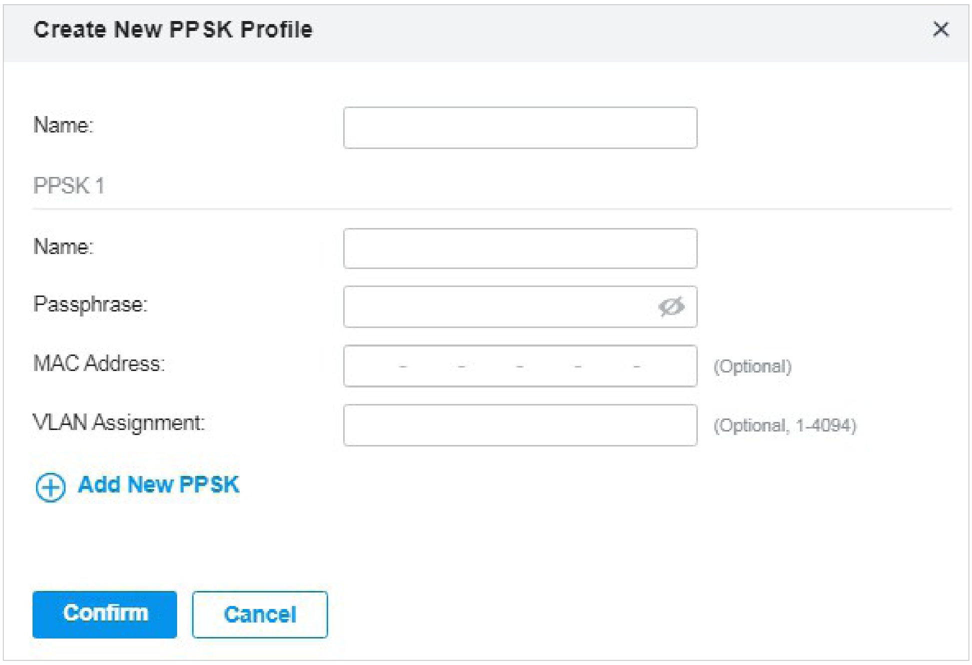
PPSK (private pre-shared key) can provide a unique PSK for each wireless user. Compared with the traditional SSID solution with one password for all users, it is more secure.



Security: PPSK without RADIUS

PPSK Profile: Please Select...

Select a PPSK Profile, which records the PPSK settings. You can create a PPSK Profile by clicking + Create New PPSK Profile from the drop-down list of PPSK Profile. For details, refer to 4. 8. 4 PPSK.


Create New PPSK Profile

Name:

PPSK 1

Name:

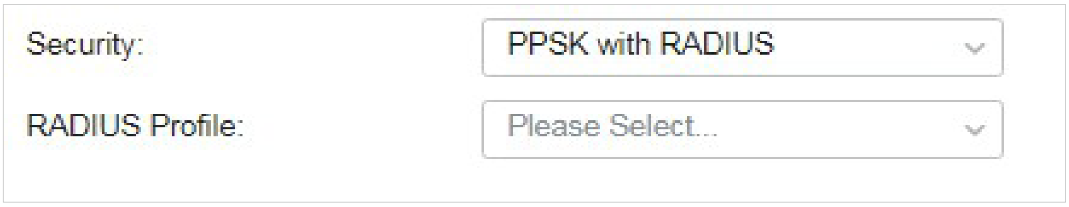
Passphrase:

MAC Address: - - - - - (Optional)

VLAN Assignment: (Optional, 1-4094)

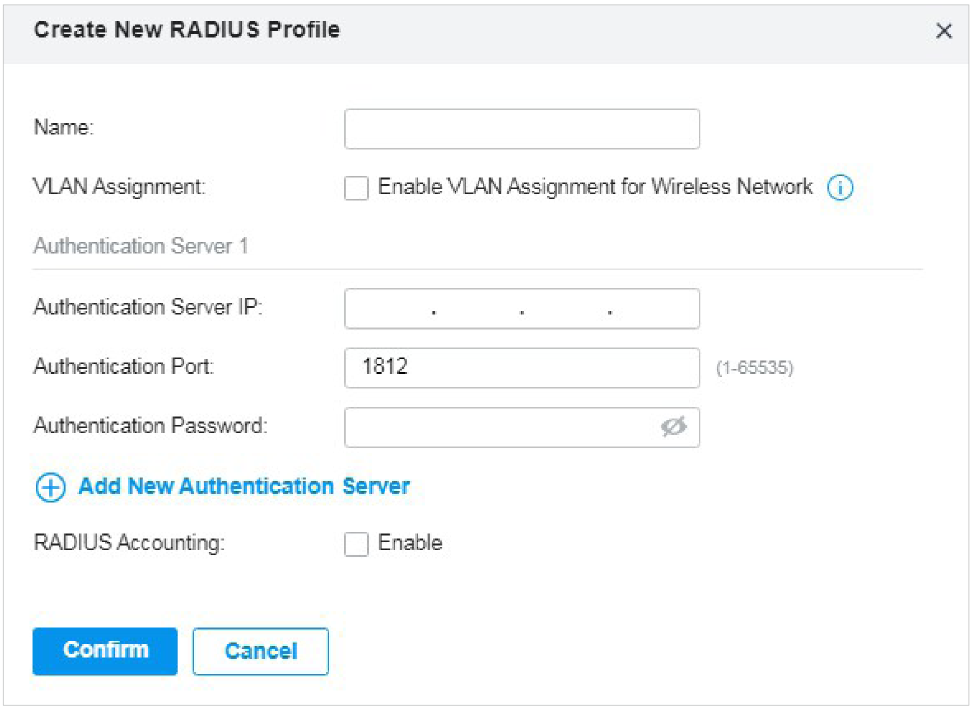
- **PPSK with RADIUS**

  PPSK (private pre-shared key) can provide a unique PSK for each wireless use. PPSK with RADIUS requires an authentication server to authenticate wireless clients and probably an accounting server to record the traffic statistics.


Security: PPSK with RADIUS

RADIUS Profile: Please Select...

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 4. 9 Authentication.

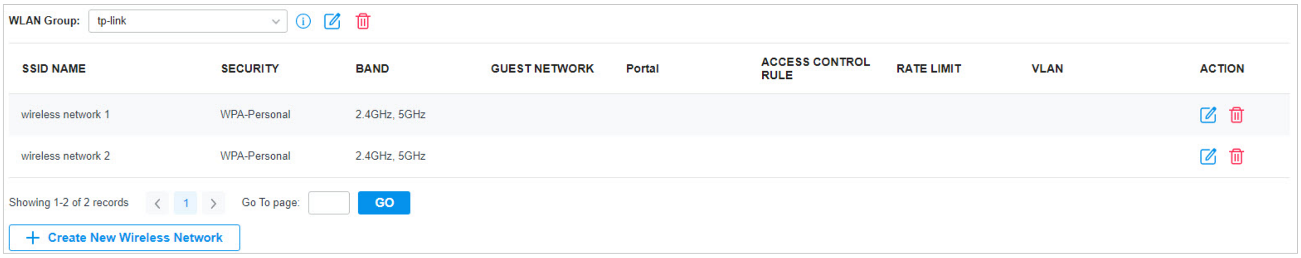


Create New RADIUS Profile ✕

Name:	
VLAN Assignment:	□ Enable VLAN Assignment for Wireless Network ⓘ
Authentication Server 1	
Authentication Server IP:	. . .
Authentication Port:	1812 (1-65535)
Authentication Password:	
⊕ Add New Authentication Server	
RADIUS Accounting:	□ Enable

4. (Optional) You can also configure 4. 4. 2 Advanced Settings, 4. 4. 3 WLAN Schedule, 4. 4. 4 802.11 Rate Control, and 4. 4. 5 MAC Filter according to your needs. Related topics are covered later in this chapter.

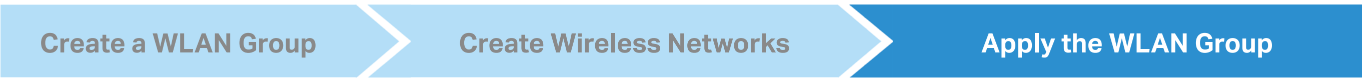
5. Click Apply. The new wireless network is added to the wireless network list under the WLAN group. You can click ✎ in the ACTION column to edit the wireless network. You can click 🗑 in the ACTION column to delete the wireless network.



WLAN Group: tp-link ⓘ ✎ 🗑

SSID NAME	SECURITY	BAND	GUEST NETWORK	Portal	ACCESS CONTROL RULE	RATE LIMIT	VLAN	ACTION
wireless network 1	WPA-Personal	2.4GHz, 5GHz						✎ 🗑
wireless network 2	WPA-Personal	2.4GHz, 5GHz						✎ 🗑

Showing 1-2 of 2 records ‹ 1 › Go To page: GO

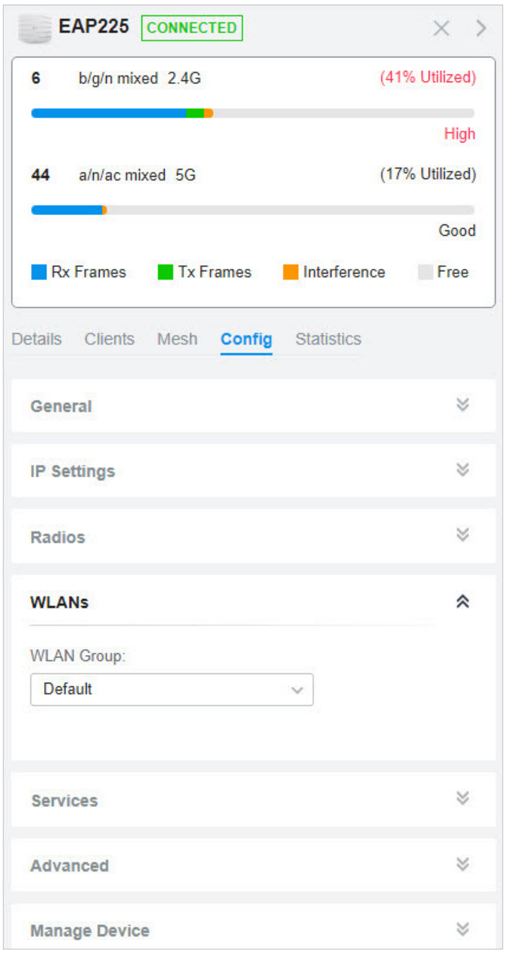


ⓘ Note:

The controller provides a default WLAN group. 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. In the Properties window, go to Config > WLANs, select the WLAN group to apply.



EAP225 CONNECTED

6 b/g/n mixed 2.4G (41% Utilized)

High

44 a/n/ac mixed 5G (17% Utilized)

Good

Rx Frames Tx Frames Interference Free

Details Clients Mesh **Config** Statistics

General

IP Settings

Radios

WLANs

WLAN Group:

Default

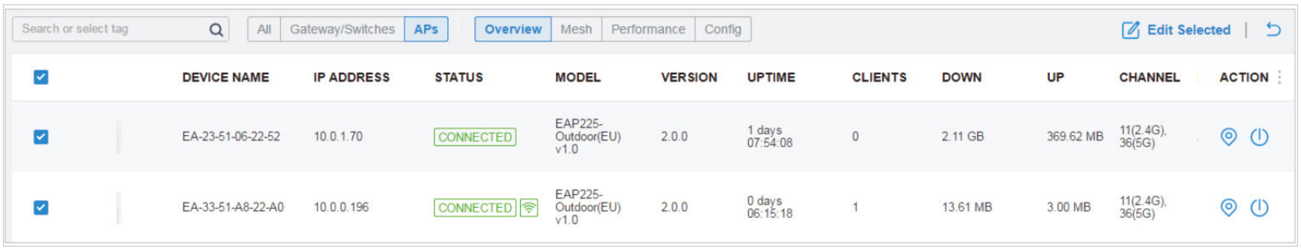
Services

Advanced

Manage Device

- **Apply to EAPs in batch**

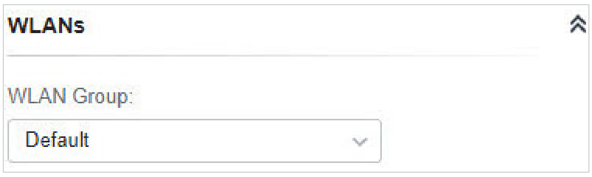
1. Go to Devices, select the APs tab, click Batch Action, and then select Batch Config, check the boxes of EAPs which you want to apply the WLAN group to, and click Done.



Search or select tag | All | Gateway/Switches | APs | Overview | Mesh | Performance | Config | Edit Selected

☑	DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	UPTIME	CLIENTS	DOWN	UP	CHANNEL	ACTION
☑	EA-23-51-06-22-52	10.0.1.70	CONNECTED	EAP225-Outdoor(EU) v1.0	2.0.0	1 days 07:54:08	0	2.11 GB	369.62 MB	11(2.4G), 36(5G)	
☑	EA-33-51-A8-22-A0	10.0.0.196	CONNECTED	EAP225-Outdoor(EU) v1.0	2.0.0	0 days 06:15:18	1	13.61 MB	3.00 MB	11(2.4G), 36(5G)	

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



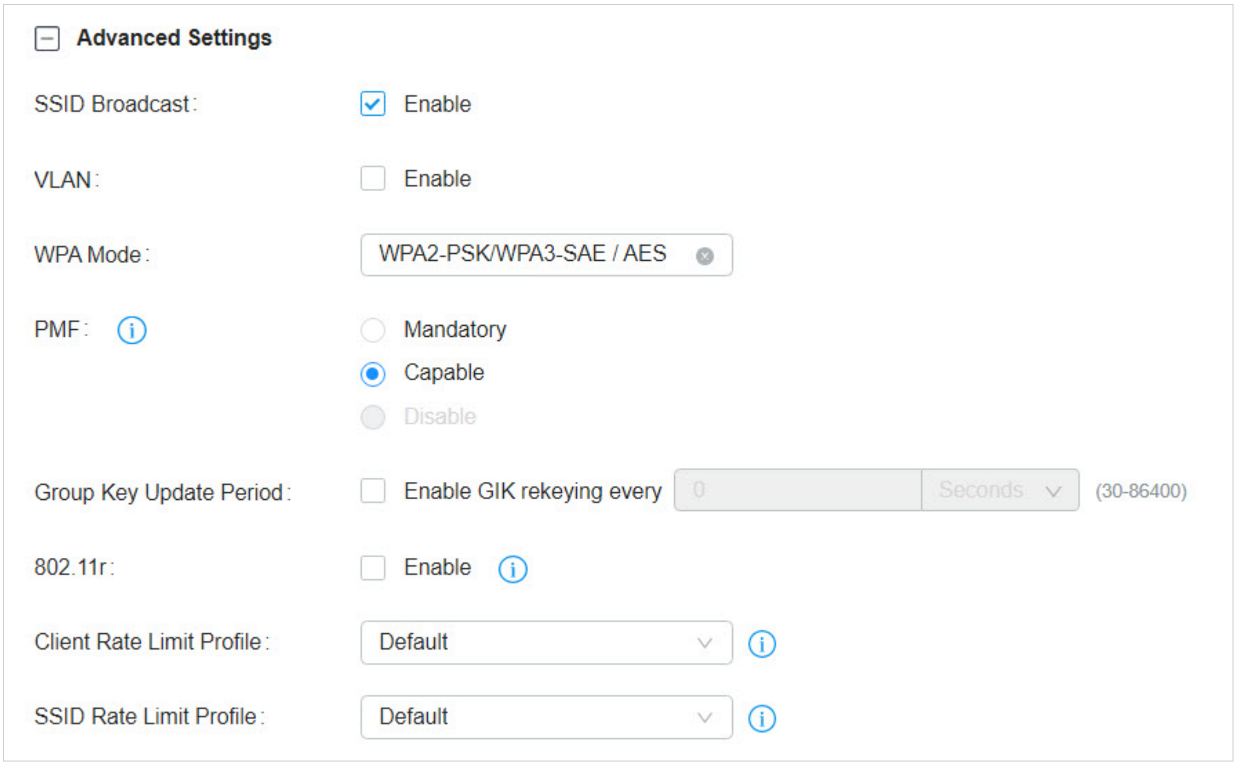
WLANs

WLAN Group:

Default

1. 4. 2 Advanced Settings

Select a site from the drop-down list of Organization. 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.



⊟ **Advanced Settings**

SSID Broadcast:	☑ Enable
VLAN:	□ Enable
WPA Mode:	WPA2-PSK/WPA3-SAE / AES
PMF: ⓘ	○ Mandatory ● Capable ○ Disable
Group Key Update Period:	□ Enable GIK rekeying every 0 Seconds (30-86400)
802.11r:	□ Enable ⓘ
Client Rate Limit Profile:	Default ⓘ
SSID Rate Limit Profile:	Default ⓘ

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.
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. AES: AES stands for Advanced Encryption Standard. Auto: EAPs automatically decide the encryption type in the authentication process.

PMF	Protected Management Frames (PMF) provide protection for unicast and multicast management action frames. When Mandatory is selected, non-PMF-capable clients may fail to connect to the network. Disable: Disables PMF for a network. It is not recommended to use this setting, only in case non-PMF-capable clients experience connection issues with the “Capable” option. Capable: Both types of clients, capable of PMF or not, can connect to the network. Clients capable of PMF will negotiate it with the AP. Mandatory: Only PMF-capable clients can connect to the network.
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.
802.11r	Enable this feature to allow faster roaming when both the AP and client have 802.11r capabilities. Currently 802.11r does not support WPA3 encryption.
Client Rate Limit Profile	Specify the profile to limit the download and upload rates of each client to balance bandwidth usage. You can use the default profile or custom a profile.
SSID Rate Limit Profile	Specify the profile to limit the download and upload rates of each wireless band. Bandwidth is shared among all clients connected to the same wireless band of the same AP. You can use the default profile or custom a profile. ⓘ Note: This feature requires new firmware updates for Omada APs, and the rate limit settings will only take effect on those APs running firmware that supports the feature.

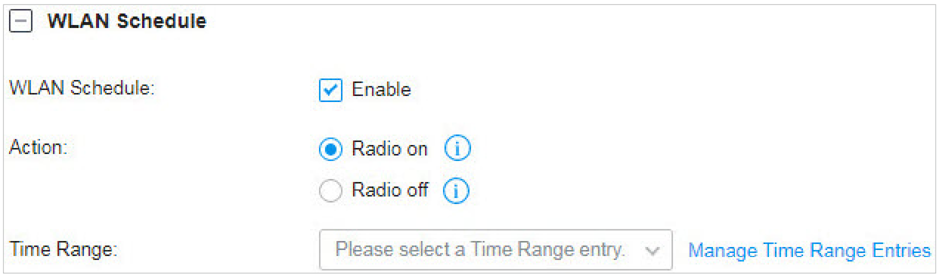
1. 4. 3 WLAN Schedule

Overview

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

Configuration

Select a site from the drop-down list of Organization. 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.



⊟ **WLAN Schedule**

WLAN Schedule: ☑ Enable

Action: ● Radio on ⓘ ○ Radio off ⓘ

Time Range: Please select a Time Range entry. Manage Time Range Entries

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 4. 8 Create Profiles.

1. 4. 4 802.11 Rate Control

Overview

ⓘ Note:

802.11 Rate Control is only available for certain devices.

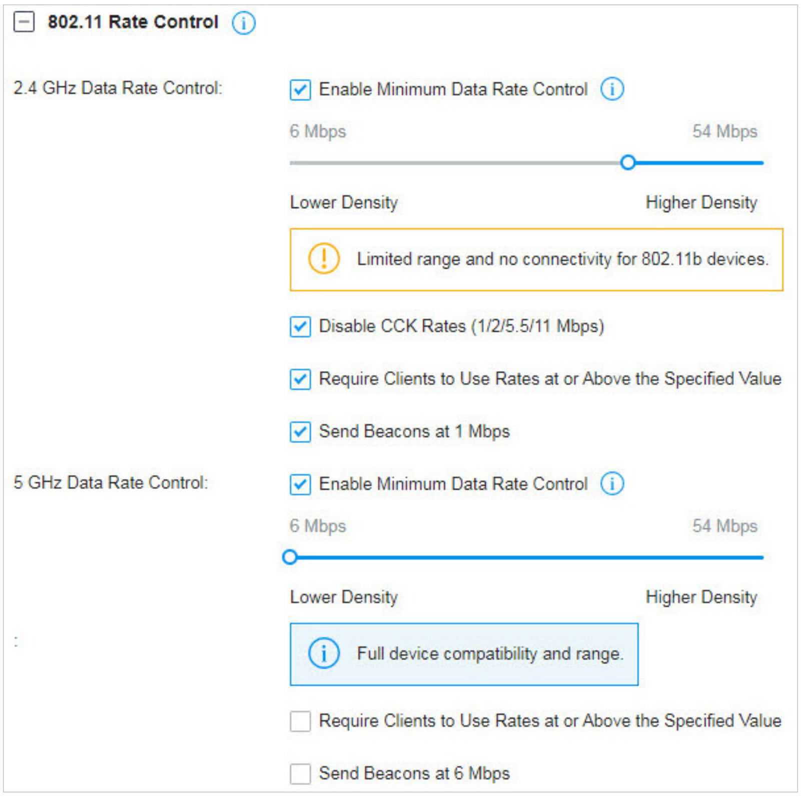
802.11 Rate Control can improve performance for higher-density networks by disabling lower bit rates and only allowing the higher. However, 802.11 Rate Control might make some legacy devices incompatible with your networks, and limit the range of your wireless networks.

Configuration

Select a site from the drop-down list of Organization. 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 one or multiple bands 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.

Note:

The 6 GHz band is only available for certain devices.



802.11 Rate Control

2.4 GHz Data Rate Control: ☑ Enable Minimum Data Rate Control

6 Mbps — 54 Mbps

Lower Density — Higher Density

Limited range and no connectivity for 802.11b devices.

☑ Disable CCK Rates (1/2/5.5/11 Mbps)

☑ Require Clients to Use Rates at or Above the Specified Value

☑ Send Beacons at 1 Mbps

5 GHz Data Rate Control: ☑ Enable Minimum Data Rate Control

6 Mbps — 54 Mbps

Lower Density — Higher Density

Full device compatibility and range.

□ Require Clients to Use Rates at or Above the Specified Value

□ Send Beacons at 6 Mbps

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 specified on the minimum data rate controller slider.
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.

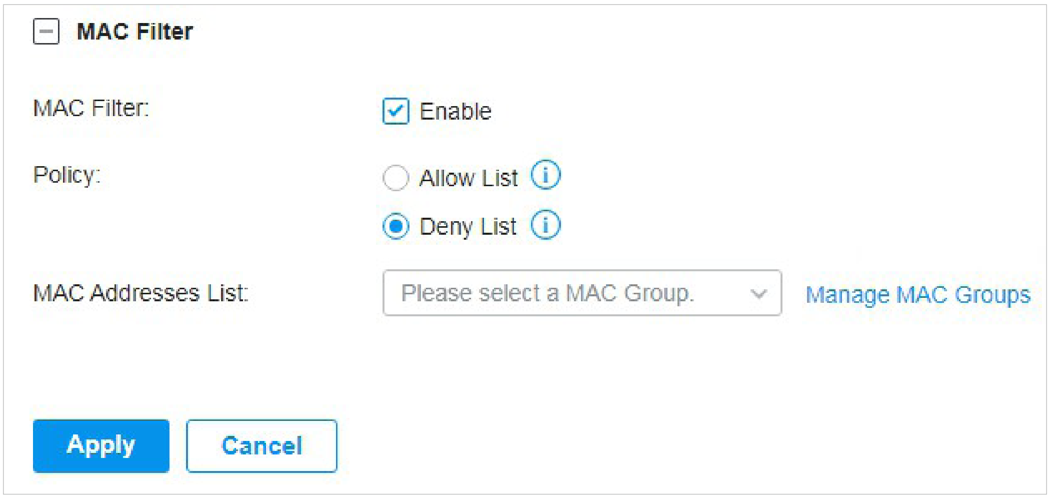
1. 4. 5 MAC Filter

Overview

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

Configuration

Select a site from the drop-down list of Organization. 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.



⊟ **MAC Filter**

MAC Filter: ☑ Enable

Policy: ○ Allow List ⓘ
● Deny List ⓘ

MAC Addresses List: Please select a MAC Group.

Policy	Allow List: Allow the connection of the clients whose MAC addresses are in the specified MAC Address List, while blocking others. Deny List: 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 4. 8 Create Profiles.

1. 4. 6 AI WLAN Optimization

Overview

AI WLAN Optimization helps improve the wireless network performance. With the AI WLAN Optimization feature, the controller will detect WiFi interference and check the wireless environment. Based on the environmental factors including traffic, network topology, deployment size, and client factors, the controller can determine the optimum operation channels and power for the access points (APs), and thus ensures that wireless clients of each AP can enjoy better WiFi experience.

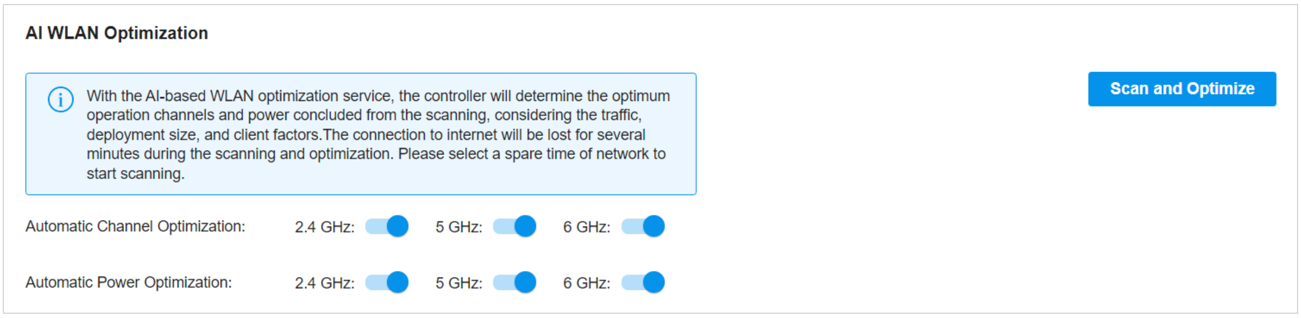
Configuration

ⓘ Note:

1. WiFi experience may be influenced during optimization, please select the spare time to scan and optimize to reduce its impact on user experience.
2. Because the APs should stay connected during optimization, please set a different time for AI WLAN Optimization and Reboot Schedule. It is recommended to stagger at least 10 minutes to avoid dissatisfactory results.

1. Select a site from the drop-down list of Organization. Go to Settings > Wireless Networks > AI WLAN Optimization.

2. Enable Automatic Channel Optimization and Automatic Power Optimization on the desired frequency bands, then click Scan and Optimize. The controller will scan the wireless environment to conclude the optimum operation channels and power for the APs.



AI WLAN Optimization

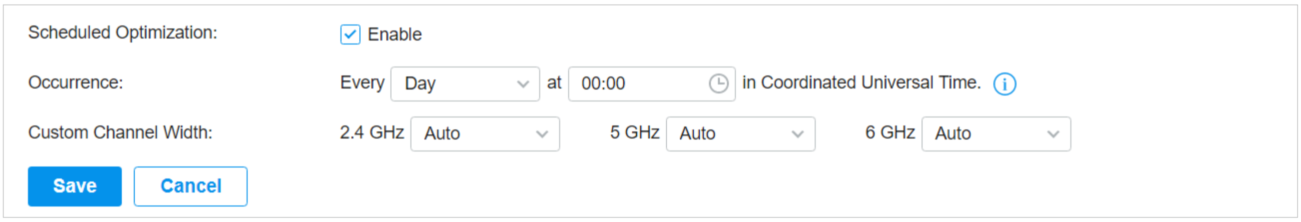
With the AI-based WLAN optimization service, the controller will determine the optimum operation channels and power concluded from the scanning, considering the traffic, deployment size, and client factors.The connection to internet will be lost for several minutes during the scanning and optimization. Please select a spare time of network to start scanning.

Automatic Channel Optimization: 2.4 GHz: ● 5 GHz: ● 6 GHz: ●

Automatic Power Optimization: 2.4 GHz: ● 5 GHz: ● 6 GHz: ●

You can view the optimization results in the Optimization Log.

3. (Optional) Set schedules for WLAN optimization, and click Save.



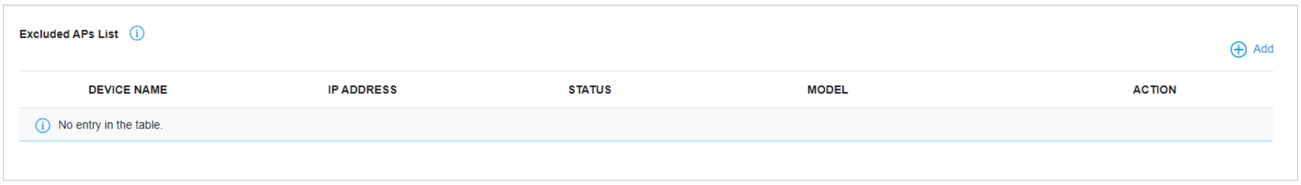
Scheduled Optimization: ☑ Enable

Occurrence: Every Day at 00:00 in Coordinated Universal Time.

Custom Channel Width: 2.4 GHz Auto 5 GHz Auto 6 GHz Auto

Scheduled Optimization	Enable scheduled optimization, and the controller will automatically adjust the channels for the APs on a regular basis.
Occurrence	Set the schedule for regular WLAN optimization.
Custom Channel Width	Select the channel width for each band, and the optimization will maintain the selected channel width.

4. (Optional) In the Excluded APs List, click Add to add the APs that will be excluded from AI WLAN Optimization. The following APs will be added in the list automatically: APs in the mesh network and APs with unsupported firmware.



Excluded APs List

DEVICE NAME	IP ADDRESS	STATUS	MODEL	ACTION
No entry in the table.				

1. 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 4. 5. 1 ACL, 4. 5. 2 URL Filtering, and 4. 5. 3 Attack Defense,4. 5. 4 Firewall, which implement policies and controls on multiple layers of defenses in the network.

1. 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

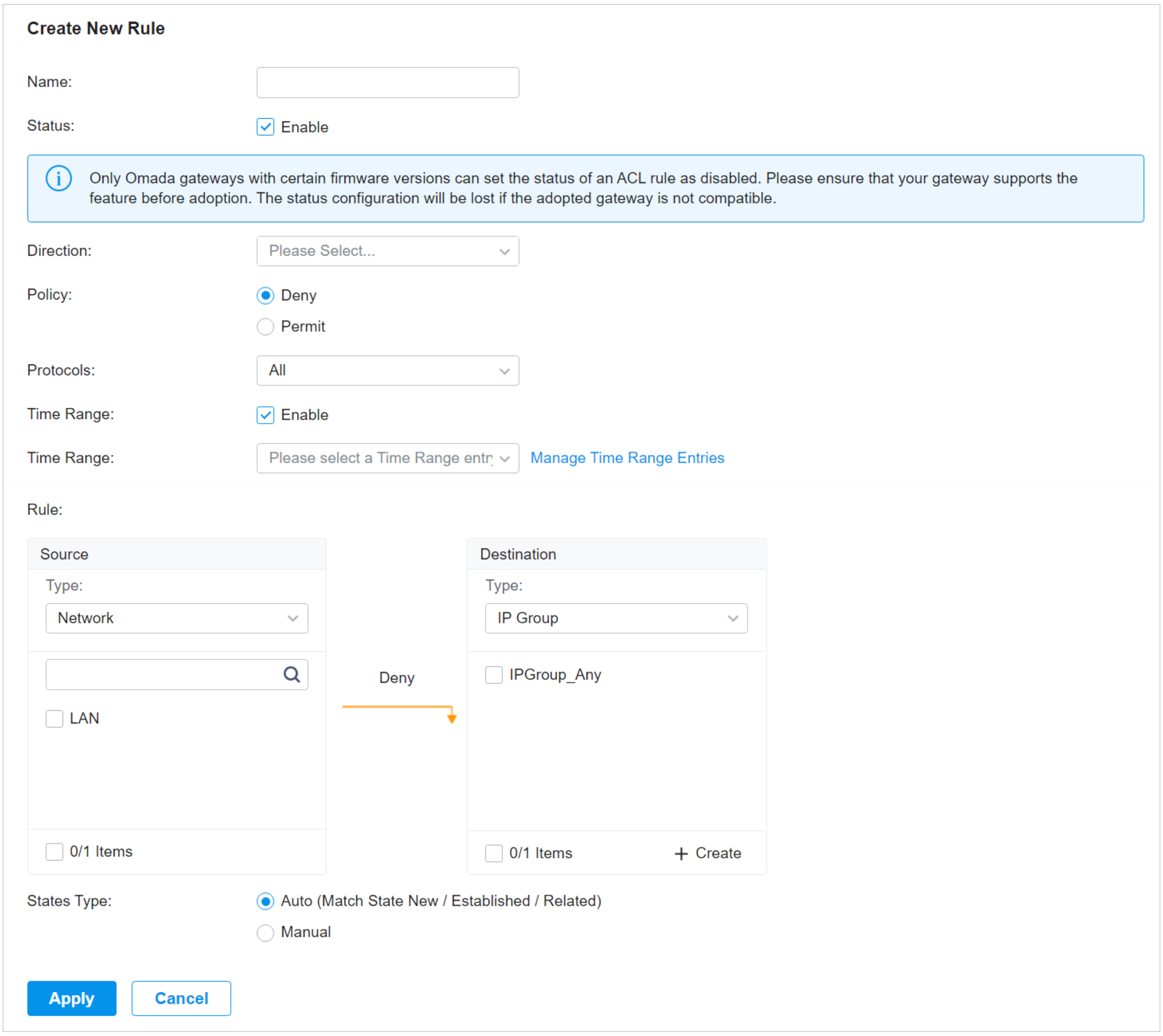
To complete the ACL configuration, follow these steps:

1) Create an ACL with the specified type.

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

■ **Configuring Gateway ACL**

1. Select a site from the drop-down list of Organization. Go to Settings > Network Security > ACL. On Gateway ACL tab, click + Create New Rule to load the following page.



Create New Rule

Name:

Status: ☑ Enable

ⓘ Only Omada gateways with certain firmware versions can set the status of an ACL rule as disabled. Please ensure that your gateway supports the feature before adoption. The status configuration will be lost if the adopted gateway is not compatible.

Direction: Please Select...

Policy: ● Deny ○ Permit

Protocols: All

Time Range: ☑ Enable

Time Range: Please select a Time Range entr Manage Time Range Entries

Rule:

States Type: ● Auto (Match State New / Established / Related) ○ Manual

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.
Direction	Select the WAN port or a VPN entry. (Each VPN entry will have a corresponding VLAN)

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.
Time Range	Select the checkbox to enable time-based ACL. You can create a time range or select an existing time range for the ACL rule to take effect.

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:

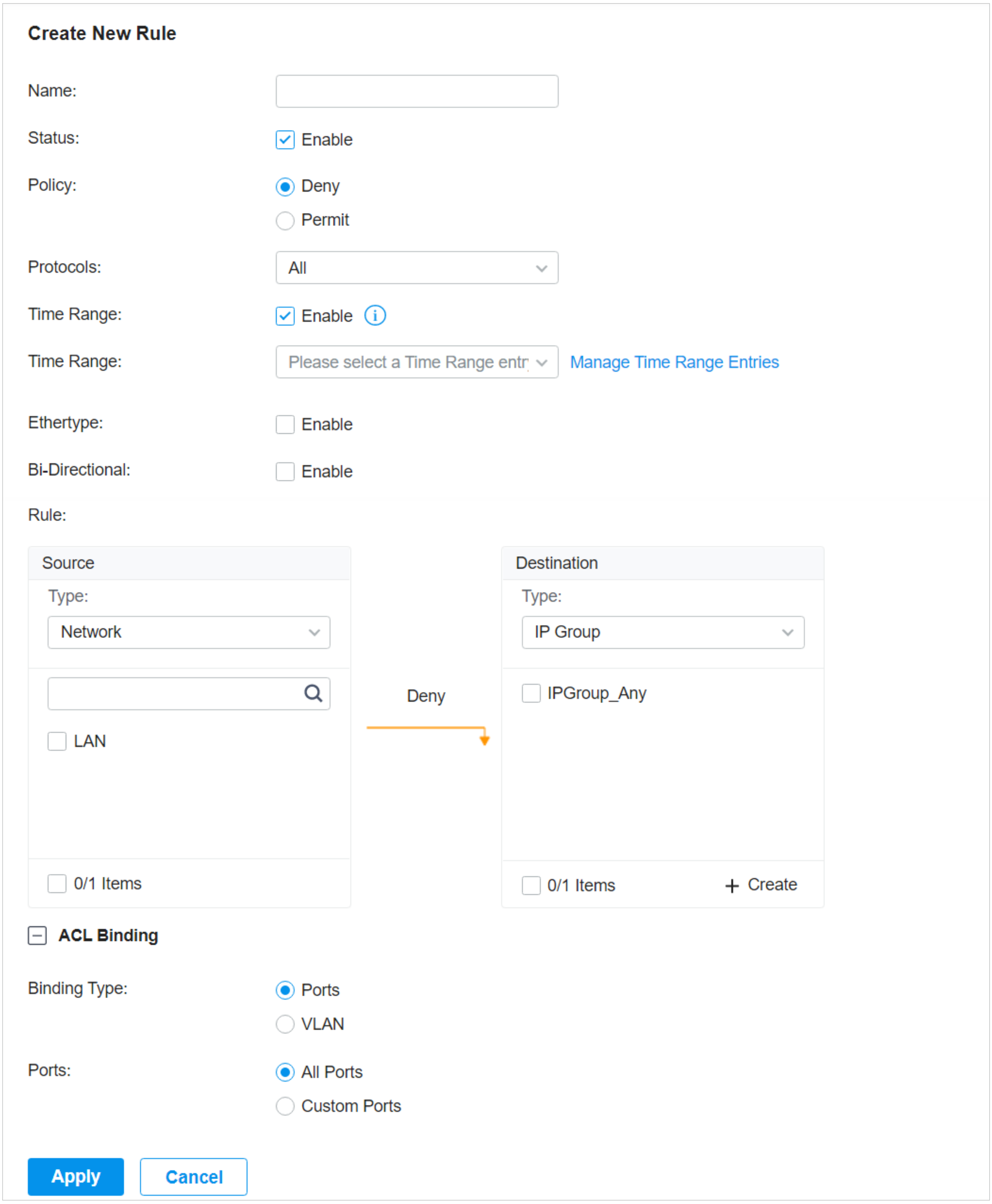
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the destination IP address of the packet is in the IP Group.
IP-Port Group	Select the IP-Port Group you have 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.
Gateway Management Page	This option will allow/block LAN network devices to access the gateway management page.

Set the States Type according to your needs:

States Type	Determine the type of stateful ACL rule. It is recommended to use the default Auto type. Auto (Match Sate New/Established/Related): Match the new, established, and related connection states. Manual: If selected, you can manually specify the connection states to match. Match State New: Match the connections of the initial state. For example, a SYN packet arrives in a TCP connection, or the router only receives traffic in one direction. Match State Established: Match the connections that have been established. In other words, the firewall has seen the bidirectional communication of this connection. Match State Related: Match the associated sub-connections of a main connection, such as a connection to a FTP data channel.

- **Configuring Switch ACL**

1. Select a site from the drop-down list of Organization. Go to Settings > Network Security > ACL. Under the Switch ACL tab, click + Create New Rule to load the following page.



Create New Rule

Name:	
Status:	☑ Enable
Policy:	● Deny ○ Permit
Protocols:	All
Time Range:	☑ Enable
Time Range:	Please select a Time Range entr Manage Time Range Entries
Ethertype:	□ Enable
Bi-Directional:	□ Enable
Rule:	

Source		Destination
Type: Network	Deny	Type: IP Group
□ LAN		□ IPGroup_Any
□ 0/1 Items		□ 0/1 Items + Create

ACL Binding

Binding Type:	● Ports ○ VLAN
Ports:	● All Ports ○ Custom Ports

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.
Time Range	Select the checkbox to enable time-based ACL. You can create a time range or select an existing time range for the ACL rule to take effect.
Ethertype	Click the checkbox if you want the switch to check the ethertype of the packets, and configure the Ethertype based on needs.
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.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 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 IPv6 Group.

IPv6-Port Group

Select the IPv6-Port Group you have created. If no IPv6-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 IPv6-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:

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.

IPv6 Group

Select the IPv6 Group you have created. If no IPv6 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 IPv6 Group.

IPv6-Port Group

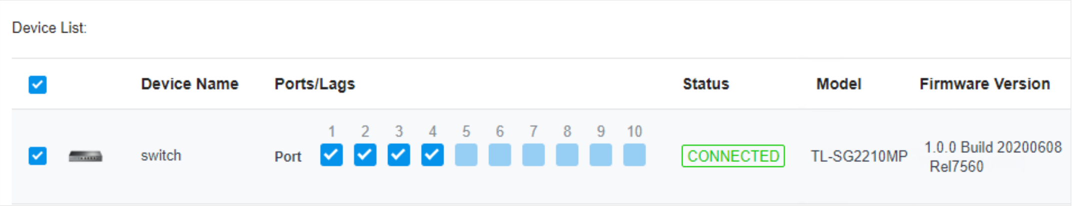
Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address and port number of the packet are in the IPv6-Port Group.

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.



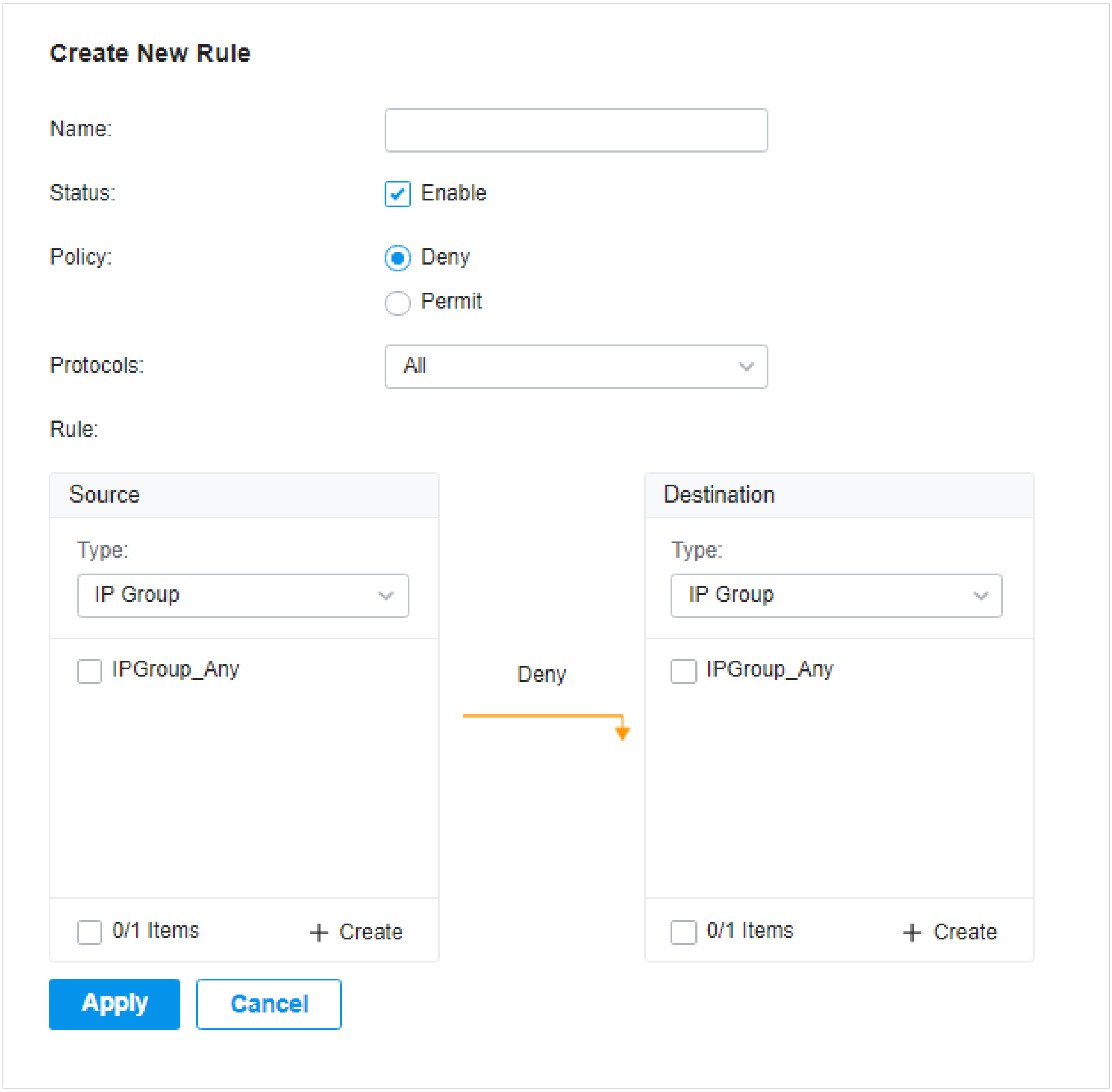
Device List:

☑	Device Name	Ports/Lags	Status	Model	Firmware Version
☑	switch	Port 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □	CONNECTED	TL-SG2210MP	1.0.0 Build 20200608 Rel7560

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. Select a site from the drop-down list of Organization. Go to Settings > Network Security > ACL. Under the EAP ACL tab, click + Create New Rule to load the following page.



Create New Rule

Name:

Status: ☑ Enable

Policy: ● Deny ○ Permit

Protocols: All

Rule:

Source — Type: IP Group — □ IPGroup_Any — □ 0/1 Items

Destination — Type: IP Group — □ IPGroup_Any — □ 0/1 Items

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.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 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 IPv6 Group.
IPv6-Port Group	Select the IPv6-Port Group you have created. If no IPv6-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 IPv6-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:

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.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 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 IPv6 Group.
IPv6-Port Group	Select the IPv6-Port Group you have created. If no IPv6-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 IPv6-Port Group.

1. 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

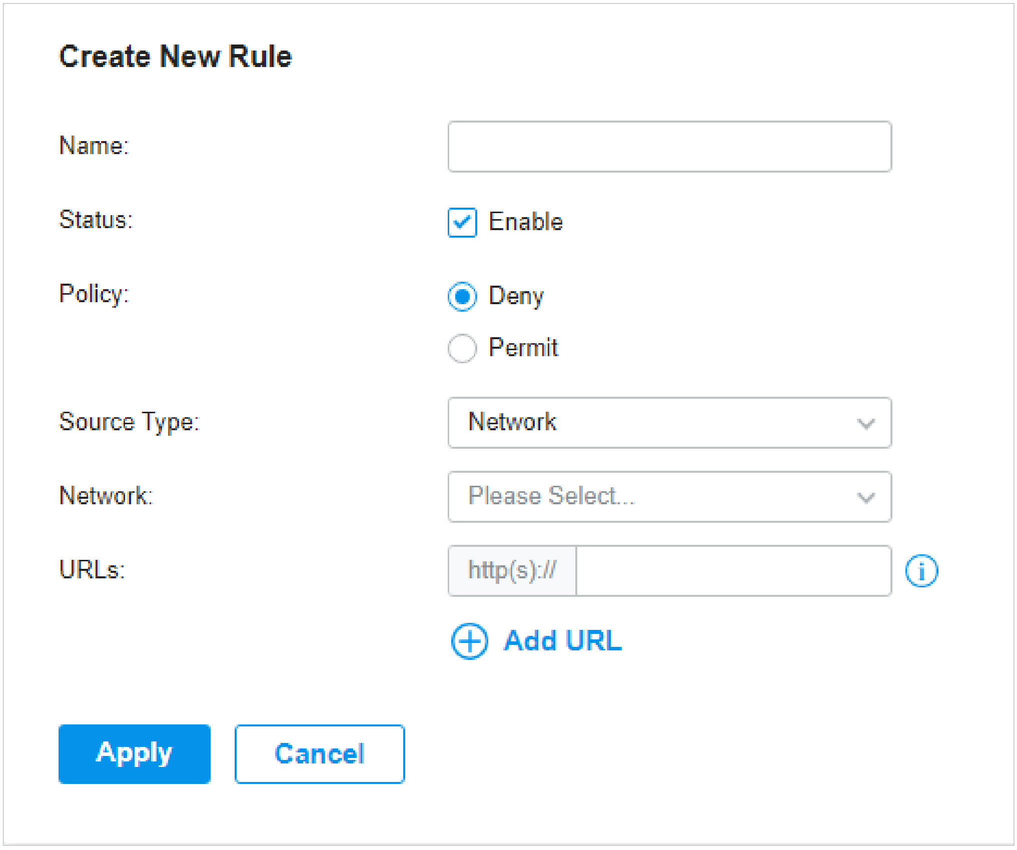
To complete the URL Filtering configuration, follow these steps:

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. Select a site from the drop-down list of Organization. Go to Settings > Network Security > URL Filtering. Under the Gateway Rules tab, click + Create New Rule to load the following page.



Create New Rule

Name:

Status: ☑ Enable

Policy: ● Deny ○ Permit

Source Type: Network

Network: Please Select...

URLs: http(s)://

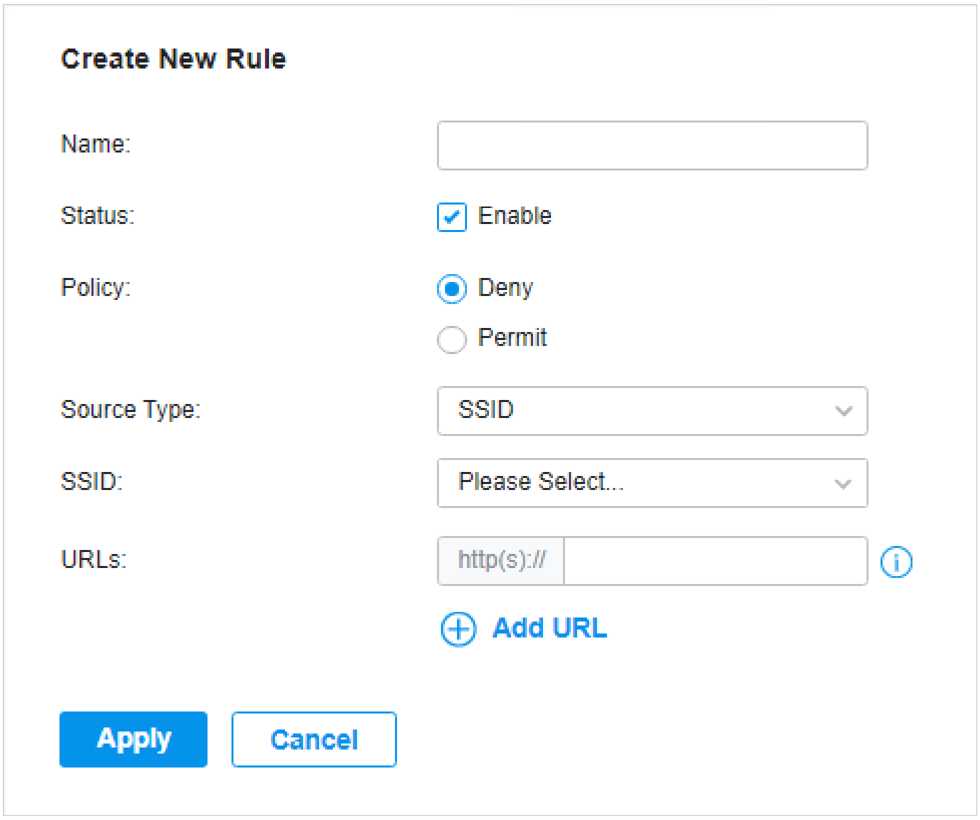
2. Define filtering criteria of the rule, including source and URLs, and determine whether to forward the matched packets. Refer to the following table to configure the required parameters and click Apply.

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. Select a site from the drop-down list of Organization. Go to Settings > Network Security > URL Filtering. On EAP Rules tab, click + Create New Rule to load the following page.



Create New Rule

Name:

Status: ☑ Enable

Policy: ● Deny ○ Permit

Source Type: SSID

SSID: Please Select...

URLs: http(s)://

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.

1. 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.

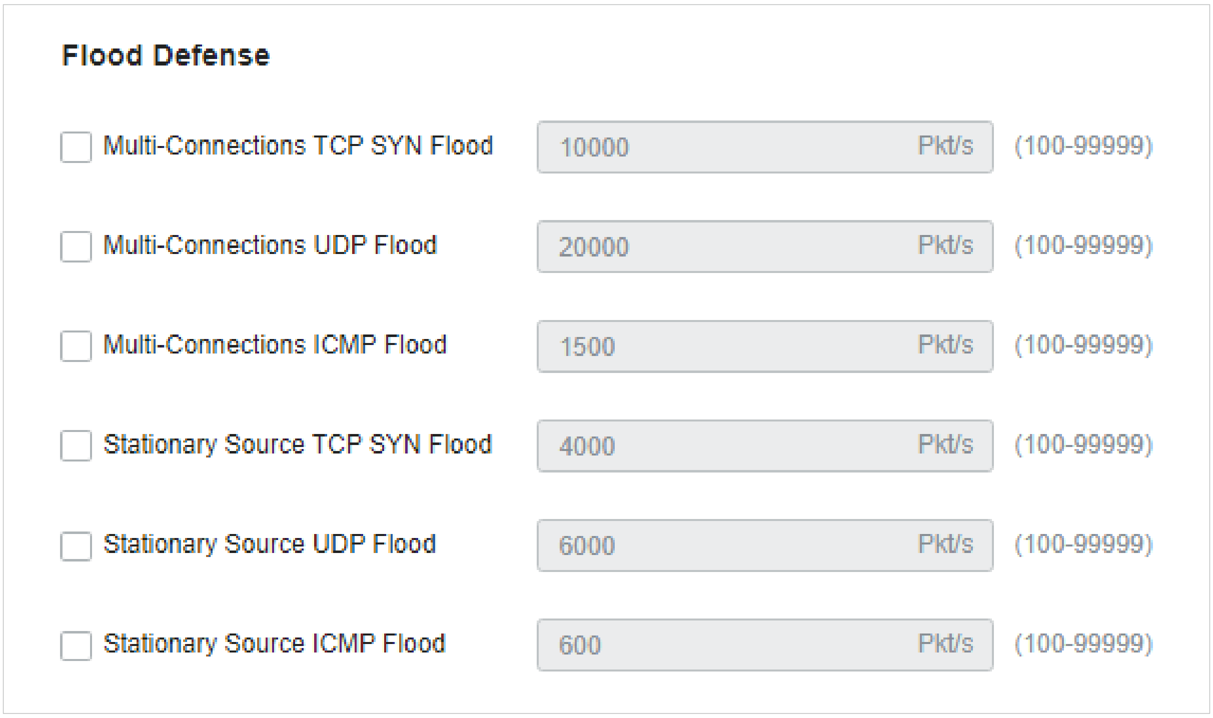
- **Packet Anomaly Defense**

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**

Select a site from the drop-down list of Organization. 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.



Flood Defense

□ Multi-Connections TCP SYN Flood 10000 Pkt/s (100-99999)

□ Multi-Connections UDP Flood 20000 Pkt/s (100-99999)

□ Multi-Connections ICMP Flood 1500 Pkt/s (100-99999)

□ Stationary Source TCP SYN Flood 4000 Pkt/s (100-99999)

□ Stationary Source UDP Flood 6000 Pkt/s (100-99999)

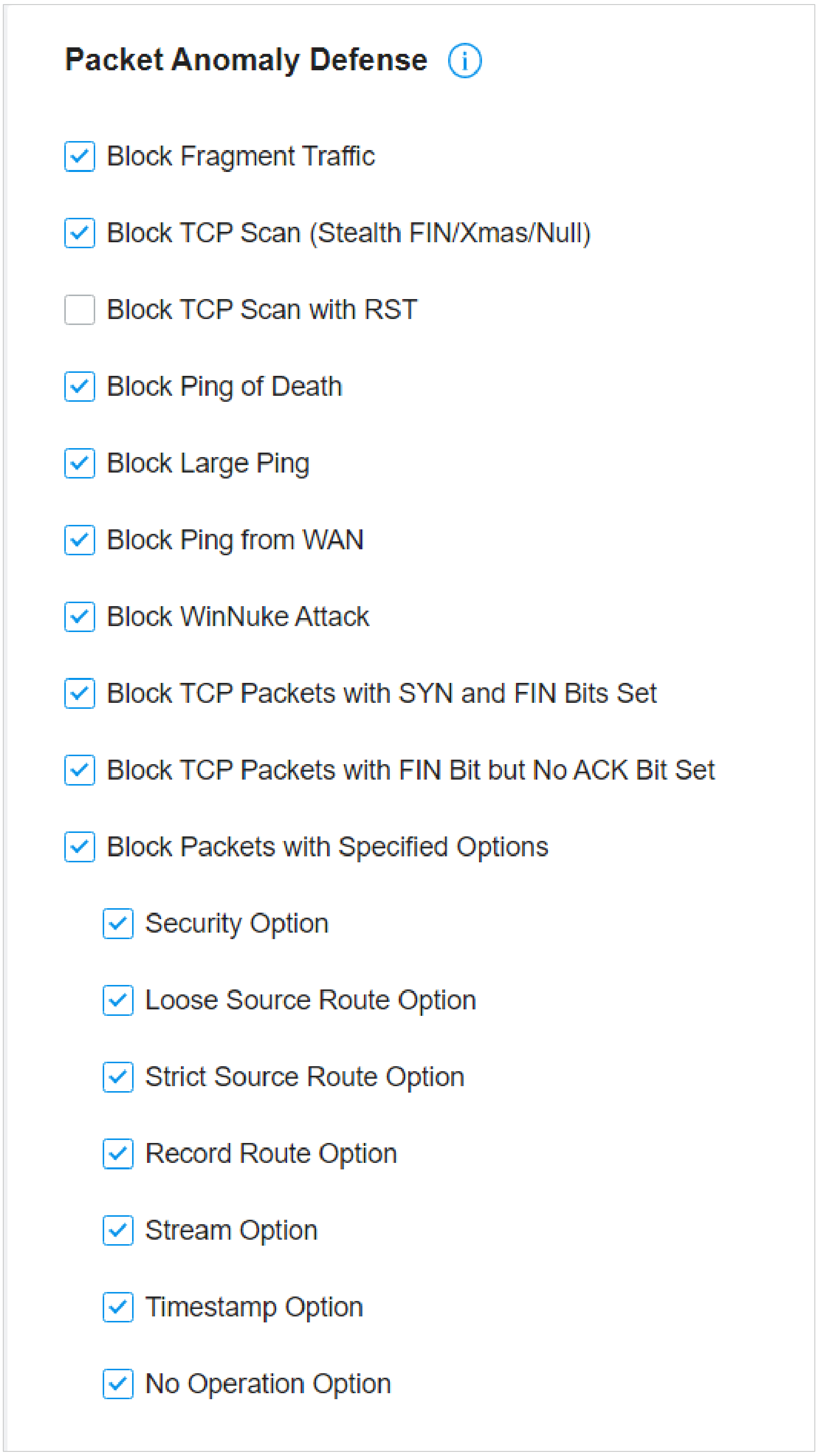
□ Stationary Source ICMP Flood 600 Pkt/s (100-99999)

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**

Select a site from the drop-down list of Organization. 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.



Packet Anomaly Defense ⓘ

- ☑ Block Fragment Traffic
- ☑ Block TCP Scan (Stealth FIN/Xmas/Null)
- □ Block TCP Scan with RST
- ☑ Block Ping of Death
- ☑ Block Large Ping
- ☑ Block Ping from WAN
- ☑ Block WinNuke Attack
- ☑ Block TCP Packets with SYN and FIN Bits Set
- ☑ Block TCP Packets with FIN Bit but No ACK Bit Set
- ☑ Block Packets with Specified Options
  - ☑ Security Option
  - ☑ Loose Source Route Option
  - ☑ Strict Source Route Option
  - ☑ Record Route Option
  - ☑ Stream Option
  - ☑ Timestamp Option
  - ☑ No Operation Option

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 TCP Scan with RST	With this option enabled, the gateway will respond to RST messages. It is disabled by default.
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.

1. 5. 4 Firewall

Overview

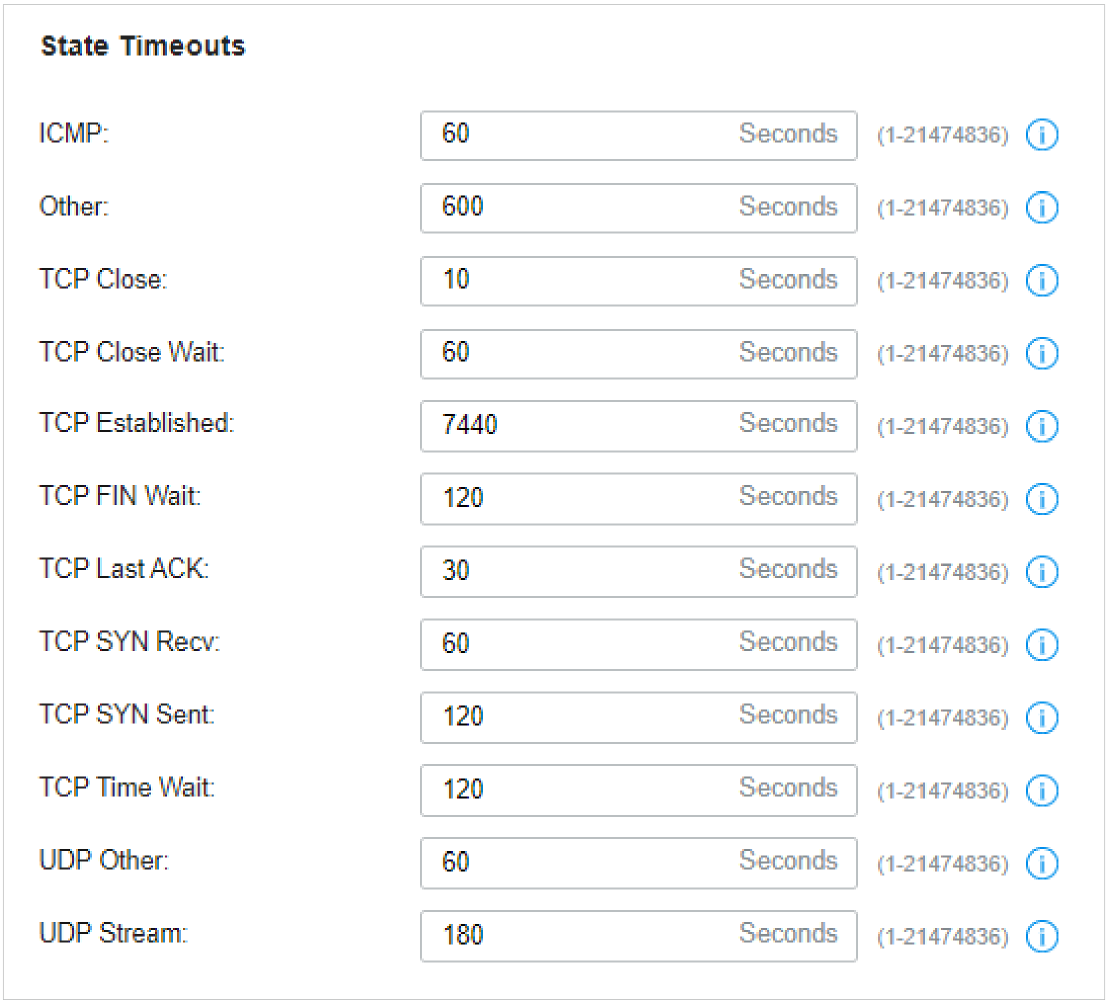
Firewall is used to enhance the network security. In State Timeouts, you can specify a number of timeouts for sessions including TCP, UDP, and ICMP connection. The packets will be forwarded within the specified timeout. When there is no response after the specified time, the session or status will be closed. State timeout will help close inactive sessions and thus avoid network malfunction. In Firewall

Options, you can further configure the gateway to prevent attacks like SYN flood attacks and broadcast ping.

Configuration

- **Configuring State Timeouts**

  Select a site from the drop-down list of Organization. Go to Settings > Network Security > Firewall. In the Sate Timeouts, set the time limit for the different sessions.



State Timeouts

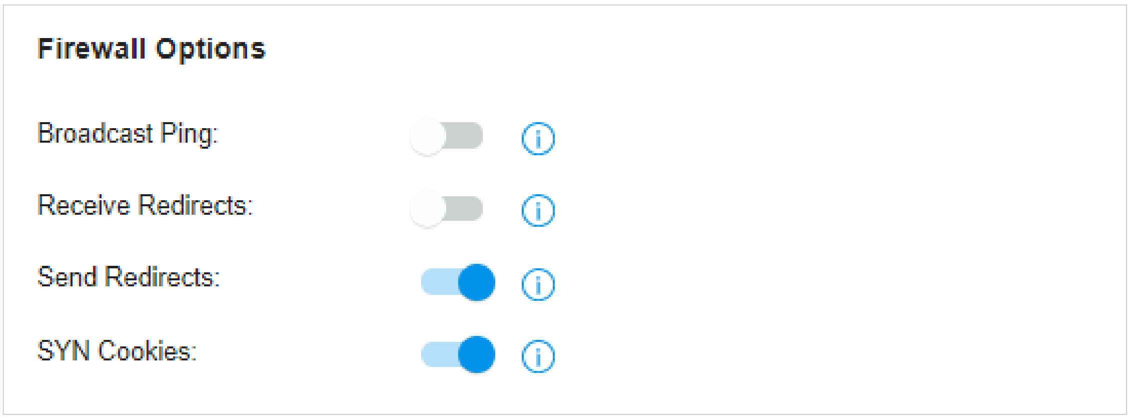
ICMP: 60 Seconds (1-21474836)
Other: 600 Seconds (1-21474836)
TCP Close: 10 Seconds (1-21474836)
TCP Close Wait: 60 Seconds (1-21474836)
TCP Established: 7440 Seconds (1-21474836)
TCP FIN Wait: 120 Seconds (1-21474836)
TCP Last ACK: 30 Seconds (1-21474836)
TCP SYN Recv: 60 Seconds (1-21474836)
TCP SYN Sent: 120 Seconds (1-21474836)
TCP Time Wait: 120 Seconds (1-21474836)
UDP Other: 60 Seconds (1-21474836)
UDP Stream: 180 Seconds (1-21474836)

ICMP	The ICMP session will be closed if there is no response after the set time.
Other	The sessions for protocols excluding TCP, UDP, and ICMP will be closed if there is no response after the set time.
TCP Close	The TCP Close status will be closed if there is no response after the set time.
TCP Close Wait	The TCP Close Wait status will be closed if there is no response after the set time.
TCP Established	The TCP Established status will be closed if there is no response after the set time.
TCP FIN Wait	The TCP FIN Wait status will be closed if there is no response after the set time.

TCP Last ACK	The TCP Last ACK status will be closed if there is no response after the set time.
TCP SYN Recv	The TCP SYN (Synchronize) Recv status will be closed if there is no response after the set time.
TCP SYN Sent	The TCP SYN (Synchronize) Sent status will be closed if there is no response after the set time.
TCP Time Wait	The TCP Time Wait status will be closed if there is no response after the set time.
UDP Other	The UDP connections with traffic in only one direction will be stopped if there is no response after the set time.
UDP Stream	The UDP connections with bidirectional traffic will be stopped if there is no response after the set time.

- **Configuring Firewall Options**

Select a site from the drop-down list of Organization. Go to Settings > Network Security > Firewall. In the Sate Timeouts, set the time limit for the different sessions.



Firewall Options

Broadcast Ping: ○ ⓘ

Receive Redirects: ○ ⓘ

Send Redirects: ● ⓘ

SYN Cookies: ● ⓘ

Broadcast Ping	With it enabled, the gateway will reply to broadcast pings.
Receive Redirects	With it enabled, the gateway will accept ICMP redirects.
Send Redirects	With it enabled, the gateway will send ICMP redirects.
SYN Cookies	With it enabled, the SYN cookies will be used to resist SYN flood attacks that want to open ports on the gateway.

1. 5. 5 IP-MAC Binding

Overview

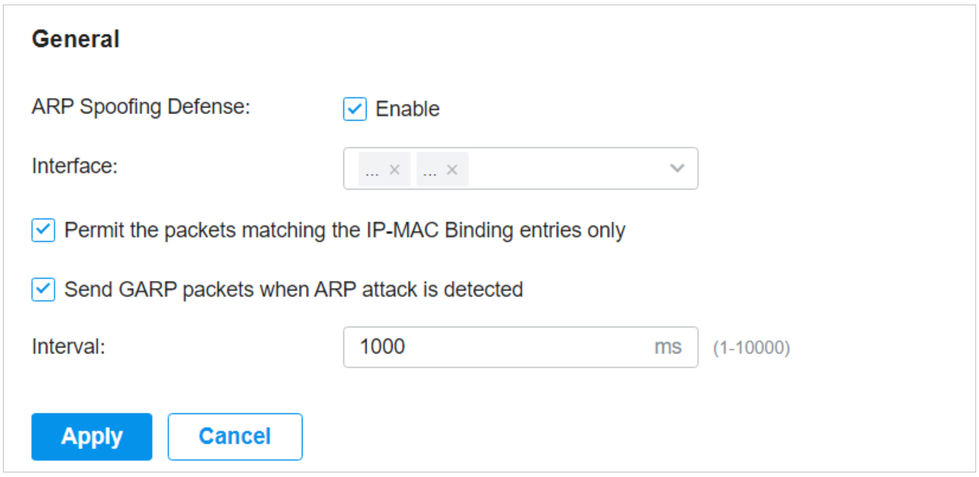
ARP (Address Resolution Protocol) is used to map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations. However, if attackers send ARP spoofing packets with false IP address-to-MAC address mapping entries, the device will update the ARP table based on the false ARP packets and record wrong mapping entries, which results in a breakdown of normal communication.

Anti ARP Spoofing can protect the network from ARP spoofing attacks. It works based on the IP-MAC Binding. These entries record the correct one-to-one relationships between IP addresses and MAC addresses. When receiving an ARP packet, the router checks whether it matches any of the IP-MAC Binding entries. If not, the router will ignore the ARP packets. In this way, the router maintains the correct ARP table.

Configuration

1. Select a site from the drop-down list of Organization. Go to Settings > Network Security > IP-MAC Binding.

2. Enable ARP Spoofing Defense and configure general settings. Click Apply.



General

ARP Spoofing Defense: ☑ Enable

Interface: ... × ... ×

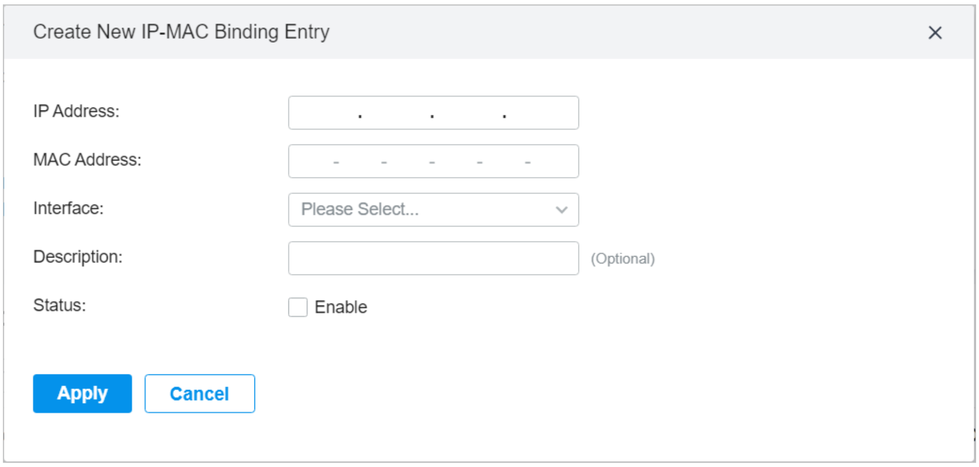
☑ Permit the packets matching the IP-MAC Binding entries only

☑ Send GARP packets when ARP attack is detected

Interval: 1000 ms (1-10000)

ARP Spoofing Defense	Check the box to globally enable ARP Spoofing Defense.
Interface	Select the interface on which the entries will take effect.
Permit the packets matching the IP-MAC Binding entries only	With this option enabled, when receiving a packet, the router will check whether the IP address, MAC address and receiving interface match any of the IP-MAC Binding entries. Only the matched packets will be forwarded. This feature can be enabled only when ARP Spoofing Defense is enabled.
Send GARP packets when ARP attack is detected	With this option enabled, the router will send GARP packets to the hosts if it detects ARP spoofing packets on the network. The GARP packets will inform the hosts of the correct ARP information, which is used to replace the wrong ARP information in the hosts. This feature can be enabled only when ARP Spoofing Defense is enabled.
Interval	Specify the time interval for sending GARP packets. The valid values are from 1 to 10000.

3. Click Create New IP-MAC Binding Entry and add an IP-MAC binding entry. Click Apply.



Create New IP-MAC Binding Entry ✕

IP Address: . . .

MAC Address: - - - - -

Interface: Please Select...

Description: (Optional)

Status: □ Enable

IP Address	Specify the IP address to be bound.
MAC Address	Specify the MAC address to be bound.
Interface	Select the interface on which the entries will take effect.
Description	Enter a description for identification.
Status	Enable the entry. Only when the status is enabled will the entry take effect.

1. 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.

1. 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.

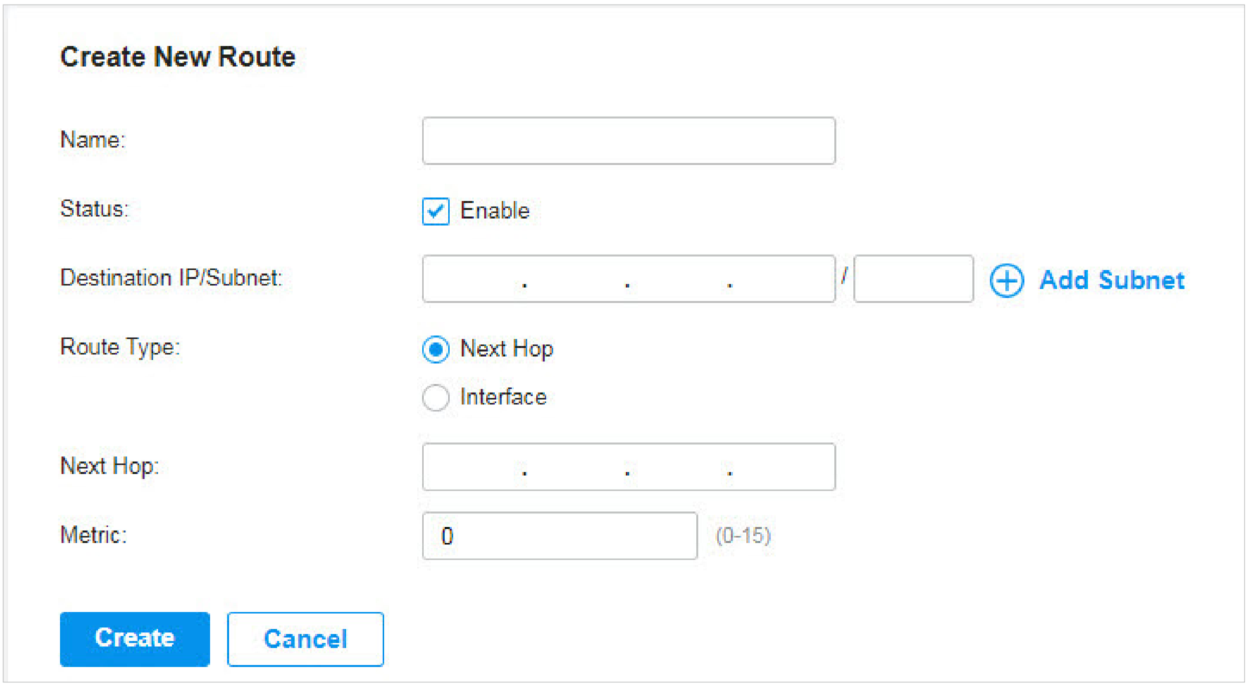
- **Policy Routing**

  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**

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



Create New Route

Name:

Status: ☑ Enable

Destination IP/Subnet: . . . /

Route Type: ● Next Hop ○ Interface

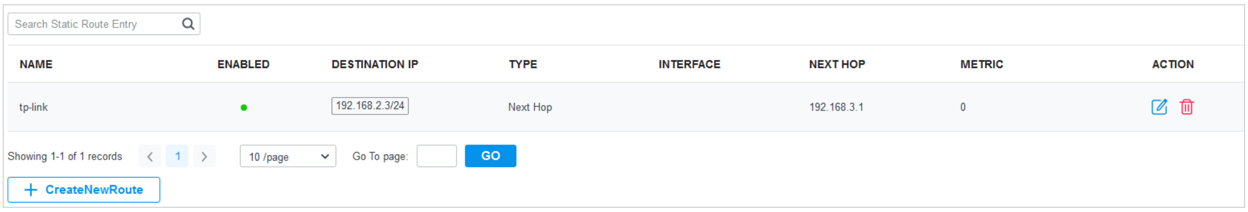
Next Hop: . . .

Metric: 0 (0-15)

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.

2. 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.

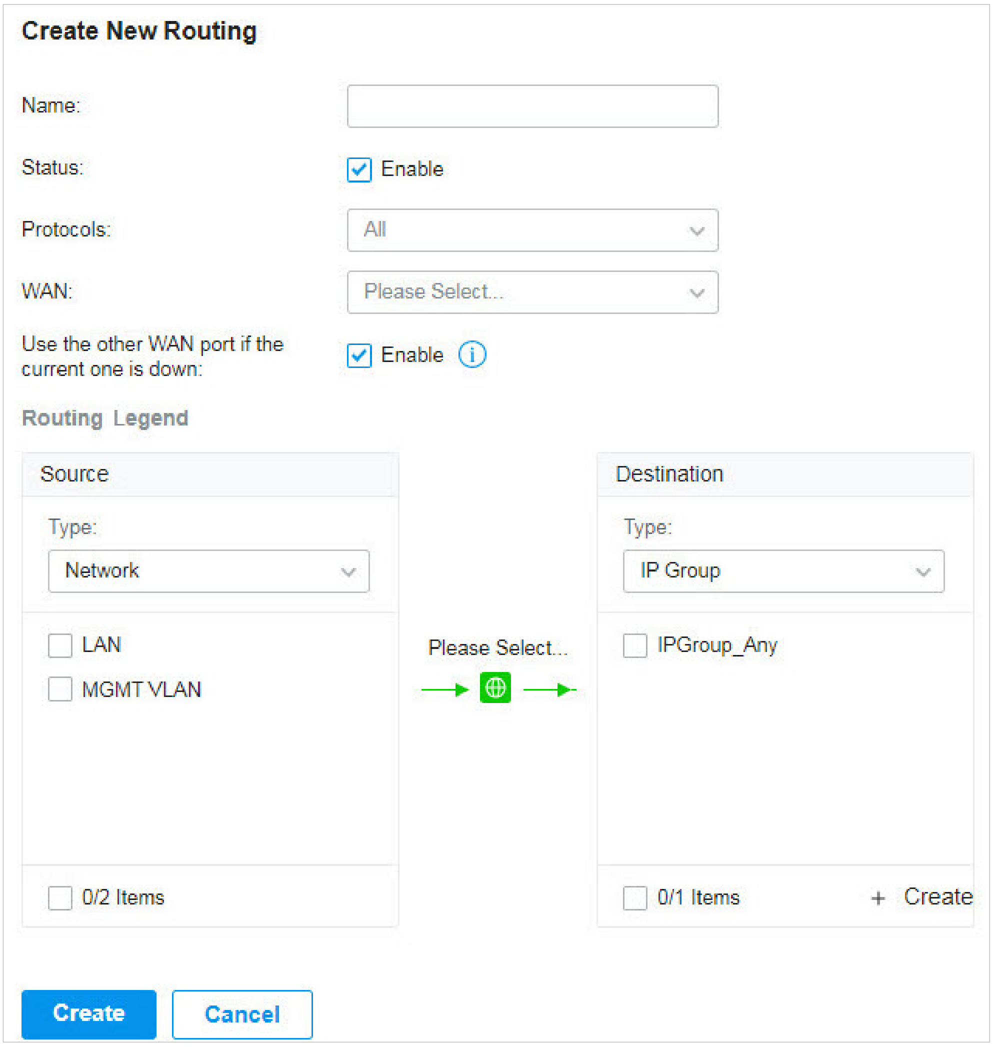


NAME	ENABLED	DESTINATION IP	TYPE	INTERFACE	NEXT HOP	METRIC	ACTION
tp-link	●	192.168.2.3/24	Next Hop		192.168.3.1	0	✎ 🗑

Showing 1-1 of 1 records

- **Policy Routing**

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



Create New Routing

Name:

Status: ☑ Enable

Protocols: All

WAN: Please Select...

Use the other WAN port if the current one is down: ☑ Enable

Routing Legend

Source

Type: Network

□ LAN

□ MGMT VLAN

□ 0/2 Items

Please Select...

Destination

Type: IP Group

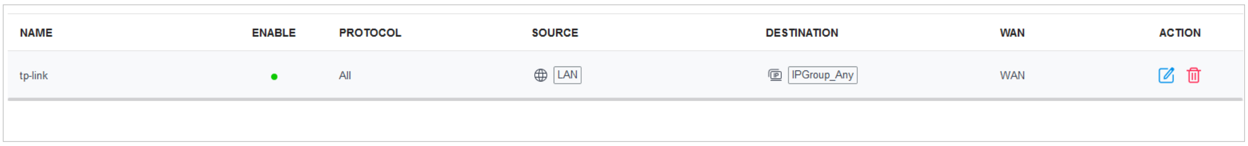
□ IPGroup_Any

□ 0/1 Items

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. IP-Port Group: Select the IP-Port Group for the traffic source or destination. You can click + Create to create a new IP-Port 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.



NAME	ENABLE	PROTOCOL	SOURCE	DESTINATION	WAN	ACTION
tp-link	●	All	LAN	IPGroup_Any	WAN	✎ 🗑

1. 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.

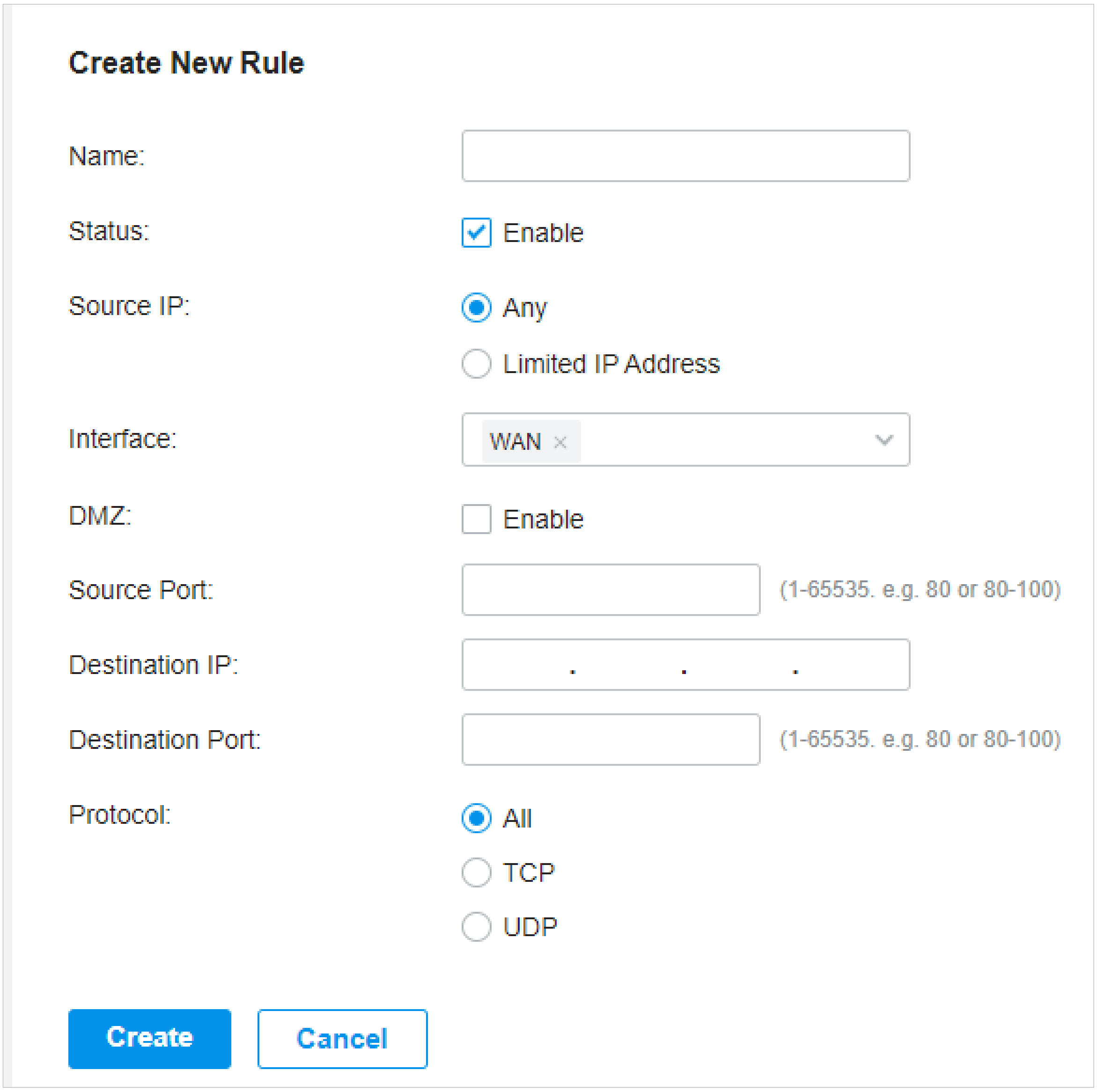
- **One-to-One NAT**

  One-to-One NAT will establish a correspondence between a private IP and a public IP, allowing access to the device with the private IP through the corresponding public IP.

Configuration

- **Port Forwarding**

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



Create New Rule

Name:

Status: ☑ Enable

Source IP: ● Any ○ Limited IP Address

Interface: WAN ×

DMZ: □ Enable

Source Port: (1-65535. e.g. 80 or 80-100)

Destination IP: . . .

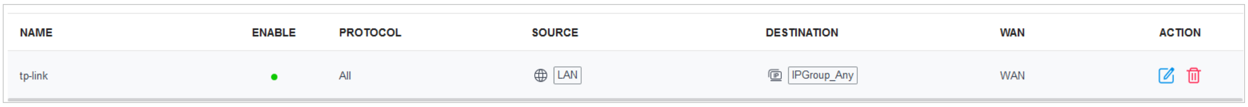
Destination Port: (1-65535. e.g. 80 or 80-100)

Protocol: ● All ○ TCP ○ UDP

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.

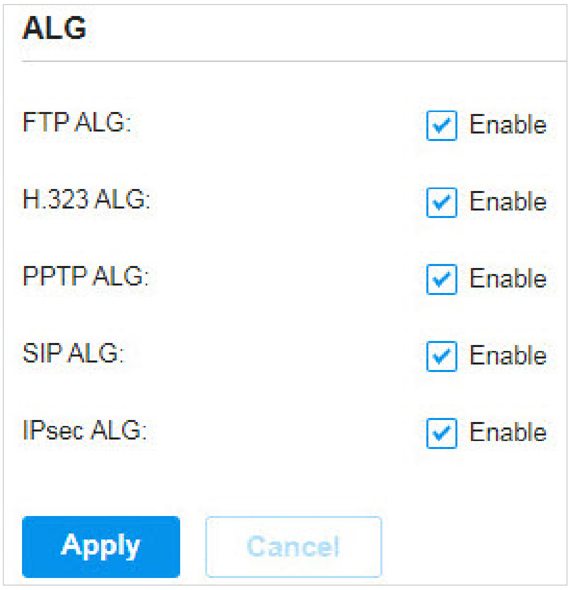
2. Click Create. The new Port Forwarding entry is added to the table. You can click ✎ to edit the entry. You can click 🗑 to delete the entry.



NAME	ENABLE	PROTOCOL	SOURCE	DESTINATION	WAN	ACTION
tp-link	●	All	LAN	IPGroup_Any	WAN	✎ 🗑

■ ALG

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



ALG

FTP ALG: ☑ Enable

H.323 ALG: ☑ Enable

PPTP ALG: ☑ Enable

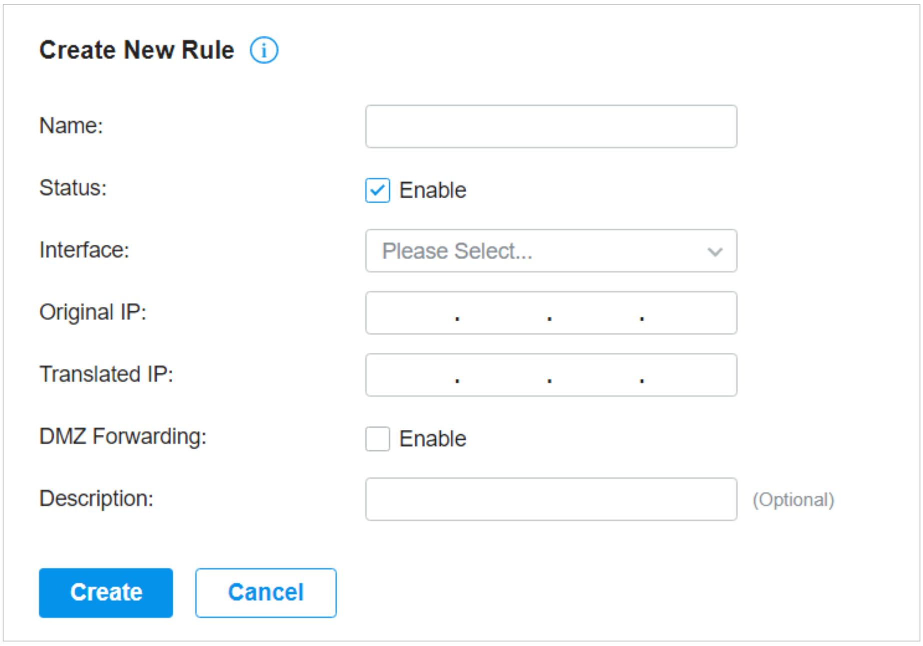
SIP ALG: ☑ Enable

IPsec ALG: ☑ Enable

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.

■ **One-to-One NAT**

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



Create New Rule

Name:

Status: ☑ Enable

Interface: Please Select...

Original IP: . . .

Translated IP: . . .

DMZ Forwarding: □ Enable

Description: (Optional)

Name	Enter the name to identify the one-to-one NAT rule.
Status	Enable or disable the one-to-one NAT rule.
Interface	Specify the effective interface for the rule only when the connection type is Static IP.
Original IP	Specify the original IP address for the rule, which means the device’s private IP. The original IP address cannot be the broadcast address, network segment or interface IP. With One-to-One NAT enabled, the original IP will map to the translated IP.
Translated IP	Specify the translated IP address for the rule, which means the public IP of device. The translated IP address cannot be the broadcast address, network segment or interface IP. With One-to-One NAT enabled, the original IP will map to the translated IP.
DMZ Forwarding	Choose to enable DMZ Forwarding. The packets transmitted to the translated IP address will be forwarded to the host with the original IP address if DMZ Forwarding is enabled.
Description	(Optional) Enter a description for identification.

2. Click Create to add the one-to-one NAT rule.

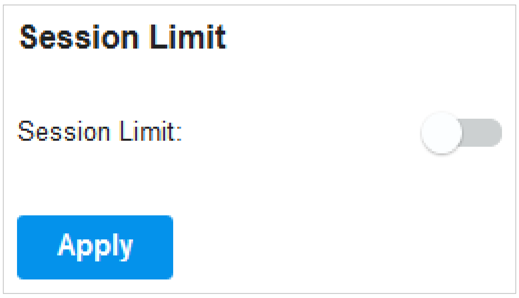
1. 6. 3 Session Limit

Overview

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

Configuration

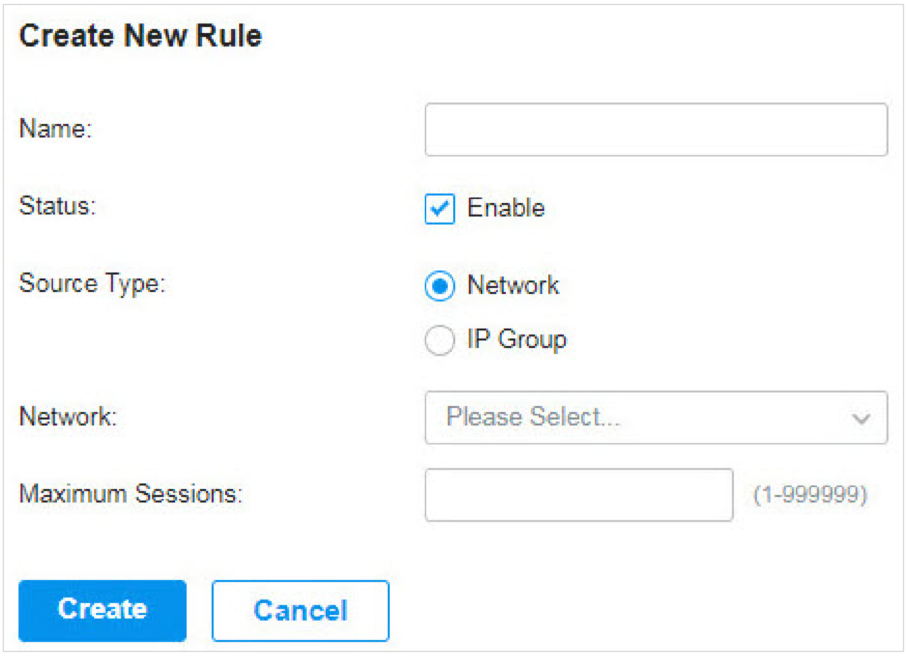
1. Go to Setting > Transmission > Session Limit. In Session Limit, enable Session Limit globally and click Apply.



Session Limit

Session Limit:

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



Create New Rule

Name:

Status: ☑ Enable

Source Type: ● Network ○ IP Group

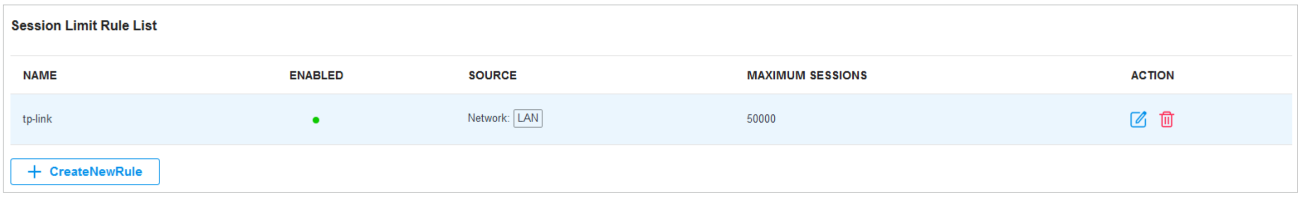
Network: Please Select...

Maximum Sessions: (1-999999)

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 4. 3. 2 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 4. 8 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.



Session Limit Rule List

NAME	ENABLED	SOURCE	MAXIMUM SESSIONS	ACTION
tp-link	●	Network: LAN	50000	✎ 🗑

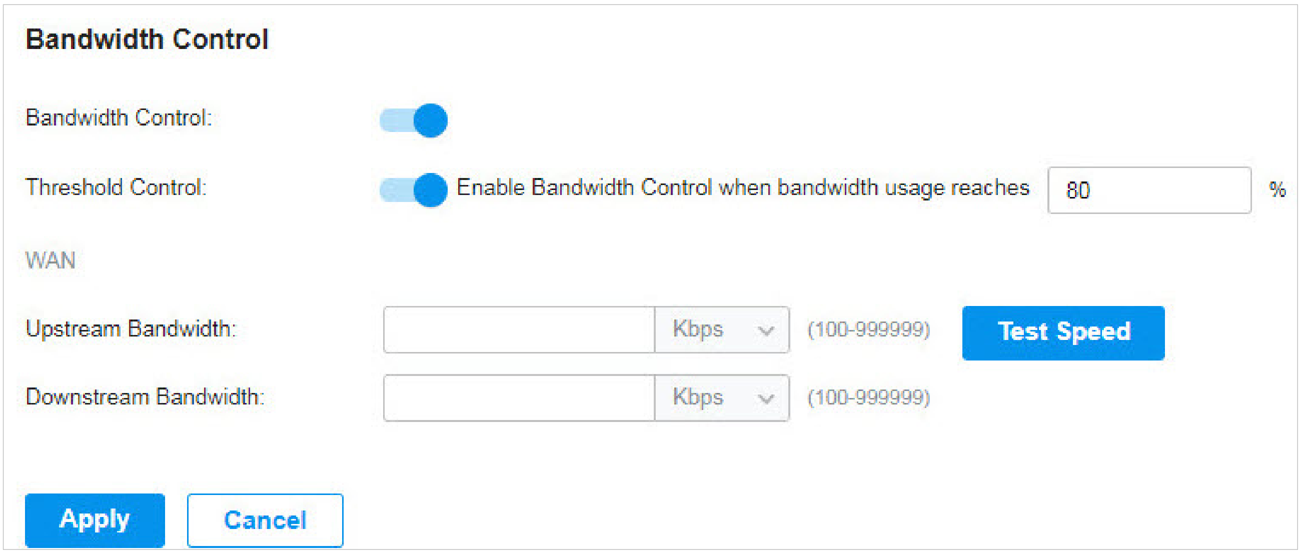
1. 6. 4 Bandwidth Control

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.



Bandwidth Control

Bandwidth Control: ●

Threshold Control: ● Enable Bandwidth Control when bandwidth usage reaches 80 %

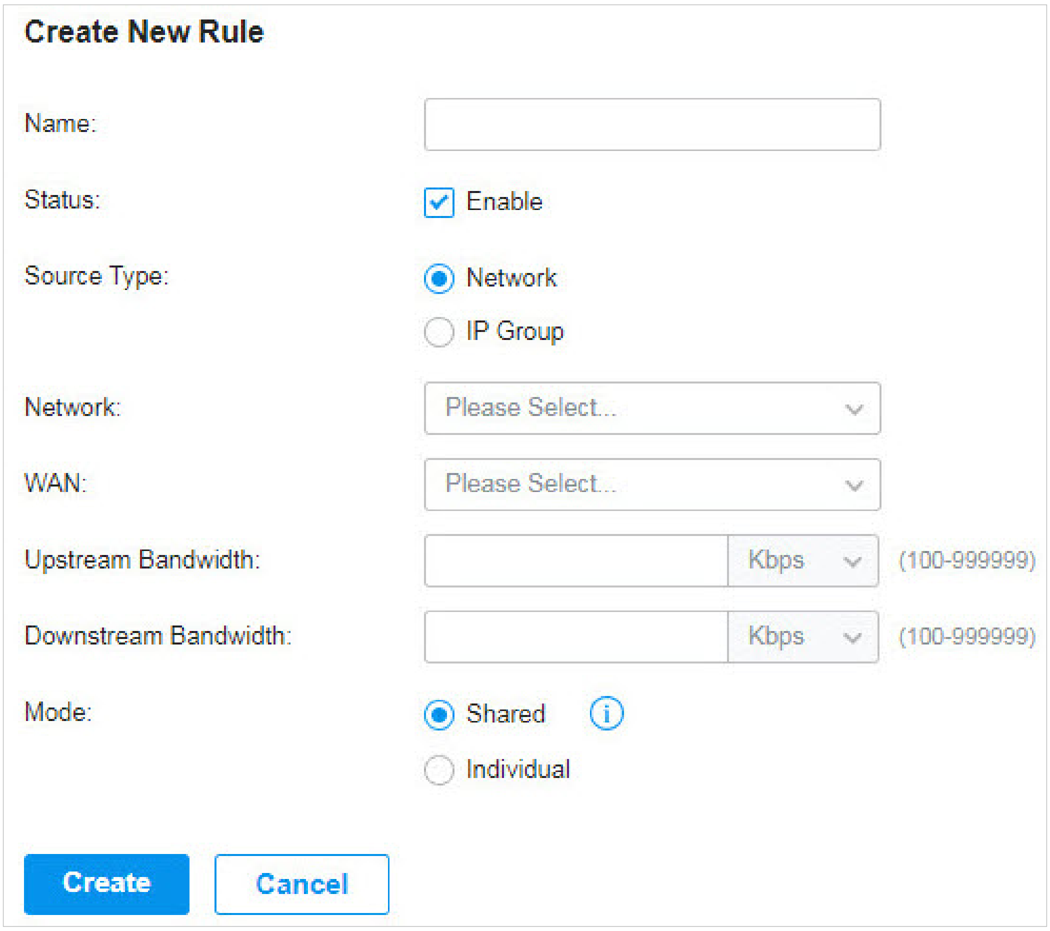
WAN

Upstream Bandwidth: Kbps (100-999999)

Downstream Bandwidth: Kbps (100-999999)

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.



Create New Rule

Name:

Status: ☑ Enable

Source Type: ● Network ○ IP Group

Network: Please Select...

WAN: Please Select...

Upstream Bandwidth: Kbps (100-999999)

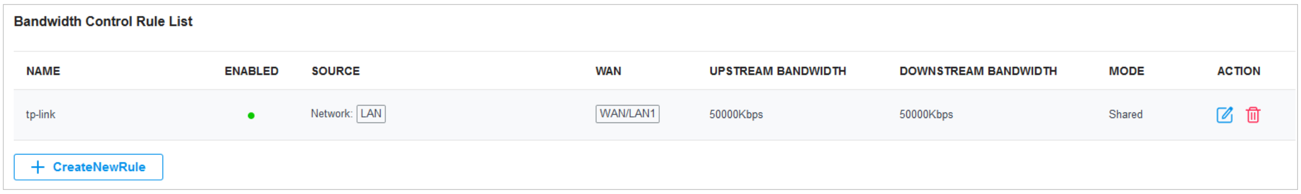
Downstream Bandwidth: Kbps (100-999999)

Mode: ● Shared ○ Individual

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 4. 3. 2 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 4. 8 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.



Bandwidth Control Rule List

NAME	ENABLED	SOURCE	WAN	UPSTREAM BANDWIDTH	DOWNSTREAM BANDWIDTH	MODE	ACTION
tp-link	●	Network: LAN	WAN/LAN1	50000Kbps	50000Kbps	Shared	✎ 🗑

1. 6. 5 Quality of Services

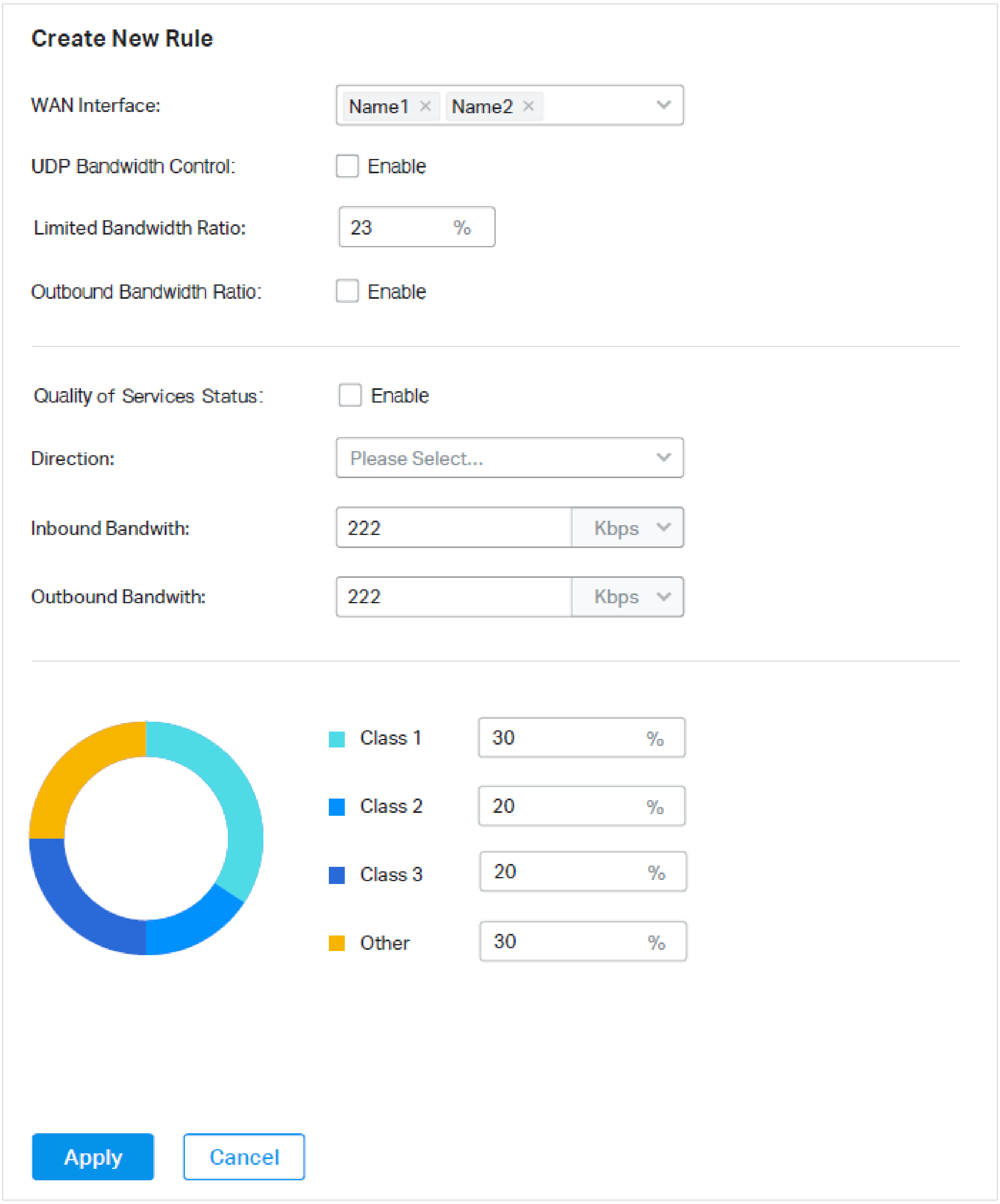
- **Bandwidth Control**

This page allows you to configure rules to limit various data flows. In this way, you can optimize the network performance by reasonably utilizing the bandwidth.

Configuration

1. Select a site from the drop-down list of Organization. Go to Setting > Transmission > Quality of Services.

2. Click Create New Rule.



Create New Rule

WAN Interface:	Name1 × Name2 ×
UDP Bandwidth Control:	□ Enable
Limited Bandwidth Ratio:	23 %
Outbound Bandwidth Ratio:	□ Enable
Quality of Services Status:	□ Enable
Direction:	Please Select...
Inbound Bandwith:	222 Kbps
Outbound Bandwith:	222 Kbps

Class 1	30 %
Class 2	20 %
Class 3	20 %
Other	30 %

3. Configure the parameters and click Apply.

WAN Interface	Select the WAN port. You can configure the QoS rule for a WAN port only when the port is enabled.
Quality of Service Status	Enable or disable QoS for the current entry.
UDP Bandwidth Control	Check the box to enable UDP bandwidth control.

Limited Bandwidth Ratio	When UDP Bandwidth Control is enabled, specify the bandwidth ratio of UDP at each level of class1/2/3/other.
Outbound TCP ACK Prioritize	Check the box to prioritize outbound TCP ACK packets. This function ensures that traffic is not slowed down by remote hosts waiting for ACK packets before sending further traffic.
Direction	Specify the direction of the controlled traffic. "out" means control sending packets. "in" means receiving packets. "both" means both are controlled.
Inbound/Outbound Bandwidth	Enter the maximum threshold of the inbound/outbound bandwidth.
Class1/Class2/Class3/ Others	Specify the proportion of the maximum bandwidth that Class1, Class2, Class3 and Others can occupy to limit the bandwidth usage of specific classification traffic.

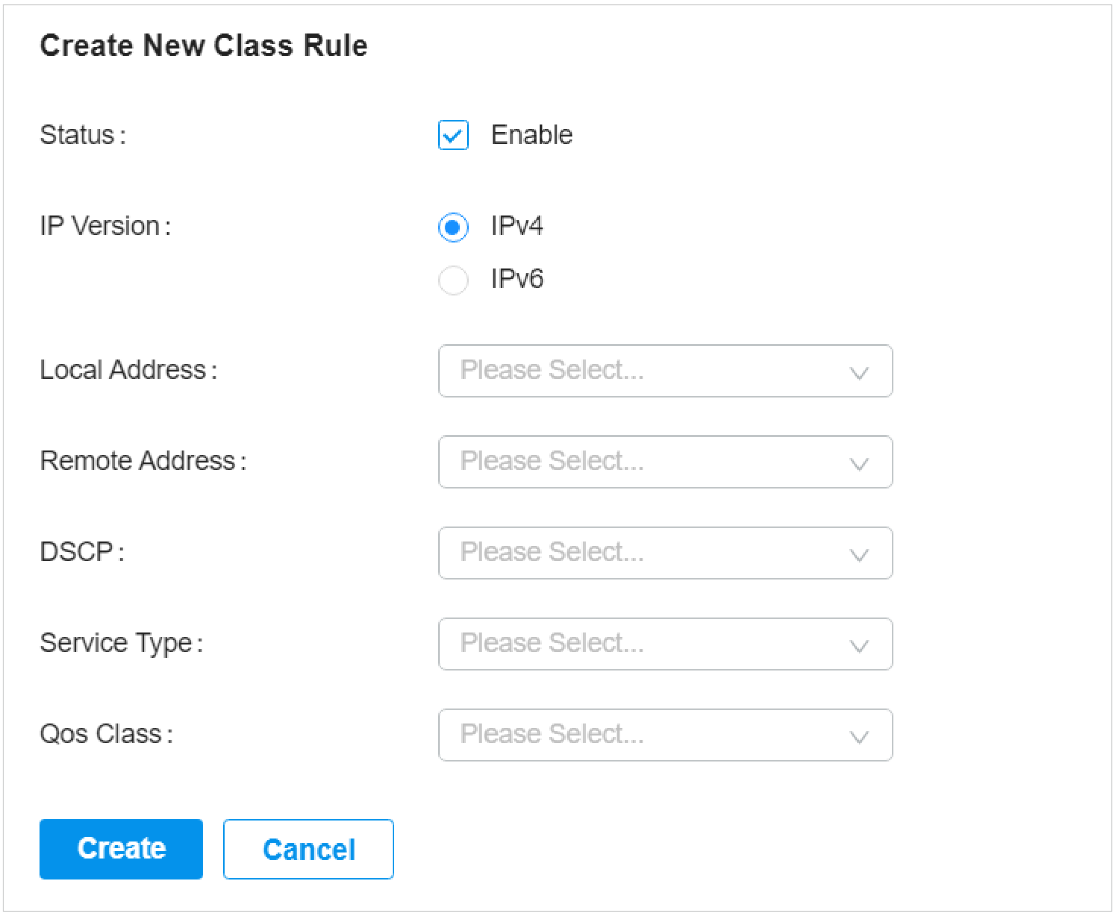
■ Class Rule

This page allows you to add or delete class rules. Rules will be matched from top to bottom according to the rule sequence number. When the traffic matches a rule, it will be assigned to the corresponding class and will not continue to match down.

Configuration

1. Select a site from the drop-down list of Organization. Go to Setting > Transmission > Quality of Services > Class Rule.

2. Click Create New Class Rule.



Create New Class Rule

Status : ☑ Enable

IP Version : ● IPv4 ○ IPv6

Local Address : Please Select...

Remote Address : Please Select...

DSCP : Please Select...

Service Type : Please Select...

Qos Class : Please Select...

3. Configure the parameters and click Apply.

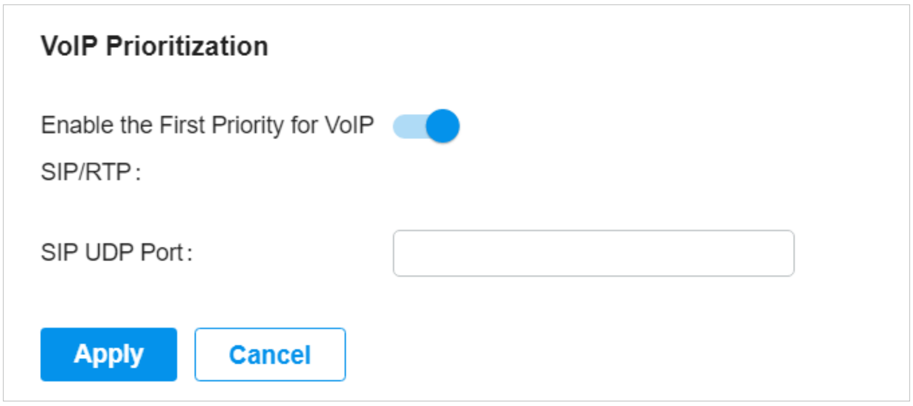
Status	Check the box to enable the rule.
IP Version	Specify the protocol version: IPv4 or IPv6.
Local Address	Match the source IP address of the traffic. For IPv4 protocol, you can use the IP Group object configured in the Profiles > Groups module. For the IPv6 protocol, you can use the IPv6 Group object configured in the Profiles > Groups module.
Remote Address	Match the destination IP address of the traffic. For IPv4 protocol, you can use the IP Group object configured in the Profiles > Groups module. For the IPv6 protocol, you can use the IPv6 Group object configured in the Profiles > Groups module.
DSCP	Match the DSCP value of the traffic: Any, IP procedure, AF, or EF.
Service Type	Match the port number of the traffic. Select the service type object defined in the Preference > Service Type module.
QoS Class	Select the category of traffic that meets the rule.

- **VoIP Prioritization**

This page allows you to configure VoIP prioritization.

Configuration

1. Select a site from the drop-down list of Organization. Go to Setting > Transmission > Quality of Services > VoIP Prioritization.
2. Enable the first priority for VoIP SIP/RTP and enter the SIP UDP port. Then apply the settings.



VoIP Prioritization

Enable the First Priority for VoIP SIP/RTP: ●

SIP UDP Port:

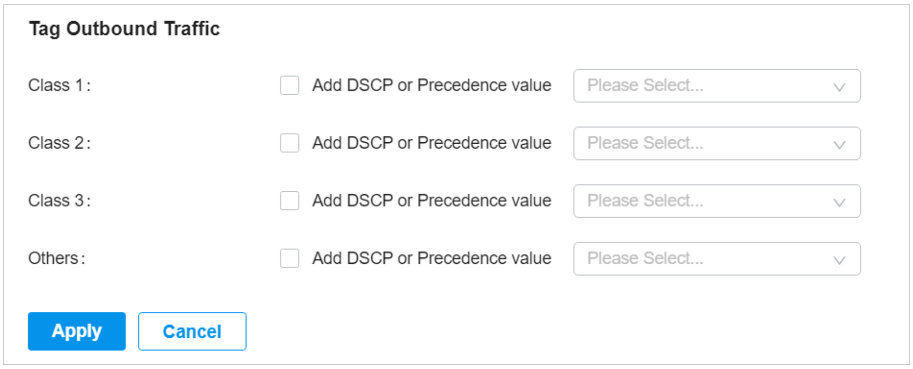
Enable the First Priority for VoIP SIP/RTP	Check the box to enable prioritize VoIP traffic.
SIP UDP Port	Enter the UDP port ID of the VoIP traffic.

- **Tag Outbound Traffic**

This page allows you to add a DSCP or Precedence value for traffic in different classes.

Configuration

1. Select a site from the drop-down list of Organization. Go to Setting > Transmission > Quality of Services > Tag Outbound Traffic.
2. Check the box for your desired class and select the DSCP or Precedence value.



Tag Outbound Traffic

Class 1: □ Add DSCP or Precedence value Please Select...

Class 2: □ Add DSCP or Precedence value Please Select...

Class 3: □ Add DSCP or Precedence value Please Select...

Others: □ Add DSCP or Precedence value Please Select...

Class 1/2/3/Others	Check the box and select the DSCP (Any, IP procedure, AF, or EF) or Precedence value for traffic.

1. 7 Configure VPN

VPN (Virtual Private Network) provides a means for secure communication between remote computers across a public wide area network (WAN), such as the internet. Omada managed gateways supports various types of VPN.

1. 7. 1 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.

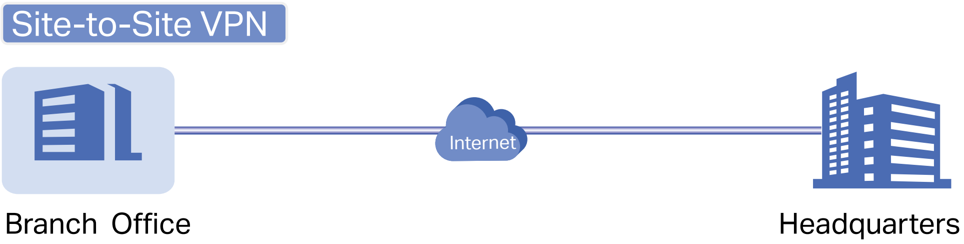
- **OpenVPN**

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:

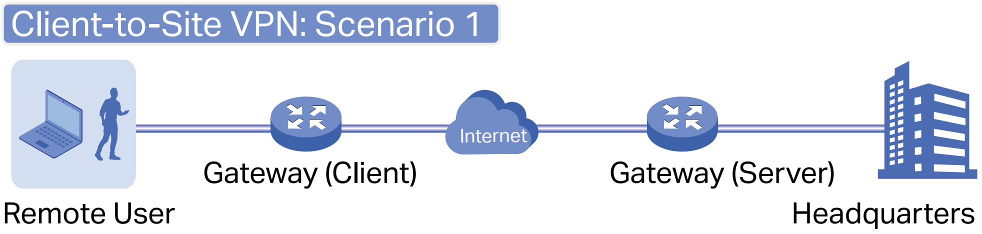
  - VPN Server

    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.

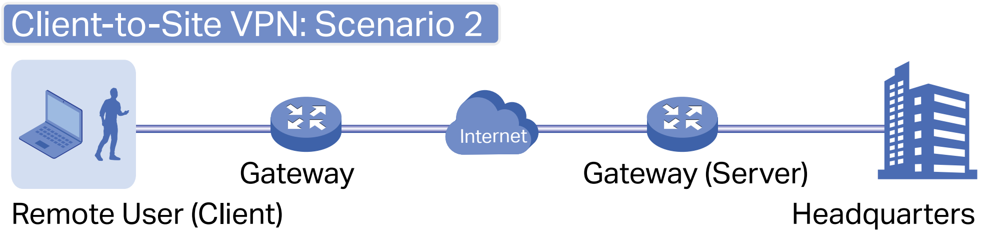
  - VPN Client

    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.

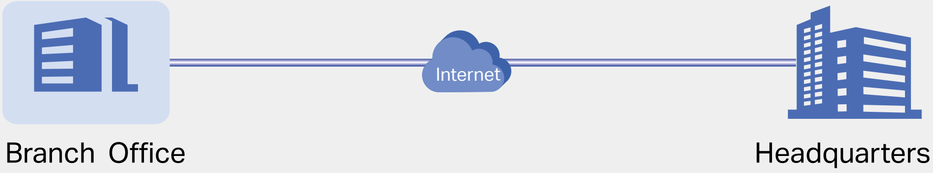
In scenario 2, you need to configure VPN server on the gateway, and then configure the VPN client software program on the remote user's laptop or PC, while the remote user's gateway doesn't need any VPN configuration.

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

Create a VPN Policy

Select the purpose of the VPN

Site-to-Site VPN



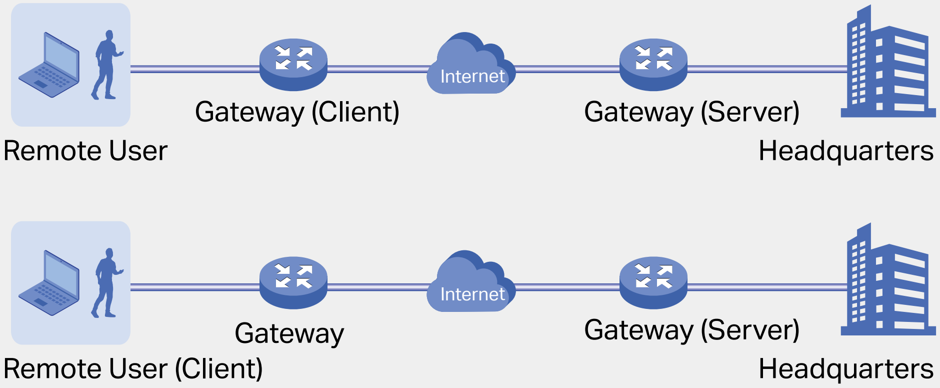
Auto IPsec VPN

The controller automatically creates an IPsec VPN tunnel between two sites on the same controller.

Manual IPsec VPN

You manually create an IPsec VPN tunnel between two peer routers over internet, from a local router to a remote router that supports IPsec.

Client-to-Site VPN



Select the role of the gateway and VPN tunneling protocol

VPN Server	VPN Client
L2TP	L2TP
PPTP	PPTP
IPsec	IPsec (Only for VPN client software)
OpenVPN	OpenVPN

Configuration

To complete the VPN configuration, follow these steps:

1) 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.

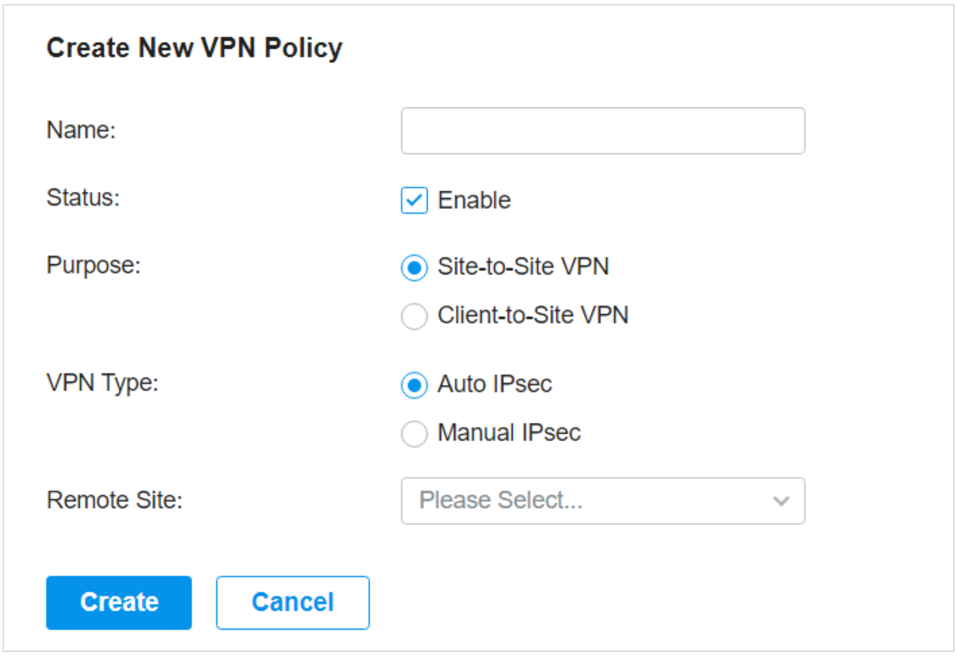
2) Select the VPN tunneling protocol and configure the VPN policy based on the protocol.

■ 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

1. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy

Name:	
Status:	☑ Enable
Purpose:	● Site-to-Site VPN ○ Client-to-Site VPN
VPN Type:	● Auto IPsec ○ Manual IPsec
Remote Site:	Please Select...

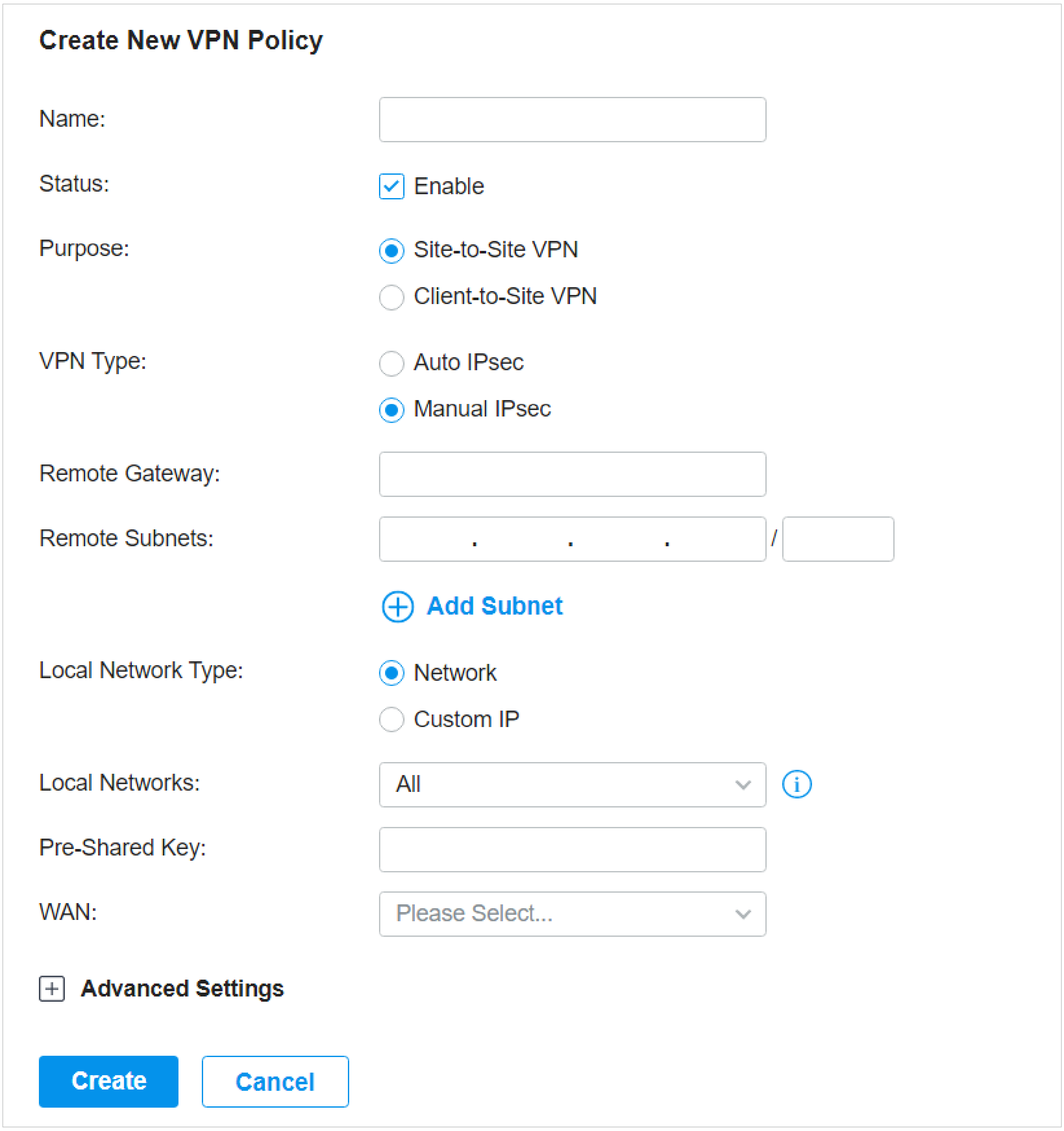
2. Enter a name to identify the VPN policy and select the purpose as Site-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Site-to-Site VPN.
VPN Type	Select the VPN type as Auto IPsec. With 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.

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. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy

Name:

Status: ☑ Enable

Purpose: ● Site-to-Site VPN ○ Client-to-Site VPN

VPN Type: ○ Auto IPsec ● Manual IPsec

Remote Gateway:

Remote Subnets: . . . /

Local Network Type: ● Network ○ Custom IP

Local Networks: All

Pre-Shared Key:

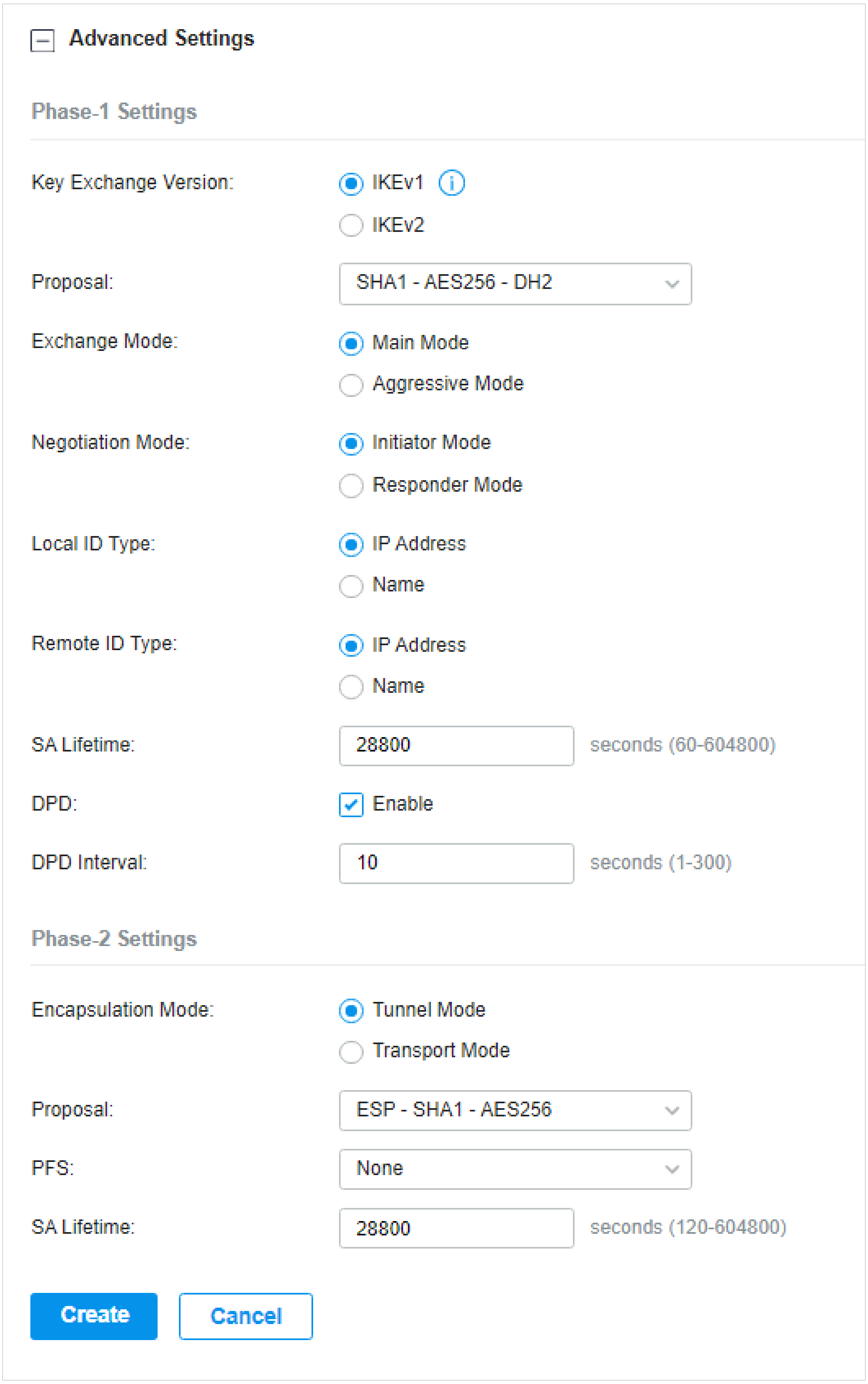
WAN: Please Select...

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.
Status	Click the checkbox to enable the VPN policy.

Purpose	Select the purpose for the VPN as Site-to-Site VPN.
VPN Type	Select the VPN type as Manual IPsec.
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. Remote subnets should not be in the same network segment as the local LAN.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
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**

Phase-1 Settings

Key Exchange Version: ● IKEv1 ⓘ ○ IKEv2

Proposal: SHA1 - AES256 - DH2

Exchange Mode: ● Main Mode ○ Aggressive Mode

Negotiation Mode: ● Initiator Mode ○ Responder Mode

Local ID Type: ● IP Address ○ Name

Remote ID Type: ● IP Address ○ Name

SA Lifetime: 28800 seconds (60-604800)

DPD: ☑ Enable

DPD Interval: 10 seconds (1-300)

Phase-2 Settings

Encapsulation Mode: ● Tunnel Mode ○ Transport Mode

Proposal: ESP - SHA1 - AES256

PFS: None

SA Lifetime: 28800 seconds (120-604800)

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. Encryption algorithms protect the data from being read by a third-party. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. 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

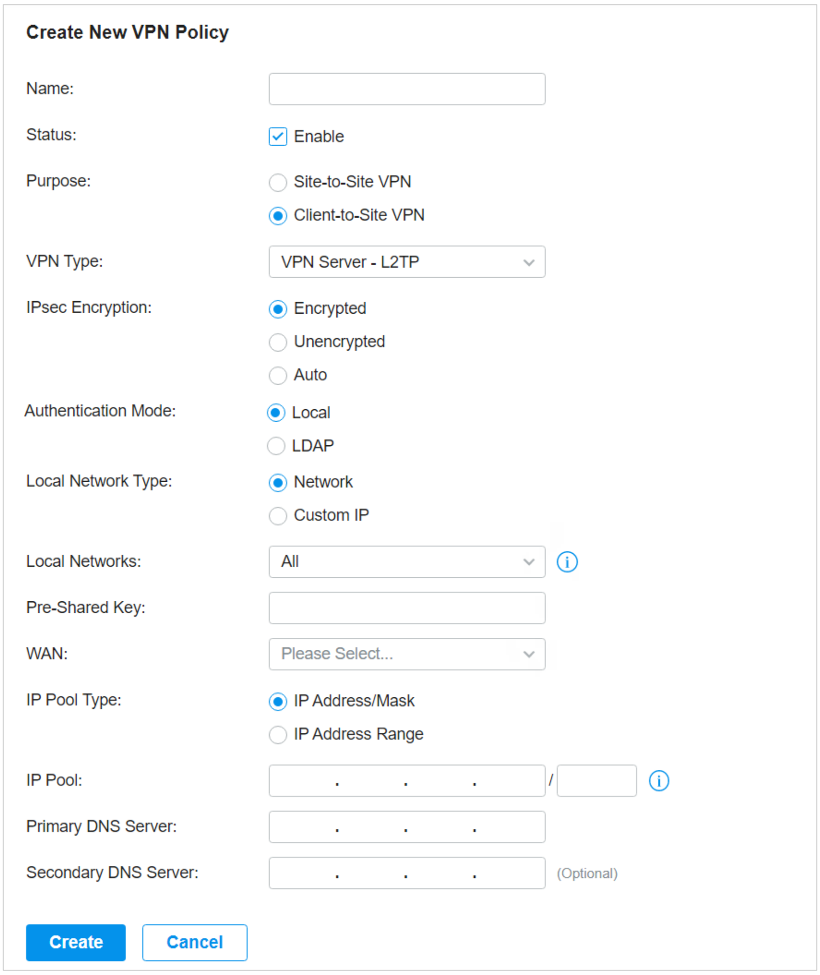
Configuring the gateway as a VPN client using L2TP

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. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy

Name:	
Status:	☑ Enable
Purpose:	○ Site-to-Site VPN ● Client-to-Site VPN
VPN Type:	VPN Server - L2TP
IPsec Encryption:	● Encrypted ○ Unencrypted ○ Auto
Authentication Mode:	● Local ○ LDAP
Local Network Type:	● Network ○ Custom IP
Local Networks:	All
Pre-Shared Key:	
WAN:	Please Select...
IP Pool Type:	● IP Address/Mask ○ IP Address Range
IP Pool:	. . . /
Primary DNS Server:	. . .
Secondary DNS Server:	. . . (Optional)

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.

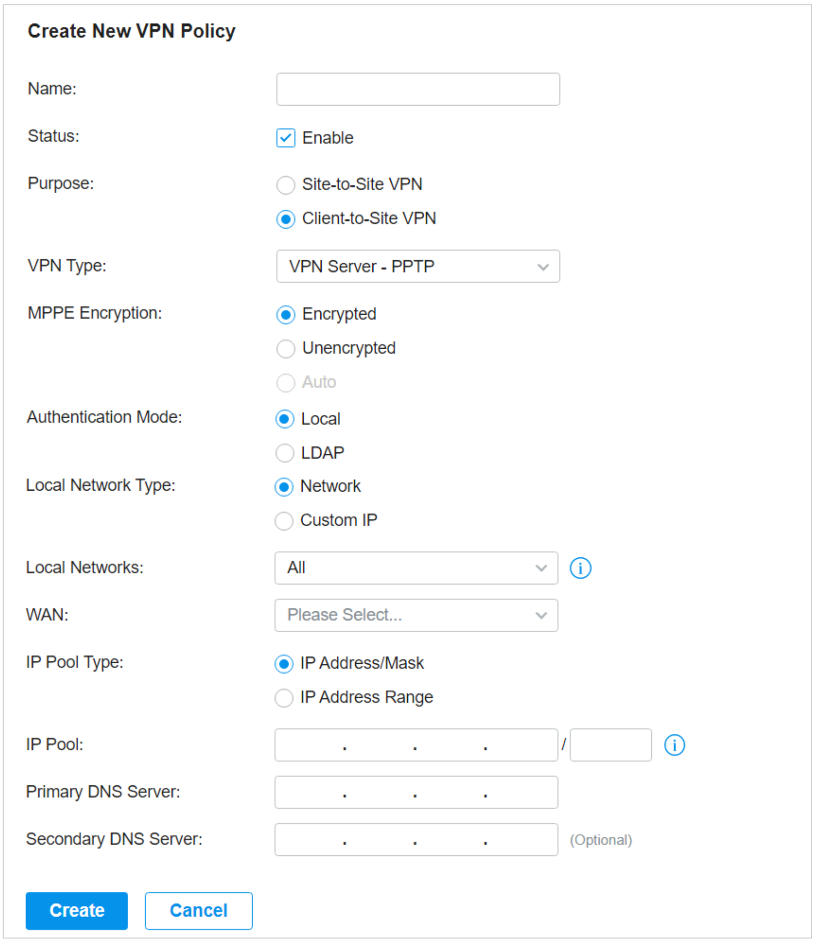
Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - L2TP.

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.
Authentication Mode	Select the authentication mode: Local or LDAP.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
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 Type	Specify the format of the IP pool.
IP Pool	If you selected IP Address/Mask type, enter the IP address and subnet mask to decide the range of the VPN IP pool. If you select IP Address Range type, enter the start and end IP addresses of the VPN IP pool.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

3. Add the VPN users account to validate remote hosts. To create VPN users, refer to 4. 7. 2 VPN User.

- Configuring the gateway as a VPN server using PPTP

1. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy

Name:

Status: ☑ Enable

Purpose: ○ Site-to-Site VPN ● Client-to-Site VPN

VPN Type: VPN Server - PPTP

MPPE Encryption: ● Encrypted ○ Unencrypted ○ Auto

Authentication Mode: ● Local ○ LDAP

Local Network Type: ● Network ○ Custom IP

Local Networks: All

WAN: Please Select...

IP Pool Type: ● IP Address/Mask ○ IP Address Range

IP Pool: . . . /

Primary DNS Server: . . .

Secondary DNS Server: . . . (Optional)

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.

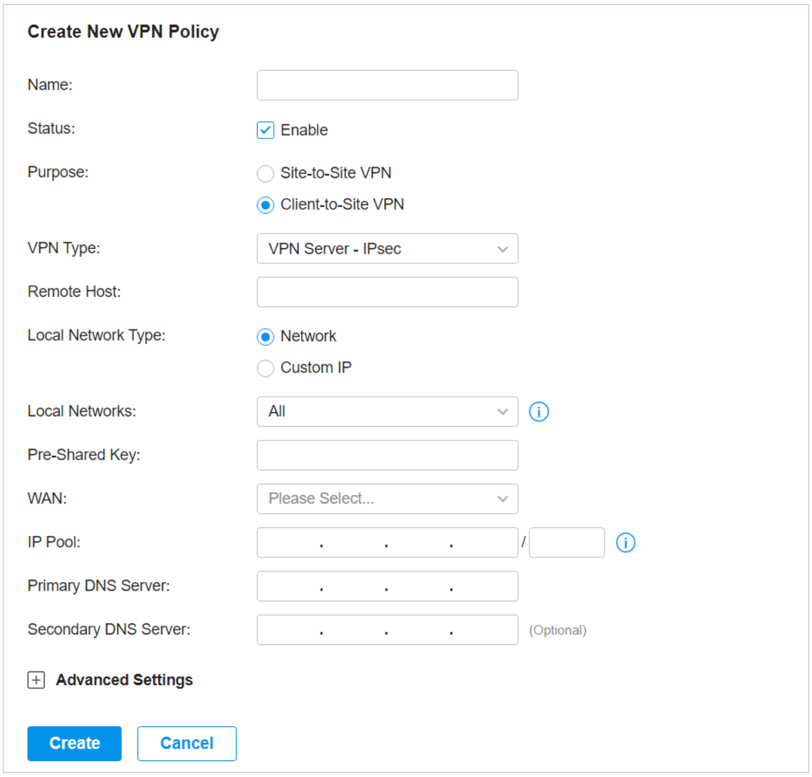
Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Purpose	Select the purpose for the VPN as Client-to-Site VPN.
VPN Type	Select the VPN type as VPN Server - PPTP.
MPPE Encryption	Specify whether to enable MPPE (Microsoft Point-to-Point Encryption) for the 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.
Authentication Mode	Select the authentication mode: Local or LDAP.

Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
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 Type	Specify the format of the IP pool.
IP Pool	If you selected IP Address/Mask type, enter the IP address and subnet mask to decide the range of the VPN IP pool. If you select IP Address Range type, enter the start and end IP addresses of the VPN IP pool.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

3. Add the VPN users account to validate remote hosts. To create VPN users, refer to 4. 7. 2 VPN User.

- Configuring the gateway as a VPN server using IPsec

1. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.


Create New VPN Policy

Name:

Status: ☑ Enable

Purpose: ○ Site-to-Site VPN ● Client-to-Site VPN

VPN Type: VPN Server - IPsec

Remote Host:

Local Network Type: ● Network ○ Custom IP

Local Networks: All

Pre-Shared Key:

WAN: Please Select...

IP Pool: . . . /

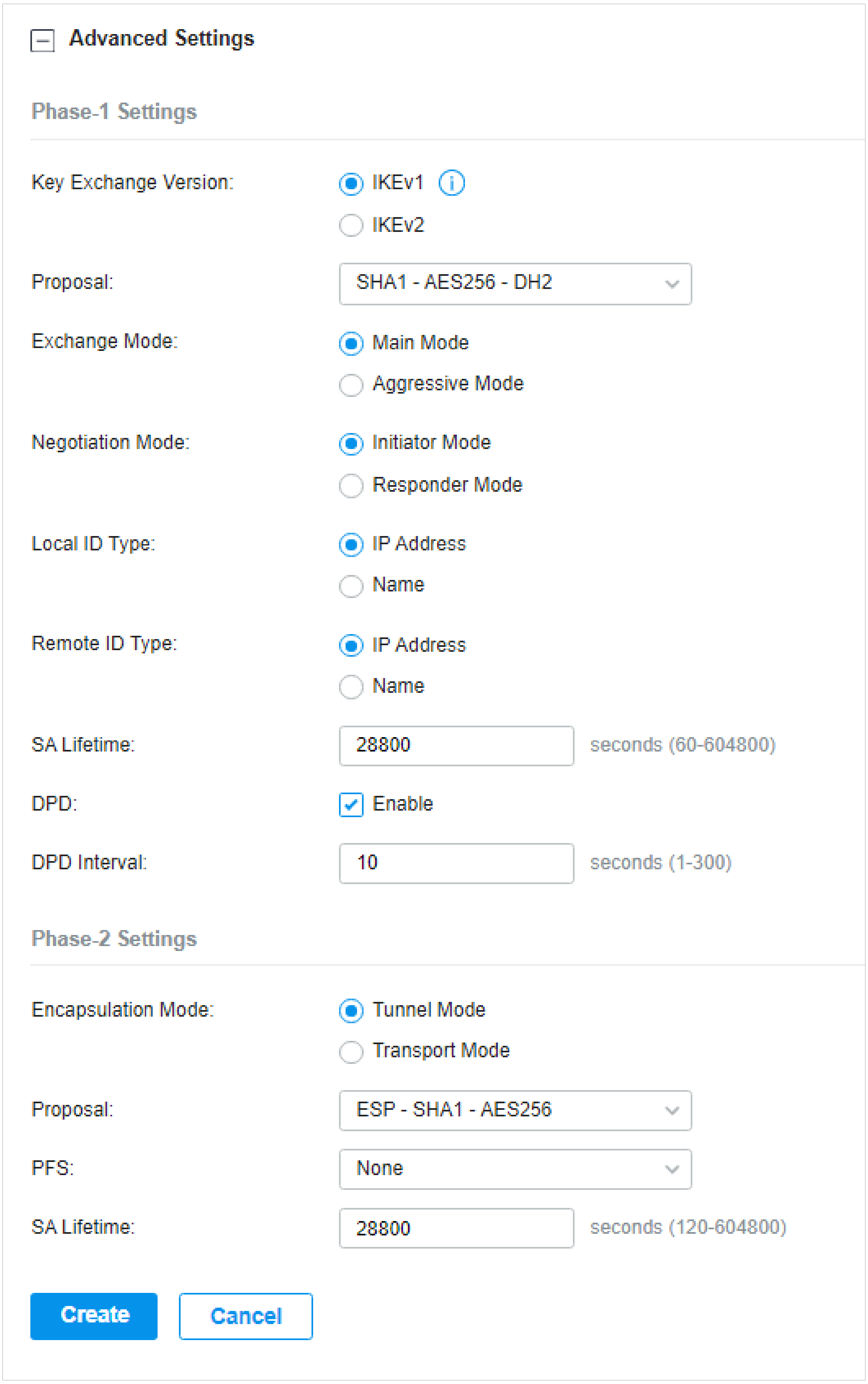
Primary DNS Server: . . .

Secondary DNS Server: . . . (Optional)

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.
Status	Click the checkbox to enable 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.
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 Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
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.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

3. Click Advanced Settings to load the following page.



⊟ **Advanced Settings**

Phase-1 Settings

Key Exchange Version: ● IKEv1 ○ IKEv2

Proposal: SHA1 - AES256 - DH2

Exchange Mode: ● Main Mode ○ Aggressive Mode

Negotiation Mode: ● Initiator Mode ○ Responder Mode

Local ID Type: ● IP Address ○ Name

Remote ID Type: ● IP Address ○ Name

SA Lifetime: 28800 seconds (60-604800)

DPD: ☑ Enable

DPD Interval: 10 seconds (1-300)

Phase-2 Settings

Encapsulation Mode: ● Tunnel Mode ○ Transport Mode

Proposal: ESP - SHA1 - AES256

PFS: None

SA Lifetime: 28800 seconds (120-604800)

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. Encryption algorithms protect the data from being read by a third-party. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. 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.

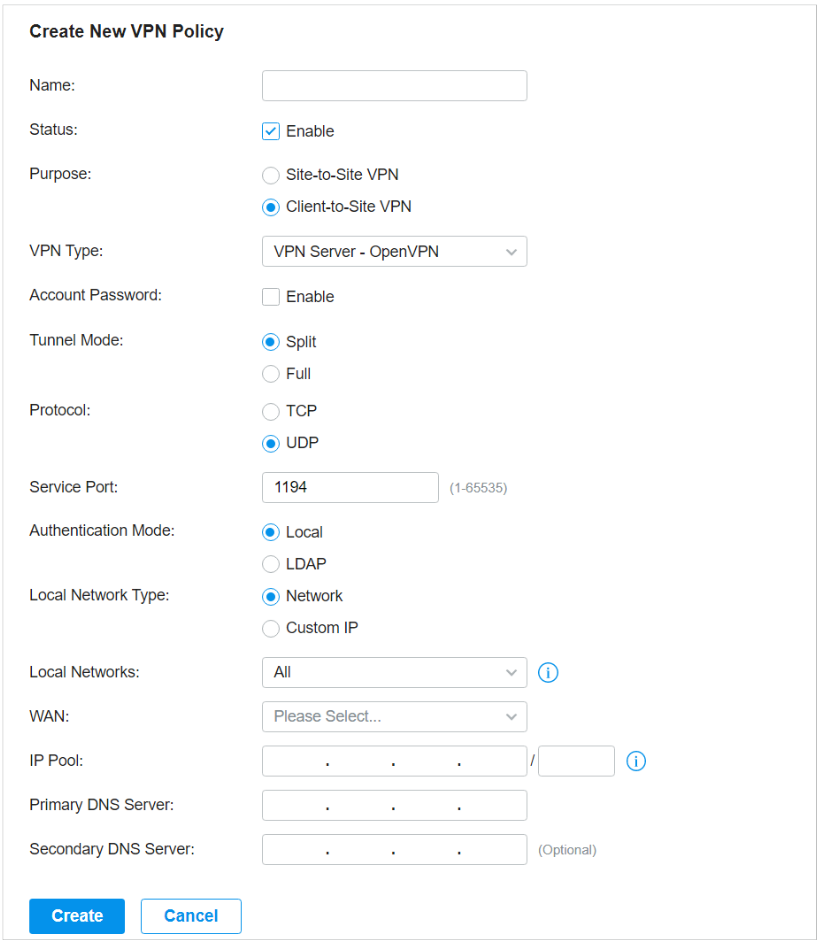
For Phase-2 Settings:

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. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy

Name:

Status: ☑ Enable

Purpose: ○ Site-to-Site VPN ● Client-to-Site VPN

VPN Type: VPN Server - OpenVPN

Account Password: □ Enable

Tunnel Mode: ● Split ○ Full

Protocol: ○ TCP ● UDP

Service Port: 1194 (1-65535)

Authentication Mode: ● Local ○ LDAP

Local Network Type: ● Network ○ Custom IP

Local Networks: All

WAN: Please Select...

IP Pool: . . . /

Primary DNS Server: . . .

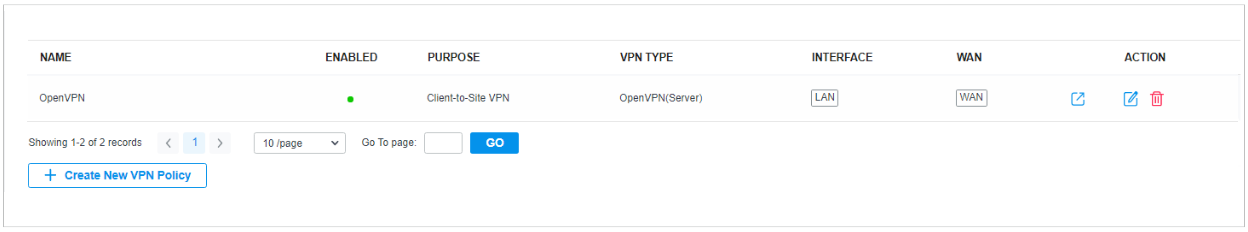
Secondary DNS Server: . . . (Optional)

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.
Status	Click the checkbox to enable 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.
Account Password	Specify whether VPN clients need to enter a user account to access the VPN tunnel. When enabled, you need to create accounts on the VPN User page.
Tunnel Mode	Select the tunnel mode: Split or Full. Full tunneling uses the VPN for all your traffic, whereas split tunneling sends part of your traffic through a VPN and part of it through the open network. Full tunneling is more secure than split tunneling.
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.
Authentication Mode	Select the authentication mode: Local or LDAP. LDAP is used for SSO (single sign-on), which enables users to use the same password in multiple services.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
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.
Primary DNS Server	Enter the IP address of the primary DNS server provided by your ISP.
Secondary DNS Server	(Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down.

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.



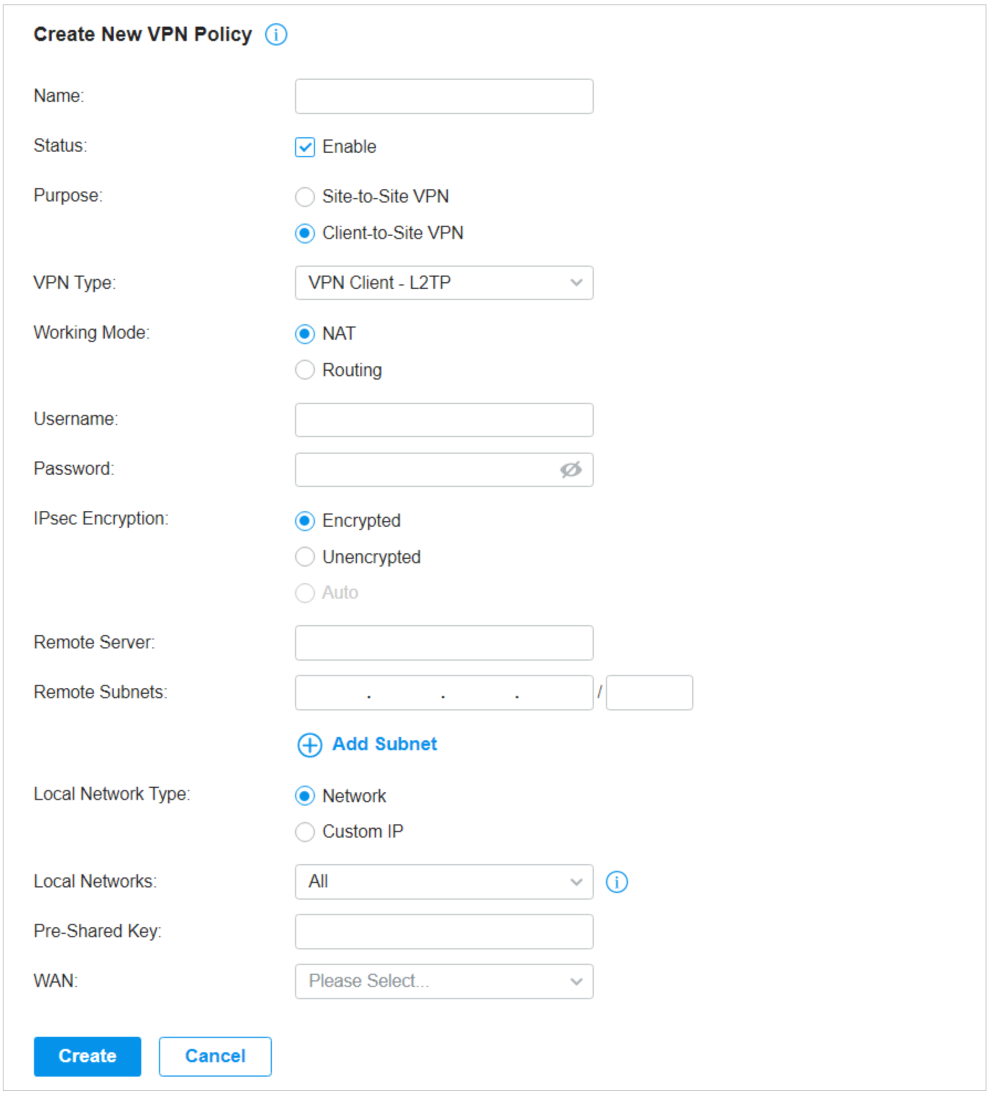
NAME	ENABLED	PURPOSE	VPN TYPE	INTERFACE	WAN	ACTION
OpenVPN	●	Client-to-Site VPN	OpenVPN(Server)	LAN	WAN	↗ ✎ 🗑

Showing 1-2 of 2 records < 1 > 10 /page Go To page: GO

+ Create New VPN Policy

- Configuring the gateway as a VPN client using L2TP

1. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy ⓘ

Name:

Status: ☑ Enable

Purpose: ○ Site-to-Site VPN
● Client-to-Site VPN

VPN Type: VPN Client - L2TP

Working Mode: ● NAT
○ Routing

Username:

Password:

IPsec Encryption: ● Encrypted
○ Unencrypted
○ Auto

Remote Server:

Remote Subnets: . . . /

⊕ Add Subnet

Local Network Type: ● Network
○ Custom IP

Local Networks: All ⓘ

Pre-Shared Key:

WAN: Please Select...

Create Cancel

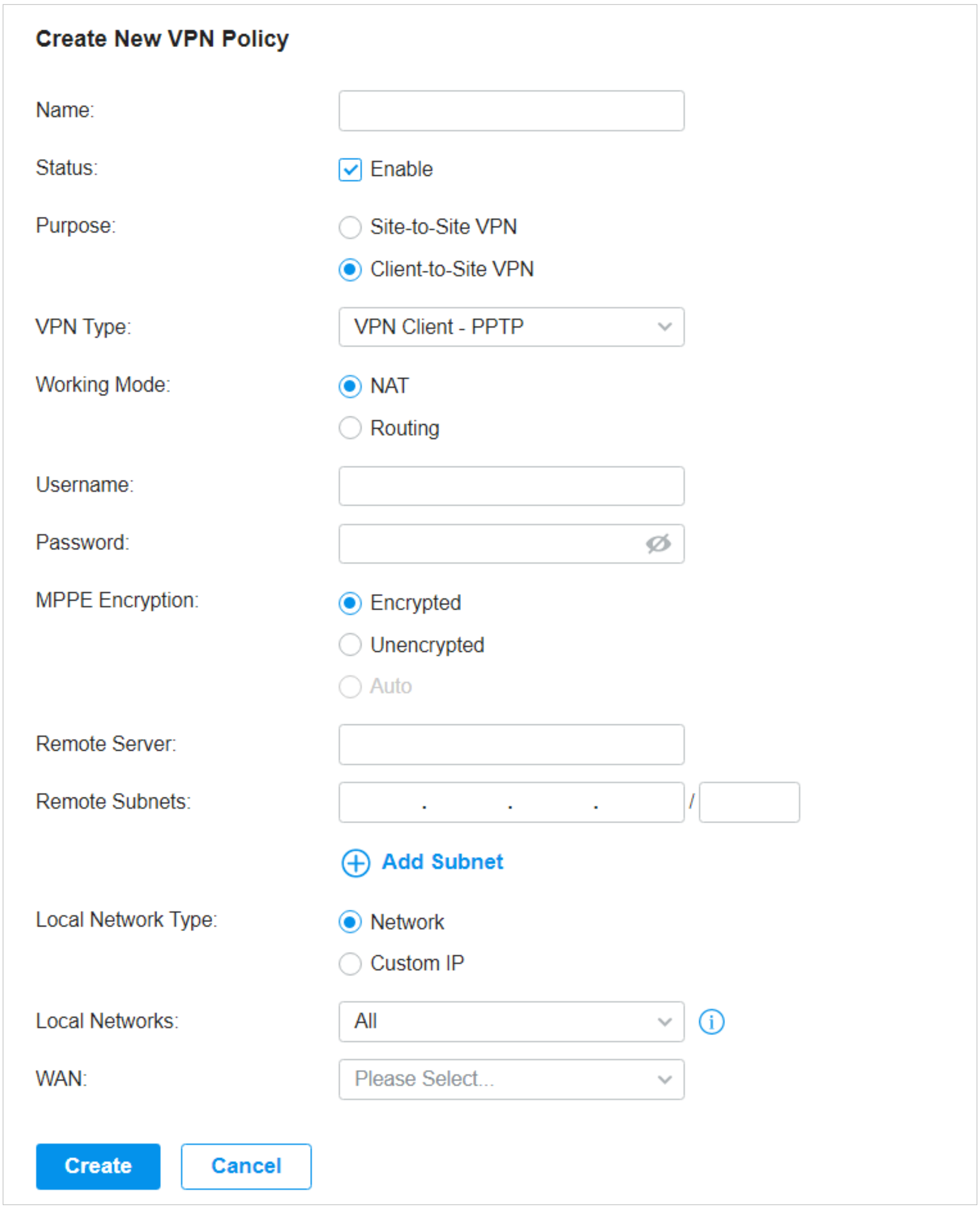
2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

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

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 Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
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. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy

Name:

Status: ☑ Enable

Purpose: ○ Site-to-Site VPN ● Client-to-Site VPN

VPN Type: VPN Client - PPTP

Working Mode: ● NAT ○ Routing

Username:

Password:

MPPE Encryption: ● Encrypted ○ Unencrypted ○ Auto

Remote Server:

Remote Subnets: . . . /

Local Network Type: ● Network ○ Custom IP

Local Networks: All

WAN: Please Select...

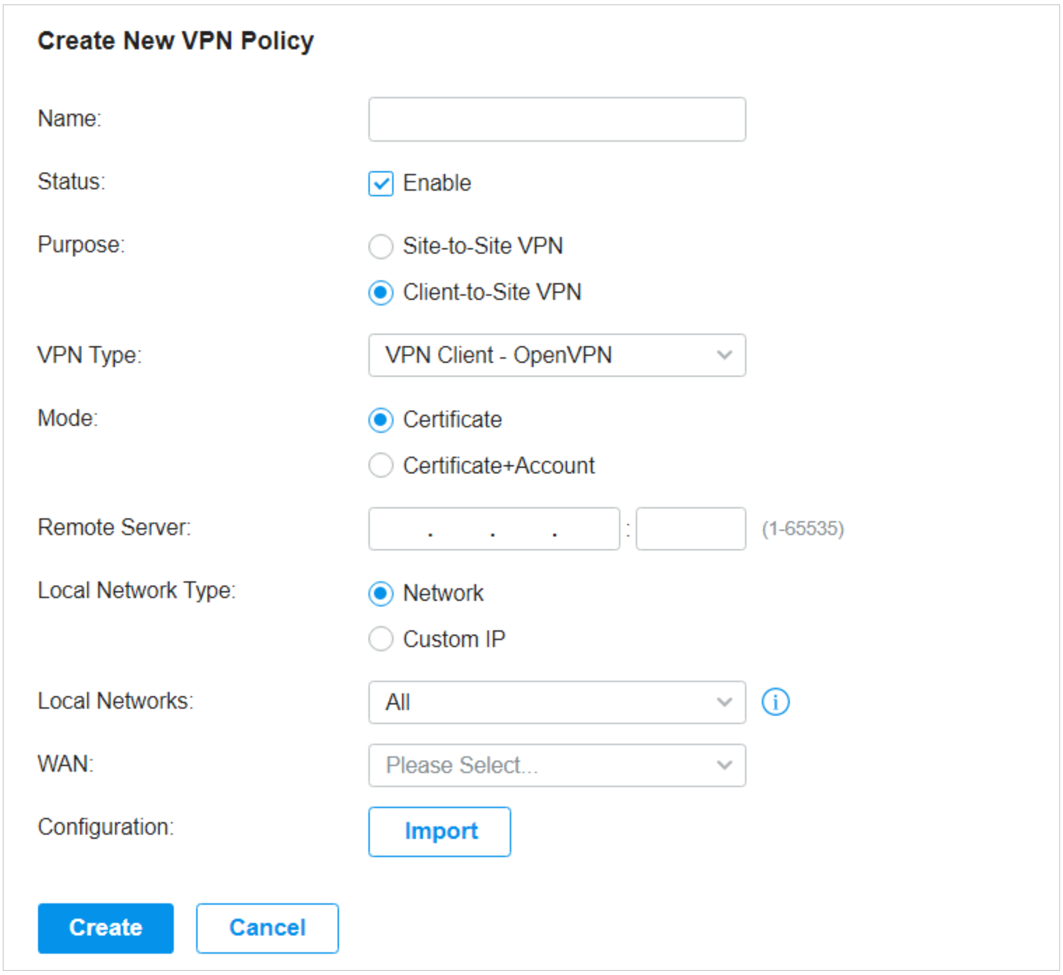
2. Enter a name to identify the VPN policy and select the purpose as Client-to-Site VPN. Refer to the following table to configure the required parameters and click Create.

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

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 Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
WAN	Select the WAN port on which the VPN tunnel is established.

- Configuring the gateway as a VPN client using OpenVPN

1. Select a site from the drop-down list of Organization. Go to Settings > VPN. Click + Create New VPN Policy to load the following page.



Create New VPN Policy

Name:

Status: ☑ Enable

Purpose: ○ Site-to-Site VPN ● Client-to-Site VPN

VPN Type: VPN Client - OpenVPN

Mode: ● Certificate ○ Certificate+Account

Remote Server: . . . : (1-65535)

Local Network Type: ● Network ○ Custom IP

Local Networks: All

WAN: Please Select...

Configuration: Import

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.
Status	Click the checkbox to enable 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.
Mode	Select the access mode according to VPN requirements. Certificate: Select this option if the VPN tunnel only requires the certificate. Certificate+Account: Select this option if the VPN tunnel requires the certificate and VPN user account. If selected, configure the following parameters: Username: Enter the username for the VPN tunnel. Password: Enter the password for the VPN tunnel.

Remote Server	Enter the IP address or domain name of the OpenVPN server.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
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.

1. 7. 2 VPN User

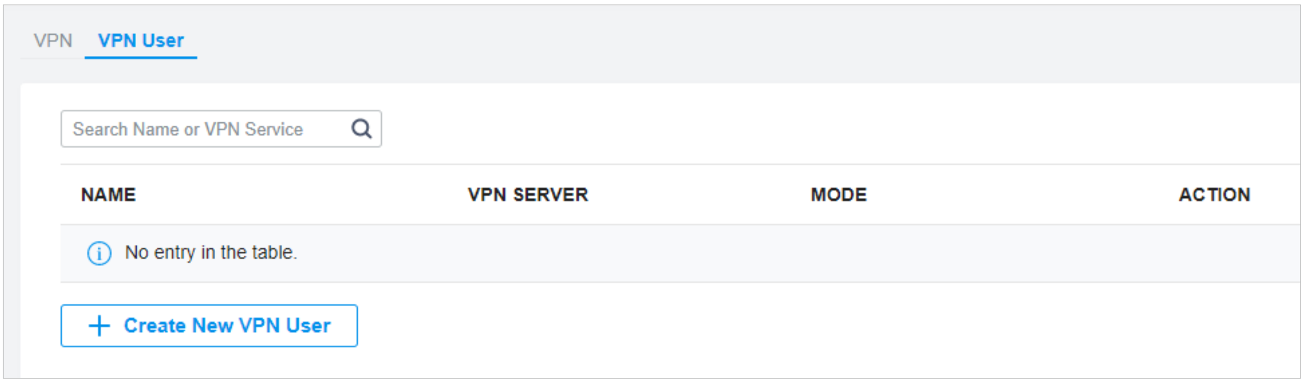
Overview

VPN User is used to configure and record your custom settings for VPN configurations, and it allows you to configure VPN users that can be used for multiple VPN servers. It saves you from setting the VPN users with the same configurations repeatedly when you want to apply the user in different VPN servers.

Configuration

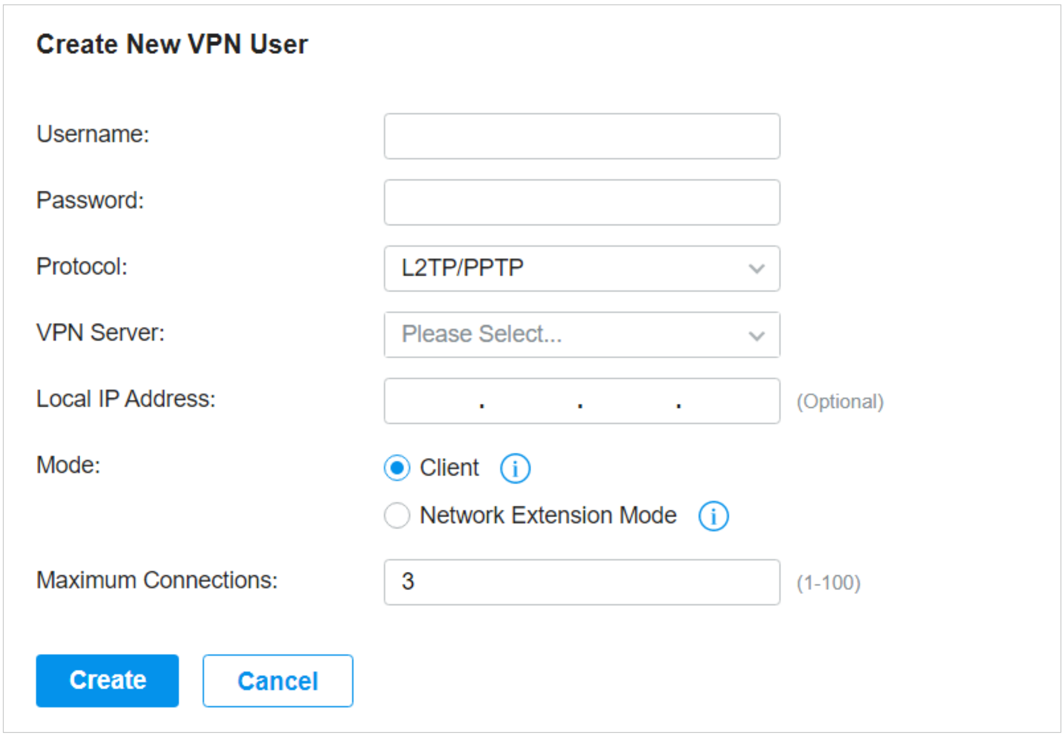
To configure the VPN users, follow these steps:

1. Select a site from the drop-down list of Organization. Go to Settings > VPN >VPN User. Click +Create New VPN User to add a new entry of VPN User.



NAME	VPN SERVER	MODE	ACTION
No entry in the table.			

2. Specify the parameters and click Create.



Create New VPN User

Username:		
Password:		
Protocol:	L2TP/PPTP	
VPN Server:	Please Select...	
Local IP Address:	. . .	(Optional)
Mode:	● Client ○ Network Extension Mode	
Maximum Connections:	3	(1-100)

Username	Enter the username used for the VPN tunnel. The client use the username for the validation before accessing the network.
Password	Enter the password of user. The client uses the password for the validation before accessing the network.
Protocol	Select the protocol type for the VPN tunnel.

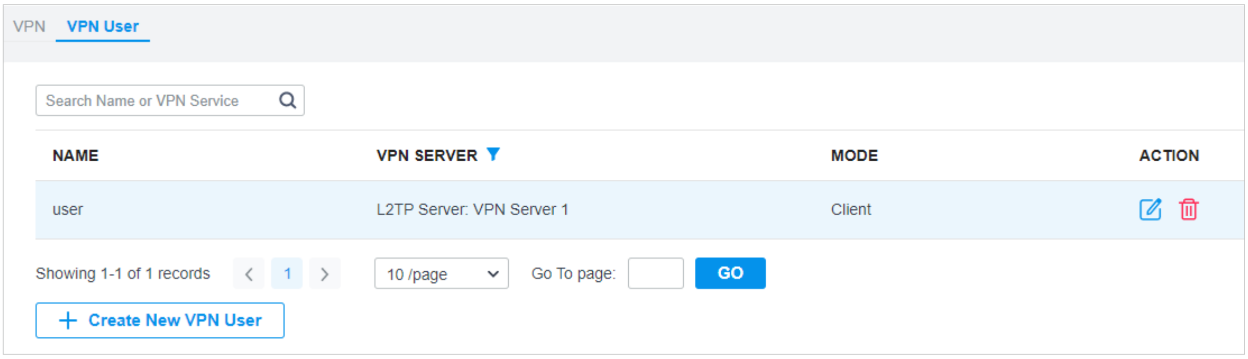
If you selected the L2TP/PPTP protocol, specify the following parameters:

VPN Server	Select the VPN server that the VPN user is applied to.
Local IP Address	(Optional) Specify the local IP address of the VPN tunnel.
Mode	Specify the connection mode for the VPN 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 subnets in Remote Subnets.

If you selected the OpenVPN protocol, specify the following parameter:

VPN Server	Select the VPN server that the VPN user is applied to.

To edit or delete the VPN users, click the icon in the Action column. You can further filter the entries based on the VPN Server.



NAME	VPN SERVER ▼	MODE	ACTION
user	L2TP Server: VPN Server 1	Client	✎ 🗑

▼	Filter the entries.
✎	View and edit the account information of users.
🗑	Delete the VPN user.

1.7.3 SSL VPN

Overview

SSL VPN uses Secure Socket Layer (SSL) to ensure information safety and provides abundant services such as user management, resource management, user lockout, authentication and accounting.

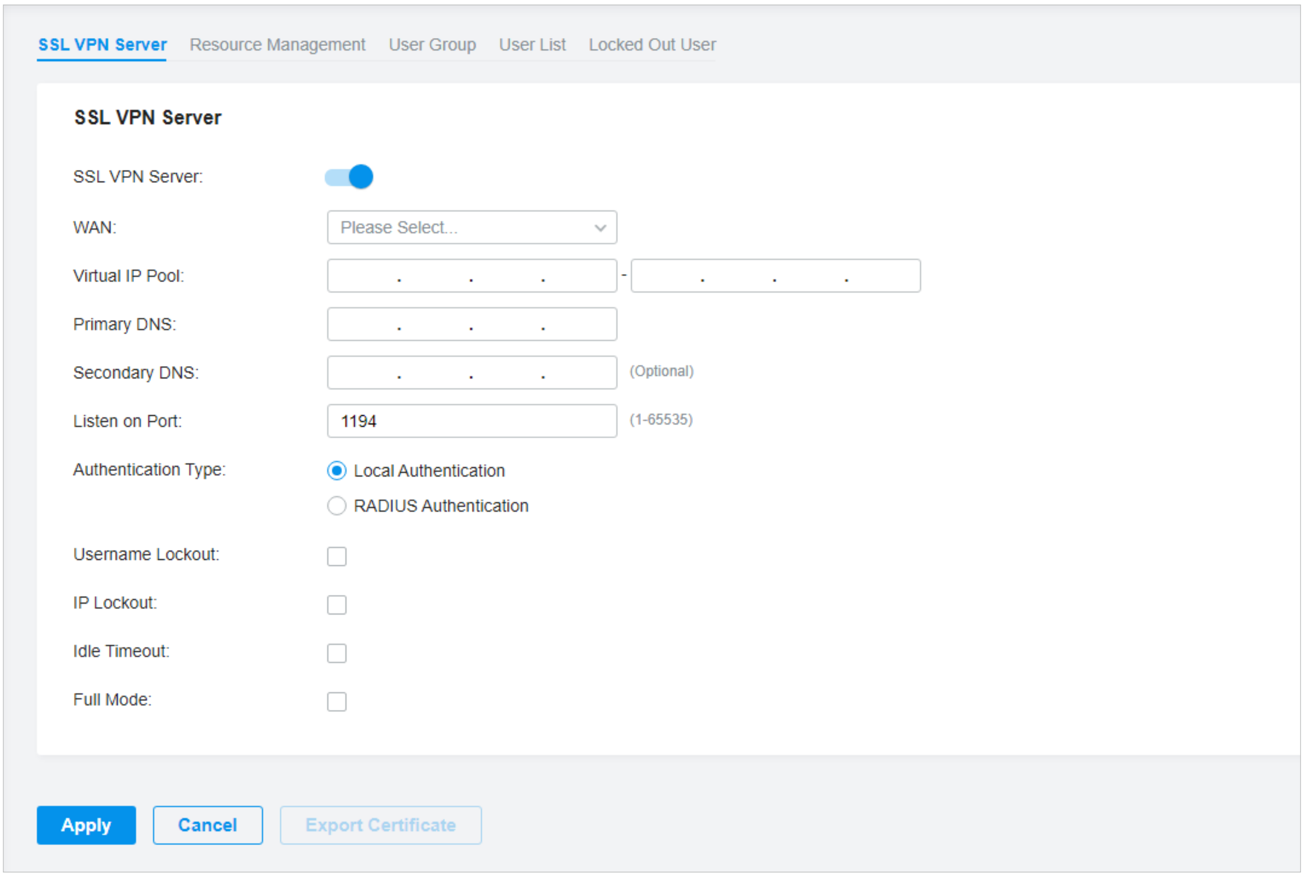
SSL VPN uses username and password for authentication and login. A network administrator can assign different resources to different types of users, and meanwhile associate the users with multiple resources, making it easy to manage and limit the services the users can access through the VPN.

Configuration

- **SSL VPN Server**

  In SSL VPN Server, you can enable the feature and configure the SSL VPN settings.

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > SSL VPN > SSL VPN Server. Enable SSL VPN Server.



SSL VPN Server

SSL VPN Server: ●

WAN: Please Select...

Virtual IP Pool: . . . - . . .

Primary DNS: . . .

Secondary DNS: . . . (Optional)

Listen on Port: 1194 (1-65535)

Authentication Type: ● Local Authentication ○ RADIUS Authentication

Username Lockout: □

IP Lockout: □

Idle Timeout: □

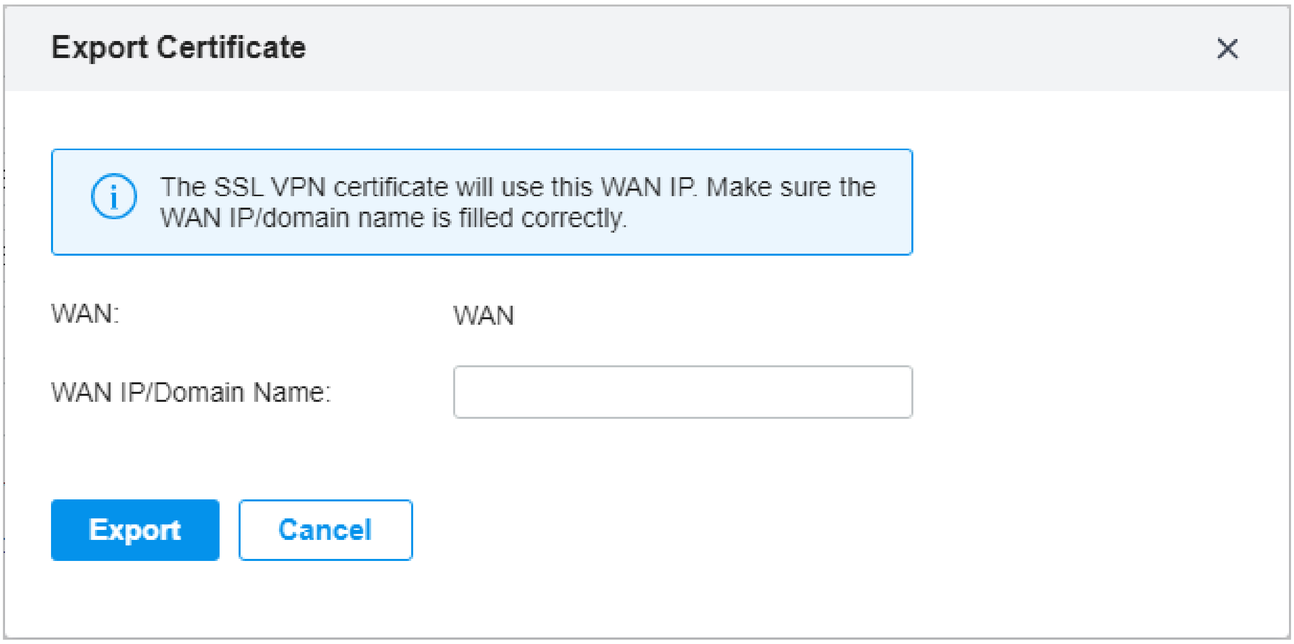
Full Mode: □

2. Configure the parameters according to your needs. Click Apply.

WAN	Select the port for the SSL VPN server to listen on, and the VPN tunnel will take effect on the port.
Virtual IP Pool	Set a virtual IP Pool, and the SSL VPN server will assign an IP address to a connected client within the pool.
Primary/Secondary DNS	Specify the IP address of the DNS server. The clients will be informed of the DNS server, and it can help the clients resolve the domain name.
Listen on Port	Specify the port for the SSL VPN server to listen on. By default, it is 1194.

Authentication Type	Select the authentication for the clients: Local Authentication or RADIUS Authentication. If you selected RADIUS Authentication, configure the following parameters: RADIUS Server: Select a RADIUS server profile. Authentication Type: Select the authentication protocol for the RADIUS server. Max Requests: Specify the maximum number of requests sent when no response is received. Request Timeout: Specify the maximum interval for request timeout. After timeout, the request will be sent again. NAS IP: Specify the IP address for the router to communicate with the RADIUS server.
Username Lockout	When enabled, you can lock out a username in case of excessive login attempts. Max Login Attempts: Specify the maximum failed login attempts for a username. If the number of attempts reaches this amount, the username will be locked out. Lockout Duration: Specify how long the username will be locked out.
IP Lockout	When enabled, you can lock out an IP address in case of excessive login attempts. Max Login Attempts: Specify the maximum failed login attempts for a login IP. If the number of attempts reaches this amount, the login IP will be locked out. Lockout Duration: Specify how long the login IP will be locked out.
Idle Timeout	When enabled, the VPN tunnel will close automatically if there is no traffic for the specified amount of time.
Full Mode	When enable, all traffic will go through the SSL VPN tunnel. When disabled, only the resource-related traffic will go through the tunnel.

3. Click Export Certificate, enter the WAN IP/Domain Name to access the VPN, then click Export. The VPN configuration file will be exported for clients to access the VPN.



Export Certificate

The SSL VPN certificate will use this WAN IP. Make sure the WAN IP/domain name is filled correctly.

WAN: WAN

WAN IP/Domain Name:

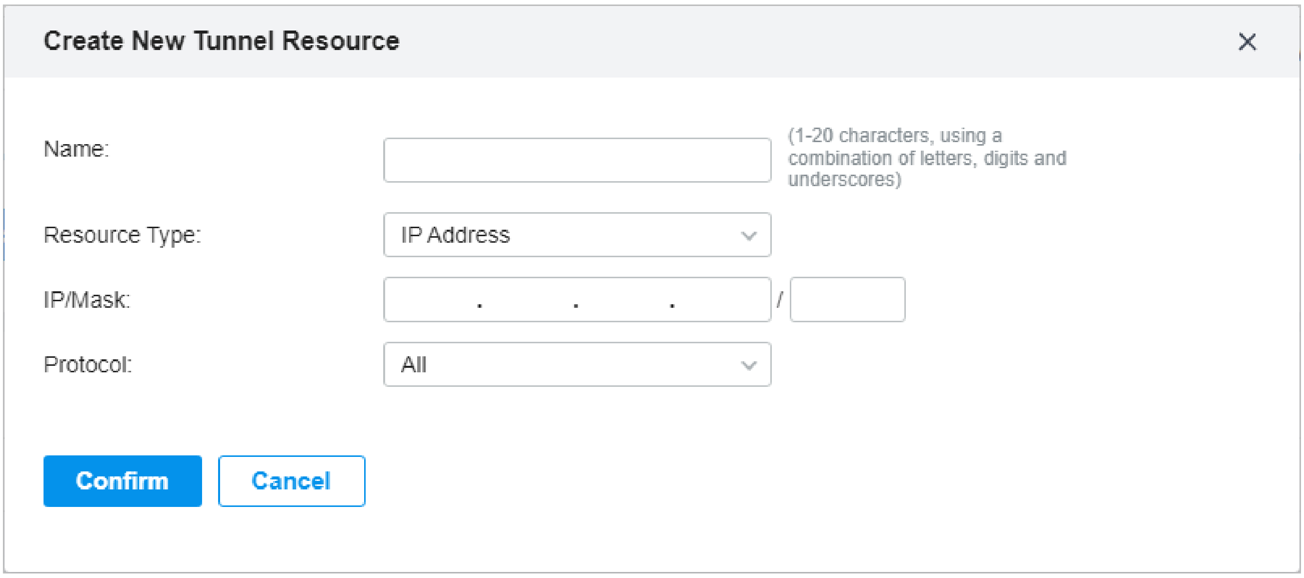
- **Resource Management**

  In Tunnel Resources, you can configure the resources the clients can access through the VPN tunnel, including IP range and domain name.

  In Resource Group, you can add the multiple tunnel resources to a group for better management. By default, two resource groups are provided: Group_ALL (indicates all resources) and Group_LAN (indicates all LAN resources).

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > SSL VPN > Resource Management.

2. Click Create New Tunnel Resource to load the following page. Configure the parameters and click Confirm.



Create New Tunnel Resource

Name: (1-20 characters, using a combination of letters, digits and underscores)

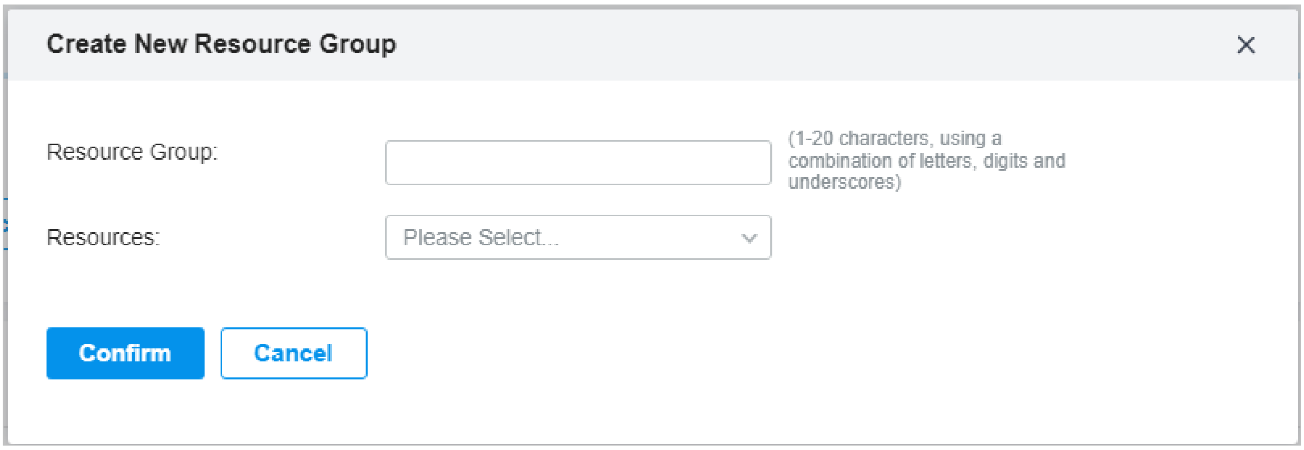
Resource Type: IP Address

IP/Mask: . . . /

Protocol: All

Name	Specify a name for the entry.
Resource Type	Select the type for the resources: IP Address or Domain Name. If you selected IP Address, configure the following parameters: IP/Mask: Specify IP range the clients can access. Protocol: Select the protocol type that the client can access in the IP range, and the router will filter illegal packets through firewall rules. By default, the value is ALL, and it means there is no restriction on the client. If you selected Domain Name, specify domain name the clients can access.

3. Click Create New Resource Group to load the following page. Configure the parameters and click Confirm.



Create New Resource Group

Resource Group: (1-20 characters, using a combination of letters, digits and underscores)

Resources: Please Select...

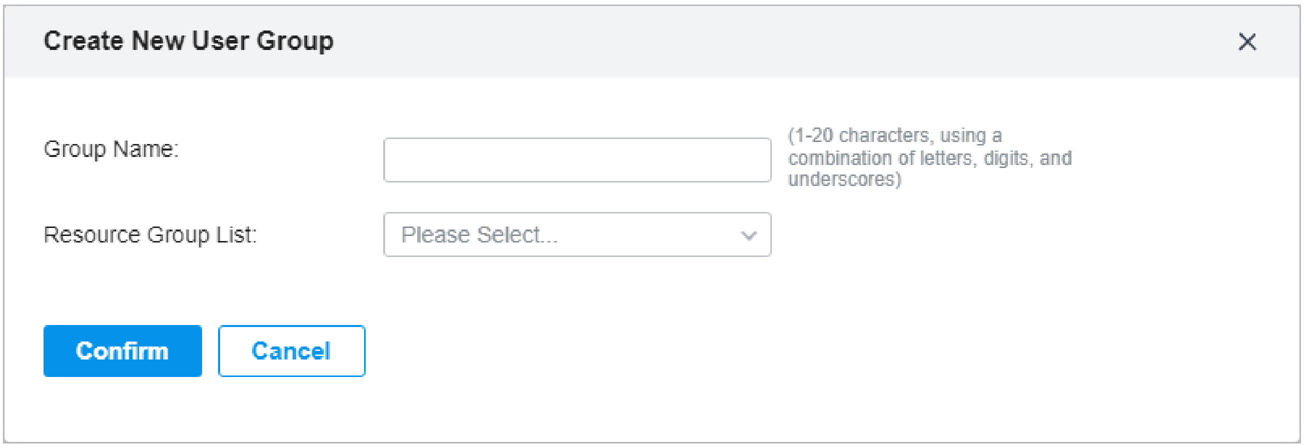
Resource Group	Specify a name for the resource group.

Resources	Select the resources for the group.

- **User Group**

In User Group, you can add multiple users to a group for better management.

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > SSL VPN > User Group.
2. Click Create New User Group to load the following page. Configure the parameters and click Confirm.



Create New User Group

Group Name: (1-20 characters, using a combination of letters, digits, and underscores)

Resource Group List: Please Select...

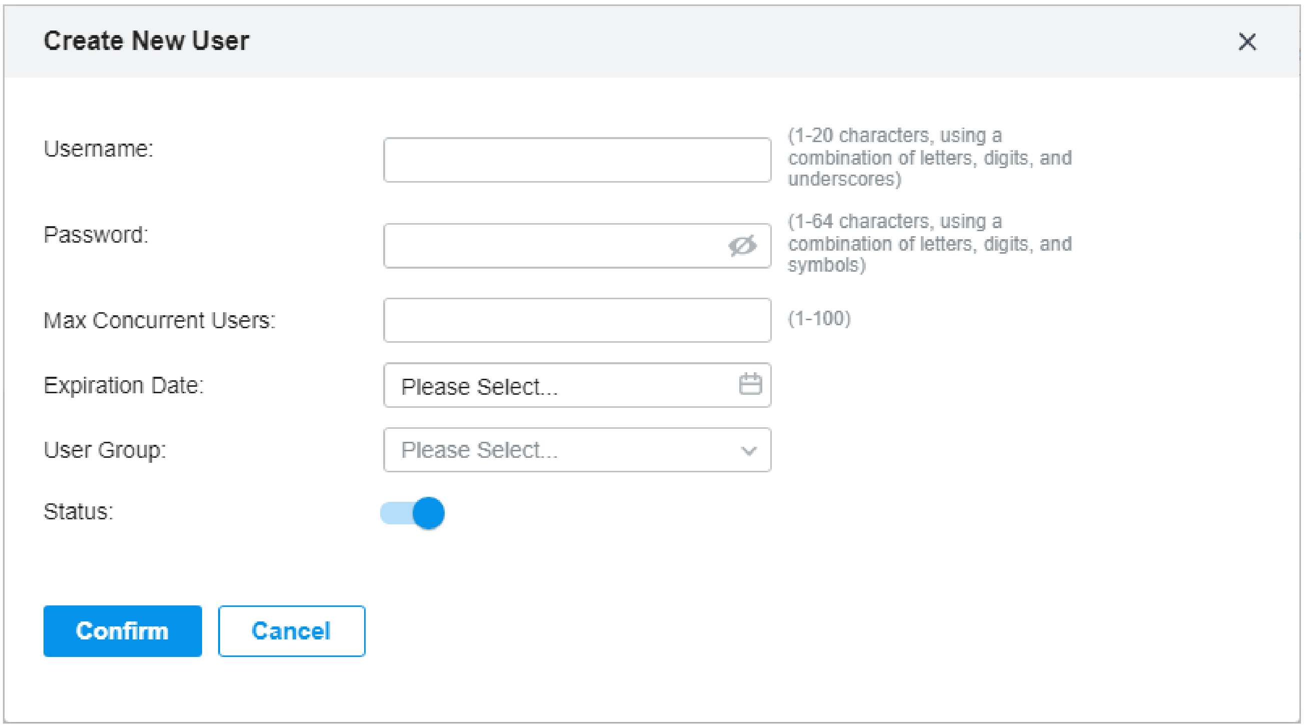
Group Name	Specify a name for the user group.
Resource Group List	Select the resource group for the user group.

- **User List**

In User List, you can view and configure all user settings of the SSL VPN.

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > SSL VPN > User List.

2. Click Create New User to load the following page. Configure the parameters and click Confirm.



Create New User

Username:		(1-20 characters, using a combination of letters, digits, and underscores)
Password:		(1-64 characters, using a combination of letters, digits, and symbols)
Max Concurrent Users:		(1-100)
Expiration Date:	Please Select...	
User Group:	Please Select...	
Status:	●	

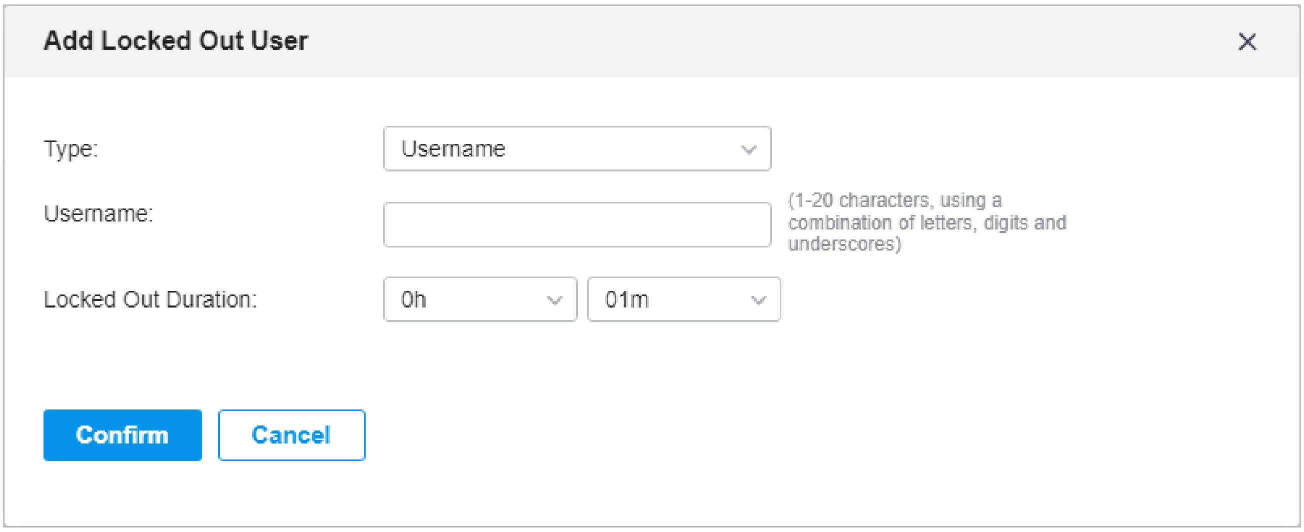
Username	Specify the username a client used for login.
Password	Specify the password a client used for login.
Max Concurrent Users	Specify the maximum number of clients using the username for login concurrently. If the number reaches this amount, new login attempts will be rejected.
Expiration Date	Specify when the user account will expire.
User Group	Select which group the user belongs to. A user can only be added to one user group.
Status	Click the checkbox to enable this entry.

- **Locked Out User**

  In Locked Out User, you can view the currently locked out users, and add, delete or edit an entry.

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > SSL VPN > Locked Out User.

2. Click Add Locked Out User to load the following page. Configure the parameters and click Confirm.



Add Locked Out User

Type: Username

Username: (1-20 characters, using a combination of letters, digits and underscores)

Locked Out Duration: 0h 01m

Type	Specify the locked out type. If you selected Username, specify the username of a locked out user. If you selected IP Address, specify the IP address of a locked out user.
Lockout Duration	Specify how long the entry will be locked out.

1. 7. 4 WireGuard VPN

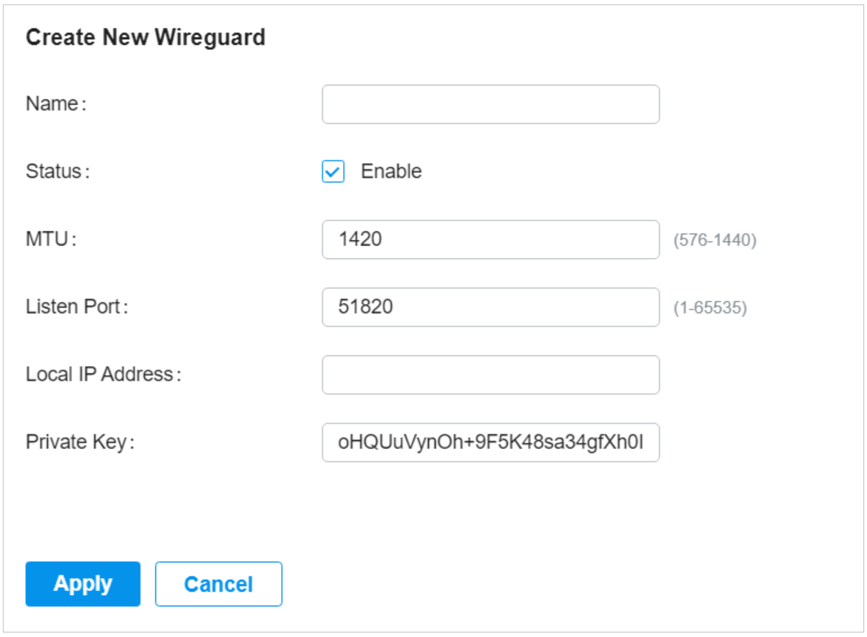
Overview

WireGuard VPN is a secure, fast and modern VPN protocol. It is based on the UDP protocol and uses modern encryption algorithms to improve work efficiency.

- **WireGuard**

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > WireGuard.

2. Click Create New WireGuard. Configure the parameters and click Apply.



Create New Wireguard

Name:

Status: ☑ Enable

MTU: 1420 (576-1440)

Listen Port: 51820 (1-65535)

Local IP Address:

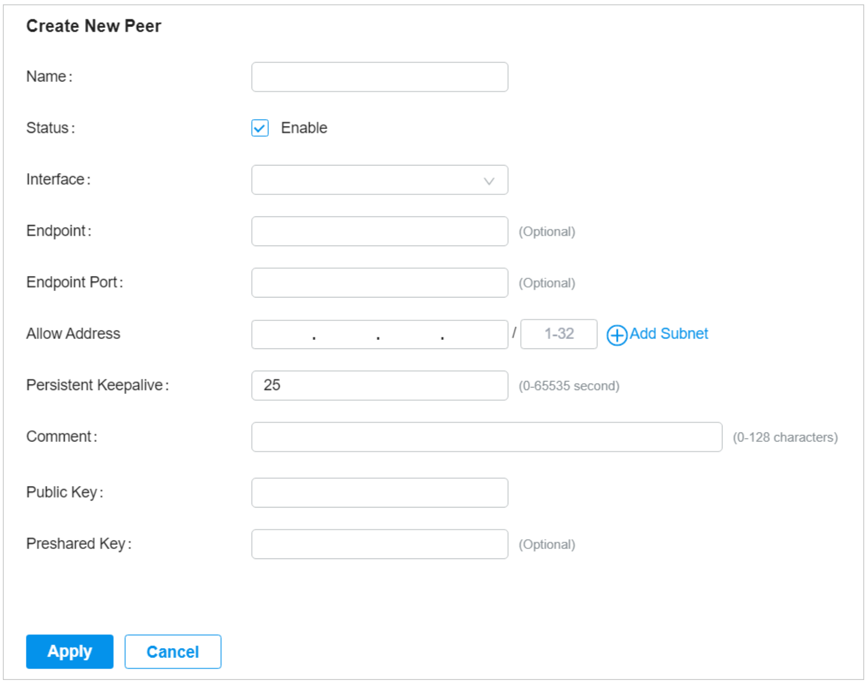
Private Key: oHQUuVynOh+9F5K48sa34gfXh0I

Name	Specify the name that identifies the WireGuard interface.
Status	Specify whether to enable the WireGuard interface.
MTU	Specify the MTU value of the WireGuard interface. The default value 1420 is recommended.
Listen Port	Specify the port number that the WireGuard interface listens to.
Local IP Address	Specify the IP address of the WireGuard interface.
Private Key	Specify the private key of the WireGuard interface. The value will be automatically generated on the device, and you can also modify it manually.

- Peers

1. Select a site from the drop-down list of Organization. Go to Settings > VPN > WireGuard > Peers.

2. Click Create New Peer. Configure the parameters and click Apply.



Create New Peer

Name:	
Status:	☑ Enable
Interface:	
Endpoint:	(Optional)
Endpoint Port:	(Optional)
Allow Address	. . . / 1-32 ⊕Add Subnet
Persistent Keepalive:	25 (0-65535 second)
Comment:	(0-128 characters)
Public Key:	
Preshared Key:	(Optional)

Name	Specify the name that identifies the peer.
Status	Specify whether to enable the peer.
Interface	Specify the WireGuard interface to which the peer belongs.
Endpoint	Specify the IP address of the peer. This parameters is required when the Omada Router actively connects to other WireGurad Server.
Endpoint Port	Specify the port number of the peer. This parameters is required when the Omada Router actively connects to other WireGurad Server.
Allowed Address	Specify the address segment that allows traffic to pass through. Generally, it is the same as the WireGuard VPN interface IP configured on the remote device.
Persistent Keepalive	Specify the tunnel keepalive packet interval.
Comment	Enter the description of the peer.
Public Key	Fill in the public key information exported from the remote device.
Preshared Key	Specify an optional shared key.

1. 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.

1. 8. 1 Time Range

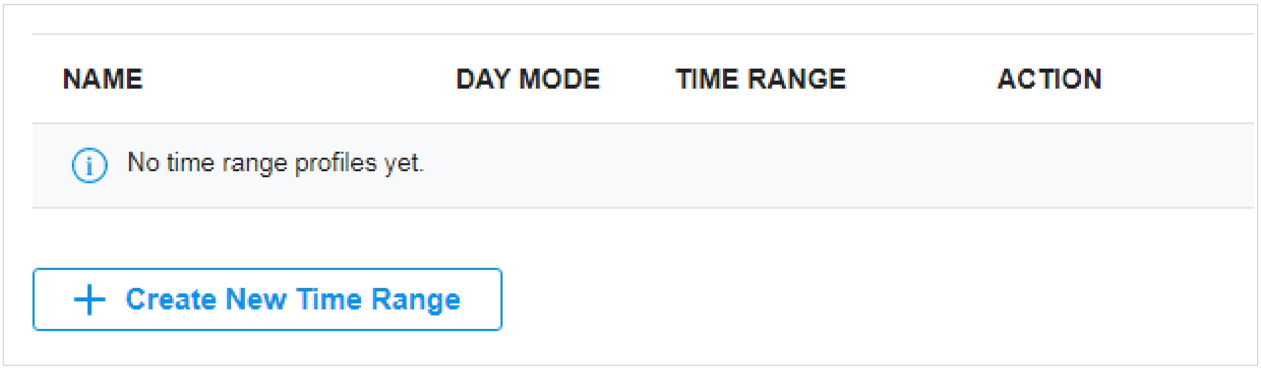
Overview

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:

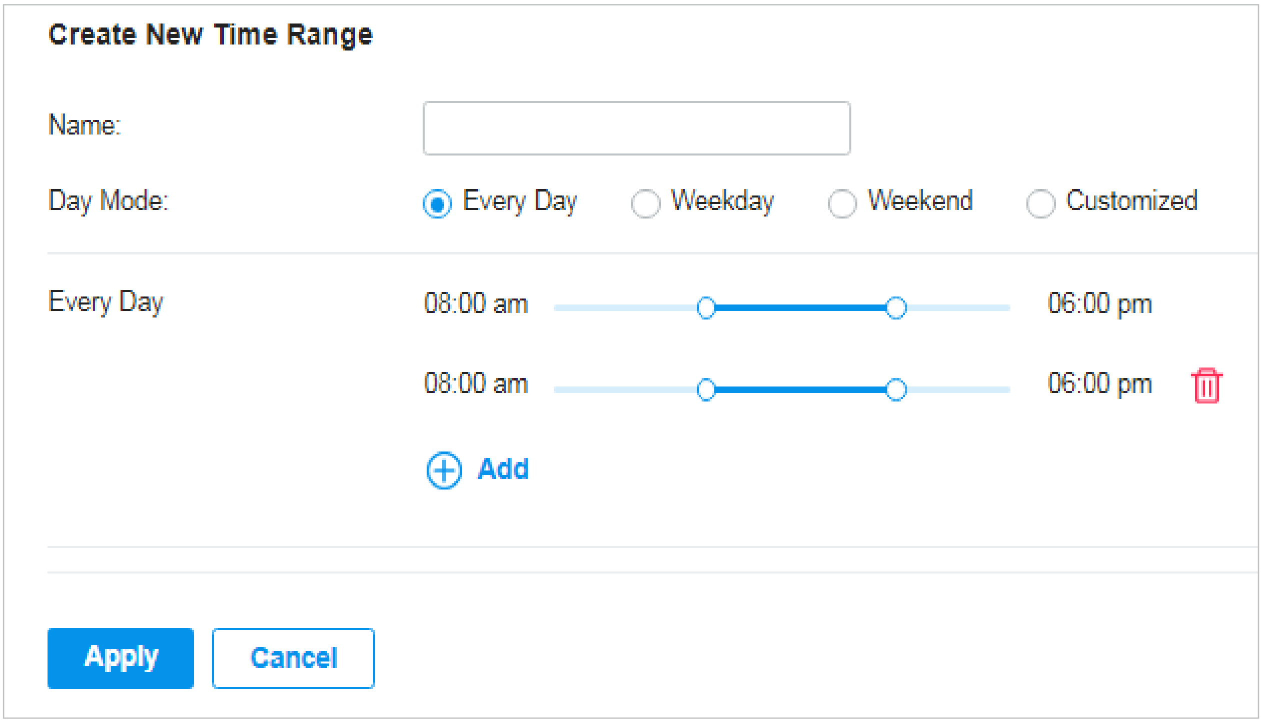
1. Select a site from the drop-down list of Organization. Go to Settings > Profiles >Time Range. Click +Create New Time Range to add a new time range entry. By default, there is no entry in the list.



NAME	DAY MODE	TIME RANGE	ACTION
ⓘ No time range profiles yet.			

2. Enter a Name for the new entry, select the Day Mode, and specify the time range. Click +Add to add a new time period, 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 4. 4. 3 WLAN Schedule, and 4. 10. 8 PoE Schedule.



Create New Time Range

Name:

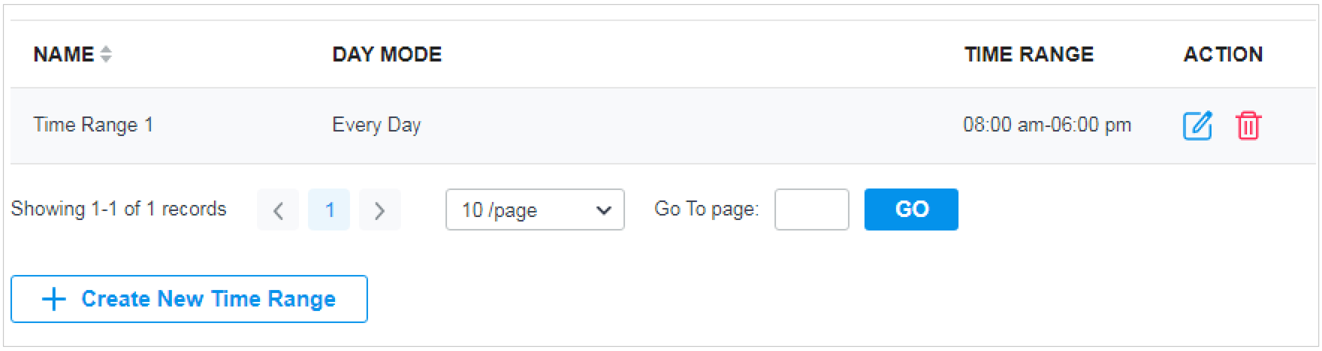
Day Mode: ● Every Day ○ Weekday ○ Weekend ○ Customized

Every Day 08:00 am 06:00 pm

08:00 am 06:00 pm

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.



NAME	DAY MODE	TIME RANGE	ACTION
Time Range 1	Every Day	08:00 am-06:00 pm	

Showing 1-1 of 1 records

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

✎	Edit the parameters in the entry.
🗑	Delete the entry.

1. 8. 2 Groups

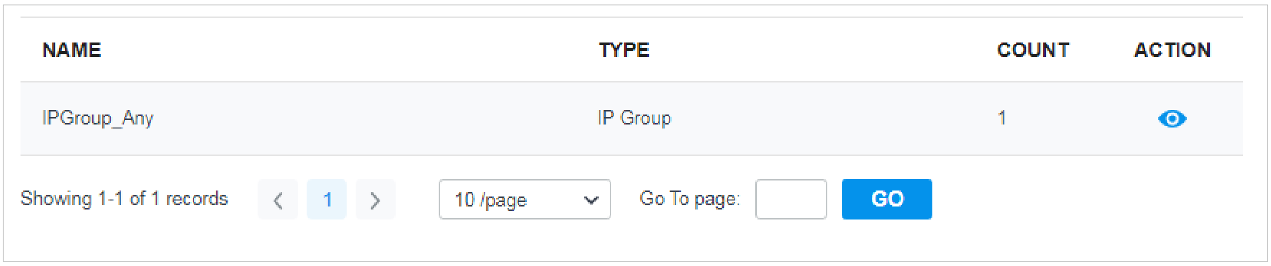
Overview

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:

1. Select a site from the drop-down list of Organization. Go to Settings > Profiles > Groups. By default, there is an entry covering all IPs, and it is not editable and deletable. Click +Create New Group to add a new group entry.



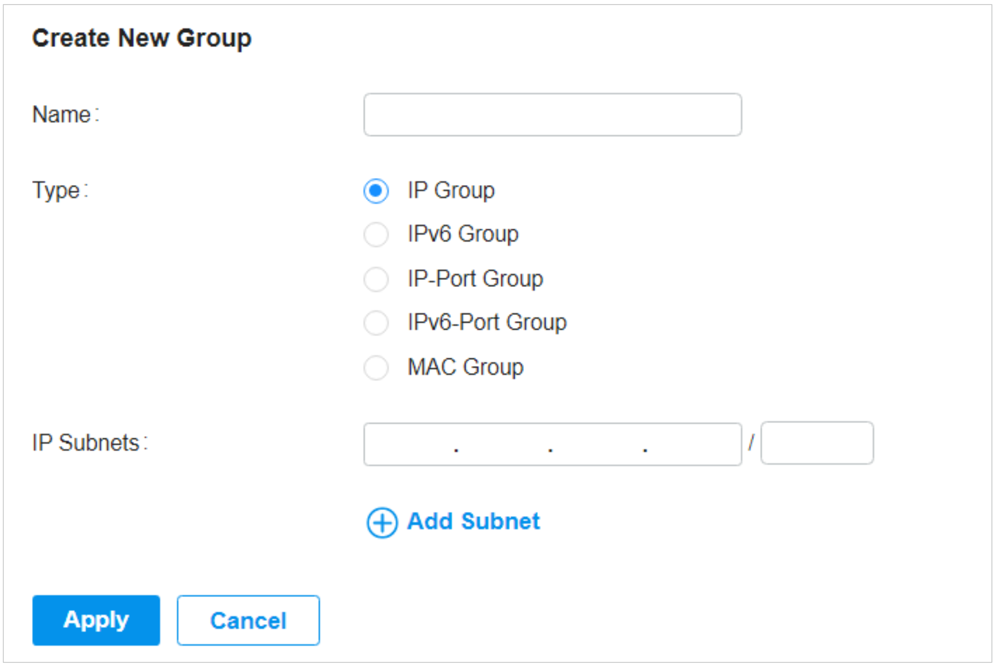
NAME	TYPE	COUNT	ACTION
IPGroup_Any	IP Group	1	👁

Showing 1-1 of 1 records

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.



Create New Group

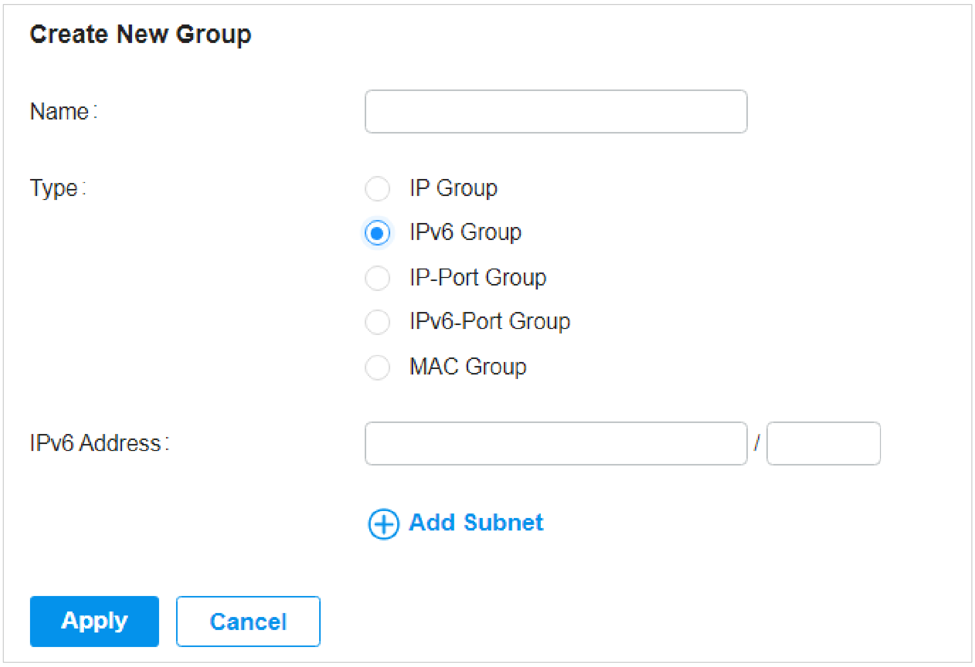
Name:

Type:
● IP Group
○ IPv6 Group
○ IP-Port Group
○ IPv6-Port Group
○ MAC Group

IP Subnets: . . . /

- **Based on IPv6 Group**

  To configure a group profile based on IPv6 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.



Create New Group

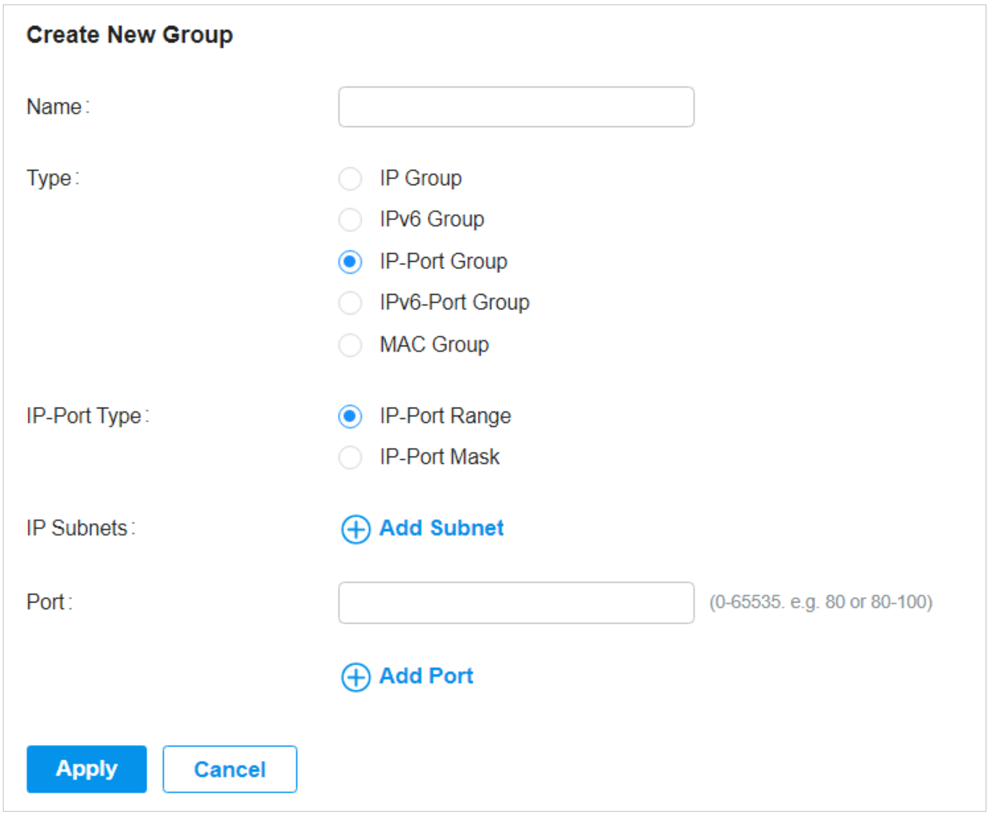
Name:

Type:
○ IP Group
● IPv6 Group
○ IP-Port Group
○ IPv6-Port Group
○ MAC Group

IPv6 Address: /

- **Based on IP-Port Group**

  To configure a group profile based on IP-Port Group, you are required to specify IP-Port type and 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.



Create New Group

Name:

Type:
○ IP Group
○ IPv6 Group
● IP-Port Group
○ IPv6-Port Group
○ MAC Group

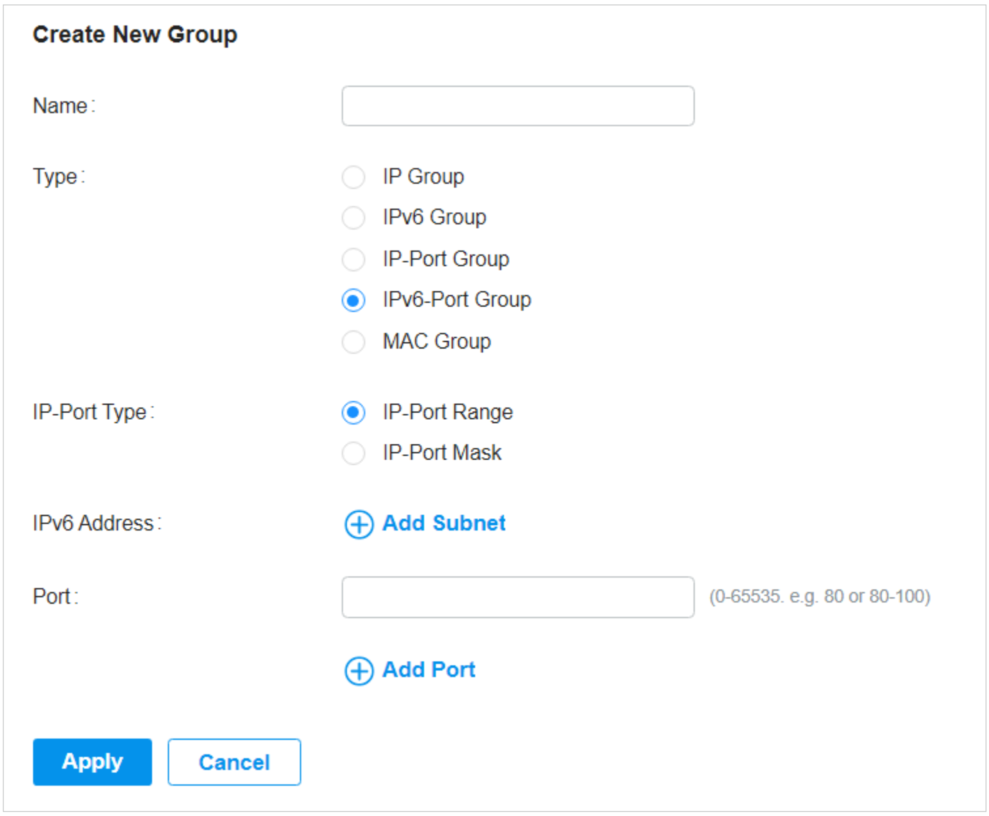
IP-Port Type:
● IP-Port Range
○ IP-Port Mask

IP Subnets: ⊕ Add Subnet

Port: (0-65535. e.g. 80 or 80-100)

- **Based on IPv6-Port Group**

  To configure a group profile based on IPv6-Port Group, you are required to specify IP-Port type and 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.



Create New Group

Name :

Type : ○ IP Group ○ IPv6 Group ○ IP-Port Group ● IPv6-Port Group ○ MAC Group

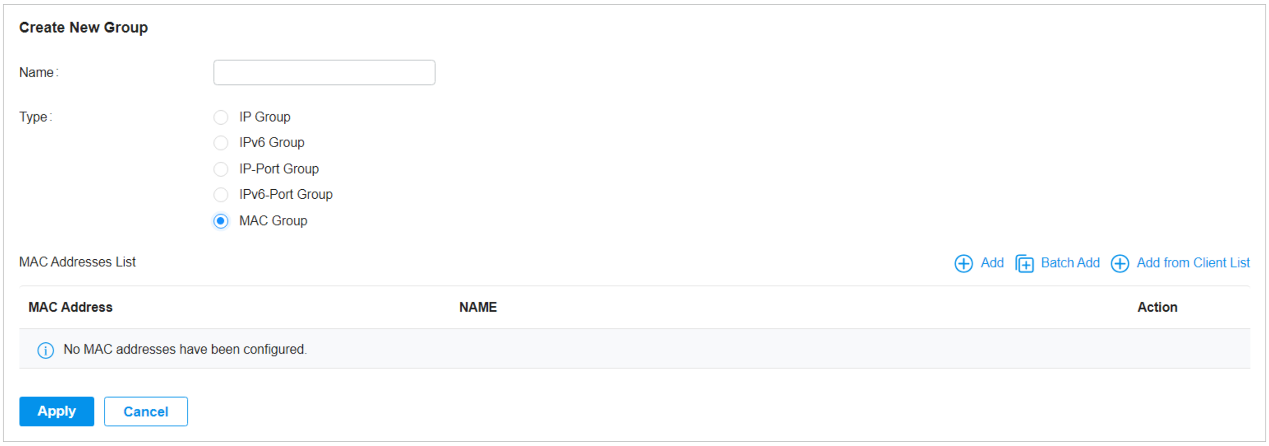
IP-Port Type : ● IP-Port Range ○ IP-Port Mask

IPv6 Address :

Port : (0-65535. e.g. 80 or 80-100)

- **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.



Create New Group

Name :

Type : ○ IP Group ○ IPv6 Group ○ IP-Port Group ○ IPv6-Port Group ● MAC Group

MAC Addresses List

MAC Address	NAME	Action
No MAC addresses have been configured.		

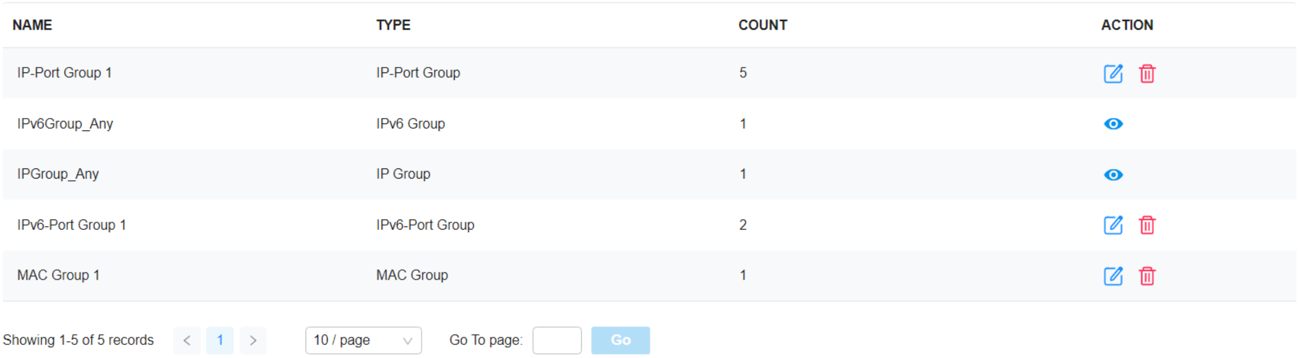
⊕ Add	Add MAC address singly.

⊞ 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 current 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.

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 4. 5. 1 ACL, 4. 6. 1 Routing, 4. 6. 2 NAT.

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



NAME	TYPE	COUNT	ACTION
IP-Port Group 1	IP-Port Group	5	✎ 🗑
IPv6Group_Any	IPv6 Group	1	👁
IPGroup_Any	IP Group	1	👁
IPv6-Port Group 1	IPv6-Port Group	2	✎ 🗑
MAC Group 1	MAC Group	1	✎ 🗑

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.

1. 8. 3 Rate Limit

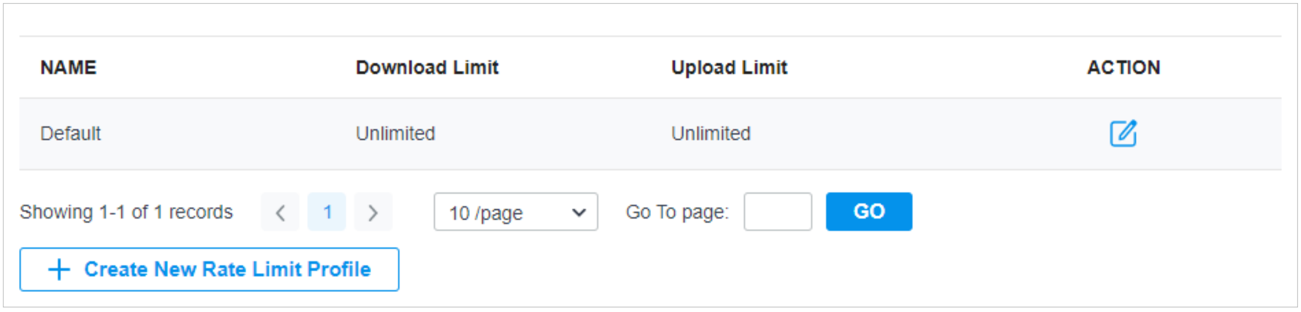
Overview

Rate Limit allows you to customize rate-related configurations. You can set different rate limit templates. They can be bound with wireless network to limit the upload/download rate of clients connected the SSID, and applied to specific types of Portal, such as Local User and Voucher. After creating the profiles, you can apply them to multiple configurations, saving you from repeatedly setting up the same information.

Configuration

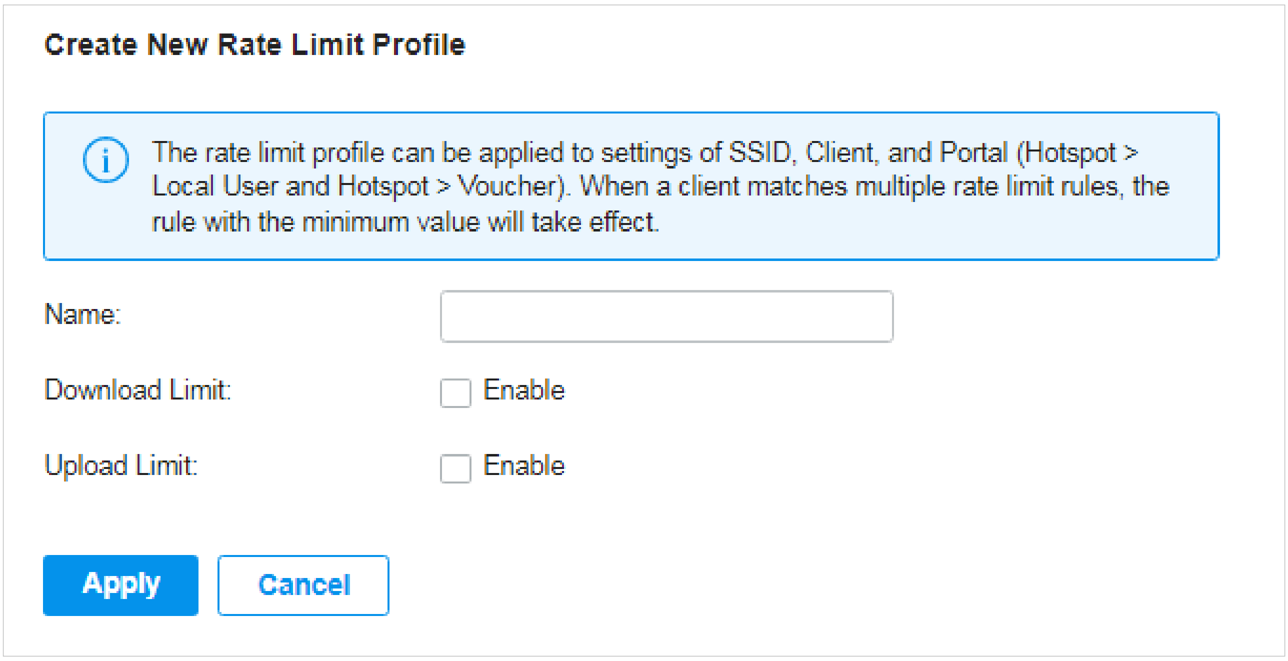
To configure the rate limit profiles, follow these steps:

1. Select a site from the drop-down list of Organization. Go to Settings > Profiles > Rate Limit. By default, there is an entry with no limits, and it can not be deleted. Click +Create New Rate Limit Profile to add a new group entry.



NAME	Download Limit	Upload Limit	ACTION
Default	Unlimited	Unlimited	✎

2. Enter a name and specify the download/upload rate limit for the new entry. After saving the newly added entry, you can apply them to other configurations. To apply the customized rate limit profiles in the related configurations, refer to 4. 9. 1 Portal, 4. 4. 1 Set Up Basic Wireless Networks, and 7. 1. 3 Using the Properties Window to Monitor and Manage the Clients.



Create New Rate Limit Profile

The rate limit profile can be applied to settings of SSID, Client, and Portal (Hotspot > Local User and Hotspot > Voucher). When a client matches multiple rate limit rules, the rule with the minimum value will take effect.

Name:

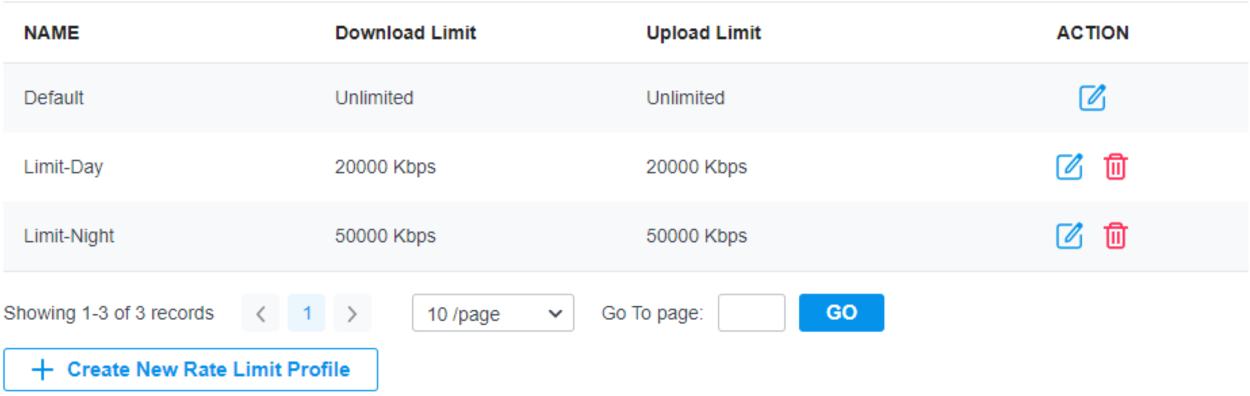
Download Limit: □ Enable

Upload Limit: □ Enable

Name	Enter a name to identify the created rate limit profile.
Download Limit	Enable the download limit, and specify the rate limit correspondingly in Kbps or Mbps.
Upload Limit	Enable the upload limit, and specify the rate limit correspondingly in Kbps or Mbps.

3. Click Apply to save the entry. After saving the newly added entry, you can apply them to site configuration. To apply the customized rate limit profiles in the related configurations, refer to 4. 9. 1 Portal, and 4. 4. 1 Set Up Basic Wireless Networks.

You can view the name, download limit, and upload limit in the list.



NAME	Download Limit	Upload Limit	ACTION
Default	Unlimited	Unlimited	✎
Limit-Day	20000 Kbps	20000 Kbps	✎ 🗑
Limit-Night	50000 Kbps	50000 Kbps	✎ 🗑

Showing 1-3 of 3 records < 1 > 10 /page Go To page: GO

+ Create New Rate Limit Profile

To view, edit or delete the rate limit profile, 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.

1. 8. 4 PPSK

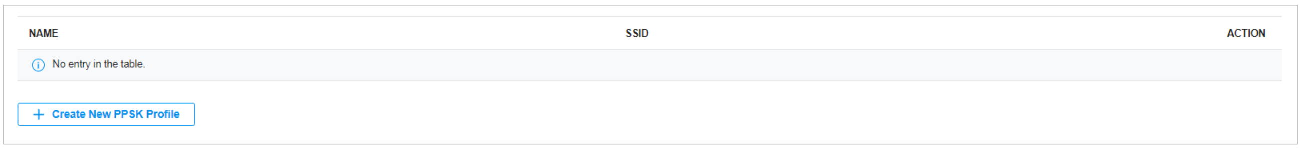
Overview

PPSK is a security solution in which individual client devices can be managed without much complexity. With PPSK, each user is assigned with a unique passphrase for authentication. Also, it allows the binding of a passphrase and the device MAC address(es), and thus only the specified device can be authenticated using the passphrase. In PPSK, you can create the PPSK list and apply them to multiple wireless networks, saving you from repeatedly setting up the same information.

Configuration

To configure the PPSK profiles, follow these steps:

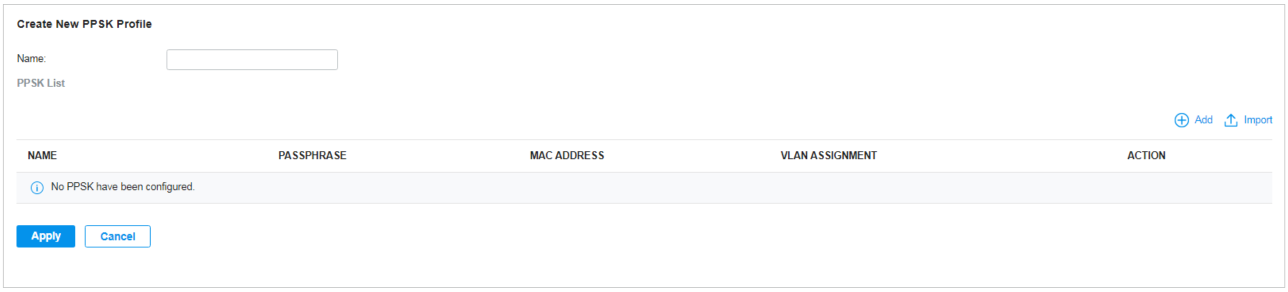
1. Select a site from the drop-down list of Organization. Go to Settings > Profiles > PPSK. Click +Create New PPSK Profile to add a new PPSK profile .



NAME	SSID	ACTION
ⓘ No entry in the table.		

+ Create New PPSK Profile

2. Enter a name for the new profile. Click +Add to add new entries in the PPSK profile or click Import to import entries in batches from a file.



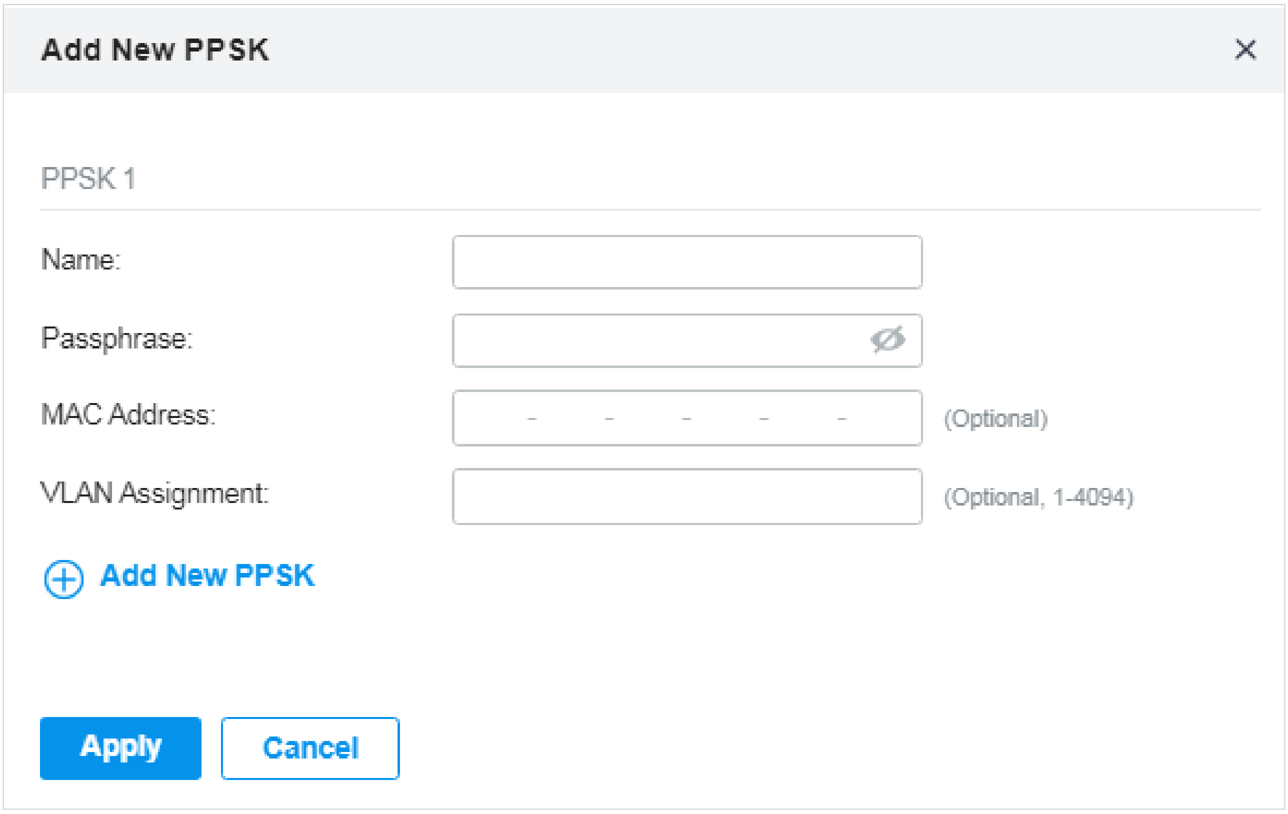
Create New PPSK Profile

Name:

PPSK List

NAME	PASSPHRASE	MAC ADDRESS	VLAN ASSIGNMENT	ACTION
No PPSK have been configured.				

Enter the parameters and click Apply to save the PPSK information.



Add New PPSK

PPSK 1

Name:

Passphrase:

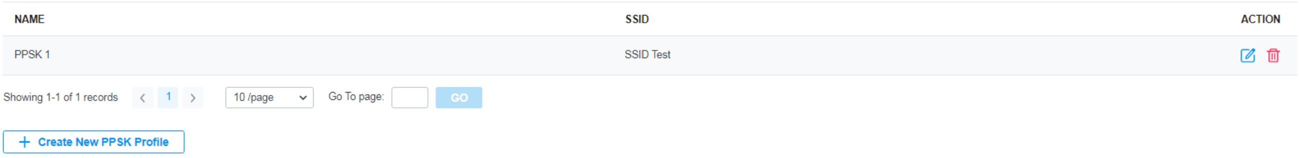
MAC Address: (Optional)

VLAN Assignment: (Optional, 1-4094)

Name	Enter a name to identify the created PPSK.
Passphrase	Enter a passphrase, and the client will use the passphrase for authentication.
MAC Address	(Optional) Enter the MAC address of the device that can use the passphrase for authentication.
VLAN Assignment	(Optional) Enter the VLAN ID, and the client who uses the passphrase for authentication will be assigned to the specified VLAN.

3. Click Apply to save the profile. After saving the newly added profile, you can apply them to wireless networks, refer to 4. 4. 1 Set Up Basic Wireless Networks.

You can view the name and which wireless network (SSID) the PPSK profile is applied to in the list.



NAME	SSID	ACTION
PPSK 1	SSID Test	✎ 🗑

Showing 1-1 of 1 records < 1 > 10 /page Go To page: GO

+ Create New PPSK Profile

To view, edit or delete the PPSK profile, click the icon in the Action column.

✎	View and edit the parameters in the entry.
🗑	Delete the entry.

1. 9 Authentication

Authentication is a portfolio of features designed to authorize network access to clients, which enhances the network security. Authentication services include 4. 9. 1 Portal, 4. 9. 2 802.1X and 4. 9. 3 MAC-Based Authentication, covering all the needs to authenticate both wired and wireless clients.

1. 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 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.

  - Form Auth

    Clients are required to fill in a survey created by the network administrator to pass the authentication. It can be used for collecting feedback from your clients.

- 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.

Portal authentication can work with Access Control Policy, which grant specific network access to the users with valid identities. You can determine that the clients which didn't pass Portal authentication can only access the network resources allowed by Access Control Policy.

- Pre-Authentication Access

  Pre-Authentication Access allows unauthenticated clients to access the specific network resources.

- Authentication-Free Client

  Authentication-Free Clients allows the specific clients to access the specific network resources without authentication.

Configuration

To complete the Portal configuration, follow these steps:

1) Click + Create New Portal to create new Portal entry.

2) Click ○ to enable Portal, 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.

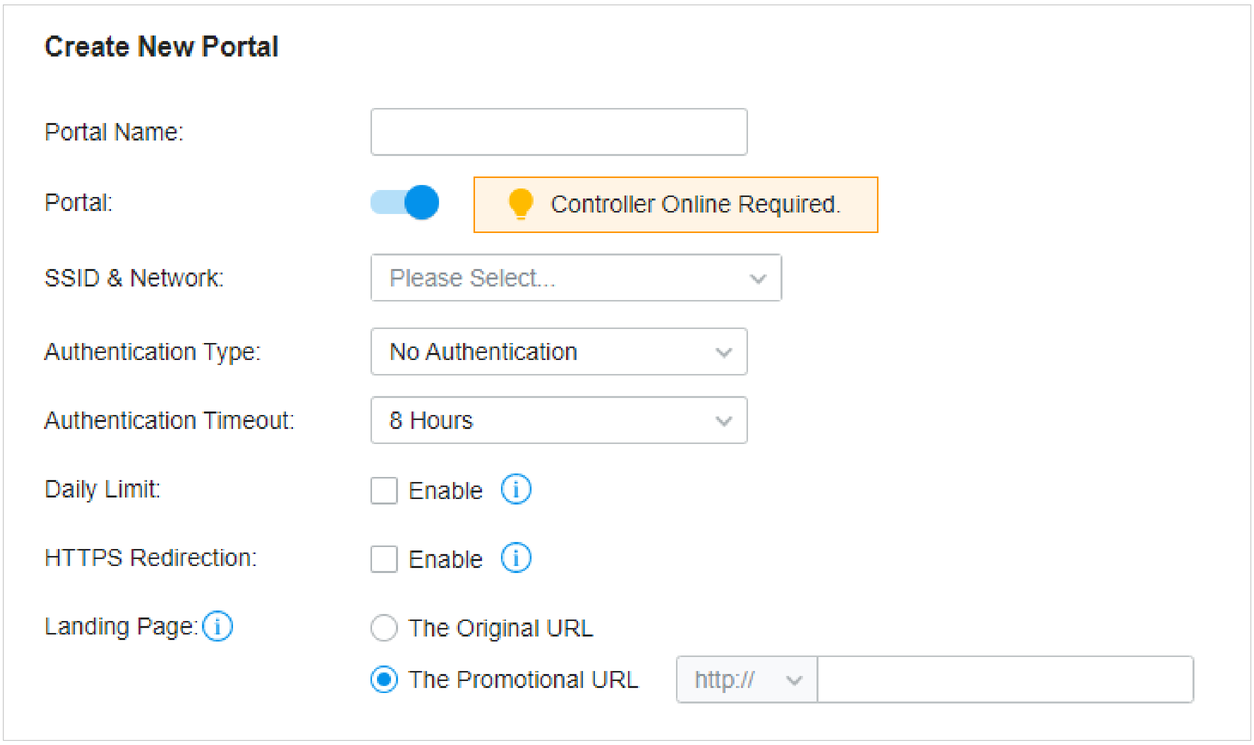
3) Customize the Portal page including the background picture, logo picture and so on.

4) (Optional) Configure access control policies including Pre-Authentication Access and Authentication-Free Clients 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**

1. Select a site from the drop-down list of Organization. Go to Settings > Authentication > Portal. On Portal tab, click + Create New Portal to create new portal entry. Then click ○ to enable Portal and load the following page.



Create New Portal

Portal Name:	
Portal:	● Controller Online Required.
SSID & Network:	Please Select...
Authentication Type:	No Authentication
Authentication Timeout:	8 Hours
Daily Limit:	□ Enable ⓘ
HTTPS Redirection:	□ Enable ⓘ
Landing Page: ⓘ	○ The Original URL ● The Promotional URL http://

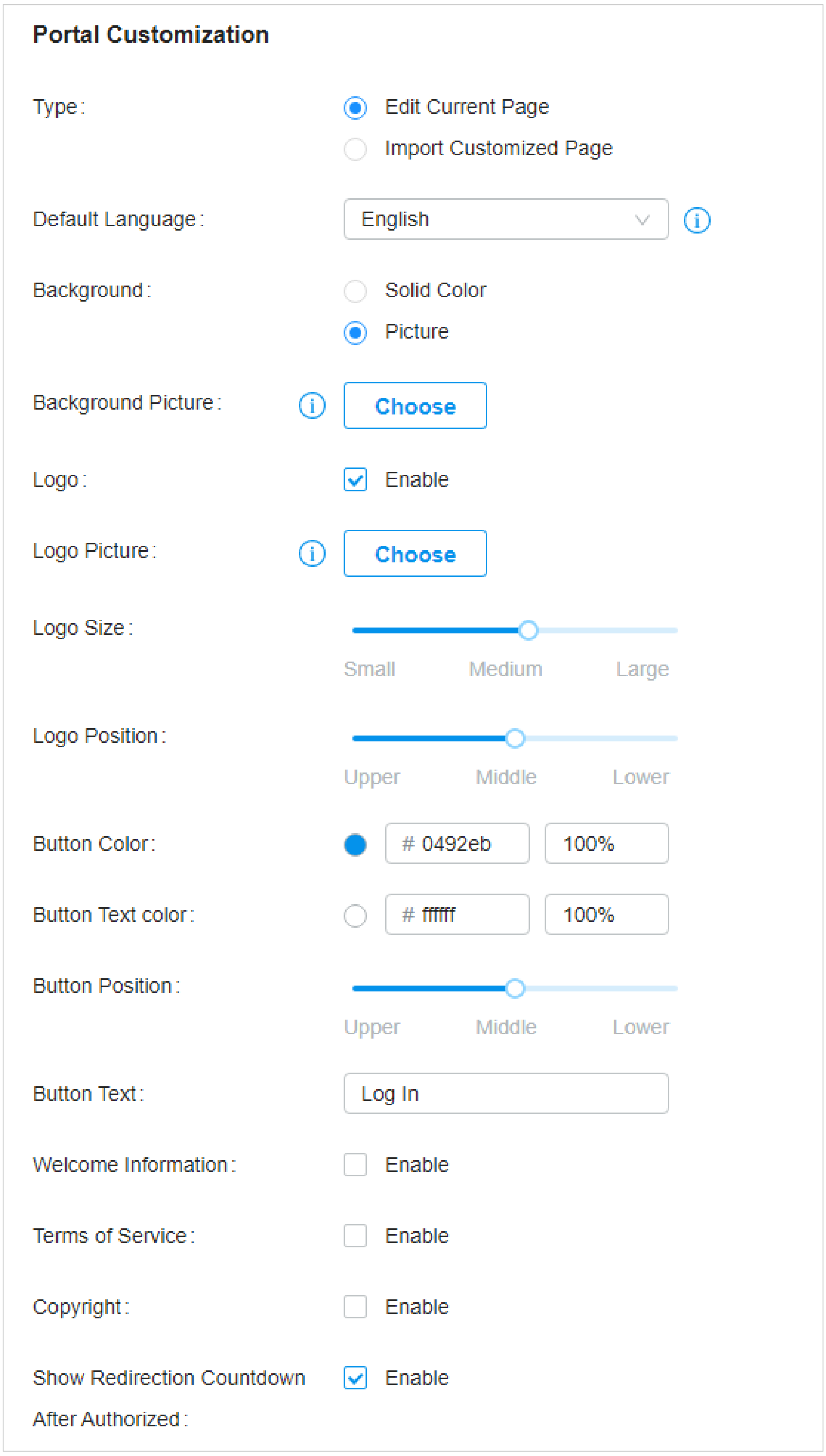
2. Select the SSIDs and LAN networks for the portal to take effect on and configure basic parameters including authentication type, authentication timeout and so on.

Portal Name	Enter a name to identify the created Portal entry.
Portal	Click ○ to enable Portal.
SSID & 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.

3. In the Portal Customization section, customize the Portal page including the background picture,

logo picture and so on.



Portal Customization

Type: ● Edit Current Page ○ Import Customized Page

Default Language: English

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo: ☑ Enable

Logo Picture: Choose

Logo Size: Small Medium Large

Logo Position: Upper Middle Lower

Button Color: ● # 0492eb 100%

Button Text color: ○ # ffffff 100%

Button Position: Upper Middle Lower

Button Text: Log In

Welcome Information: □ Enable

Terms of Service: □ Enable

Copyright: □ Enable

Show Redirection Countdown After Authorized: ☑ Enable

Type

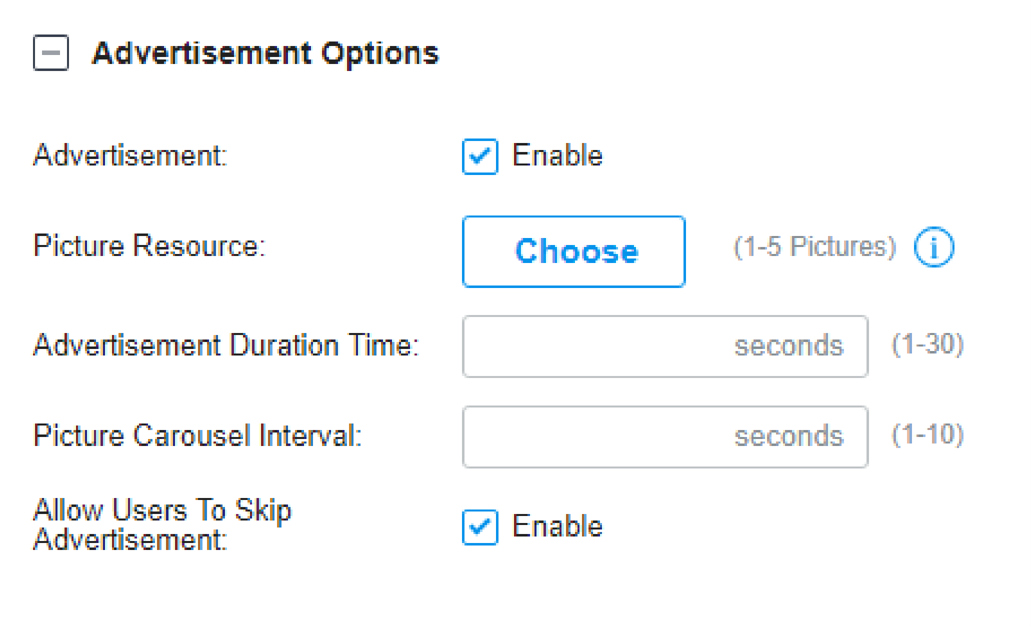
Select the type of the Portal page.

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	Click to show the logo on the portal page.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Size	Adjust the logo size on the Portal Page.
Logo Position	Adjust the logo position on the Portal page.
Button 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 on the Portal Page.
Button Text	Enter the text for the button.
Welcome Information	Click the checkbox and enter text as the welcome information. You can specify the desired text font size and configure the text color 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. Click Add Terms to enter the name and context of the terms which will appear after a client clicks the link in Terms of Service.
Copyright	Click the checkbox and enter text as the copyright in the following box. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.
Show Redirection Countdown After Authorized	When enabled, the system will show the portal's redirection countdown.

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



Advertisement Options

Advertisement: ☑ Enable

Picture Resource: Choose (1-5 Pictures)

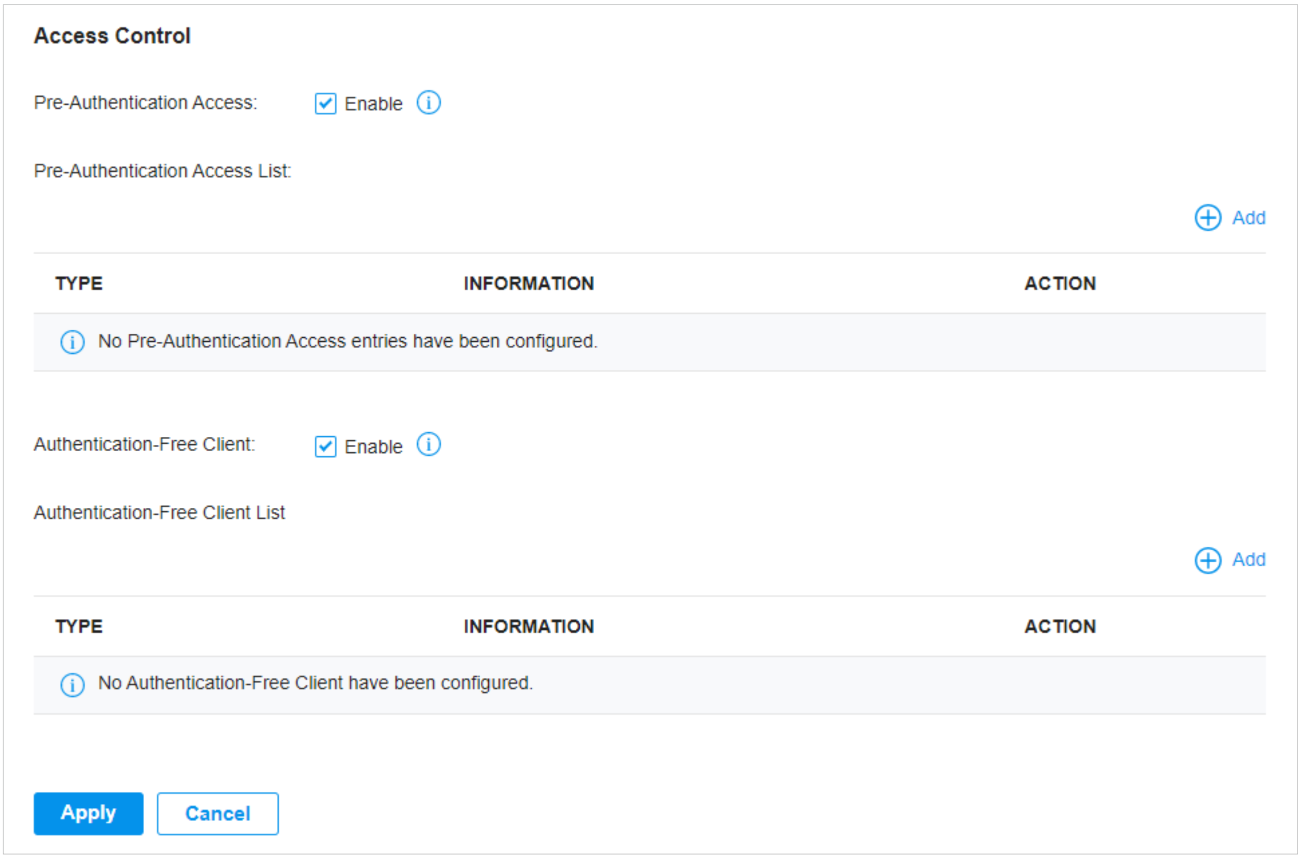
Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: ☑ Enable

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. (Optional) Configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed. Go to Settings > Authentication > Portal. On Access Control tab, click the checkbox to enable Pre-Authentication Access and Authentication-Free Policy.



Access Control

Pre-Authentication Access: ☑ Enable ⓘ

Pre-Authentication Access List:

⊕ Add

TYPE	INFORMATION	ACTION
ⓘ No Pre-Authentication Access entries have been configured.		

Authentication-Free Client: ☑ Enable ⓘ

Authentication-Free Client List

⊕ Add

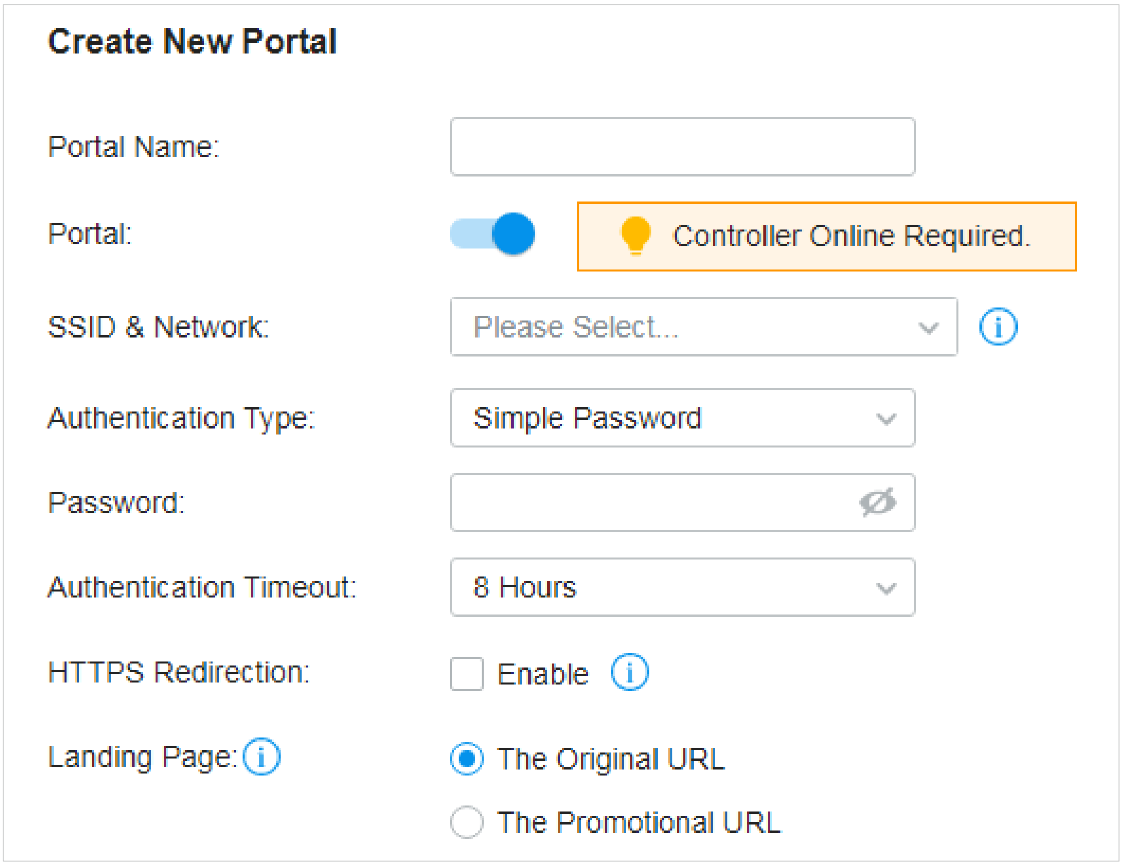
TYPE	INFORMATION	ACTION
ⓘ No Authentication-Free Client have been configured.		

Apply Cancel

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. Select a site from the drop-down list of Organization. Go to Settings > Authentication > Portal. On Portal tab, click + Create New Portal to create new portal entry. Then click to enable Portal and load the following page.



Create New Portal

Portal Name:

Portal: ● Controller Online Required.

SSID & Network: Please Select...

Authentication Type: Simple Password

Password:

Authentication Timeout: 8 Hours

HTTPS Redirection: □ Enable

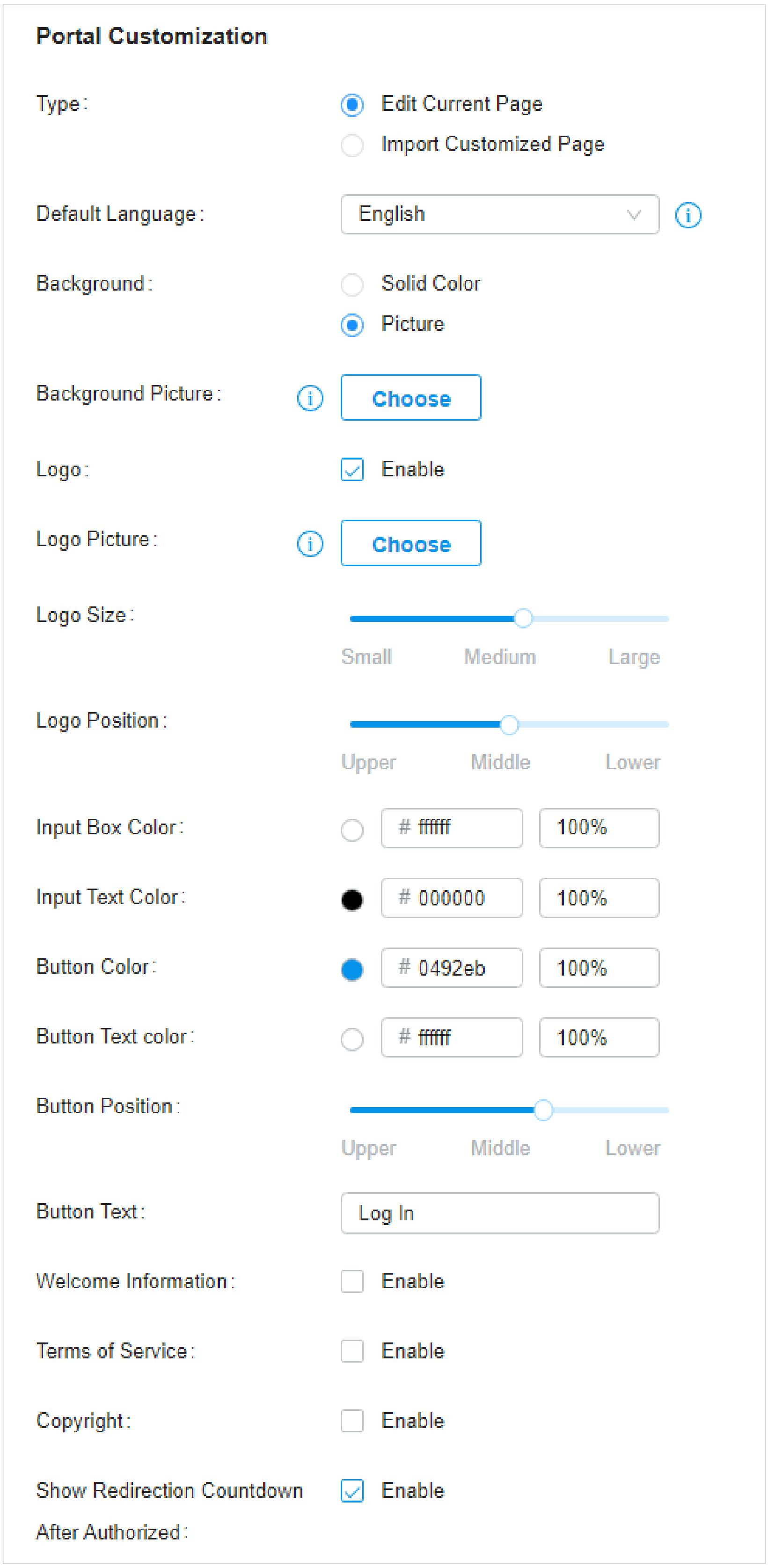
Landing Page: ● The Original URL ○ The Promotional URL

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 & 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.
Password	Specify the password for the portal.
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.



Portal Customization

Type: ● Edit Current Page ○ Import Customized Page

Default Language: English

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo: ☑ Enable

Logo Picture: Choose

Logo Size: Small Medium Large

Logo Position: Upper Middle Lower

Input Box Color: ○ # ffffff 100%

Input Text Color: ● # 000000 100%

Button Color: ● # 0492eb 100%

Button Text color: ○ # ffffff 100%

Button Position: Upper Middle Lower

Button Text: Log In

Welcome Information: □ Enable

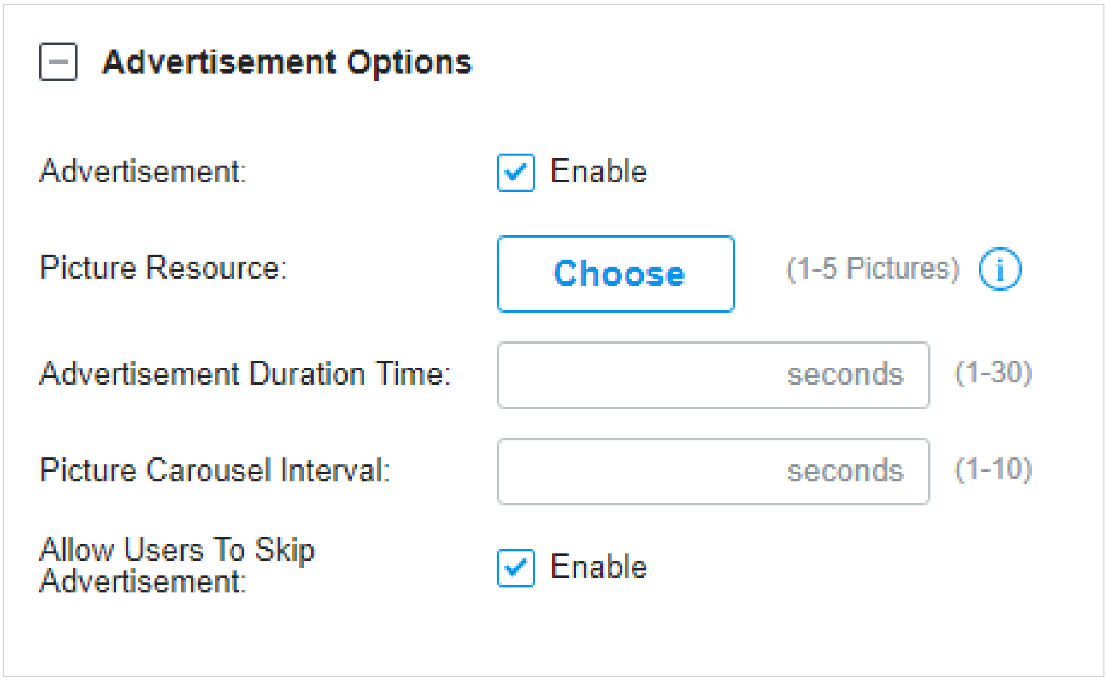
Terms of Service: □ Enable

Copyright: □ Enable

Show Redirection Countdown After Authorized: ☑ Enable

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	Click to show the logo on the portal page.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Size	Adjust the logo size on the Portal Page.
Logo Position	Adjust the logo position on the Portal Page.
Button 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 on the Portal Page.
Button Text	Enter the text for the button.
Welcome Information	Click the checkbox and enter text as the welcome information. You can specify the desired text font size and configure the text color 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. Click Add Terms to enter the name and context of the terms which will appear after a client clicks the link in Terms of Service.
Copyright	Click the checkbox and enter text as the copyright in the following box. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.
Show Redirection Countdown After Authorized	When enabled, the system will show the portal's redirection countdown.

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



⊟ Advertisement Options

Advertisement: ☑ Enable

Picture Resource: Choose (1-5 Pictures)

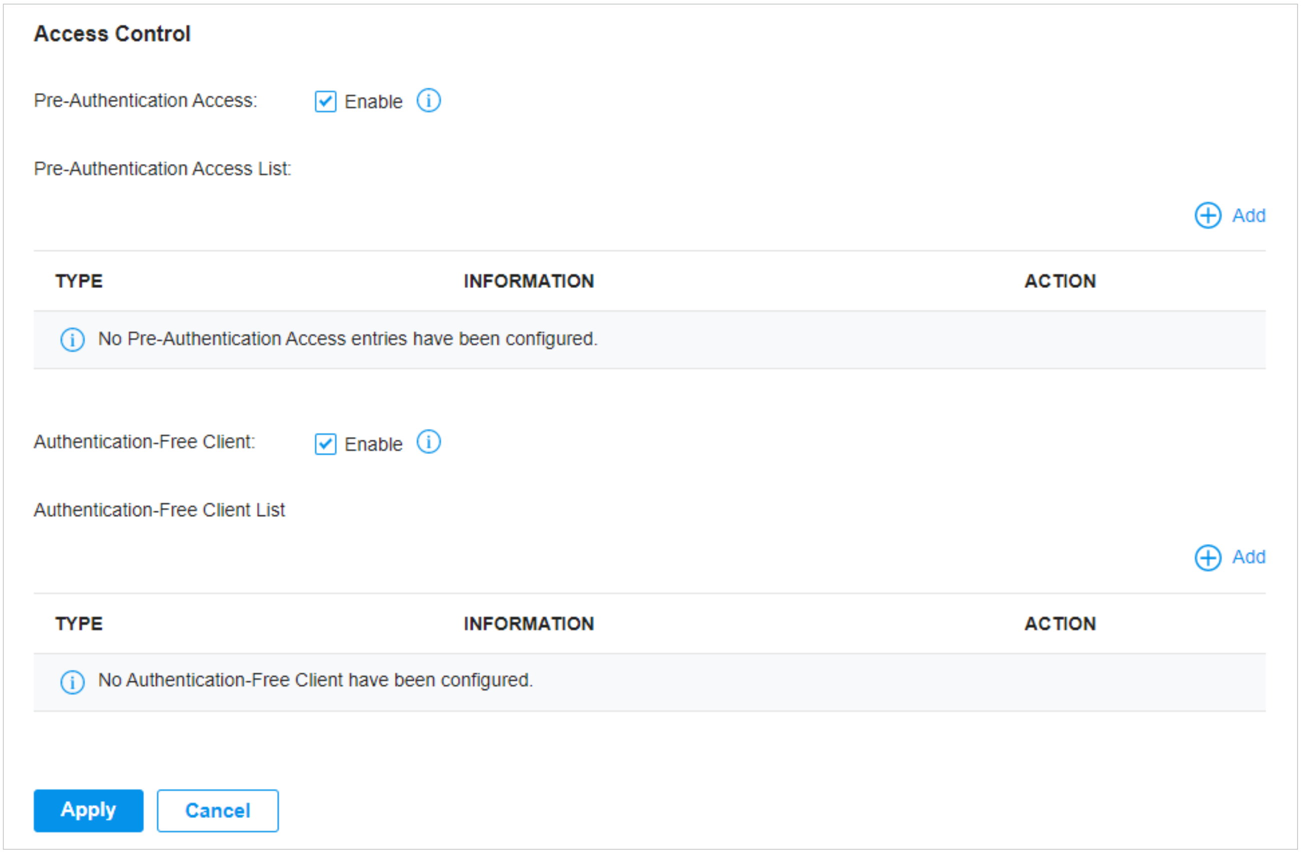
Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: ☑ Enable

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. (Optional) Configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed. Go to Settings > Authentication > Portal. On Access Control tab, click the checkbox to enable Pre-Authentication Access and Authentication-Free Policy.



Access Control

Pre-Authentication Access: ☑ Enable

Pre-Authentication Access List:

TYPE	INFORMATION	ACTION
No Pre-Authentication Access entries have been configured.		

Authentication-Free Client: ☑ Enable

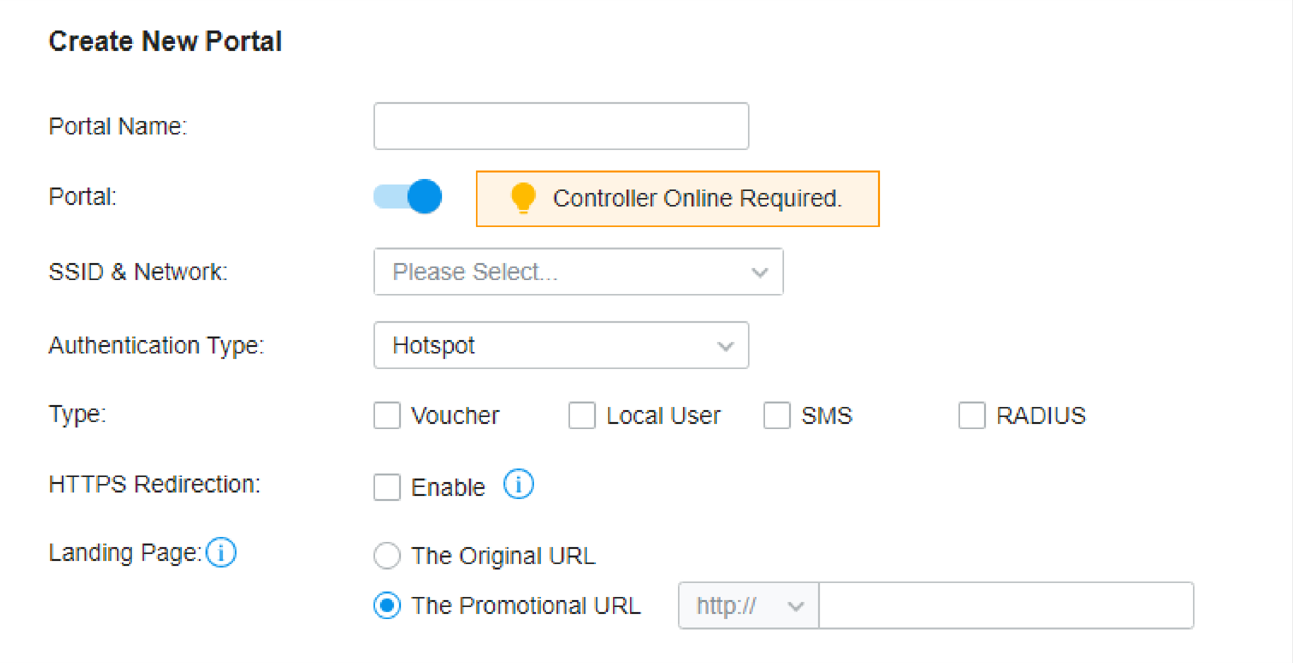
Authentication-Free Client List

TYPE	INFORMATION	ACTION
No Authentication-Free Client have been configured.		

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. Select a site from the drop-down list of Organization. Go to Settings > Authentication > Portal. On Portal tab, click + Create New Portal to create new portal entry. Then click ○ to enable Portal and load the following page.



Create New Portal

Portal Name:

Portal: ● Controller Online Required.

SSID & Network: Please Select...

Authentication Type: Hotspot

Type: □ Voucher □ Local User □ SMS □ RADIUS

HTTPS Redirection: □ Enable

Landing Page: ○ The Original URL ● The Promotional URL http://

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

SSID & 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.
Type	Select one or more authentication types according to your needs. Clients can access the network after passing any type of the authentication.
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. With different types of Hotspot selected, configure the related parameters.

- **Configuring Voucher Portal**

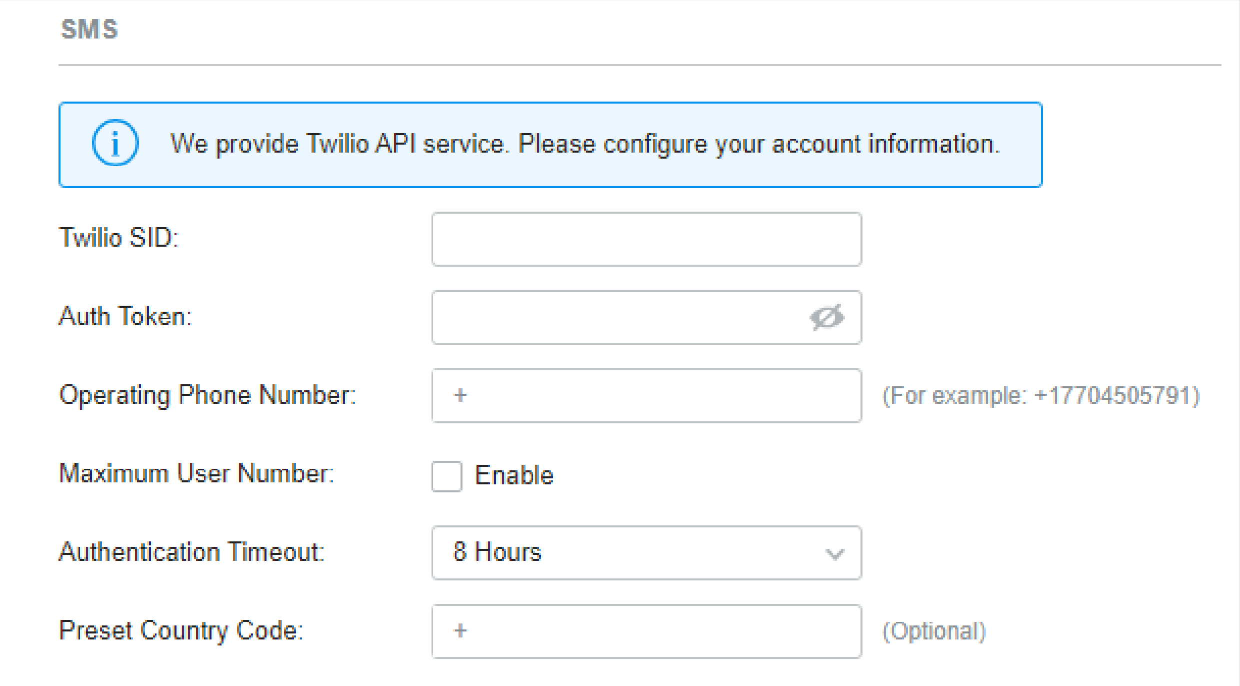
Voucher	Select Voucher and click **Voucher Manager** to manage the voucher codes. Refer to 7. 2. 2 Vouchers for detailed information about how to create vouchers.

- **Configuring Local Portal**

Local User	Select Local User and click **User Management** to manage the information of the login accounts. Refer to 7. 2. 3 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

We provide Twilio API service. Please configure your account information.

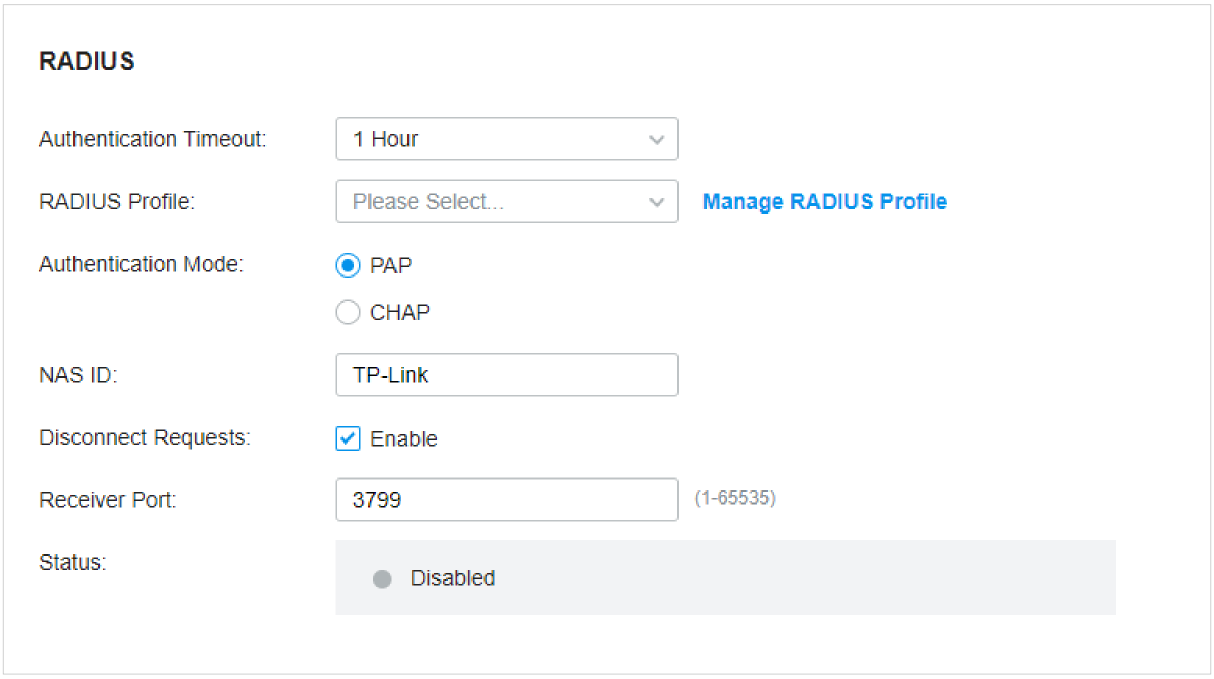
Twilio SID:		
Auth Token:		
Operating Phone Number:	+	(For example: +17704505791)
Maximum User Number:	□ Enable	
Authentication Timeout:	8 Hours	
Preset Country Code:	+	(Optional)

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

Authentication Timeout: 1 Hour

RADIUS Profile: Please Select... Manage RADIUS Profile

Authentication Mode: ● PAP ○ CHAP

NAS ID: TP-Link

Disconnect Requests: ☑ Enable

Receiver Port: 3799 (1-65535)

Status: ● Disabled

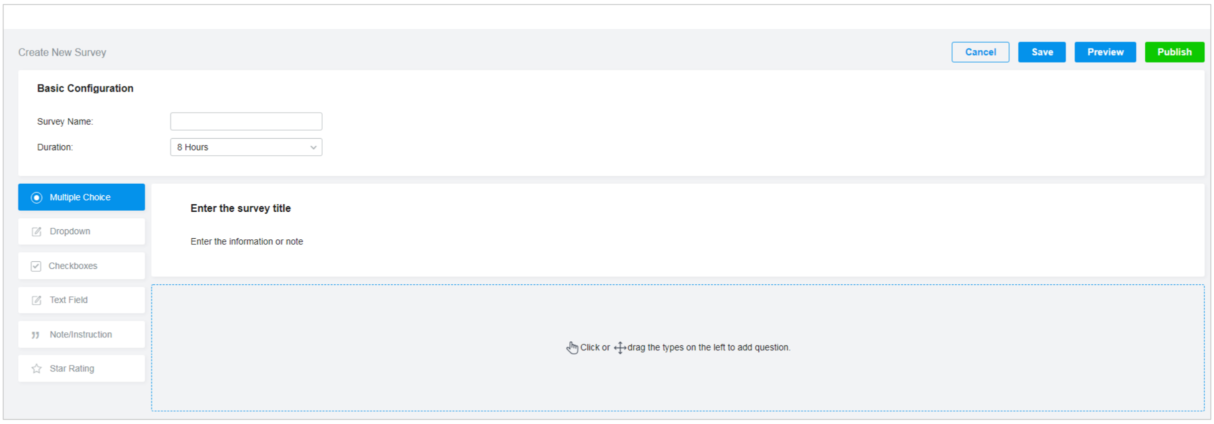
Authentication Timeout	Clients are required to enter the correct username and password which are stored in the RADIUS server to pass the authentication.
RADIUS Profile	Select the RADIUS profile you have created. If no RADIUS profiles have been created, click + Create New RADIUS Profile from the drop-down 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.
Disconnected Requests	With the feature enabled, the controller will listen on the receiver port for disconnect requests from the RADIUS server. When the controller receives the disconnect requests in correct format, the controller will terminate the RADIUS authentication session of the clients. Note that the feature is available only when the controller is accessible to the RADIUS server.

Receiver Port	Specify the port on which the controller listens when there are disconnect requests from the RADIUS server. Make sure that the specified port is not in use.
Status	The entry displays the status of the receiver port, including Running, Disabled, and Error. Running means that the port is available, Disabled means that the port is closed, and Error means that the port is already in use.

- **Configuring Form Authentication**

Select Form Auth and click + Create New Survey in the Form Authentication section. Then follow the on-screen instructions to create a survey by adding the type and number of questions you need. You can click Preview to view how the survey looks like on website and phone.

Click Publish and then the created survey can be used for form authentication. A survey cannot be edited after it is published.



Basic Configuration

Survey Name:

Duration: 8 Hours

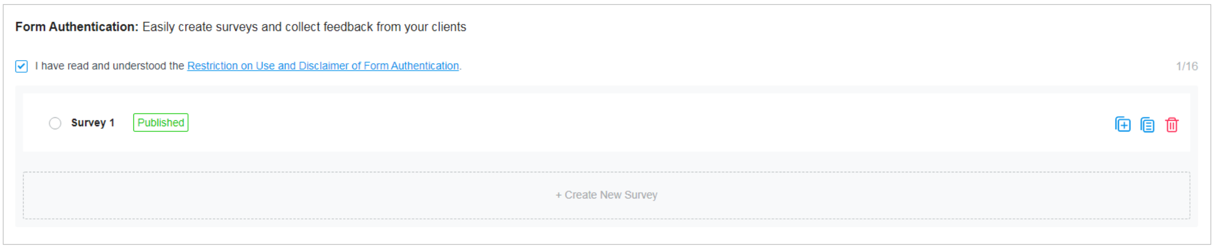
Enter the survey title

Enter the information or note

Click or drag the types on the left to add question.

Survey Name	Specify a name for the survey for identification.
Duration	Specify how long clients can use the network after they pass the form authentication.

Created surveys will be displayed for you to choose for the form authentication.



Form Authentication: Easily create surveys and collect feedback from your clients

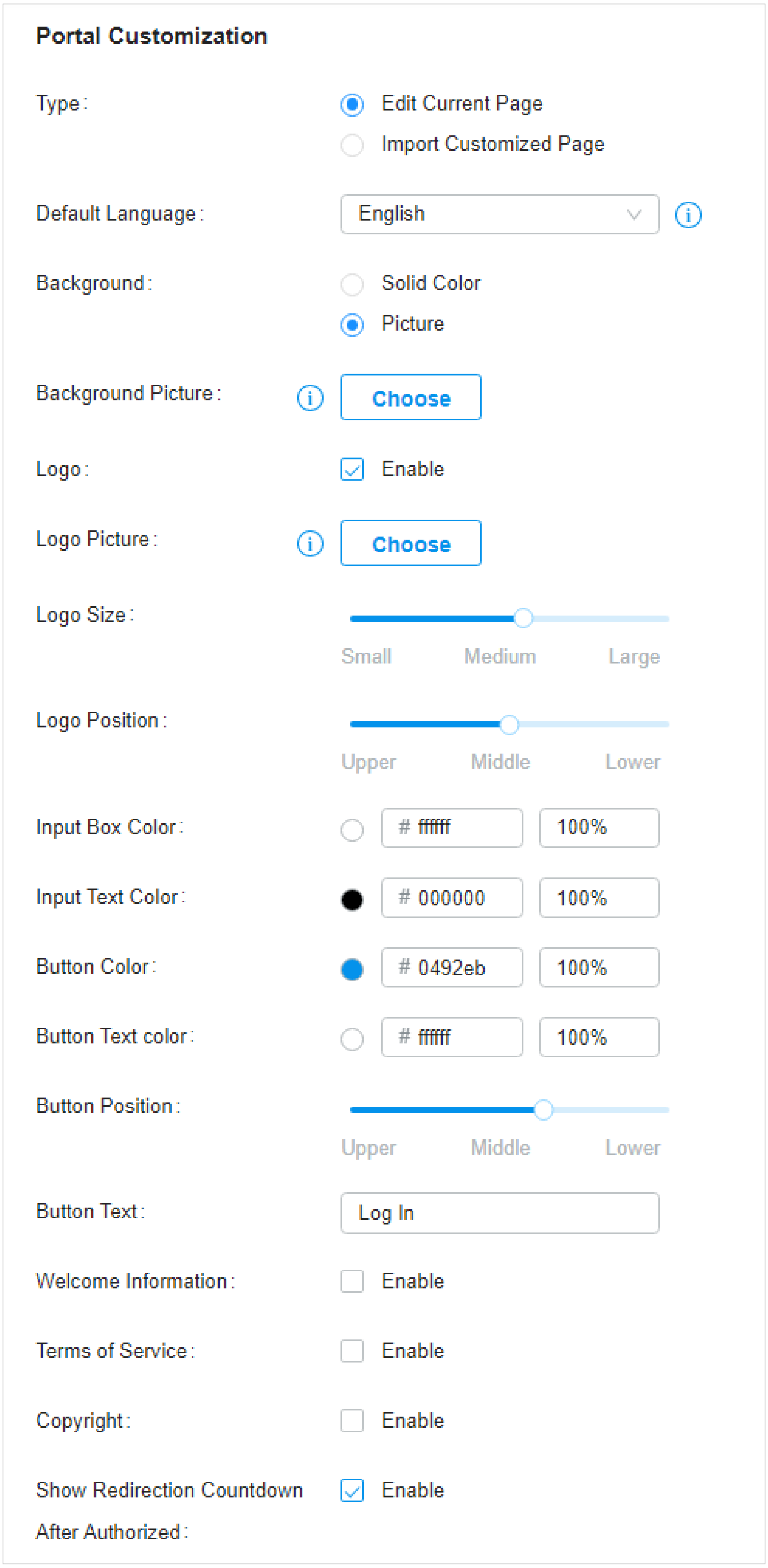
☑ I have read and understood the Restriction on Use and Disclaimer of Form Authentication.

1/16

○ **Survey 1** Published

⧉	Click to copy the survey.
🗐	Click to view the created survey.
🗑	Click to delete the survey..

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



Portal Customization

Type: ● Edit Current Page ○ Import Customized Page

Default Language: English

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo: ☑ Enable

Logo Picture: Choose

Logo Size: Small Medium Large

Logo Position: Upper Middle Lower

Input Box Color: ○ # ffffff 100%

Input Text Color: ● # 000000 100%

Button Color: ● # 0492eb 100%

Button Text color: ○ # ffffff 100%

Button Position: Upper Middle Lower

Button Text: Log In

Welcome Information: □ Enable

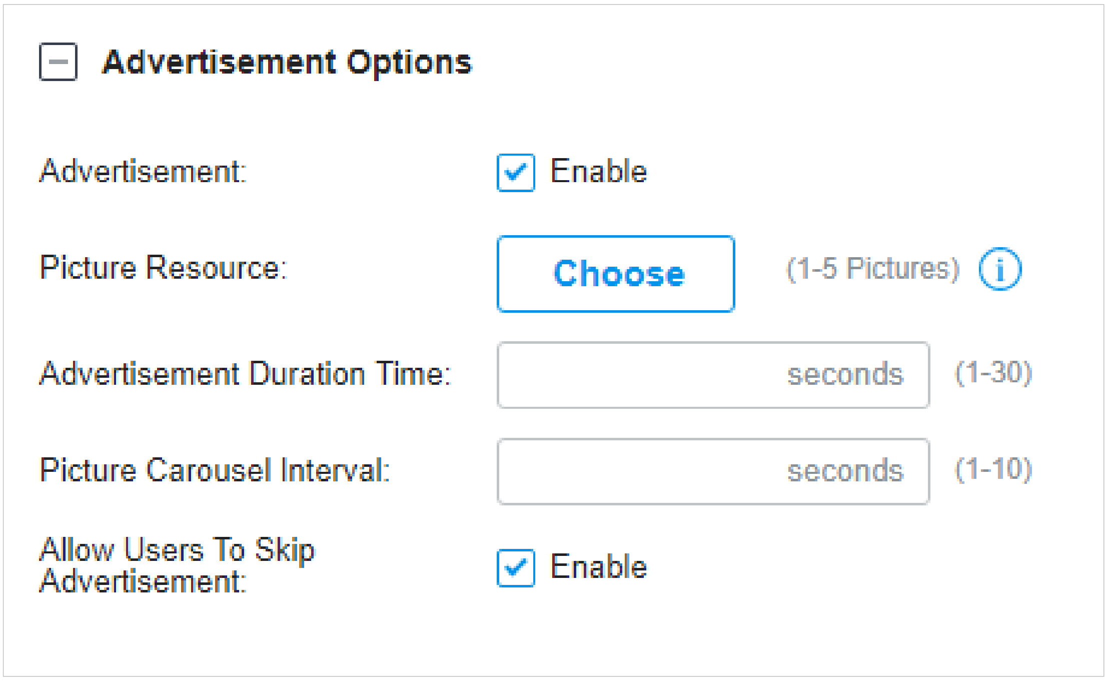
Terms of Service: □ Enable

Copyright: □ Enable

Show Redirection Countdown After Authorized: ☑ Enable

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	Click to show the logo on the portal page.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Size	Adjust the logo size on the Portal Page.
Logo Position	Adjust the logo position on the Portal Page.
Button 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 on the Portal Page.
Button Text	Enter the text for the button.
Welcome Information	Click the checkbox and enter text as the welcome information. You can specify the desired text font size and configure the text color 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. Click Add Terms to enter the name and context of the terms which will appear after a client clicks the link in Terms of Service.
Copyright	Click the checkbox and enter text as the copyright in the following box. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.
Show Redirection Countdown After Authorized	When enabled, the system will show the portal's redirection countdown.

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



Advertisement Options

Advertisement: ☑ Enable

Picture Resource: (1-5 Pictures)

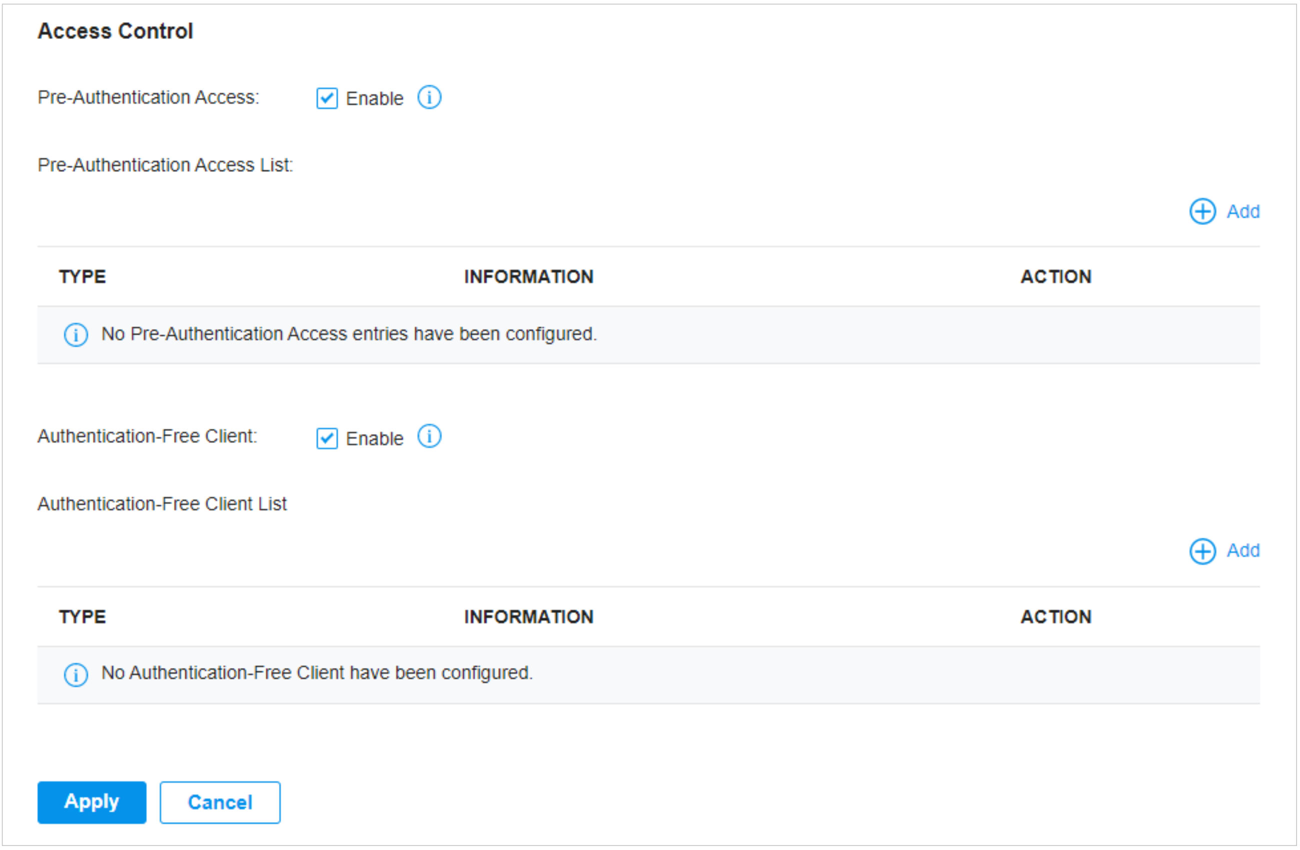
Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: ☑ Enable

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. (Optional) Configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed. Go to Settings > Authentication > Portal. On Access Control tab, click the checkbox to enable Pre-Authentication Access and Authentication-Free Policy.



Access Control

Pre-Authentication Access: ☑ Enable ⓘ

Pre-Authentication Access List:

⊕ Add

TYPE	INFORMATION	ACTION
ⓘ No Pre-Authentication Access entries have been configured.		

Authentication-Free Client: ☑ Enable ⓘ

Authentication-Free Client List

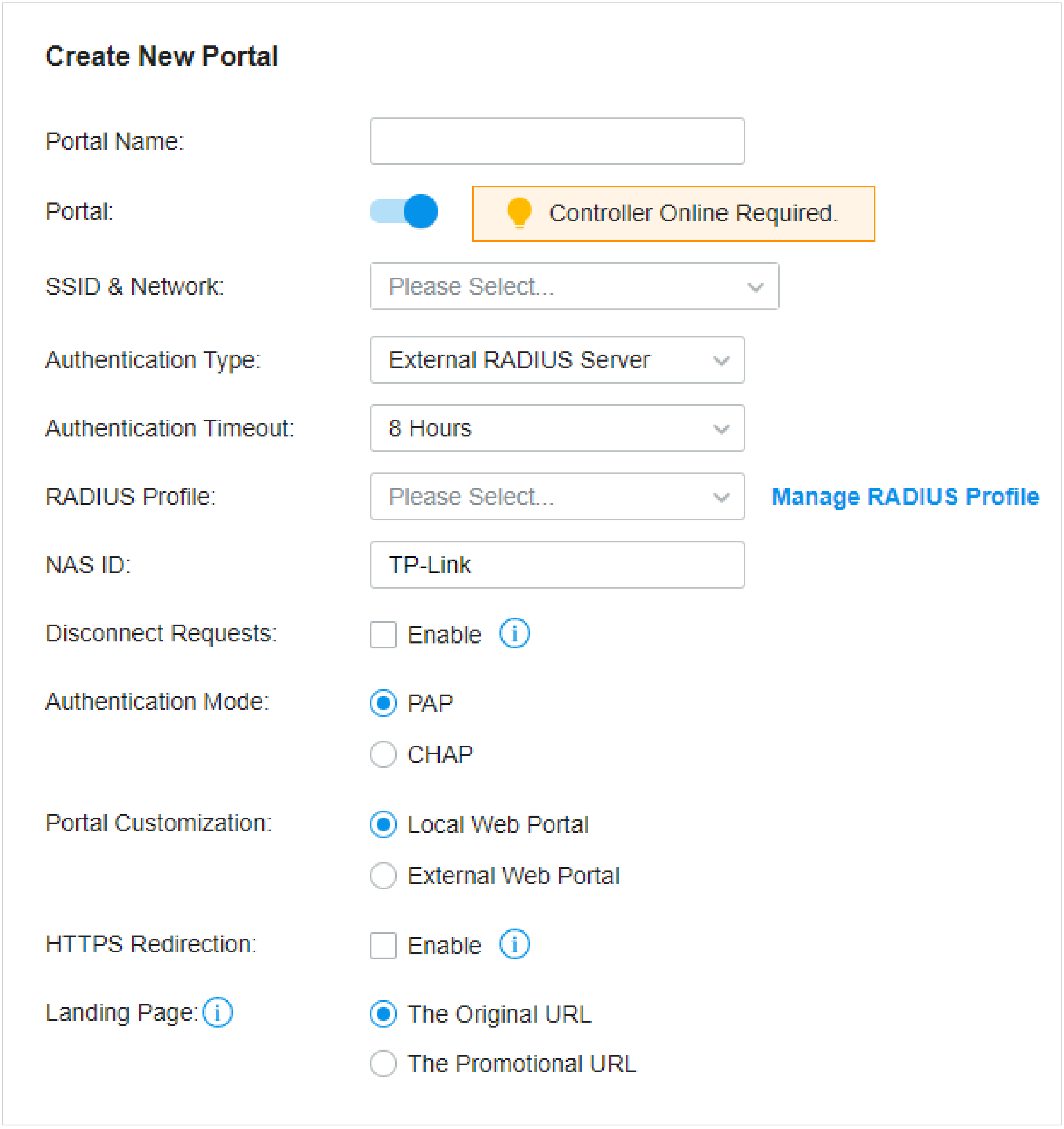
⊕ Add

TYPE	INFORMATION	ACTION
ⓘ No Authentication-Free Client have been configured.		

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. Select a site from the drop-down list of Organization. Go to Settings > Authentication > Portal. Click to enable Portal and load the following page.



Create New Portal

Portal Name:

Portal: ● Controller Online Required.

SSID & Network: Please Select...

Authentication Type: External RADIUS Server

Authentication Timeout: 8 Hours

RADIUS Profile: Please Select... Manage RADIUS Profile

NAS ID: TP-Link

Disconnect Requests: □ Enable

Authentication Mode: ● PAP ○ CHAP

Portal Customization: ● Local Web Portal ○ External Web Portal

HTTPS Redirection: □ Enable

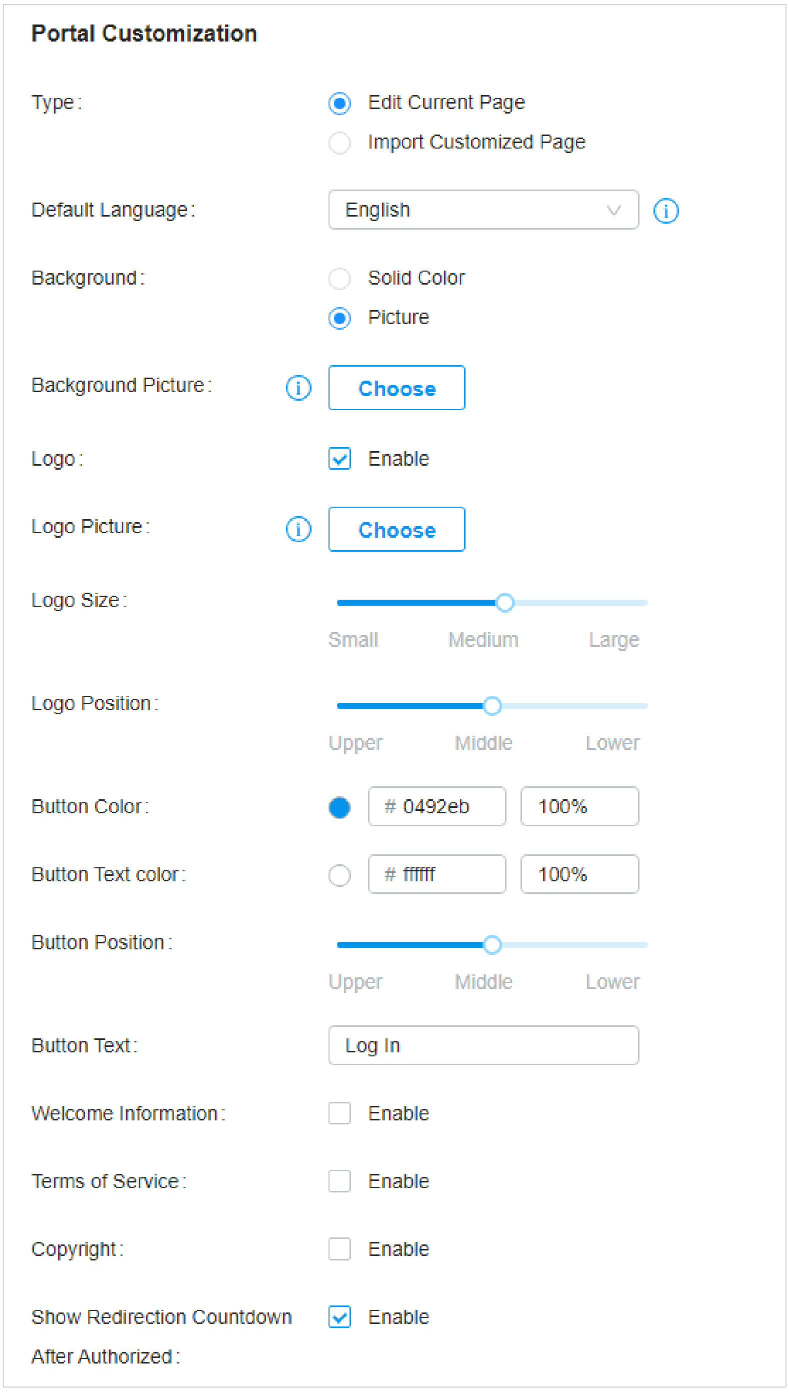
Landing Page: ● The Original URL ○ The Promotional URL

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 & 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.
Disconnected Requests	With the feature enabled, the controller will listen on the receiver port for disconnect requests from the RADIUS server. When the controller receives the disconnect requests in correct format, the controller will terminate the RAIDIUS authentication session of the clients. Note that the feature is available only when the controller is accessible to the RADIUS server.
Receiver Port	Specify the port on which the controller listens when there are disconnect requests from the RADIUS server. Make sure that the specified port is not in use.
Status	The entry displays the status of the receiver port, including Running, Disabled, and Error. Running means that the port is available, Disabled means that the port is closed, and Error means that the port is already in use.
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.



Portal Customization

Type: ● Edit Current Page ○ Import Customized Page

Default Language: English

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo: ☑ Enable

Logo Picture: Choose

Logo Size: Small Medium Large

Logo Position: Upper Middle Lower

Button Color: ● # 0492eb 100%

Button Text color: ○ # ffffff 100%

Button Position: Upper Middle Lower

Button Text: Log In

Welcome Information: □ Enable

Terms of Service: □ Enable

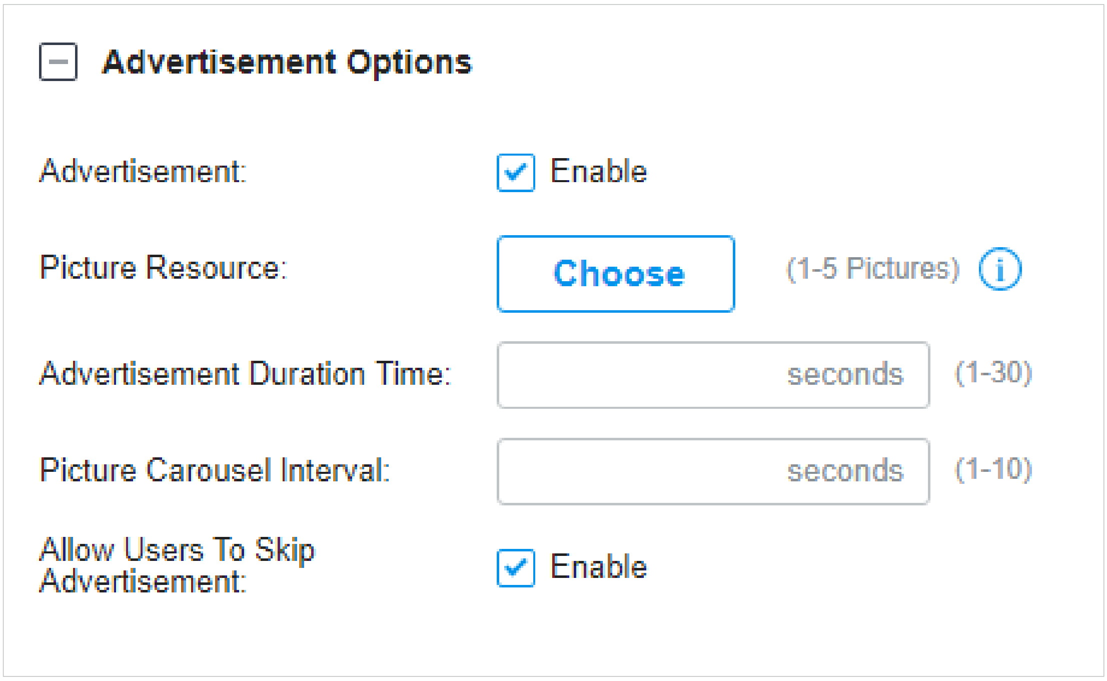
Copyright: □ Enable

Show Redirection Countdown After Authorized: ☑ Enable

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	Click to show the logo on the portal page.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Size	Adjust the logo size on the Portal Page.
Logo Position	Adjust the logo position on the Portal Page.
Button 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 on the Portal Page.
Button Text	Enter the text for the button.
Welcome Information	Click the checkbox and enter text as the welcome information. You can specify the desired text font size and configure the text color 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. Click Add Terms to enter the name and context of the terms which will appear after a client clicks the link in Terms of Service.
Copyright	Click the checkbox and enter text as the copyright in the following box. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.
Show Redirection Countdown After Authorized	When enabled, the system will show the portal's redirection countdown.

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



⊟ Advertisement Options

Advertisement: ☑ Enable

Picture Resource: Choose (1-5 Pictures) ⓘ

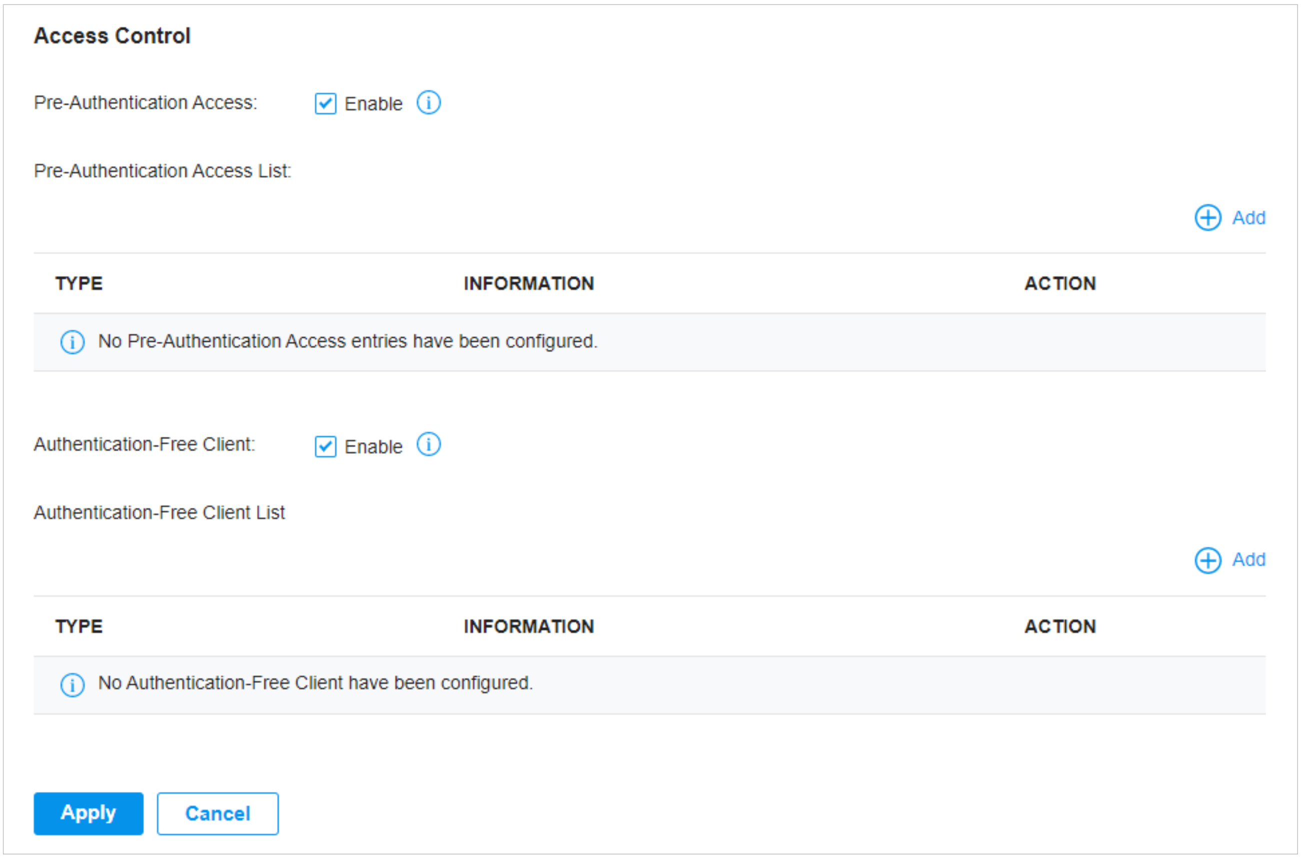
Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: ☑ Enable

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. (Optional) Configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed. Go to Settings > Authentication > Portal. On Access Control tab, click the checkbox to enable Pre-Authentication Access and Authentication-Free Policy.



Access Control

Pre-Authentication Access: ☑ Enable ⓘ

Pre-Authentication Access List:

⊕ Add

TYPE	INFORMATION	ACTION
ⓘ No Pre-Authentication Access entries have been configured.		

Authentication-Free Client: ☑ Enable ⓘ

Authentication-Free Client List

⊕ Add

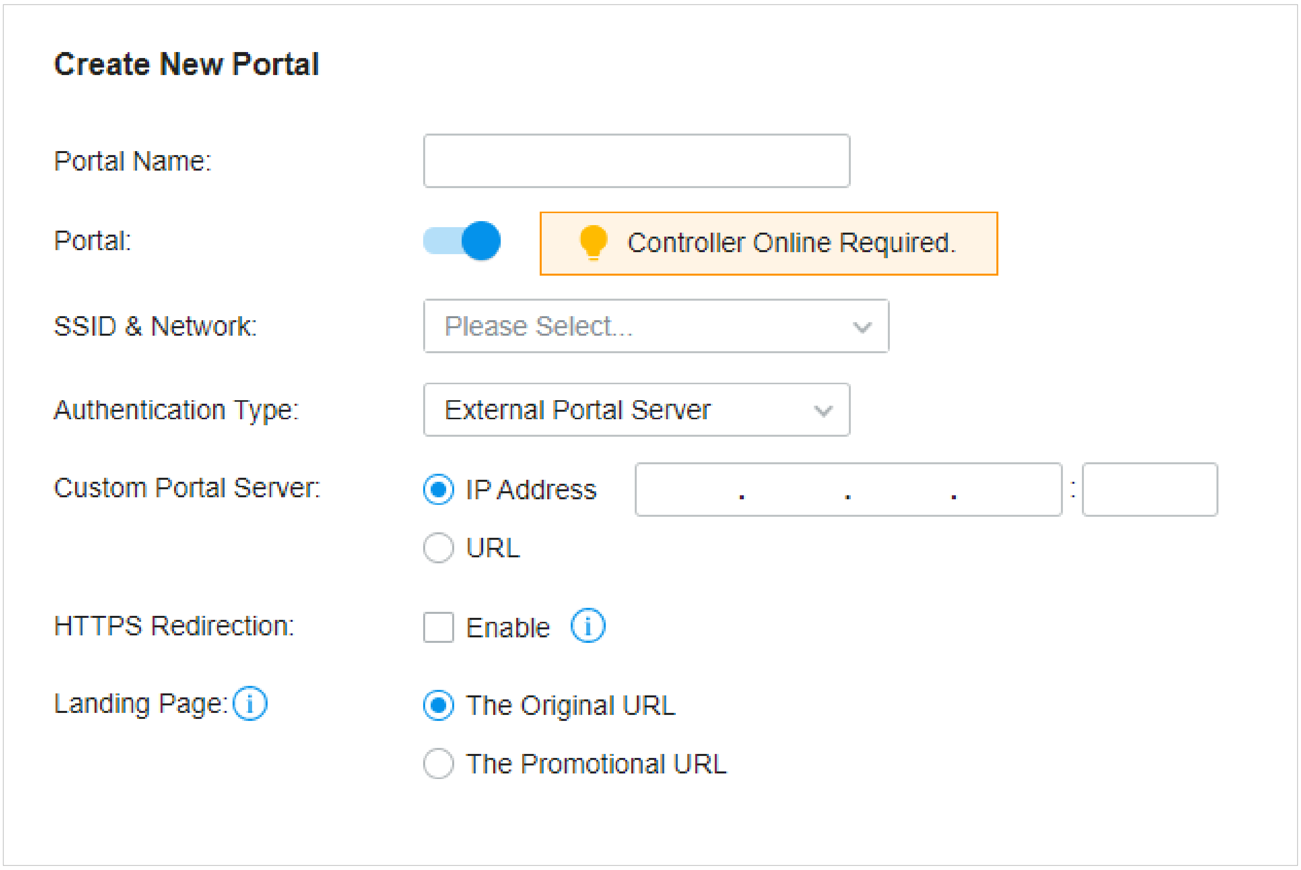
TYPE	INFORMATION	ACTION
ⓘ No Authentication-Free Client have been configured.		

Apply Cancel

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. Select a site from the drop-down list of Organization. Go to Settings > Authentication > Portal. On Portal tab, click + Create New Portal to create new portal entry. Then click to enable Portal and load the following page.



Create New Portal

Portal Name:

Portal: Controller Online Required.

SSID & Network: Please Select...

Authentication Type: External Portal Server

Custom Portal Server: ● IP Address . . . : ○ URL

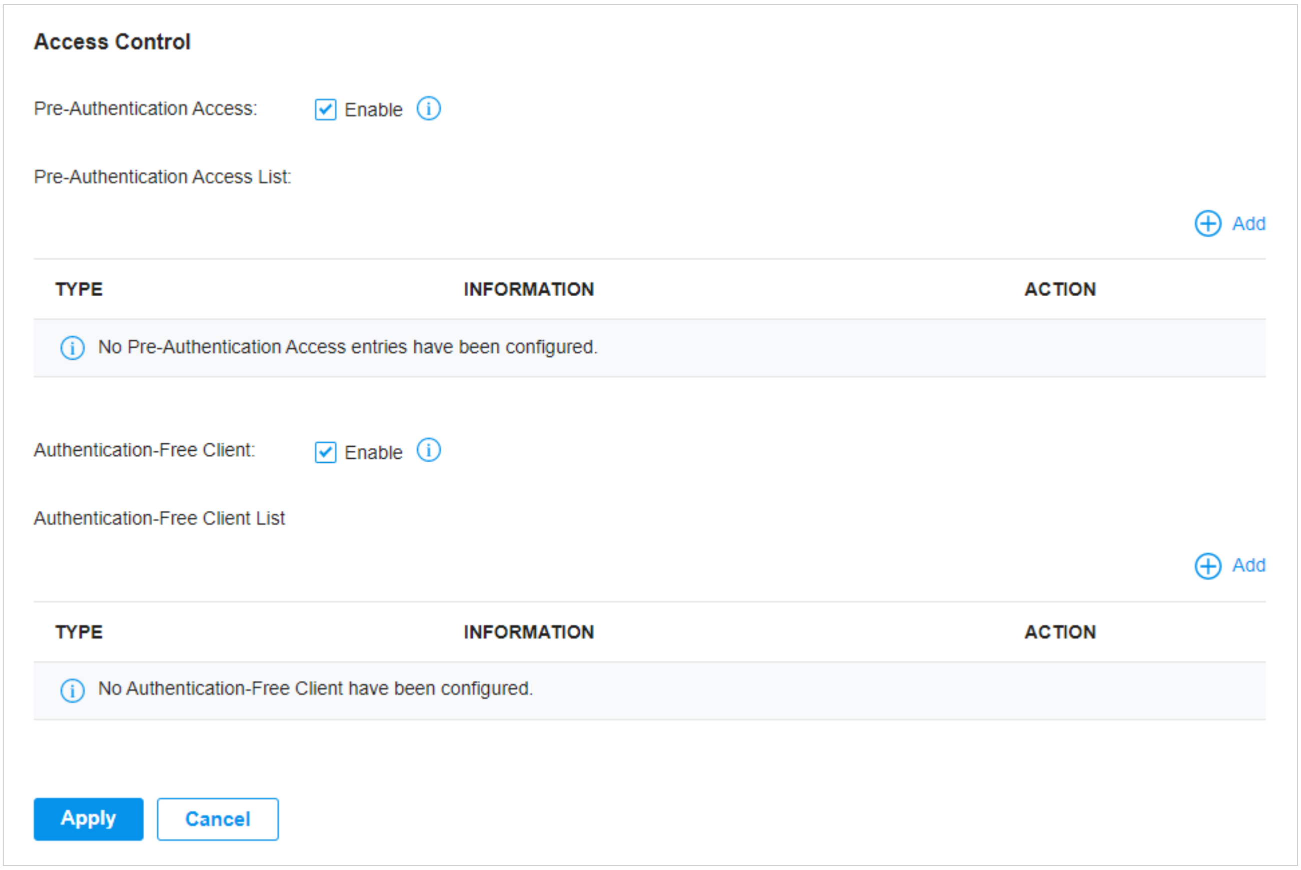
HTTPS Redirection: □ Enable

Landing Page: ● The Original URL ○ The Promotional URL

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 & 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. (Optional) Configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed. Go to Settings > Authentication > Portal. On Access Control tab, click the checkbox to enable Pre-Authentication Access and Authentication-Free Policy.



Access Control

Pre-Authentication Access: ☑ Enable ⓘ

Pre-Authentication Access List:

⊕ Add

TYPE	INFORMATION	ACTION
ⓘ No Pre-Authentication Access entries have been configured.		

Authentication-Free Client: ☑ Enable ⓘ

Authentication-Free Client List

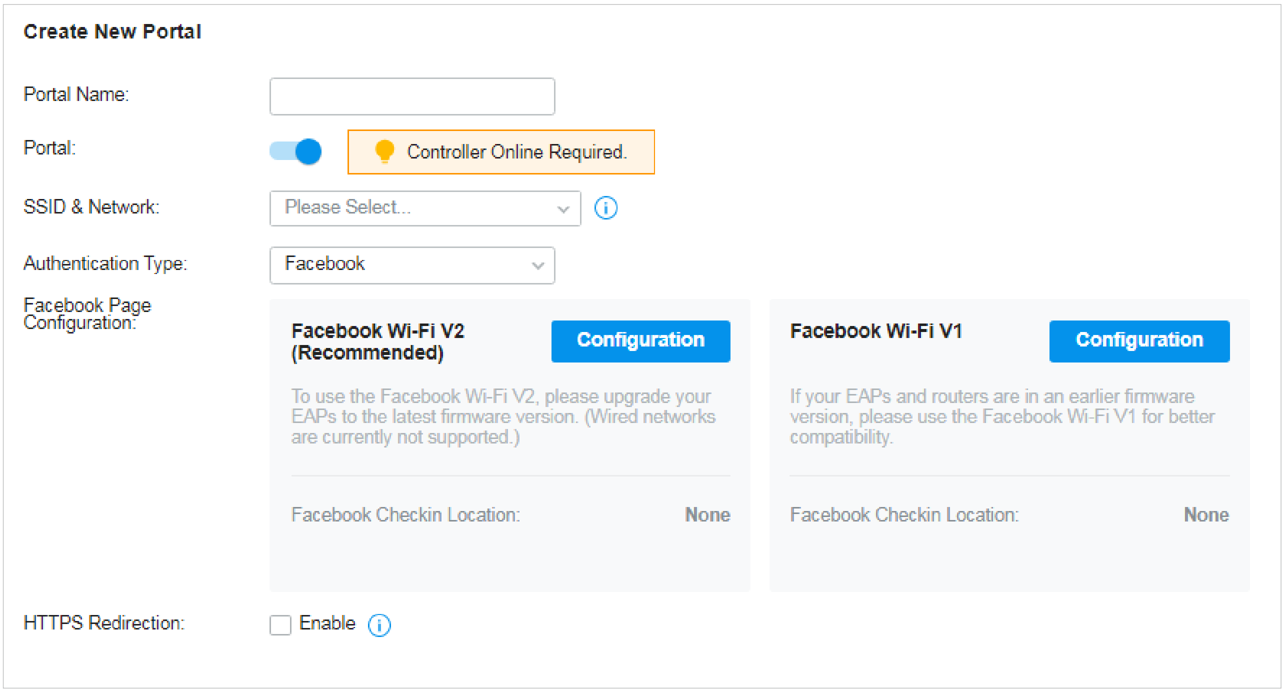
⊕ Add

TYPE	INFORMATION	ACTION
ⓘ No Authentication-Free Client have been configured.		

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. Select a site from the drop-down list of Organization. Go to Settings > Authentication > Portal. Click to enable Portal and load the following page.



Create New Portal

Portal Name:

Portal: ● Controller Online Required.

SSID & Network: Please Select...

Authentication Type: Facebook

Facebook Page Configuration:

Facebook Wi-Fi V2 (Recommended) Configuration

To use the Facebook Wi-Fi V2, please upgrade your EAPs to the latest firmware version. (Wired networks are currently not supported.)

Facebook Checkin Location: **None**

Facebook Wi-Fi V1 Configuration

If your EAPs and routers are in an earlier firmware version, please use the Facebook Wi-Fi V1 for better compatibility.

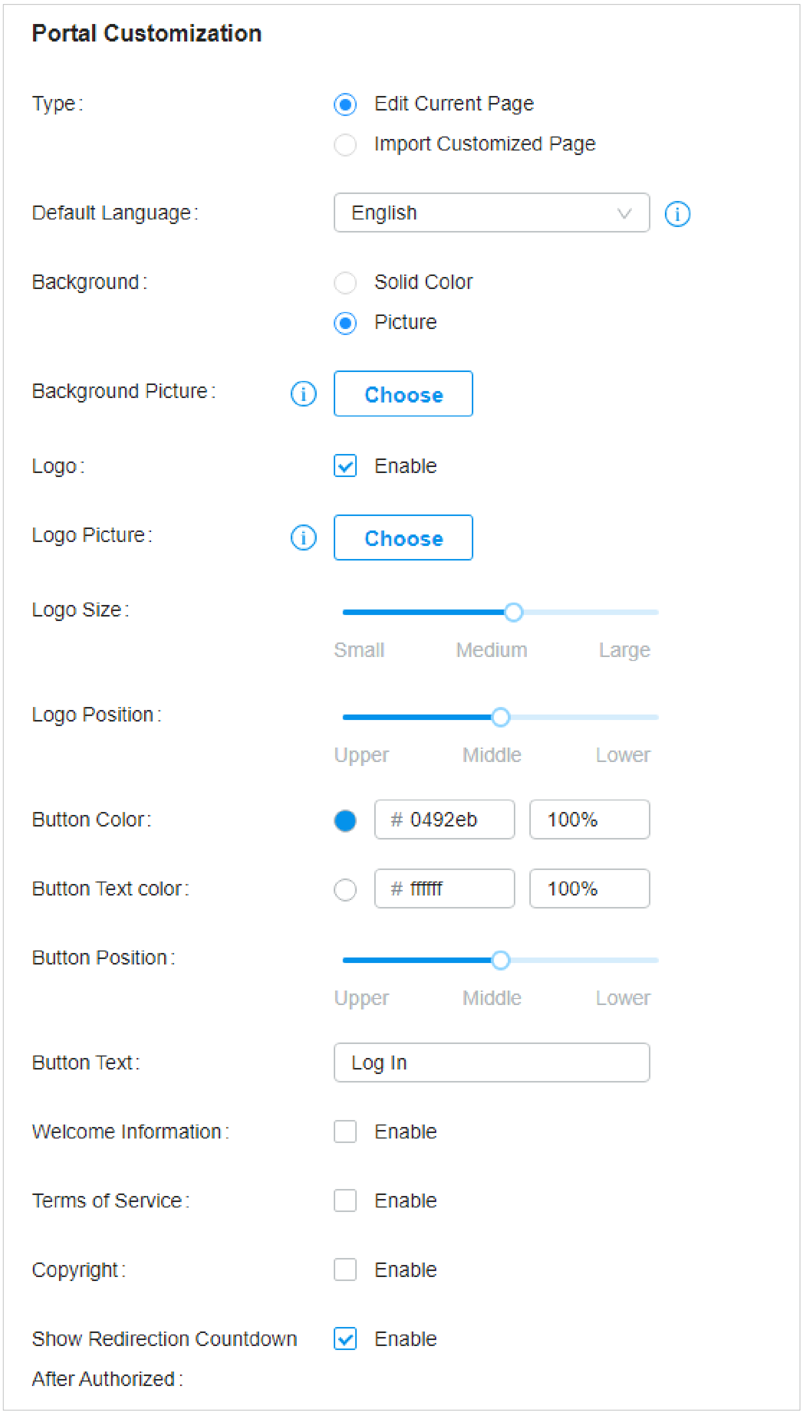
Facebook Checkin Location: **None**

HTTPS Redirection: □ Enable

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

SSID & 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. For Facebook Wi-Fi V1, clients can use Facebook account to authenticate, and for Facebook Wi-Fi V2, clients can use Facebook or Instagram account to authenticate.
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.



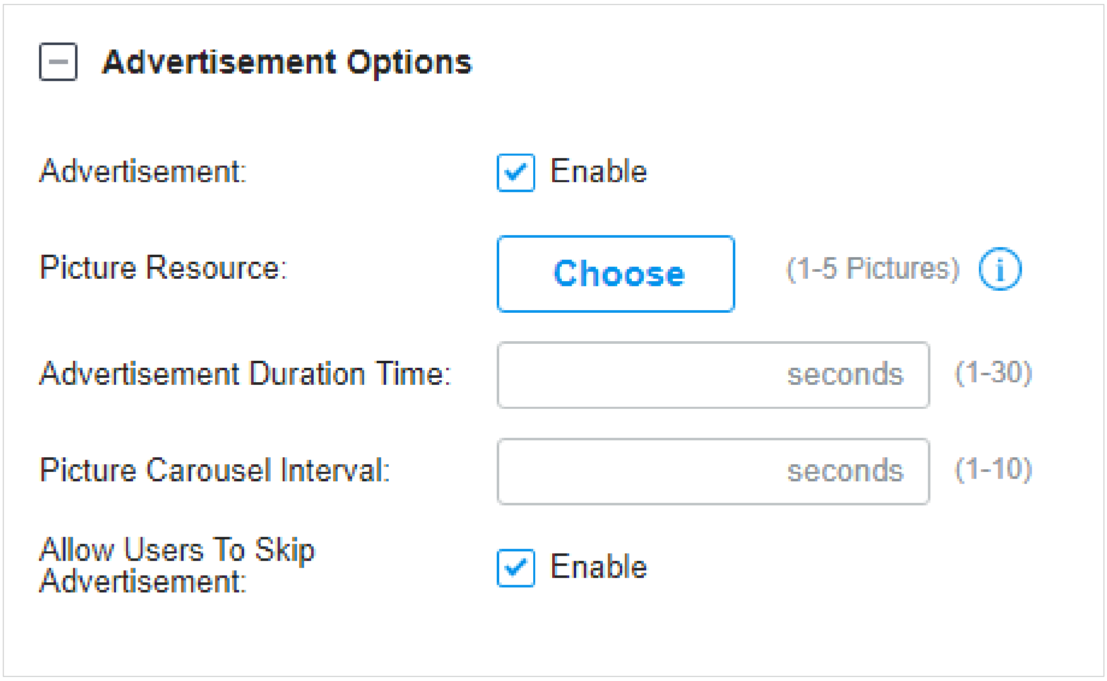
Portal Customization

Type:	● Edit Current Page ○ Import Customized Page
Default Language:	English ⓘ
Background:	○ Solid Color ● Picture
Background Picture: ⓘ	Choose
Logo:	☑ Enable
Logo Picture: ⓘ	Choose
Logo Size:	Small Medium Large
Logo Position:	Upper Middle Lower
Button Color:	● # 0492eb 100%
Button Text color:	○ # ffffff 100%
Button Position:	Upper Middle Lower
Button Text:	Log In
Welcome Information:	□ Enable
Terms of Service:	□ Enable
Copyright:	□ Enable
Show Redirection Countdown After Authorized:	☑ Enable

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	Click to show the logo on the portal page.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Size	Adjust the logo size on the Portal Page.
Logo Position	Adjust the logo position on the Portal Page.
Button 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 on the Portal Page.
Button Text	Enter the text for the button.
Welcome Information	Click the checkbox and enter text as the welcome information. You can specify the desired text font size and configure the text color 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. Click Add Terms to enter the name and context of the terms which will appear after a client clicks the link in Terms of Service.
Copyright	Click the checkbox and enter text as the copyright in the following box. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.
Show Redirection Countdown After Authorized	When enabled, the system will show the portal's redirection countdown.

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



Advertisement Options

Advertisement: ☑ Enable

Picture Resource: Choose (1-5 Pictures)

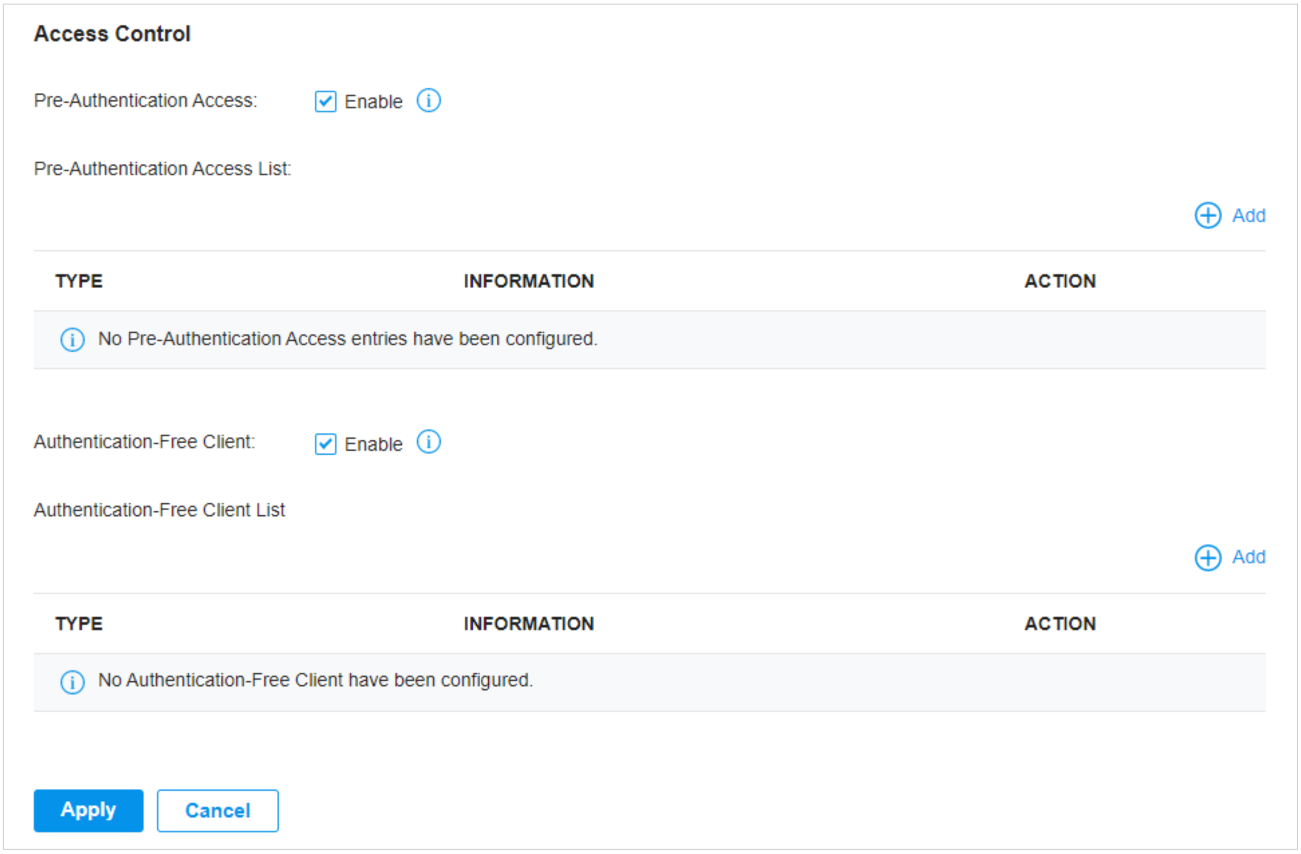
Advertisement Duration Time: seconds (1-30)

Picture Carousel Interval: seconds (1-10)

Allow Users To Skip Advertisement: ☑ Enable

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. (Optional) Configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed. Go to Settings > Authentication > Portal. On Access Control tab, click the checkbox to enable Pre-Authentication Access and Authentication-Free Policy.



Access Control

Pre-Authentication Access: ☑ Enable

Pre-Authentication Access List:

TYPE	INFORMATION	ACTION
No Pre-Authentication Access entries have been configured.		

Authentication-Free Client: ☑ Enable

Authentication-Free Client List

TYPE	INFORMATION	ACTION
No Authentication-Free Client have been configured.		

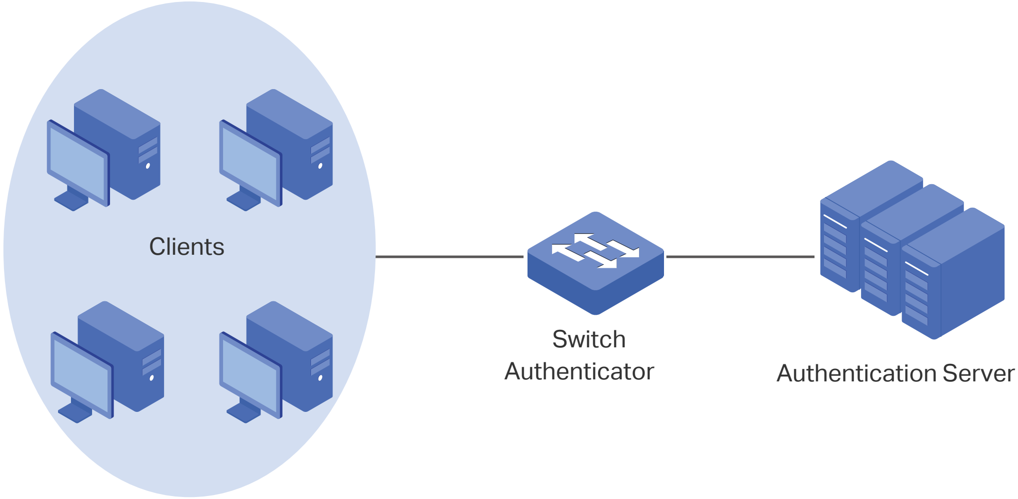
Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click ⊕ Add to configure the IP 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.

1.9.2 802.1X

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:

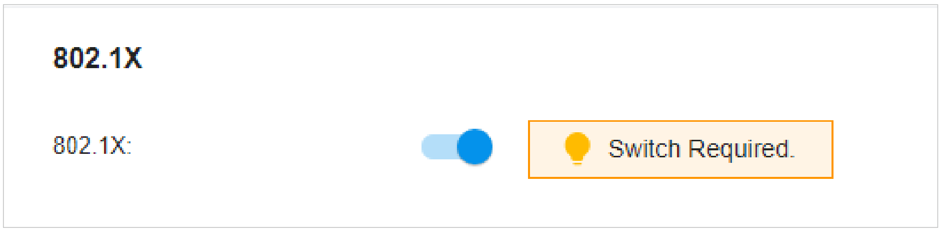
1) Click ○ to enable 802.1X.

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

Select a site from the drop-down list of Organization. Go to Settings > Authentication > 802.1X. Click ○ to enable 802.1X.

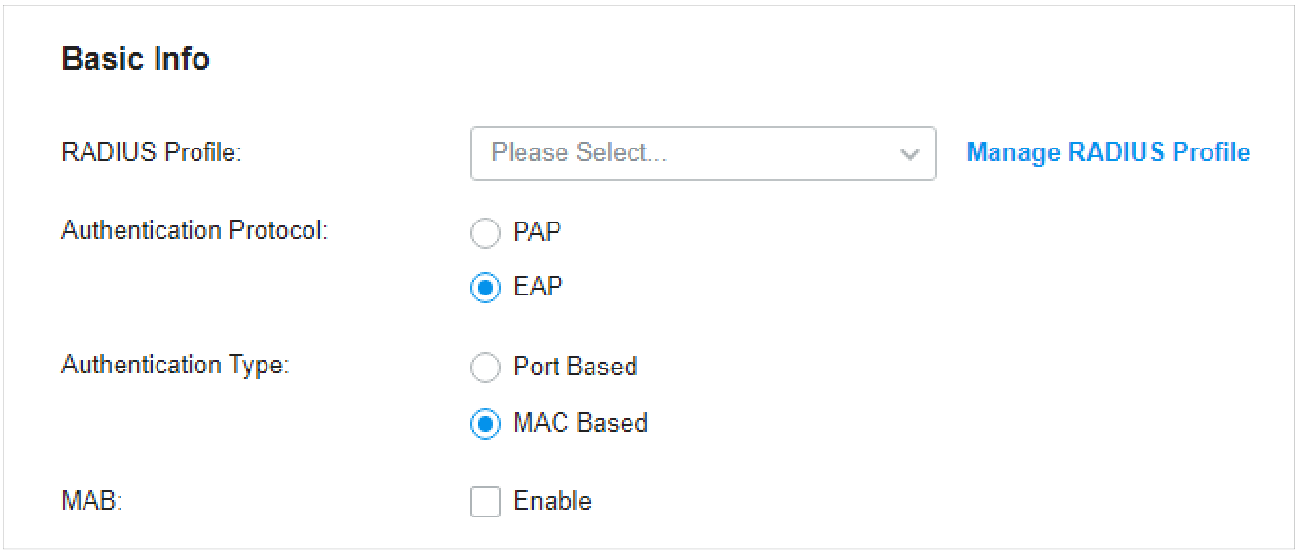


802.1X

802.1X: ● Switch Required.

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.



Basic Info

RADIUS Profile: Please Select... Manage RADIUS Profile

Authentication Protocol: ○ PAP ● EAP

Authentication Type: ○ Port Based ● MAC Based

MAB: □ Enable

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.

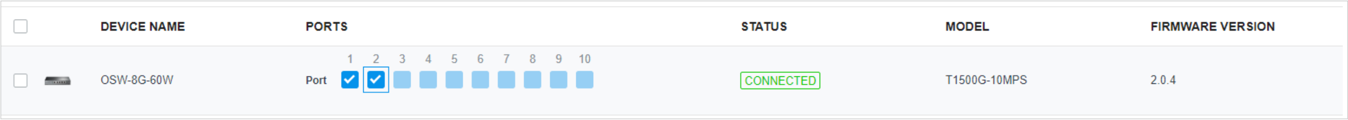
PAP: The EAP packets are converted to other protocol (such as RADIUS) packets, and transmitted to the RADIUS server.

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 ☑.



□	DEVICE NAME	PORTS	STATUS	MODEL	FIRMWARE VERSION
□	OSW-8G-60W	Port 1 ☑ 2 ☑ 3 4 5 6 7 8 9 10	CONNECTED	T1500G-10MPS	2.0.4

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.

1. 9. 3 MAC-Based Authentication

Overview

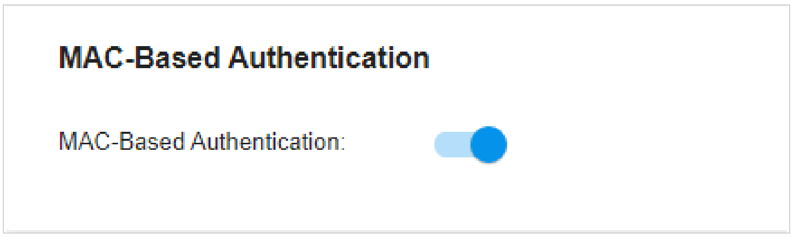
MAC-Based Authentication allows or disallows clients access to wireless networks based on the MAC addresses of the clients. In this authentication method, the controller takes wireless clients’ MAC addresses as their usernames and passwords for authentication. The RADIUS server authenticates the MAC 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

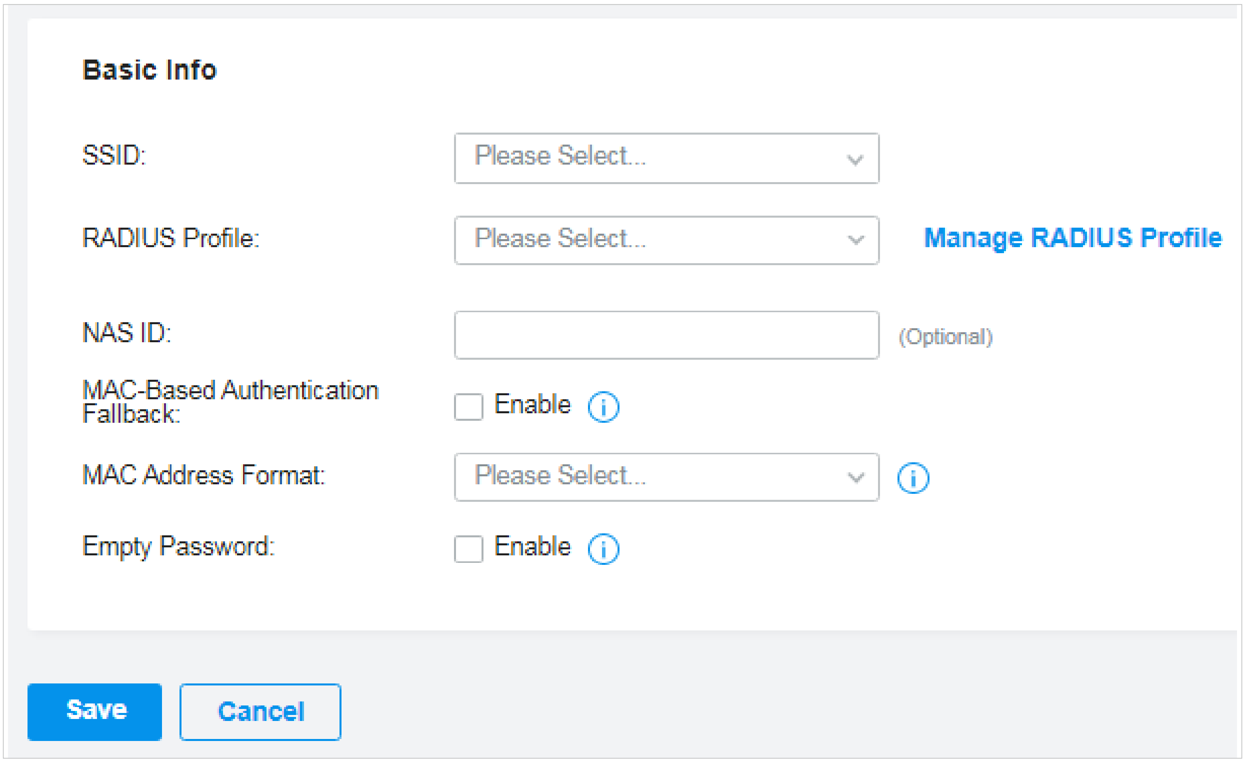
1. Select a site from the drop-down list of Organization. Go to Settings > Authentication > MAC-Based Authentication. Click to enable MAC-Based Authentication.



MAC-Based Authentication

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.



Basic Info

SSID: Please Select...

RADIUS Profile: Please Select... Manage RADIUS Profile

NAS ID: (Optional)

MAC-Based Authentication Fallback: □ Enable

MAC Address Format: Please Select...

Empty Password: □ Enable

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.

NAS ID	Configure a Network Access Server Identifier (NAS ID) for the authentication. 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.
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.

1. 9. 4 RADIUS Profile

Overview

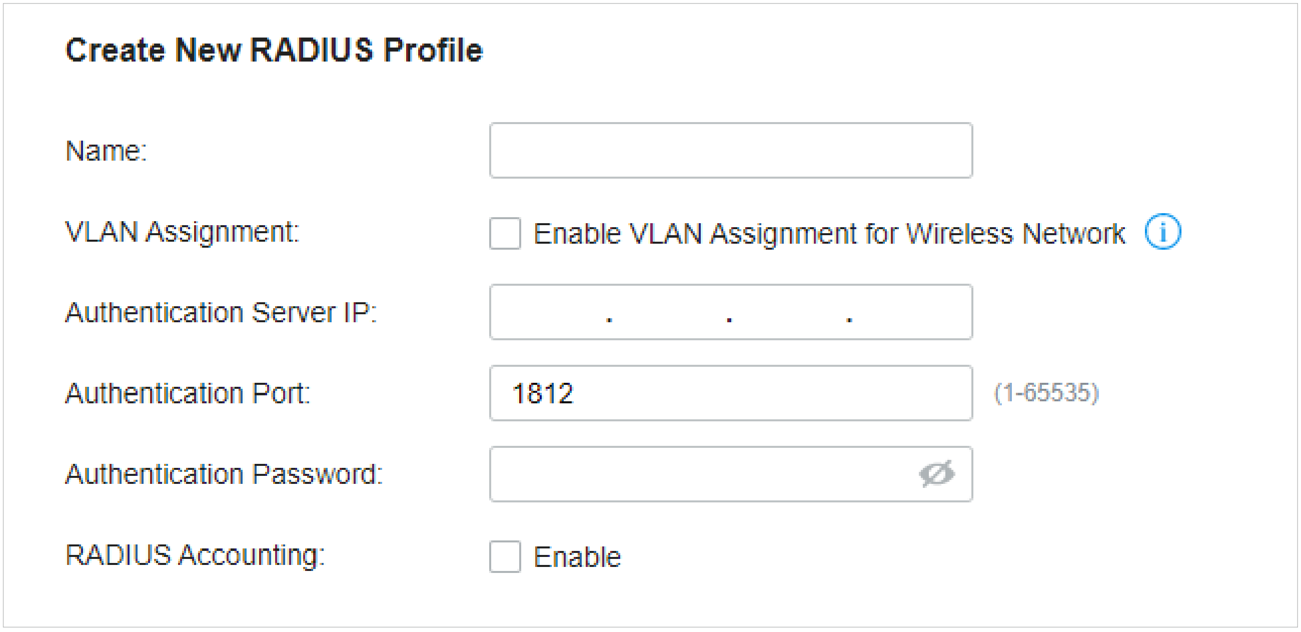
RADIUS (Remote Authentication Dial In User Service) is a client/server protocol that provides for the AAA (Authentication, Authorization, and Accounting) needs in modern IT environments.

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. Select a site from the drop-down list of Organization. Go to Settings > Authentication > RADIUS Profile. Click + Create New RADIUS Profile to load the following page.



Create New RADIUS Profile

Name:	
VLAN Assignment:	□ Enable VLAN Assignment for Wireless Network ⓘ
Authentication Server IP:	. . .
Authentication Port:	1812 (1-65535)
Authentication Password:	
RADIUS Accounting:	□ Enable

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.
VLAN Assignment	This feature allows the RADIUS server to place a wireless user into a specific VLAN based on the credentials supplied by the user. To use the feature, you should create the specific VLAN first. And the user-to-VLAN mappings must be already stored in the RADIUS server database. Note: 1. VLAN Assignment is not currently supported when a client is authenticated by Portal with External RADIUS Server or RADIUS Hotspot. 2. VLAN Assignment is applicable only when the device supports the feature. To make this feature work properly, it is recommended to upgrade your devices to the latest firmware version.
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.

1. 10 Services

Services provide convenient network services and facilitate network management. You can set fixed IP address for certain device in DHCP Reservation, configure servers or terminals in DDNS, SNMP, UPnP, and SSH, schedule the devices in Reboot Schedule, PoE Schedule and Upgrade Schedule, and export the information in Export Data, and more.

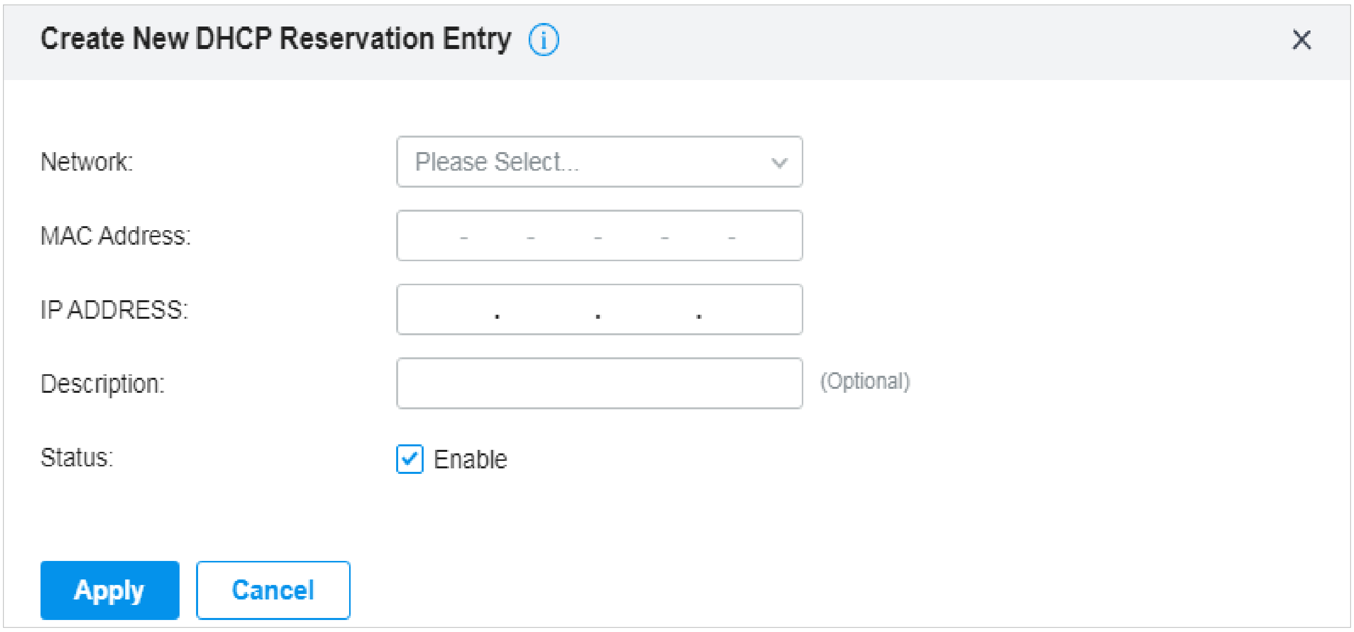
1. 10. 1 DHCP Reservation

Overview

It is convenient for networks to use Dynamic IP addresses assigned by Dynamic Host Configuration Protocol (DHCP), however, for devices that need to be reliably accessed, it is ideal to set fixed IP addresses for them. DHCP Reservation allows you to reserve specific IP addresses for devices in your network, and centrally manage the IP addresses.

Configuration

Select a site from the drop-down list of Organization. Go to Settings > Services > DHCP Reservation, click +Create New DHCP Reservation Entry and configure the parameters. Then click Apply.



Create New DHCP Reservation Entry

Network:	Please Select...
MAC Address:	- - - - -
IP ADDRESS:	. . .
Description:	(Optional)
Status:	☑ Enable

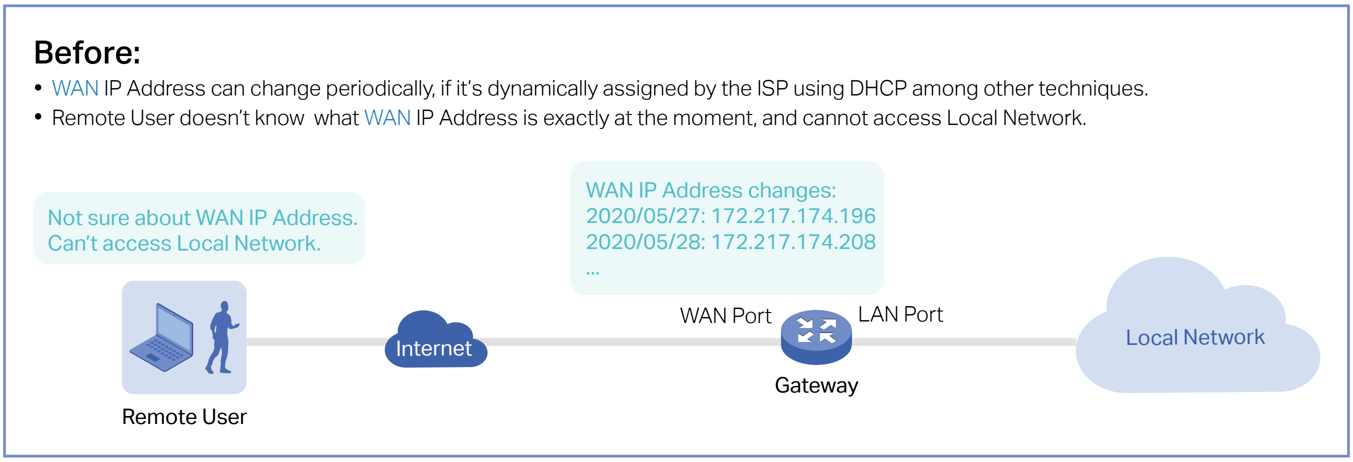
Network	Select the network the DHCP reservation entry is used for.
MAC Address	Specify the MAC address of the device for which you want to reserve an IP address.
IP Address	Specify the fixed IP address for the device.
Description	Enter description for the entry for identification.
Status	Enable or disable the entry.

1. 10. 2 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.

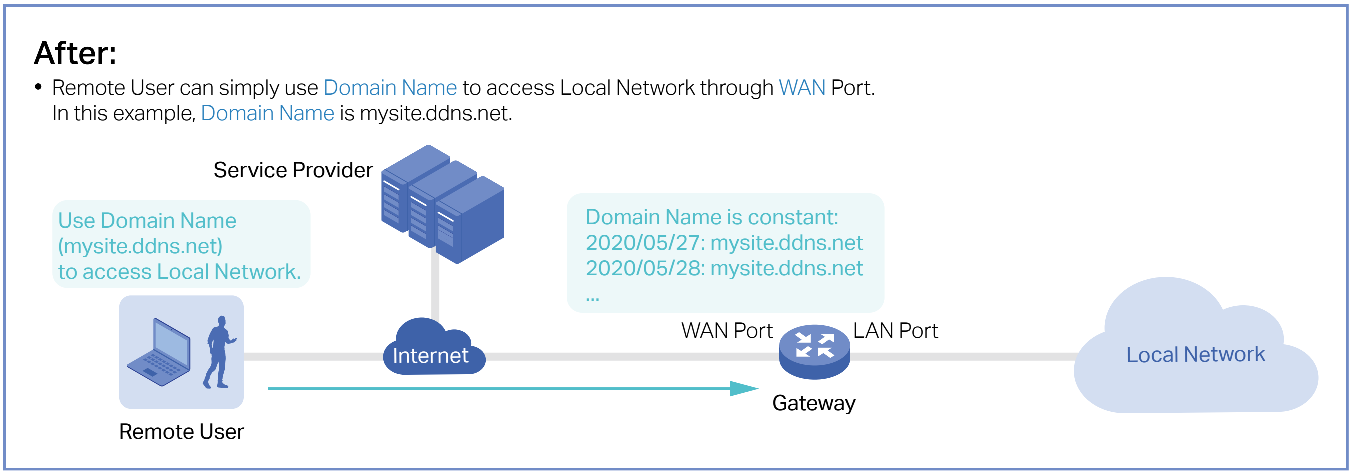


Before:

- WAN IP Address can change periodically, if it's dynamically assigned by the ISP using DHCP among other techniques.
- Remote User doesn't know what WAN IP Address is exactly at the moment, and cannot access Local Network.

Not sure about WAN IP Address.
Can't access Local Network.

WAN IP Address changes:
2020/05/27: 172.217.174.196
2020/05/28: 172.217.174.208
...



After:

- Remote User can simply use Domain Name to access Local Network through WAN Port. In this example, Domain Name is mysite.ddns.net.

Use Domain Name
(mysite.ddns.net)
to access Local Network.

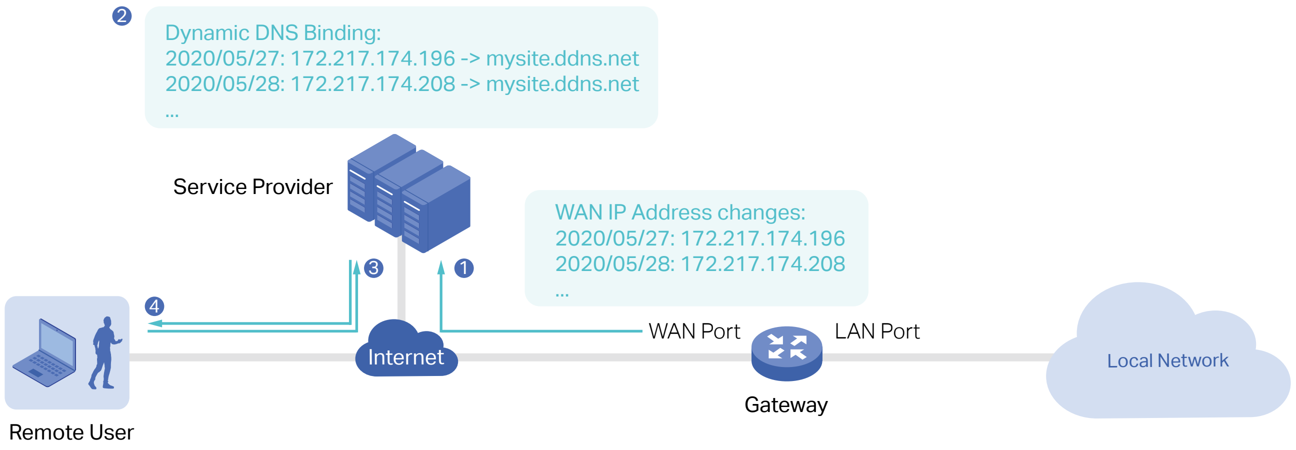
Domain Name is constant:
2020/05/27: mysite.ddns.net
2020/05/28: mysite.ddns.net
...

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.

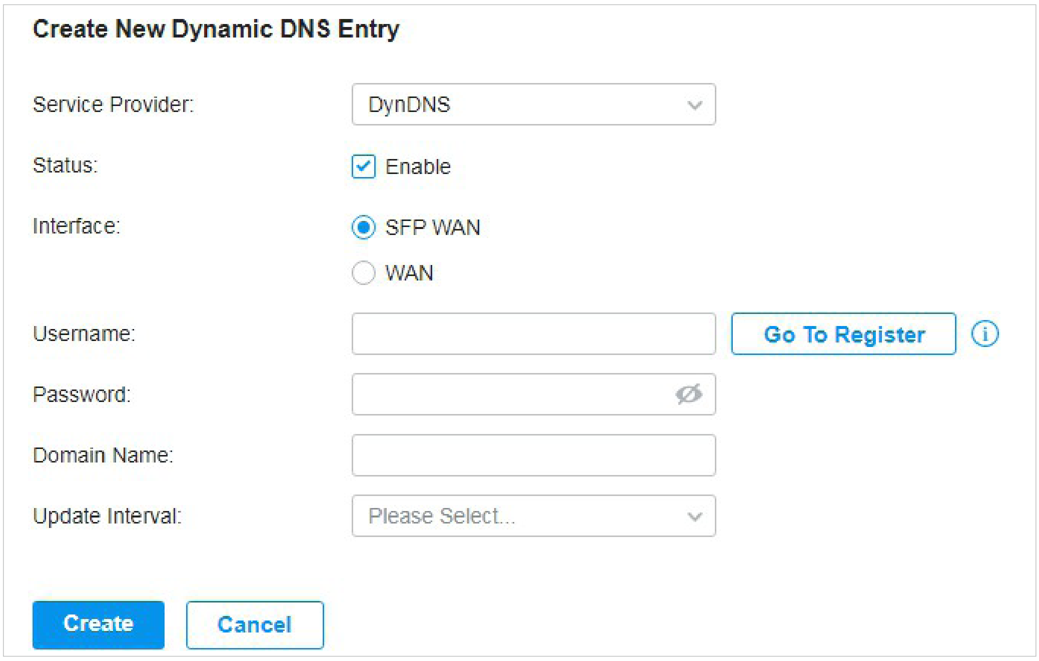
How Dynamic DNS works:

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



Configuration

Select a site from the drop-down list of Organization. Go to Settings > Services > Dynamic DNS. Click + Create New Dynamic DNS Entry, to load the following page. Configure the parameters and click Create.



Create New Dynamic DNS Entry

Service Provider: DynDNS

Status: ☑ Enable

Interface: ● SFP WAN ○ WAN

Username: Go To Register

Password:

Domain Name:

Update Interval: Please Select...

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.

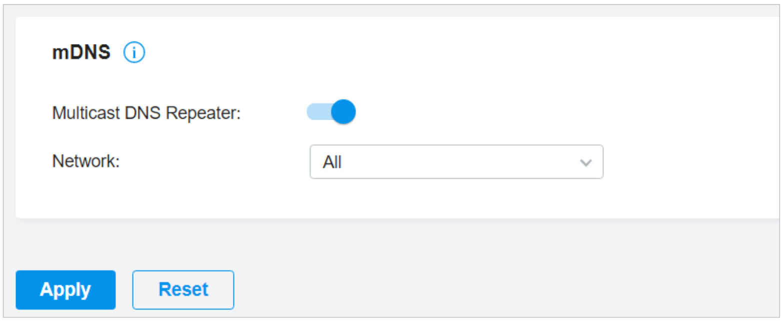
1. 10. 3 mDNS

Overview

mDNS (Multicast DNS) Repeater can help mDNS request/reply packets spread across different network segments. With this function, services published using the mDNS protocol can be discovered across network segments.

Configuration

1. Select a site from the drop-down list of Organization. Go to Settings > Services > mDNS.
2. Enable Multicast DNS Repeater.
3. Specify the Network to determine the network segments that mDNS request/reply packets can cross, that is, the range of services that can be found across network segments.
4. Apply the settings.



mDNS

Multicast DNS Repeater: ●

Network: All

1. 10. 4 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).

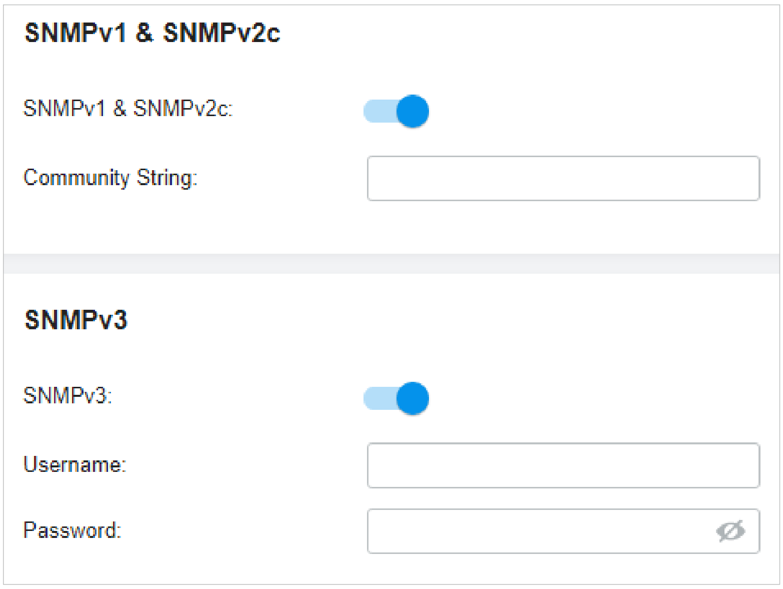
The controller supports multiple SNMP versions including SNMPv1, SNMPv2c and SNMPv3.

ⓘ 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

Select a site from the drop-down list of Organization. Go to Settings > Services > SNMP and configure the parameters. Then click Apply.



SNMPv1 & SNMPv2c

SNMPv1 & SNMPv2c: ●

Community String:

SNMPv3

SNMPv3: ●

Username:

Password:

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.

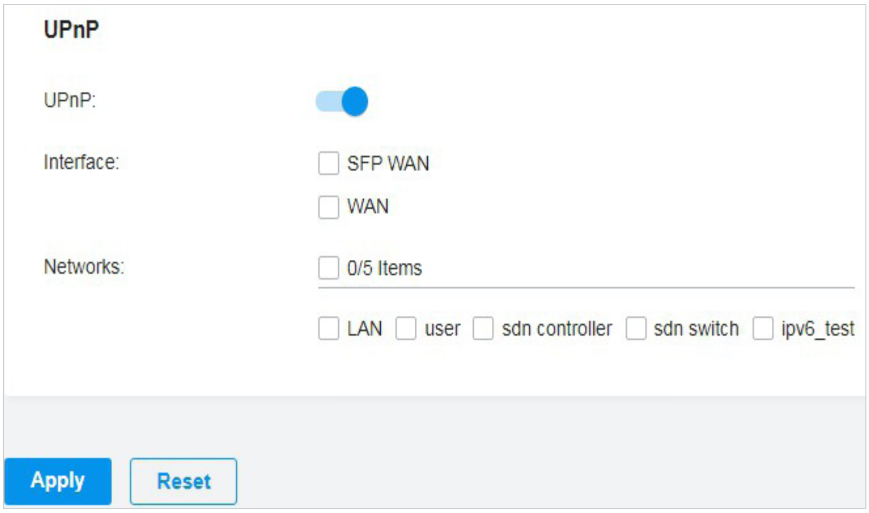
1. 10. 5 UPnP

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

Select a site from the drop-down list of Organization. Go to Settings > Services > UPnP. Enable UPnP globally and configure the parameters. Then click Apply.



UPnP

UPnP: ●

Interface: □ SFP WAN □ WAN

Networks: □ 0/5 Items

□ LAN □ user □ sdn controller □ sdn switch □ ipv6_test

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

1. 10. 6 SSH

Overview

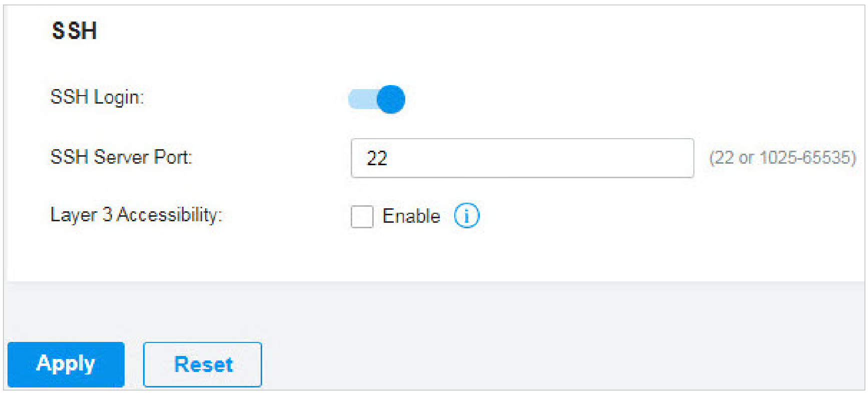
SSH (Secure Shell) provides a method for you to securely configure and monitor network devices via a command-line user interface on your SSH terminal.

Note:

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

Configuration

Select a site from the drop-down list of Organization. Go to Settings > Services > SSH. Enable SSH Login globally and configure the parameters. Then click Apply.



SSH

SSH Login: ●

SSH Server Port: 22 (22 or 1025-65535)

Layer 3 Accessibility: □ Enable

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.

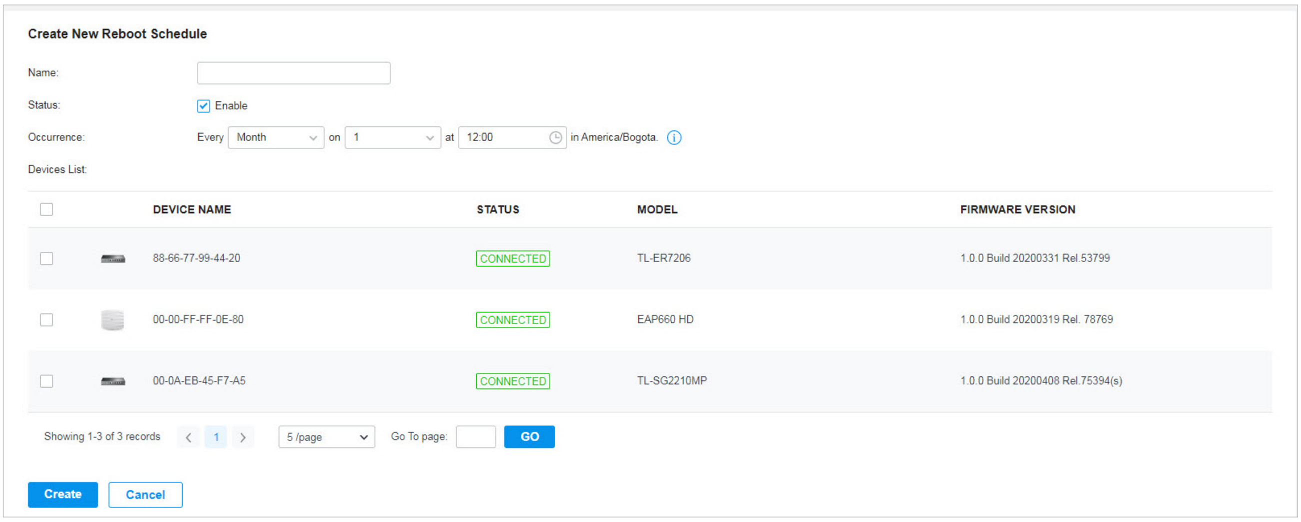
1. 10. 7 Reboot Schedule

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

1. Select a site from the drop-down list of Organization. Go to Settings > Services > Reboot Schedule. Click + Create New Reboot Schedule to load the following page and configure the parameters.



Create New Reboot Schedule

Name:

Status: ☑ Enable

Occurrence: Every Month on 1 at 12:00 in America/Bogota.

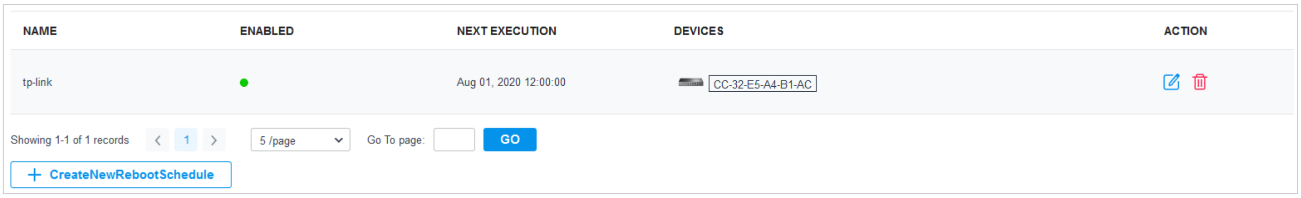
Devices List:

□	DEVICE NAME	STATUS	MODEL	FIRMWARE VERSION
□	88-66-77-99-44-20	CONNECTED	TL-ER7206	1.0.0 Build 20200331 Rel.53799
□	00-00-FF-FF-0E-80	CONNECTED	EAP660 HD	1.0.0 Build 20200319 Rel. 78769
□	00-0A-EB-45-F7-A5	CONNECTED	TL-SG2210MP	1.0.0 Build 20200408 Rel.75394(s)

Showing 1-3 of 3 records

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.

2. 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.



NAME	ENABLED	NEXT EXECUTION	DEVICES	ACTION
tp-link	●	Aug 01, 2020 12:00:00	CC-32-E5-A4-B1-AC	✎ 🗑

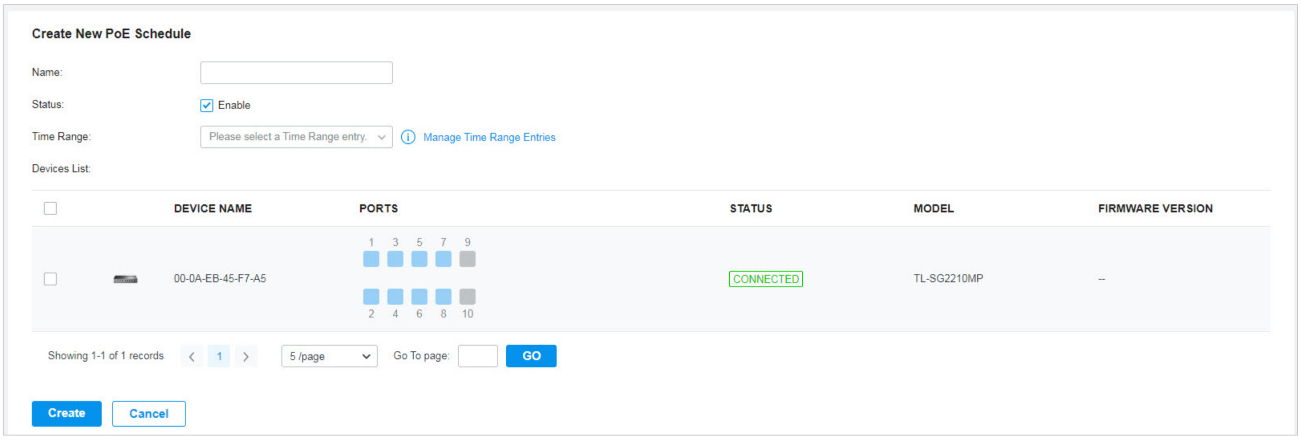
1. 10. 8 PoE Schedule

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

1. Select a site from the drop-down list of Organization. Go to Settings > Services > PoE Schedule. Click + Create New PoE Schedule to load the following page and configure the parameters.



Create New PoE Schedule

Name:

Status: ☑ Enable

Time Range: Please select a Time Range entry. ⓘ Manage Time Range Entries

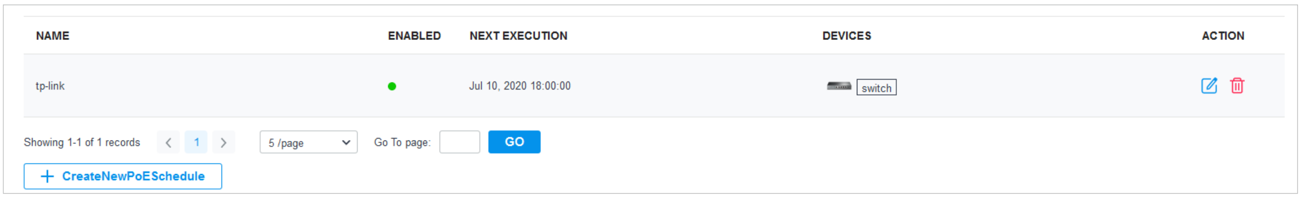
Devices List:

□	DEVICE NAME	PORTS	STATUS	MODEL	FIRMWARE VERSION
□	00-0A-EB-45-F7-A5	1 3 5 7 9 2 4 6 8 10	CONNECTED	TL-SG2210MP	--

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.

2. 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.



NAME	ENABLED	NEXT EXECUTION	DEVICES	ACTION
tp-link	●	Jul 10, 2020 18:00:00	switch	✎ 🗑

Showing 1-1 of 1 records < 1 > 5 /page Go To page: GO

+ CreateNewPoESchedule

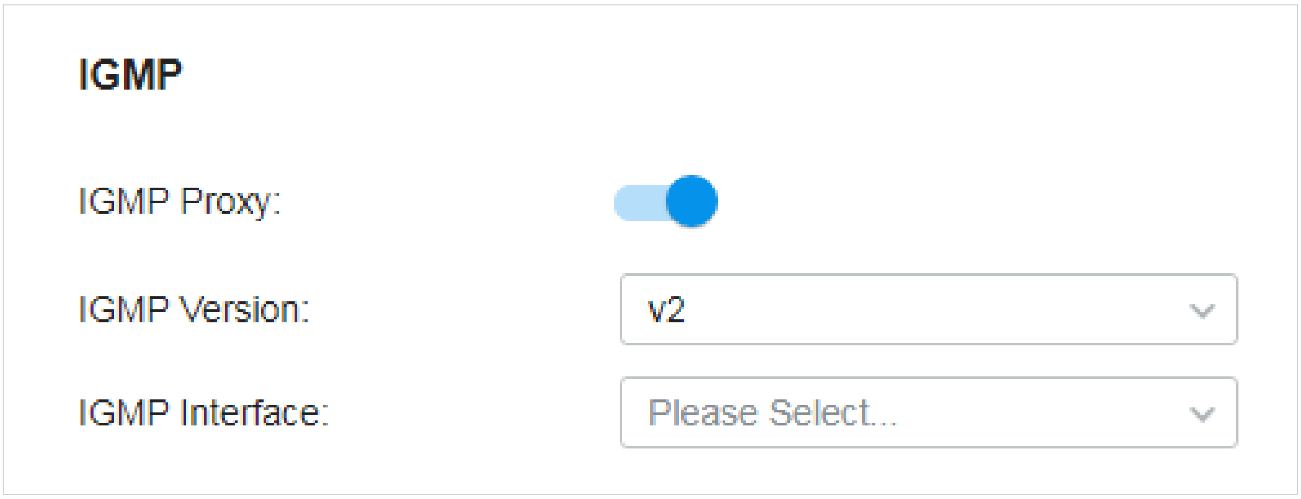
1. 10. 9 IPTV

Overview

IPTV includes two sections: IGMP and IPTV. In IGMP settings, you can enable IGMP proxy to detect multicast group membership information and thus the router is able to forward multicast packets based upon the information. IPTV settings allows you to enable Internet/IPTV/Phone service provided by your ISP.

Configuration

1. Select a site from the drop-down list of Organization. Go to Settings > Services > IPTV > IGMP, configure the parameters. If you want to configure the IPTV settings, go to next step; if you don't want to configure the IPTV settings, click Apply.



IGMP

IGMP Proxy: ●

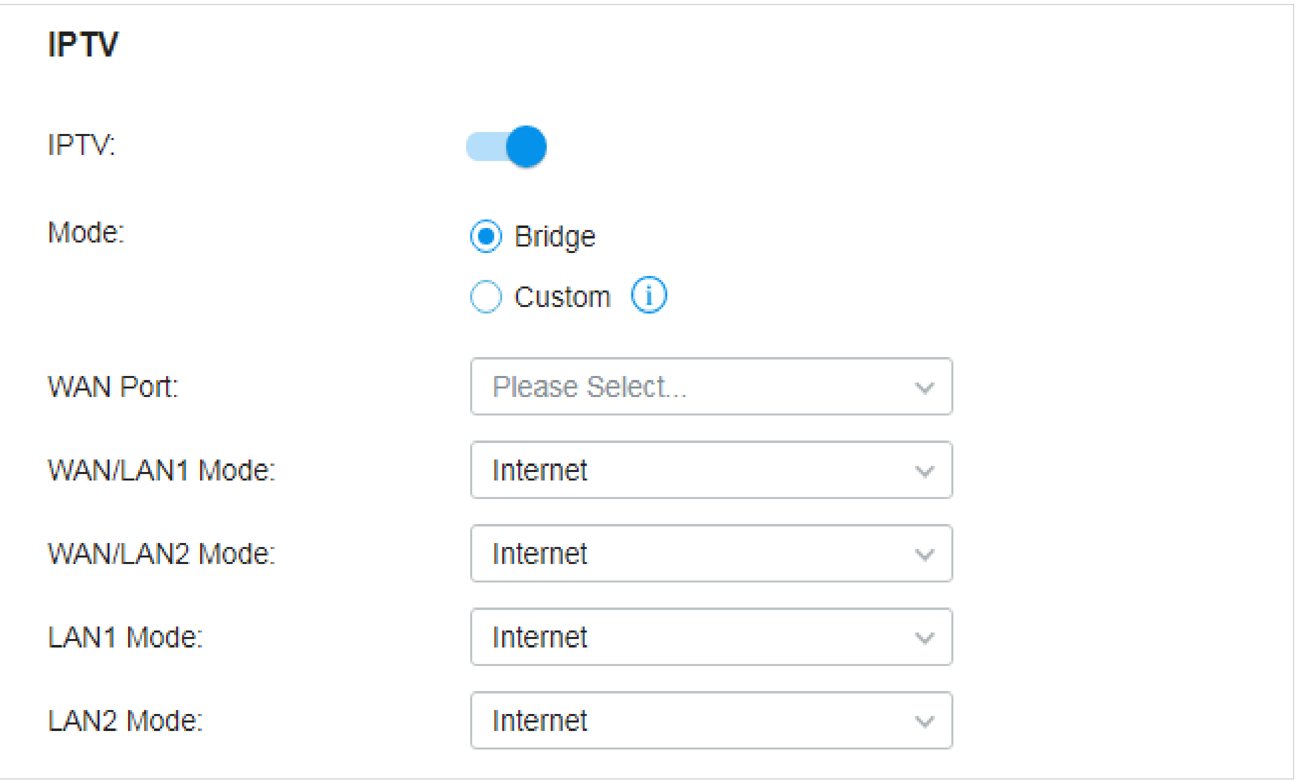
IGMP Version: v2

IGMP Interface: Please Select...

IGMP Proxy	Enable IGMP Proxy. IGMP Proxy sends IGMP querier packets to the LAN ports to detect if there is any multicast member connected to the LAN ports.
IGMP Version	Select the IGMP version as V2 or V3. The default is IGMP V2.
IGMP Interface	Select the WAN port on which the IGMP Proxy takes effect.

2. Go to Settings > Services > IPTV > IPTV, enable the IPTV features and choose the mode as Bridge or Custom according to your ISP. Then configure the corresponding parameters. Click Apply.

Note that the IPTV section will be hidden if your device is an earlier version that does not support this feature.



IPTV

IPTV: on

Mode: ● Bridge ○ Custom

WAN Port: Please Select...

WAN/LAN1 Mode: Internet

WAN/LAN2 Mode: Internet

LAN1 Mode: Internet

LAN2 Mode: Internet

IPTV	Enable IPTV feature.
Mode	Select the appropriate Mode according to your ISP. Bridge: Select this mode if your ISP requires no other parameters. Custom: Select this mode if your ISP provides necessary parameters, and configure the parameters according to the requirements of your ISP.
WAN Port	Select the WAN port on which the IPTV settings take effect.
Port Mode	Select the appropriate Port Mode of the LAN ports to determine which port is used to support Internet service, IPTV service, or IP Phone service.

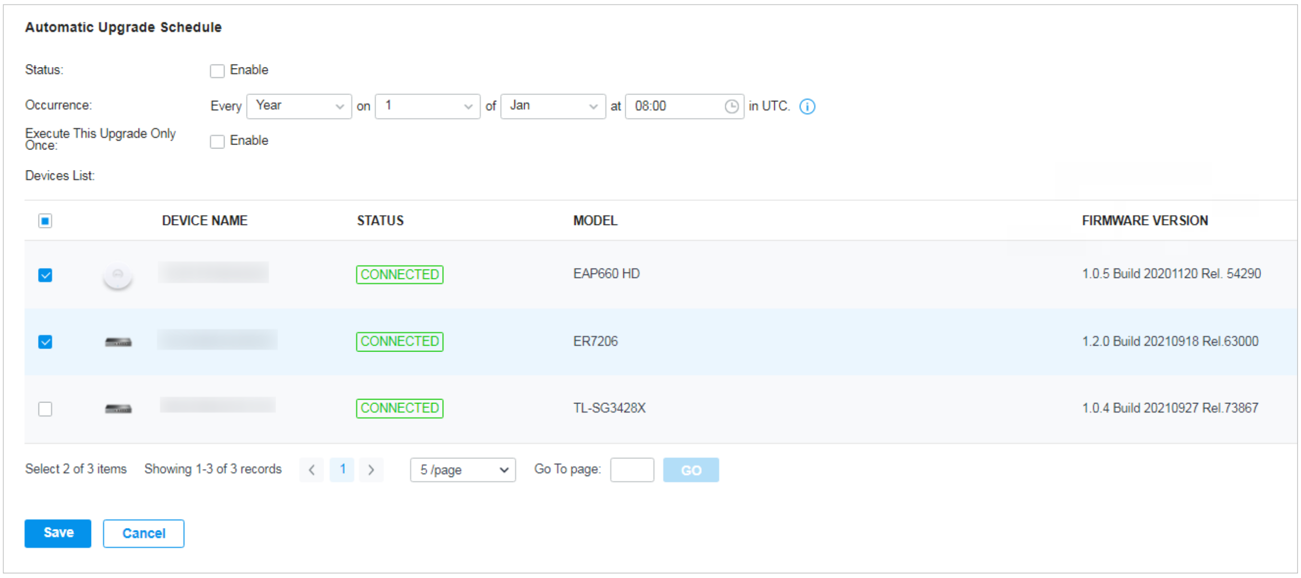
1. 10. 10 Upgrade Schedule

Overview

Upgrade Schedule allows you to schedule the device upgrade as desired. You can set recurring upgrades or a one-time schedule.

Configuration

Select a site from the drop-down list of Organization. Go to Settings > Services > Upgrade Schedule. Set the automatic upgrade schedule and select devices. Click Apply.



Automatic Upgrade Schedule

Status: ☐ Enable

Occurrence: Every Year on 1 of Jan at 08:00 in UTC.

Execute This Upgrade Only Once: ☐ Enable

Devices List:

■		DEVICE NAME	STATUS	MODEL	FIRMWARE VERSION
☑			CONNECTED	EAP660 HD	1.0.5 Build 20201120 Rel. 54290
☑			CONNECTED	ER7206	1.2.0 Build 20210918 Rel.63000
☐			CONNECTED	TL-SG3428X	1.0.4 Build 20210927 Rel.73867

Select 2 of 3 items Showing 1-3 of 3 records < 1 > 5 /page Go To page: GO

Status	Enable or disable the upgrade schedule.
Occurrence	Specify the time for automatic upgrade.
Execute This Upgrade Only Once	Enable this option if you only want to execute the set schedule once.
Devices List	Select the devices that will upgrade according to the set schedule.

1. 10. 11 DNS Proxy

Overview

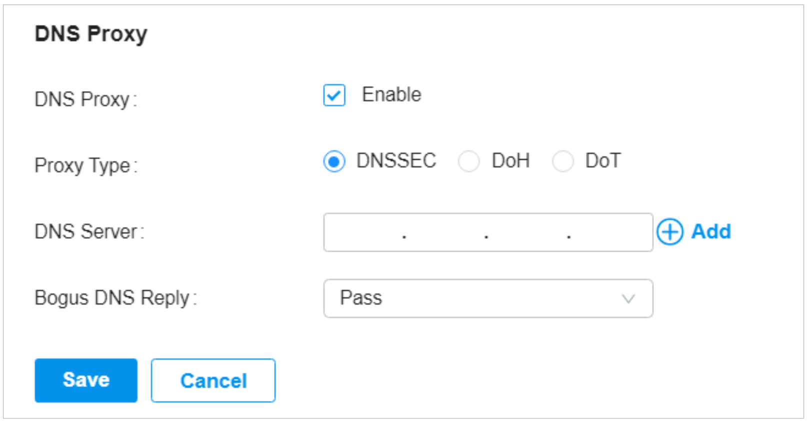
DNS Proxy provides the LAN side clients with the DNS query service. It forwards the DNS request from the LAN side clients to the selected upstream DNS server and forwards the DNS reply accordingly.

DNSSEC (DNS Security Extensions), DoT (DNS over TLS), and DoH (DNS over Https) are three security options for DNS Proxy. DNSSEC will verify the integrity of DNS records, and DoT / DoH will encrypt the query.

All of the three options need an upstream DNS server that supports them.

Configuration

1. Select a site from the drop-down list of Organization. Go to Settings > Services > DNS Proxy.
2. Enable DNS Proxy, configure the parameters, then save the settings.



DNS Proxy

DNS Proxy: ☑ Enable

Proxy Type: ● DNSSEC ○ DoH ○ DoT

DNS Server: . . . ⊕ Add

Bogus DNS Reply: Pass

Proxy Type	Specify a security option to apply.
DNS Server	Specify the upstream DNS server which the DNS requests will be forwarded to. For DoT and DoH, the system provides some known public DNS servers that support these security options. For DoH, the upstream DNS servers are usually websites with https URLs. For DNSSEC and DoT, servers are usually IP address.
Bogus DNS Reply	This is an special option for DNSSEC. Choose to drop/accept the bogus reply if the integrity of DNS records failed to be verified (which means the DNS record may be modified and is not trustable).

1. 10. 12 Export Data

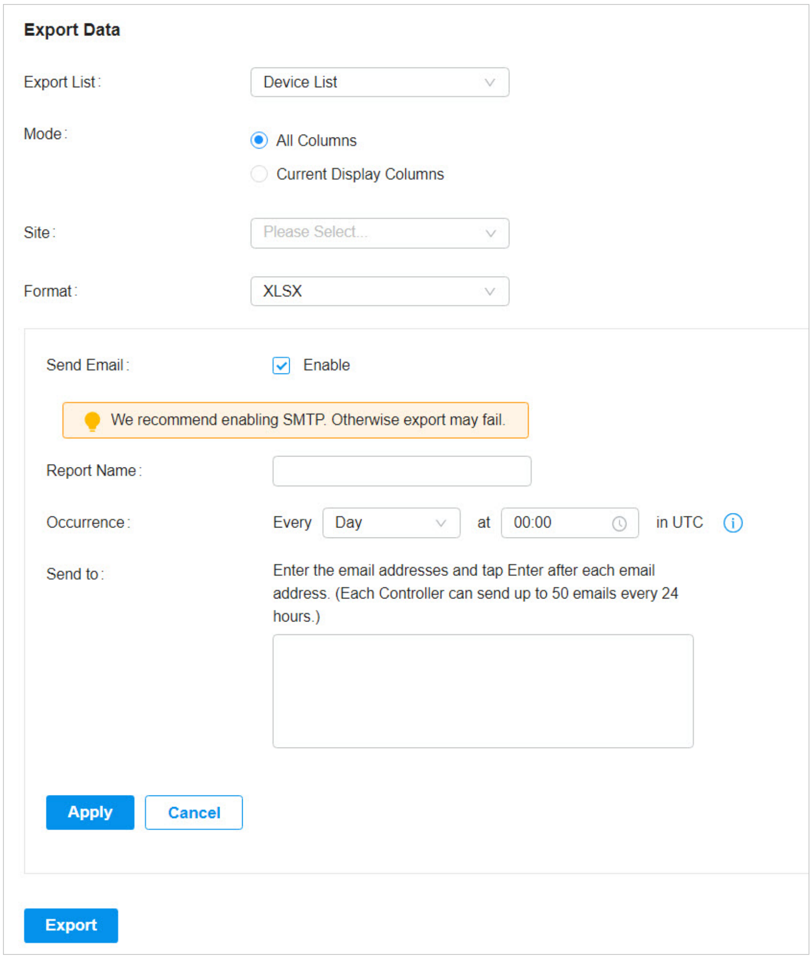
Overview

You can export data to monitor or debug your devices.

Configuration

1. Select Global View from the drop-down list of Organization. If you want to export data of only one site, you can also select the site to access the site view instead.

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



Export Data

Export List: Device List

Mode: ● All Columns ○ Current Display Columns

Site: Please Select...

Format: XLSX

Send Email: ☑ Enable

We recommend enabling SMTP. Otherwise export may fail.

Report Name:

Occurrence: Every Day at 00:00 in UTC

Send to: Enter the email addresses and tap Enter after each email address. (Each Controller can send up to 50 emails every 24 hours.)

Export List	Device List: Export the list of managed devices. Client List: Export the list of all clients that are connected to the networks. Insight-Rogue AP List: Export the list of the rogue APs scanned before. For detailed information, refer to 8. 5. 9 Rogue APs. Log List: Export the list of the logs generated by the controller. Authorized Client List: Export the list of authorized clients. Voucher Codes: Export the list of the voucher codes.
Mode	All Columns: Export the data list that contains all columns. Current Display Columns: Export the data list that contains only the displayed columns currently.
Site	Choose one or multiple sites to export data. Note: In site view, only the data of current site can be exported.
Format	The data can be exported to the file in the format of .CSV or .XLSX.

Send Email	If you want to send the exported data via email, enable Send Email and configure the parameters below: Report Name: Specify the report name of the email to send. Occurrence: Specify when to send the email. Send to: Specify the email addresses to send the exported data to.

1. 11 CLI Configuration

CLI configuration is essentially to configure devices via command lines. It is a supplementary means of GUI configuration. CLI configuration may conflict with GUI configuration.

The Omada Controller supports two types of CLI configuration: Site CLI and Device CLI.

- **Site CLI**

  Site CLI supports batch configuration of devices that support CLI configuration on the site.

- **Device CLI**

  Device CLI supports batch configuration of selected devices.

Currently, CLI configuration only supports switches. Please refer to CLI Reference Guide to understand the CLI commands of TP-Link switches.

If you need to use CLI configuration, please read the precautions and User Guide carefully. You can contact TP-Link technical support if necessary.

After applying the CLI configuration, you can go to **Devices** > **Application Result** to view the configuration results.

General Precautions

1. The GUI and CLI configuration should be planned globally according to the actual network topology and requirements.

2. To avoid conflicts, it is recommended not to use the CLI to configure the existing functions of the GUI.

   a. When adopting a new device, the Controller will apply configurations to the device in the order of GUI, Site CLI, and then Device CLI. If there is a configuration conflict, the configuration applied last takes effect.

   b. CLI profiles (including Site CLI profiles and Device CLI profiles) will only be sent to devices once after applied, unless the “Apply Again” button in the Application Result is clicked to trigger the full configurations application.

   c. When a device upgrades its firmware, the Controller will apply the full configurations to the device in the order of GUI, Site CLI, and then Device CLI.

   d. Since the configurations applied later will overwrite the previous configurations, the configuration results of different devices may be different after the same function has been modified repeatedly via GUI, Site CLI and Device CLI.

3. The Omada Controller will not verify the existing GUI and CLI configurations of devices. Be sure to check the existing configurations before performing new configurations. Otherwise, unexpected results may occur after the configurations are applied, and the devices may even go offline.

4. To avoid configuration conflicts, if you really need to use the CLI to configure a certain function, it is recommended not to configure it via GUI at the same time.

5. To avoid disconnection of devices from the Controller due to configuration errors or conflicts, it is recommended to configure VLAN, VLAN Interface, IP Address, ACL, etc. via GUI, and avoid modifying related configurations via CLI.

Repeated Configurations

When the same function is configured via CLI multiple times, the previous configuration may be overwritten, and the last configuration shall prevail.

a. It is recommended to confirm the currently effective commands via the CLI configuration viewing function “Show Running Config”.

b. If you need to cancel a certain configuration, use the “no” command.

c. If you need to modify a certain configuration, you can enter a new command to overwrite the configuration.

d. Apply the final configuration, and confirm that the function is configured correctly and takes effect via the CLI configuration viewing function.

Execution Failures

If a CLI command fails to be executed, an error will be reported and subsequent commands will be executed. You can view the error details via the error message, and the commands that have been successfully executed before will not be undone. It is recommended to follow the steps below:

a. Use the CLI configuration viewing function (Show Running Config) to confirm the commands that have taken effect. If you need to cancel them, you can enter “no” commands and apply them to devices.

b. Troubleshoot and correct the command error, regenerate the CLI configuration, and apply it to devices.

Command Modification

If you need to modify the commands issued via CLI, please follow the steps below:

a. Use the CLI configuration view function (Show Running Config) to confirm the commands that have taken effect, and sort out the commands that need to be canceled.

b. Enter “no” commands to cancel the configurations, and apply them to devices.

Prohibited Commands

1. CLI commands such as modifying user name and password, managing VLAN, SDM profile, reboot, reset, upgrade, import and export configurations have been prohibited. When using other CLI commands, please also pay attention to avoid affecting the management of the Controller.

2. Device CLI supports the variable function. The variable content does not have too many restrictions, for example, you can enter CLI commands, but it is not recommended to use it in this way.

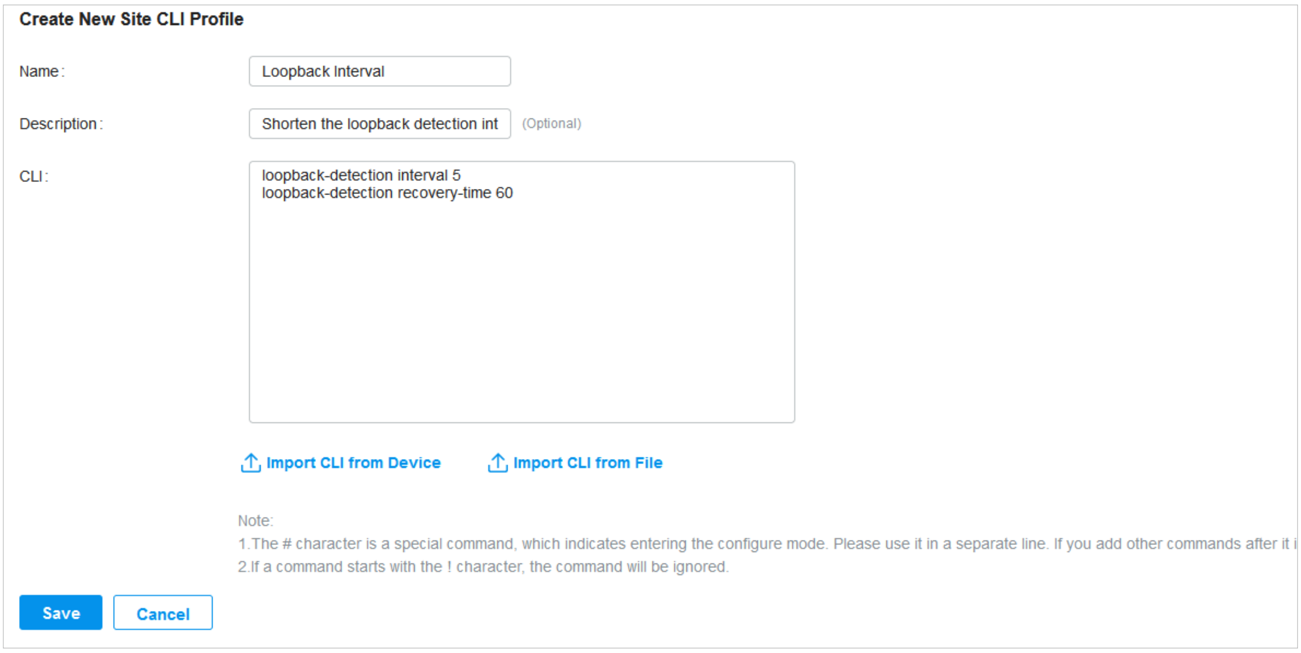
1. 11. 1 Site CLI

Overview

Site CLI enables batch configurations of all devices that support CLI configuration on the site via command lines.

Configuration

1. Go to Settings > CLI Configuration > Site CLI.
2. Click Create New Site CLI Profile and create a CLI profile according to your needs.



Create New Site CLI Profile

Name: Loopback Interval

Description: Shorten the loopback detection int (Optional)

CLI:

```
loopback-detection interval 5
loopback-detection recovery-time 60
```

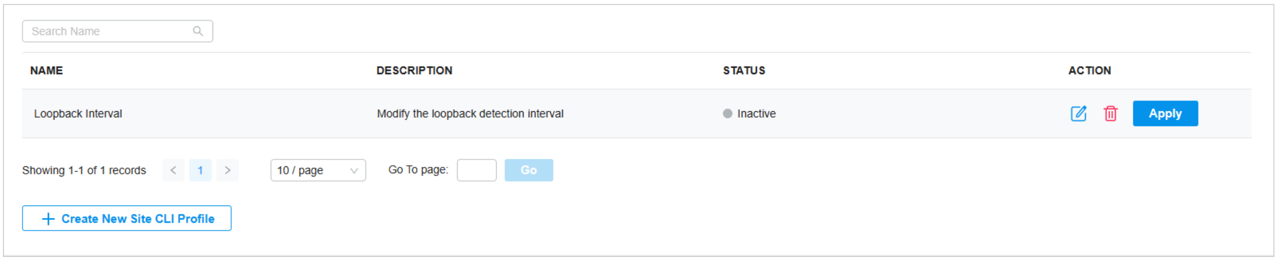
Note:
1.The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it i
2.If a command starts with the ! character, the command will be ignored.

ⓘ Note:

- The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.
- If a command starts with the ! character, the command will be ignored.

Name	Specify the name of the CLI profile.
Description	(Optional) Enter a description for identification.
CLI	Enter the command lines manually.
Import CLI from Device	Click and select a device that supports CLI configuration to import its running config.
Import CLI from File	Click and select an existing command file to import command lines.

3. Click Save to add the profile. The new profile is in inactive state and will not be applied to devices.

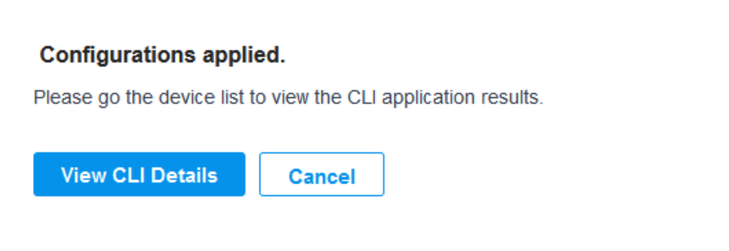


NAME	DESCRIPTION	STATUS	ACTION
Loopback Interval	Modify the loopback detection interval	● Inactive	Apply

4. Click Apply to apply the CLI. The profile will change to active state and apply configurations to all devices that support CLI configuration on the site.

Note:

Once the profile becomes active, you will be unable to edit it.



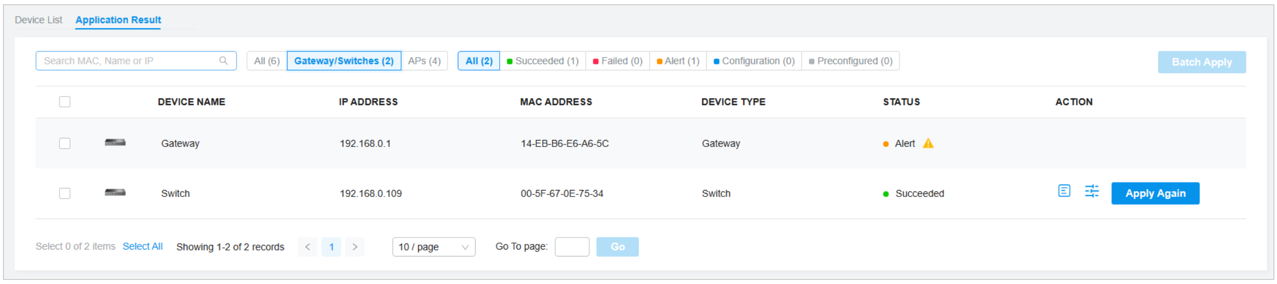
Configurations applied.

Please go the device list to view the CLI application results.

To check whether the profile is successfully applied to devices and takes effect, click View CLI Details to view the configuration results on the Devices > Application Result page.

Note:

Deleting a CLI profile will not take effect on existing configurations on devices. To delete the configurations, use the “no” command.



□	DEVICE NAME	IP ADDRESS	MAC ADDRESS	DEVICE TYPE	STATUS	ACTION
□	Gateway	192.168.0.1	14-EB-B6-E6-A6-5C	Gateway	● Alert ⚠	
□	Switch	192.168.0.109	00-5F-67-0E-75-34	Switch	● Succeeded	Apply Again

1. 11. 2 Device CLI

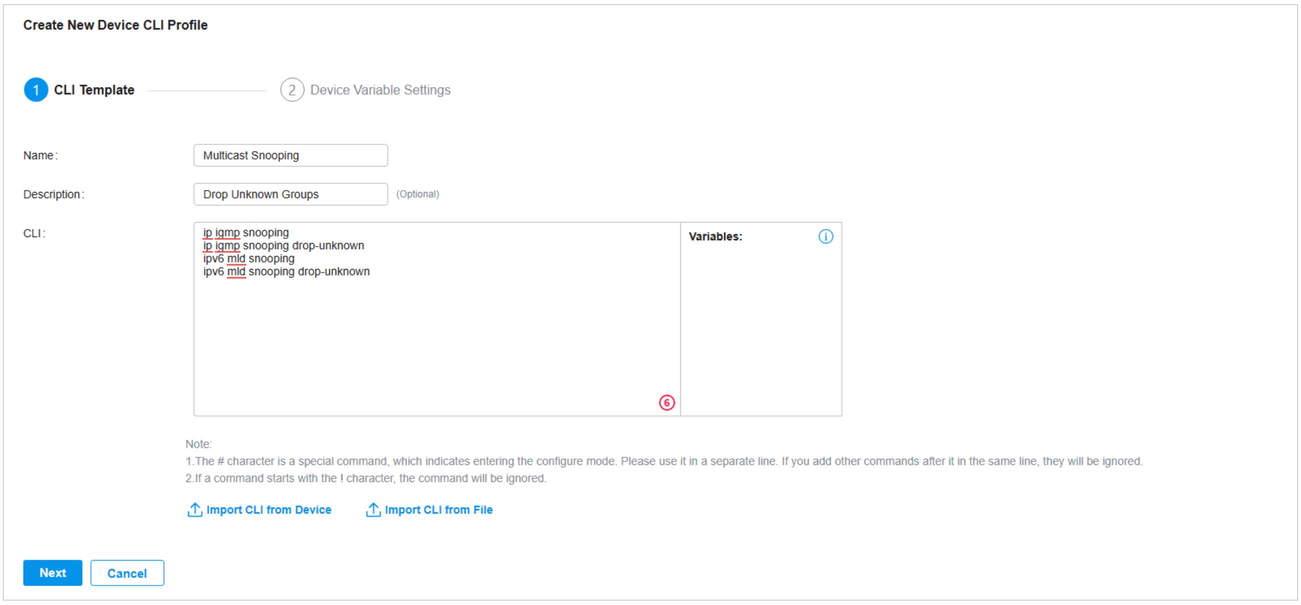
Overview

Device CLI enables batch configuration of specific devices via command lines.

Device CLI supports variables. You can use the %x% format to define a variable *x*, and then set different values for different switches. When the Controller applies the Device CLI configuration to switches, it will automatically modify the variable %x% to the values you set.

Configuration

1. Go to Settings > CLI Configuration > Device CLI. Click Create New Device CLI Profile and create a CLI profile according to your needs.



Name: Multicast Snooping

Description: Drop Unknown Groups (Optional)

CLI:

```
ip igmp snooping
ip igmp snooping drop-unknown
ipv6 mld snooping
ipv6 mld snooping drop-unknown
```

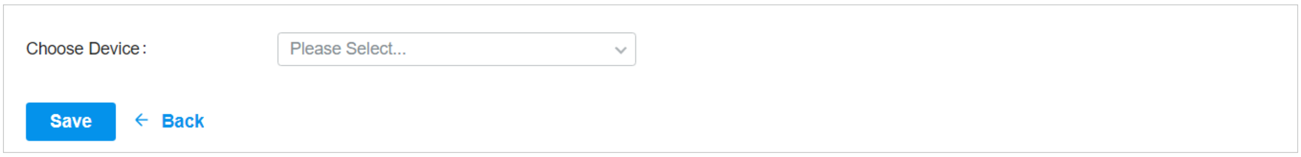
Note:
1.The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.
2.If a command starts with the ! character, the command will be ignored.

Note:

- The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.
- If a command starts with the ! character, the command will be ignored.

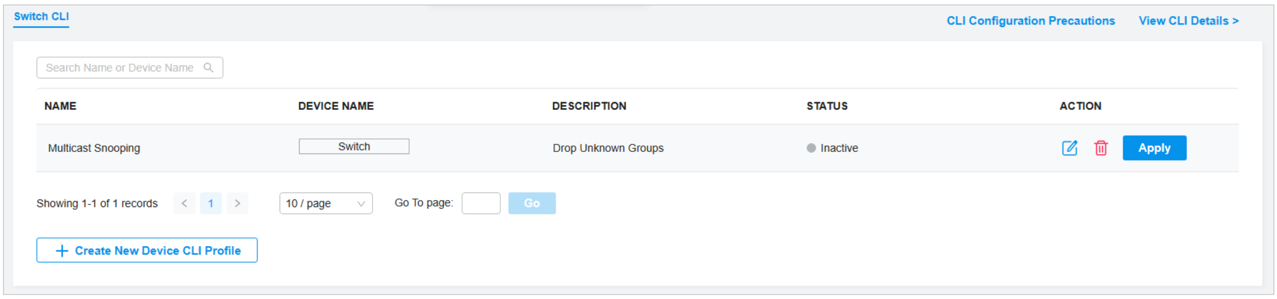
Name	Specify the name of the CLI profile.
Description	(Optional) Enter a description for identification.
CLI	Enter the command lines manually. You can enter %xxx% in the CLI template to define variables.
Import CLI from Device	Click and select a device that supports CLI configuration to import its running config.
Import CLI from File	Click and select an existing command file to import command lines.

2. Click Next. Select the devices to apply the CLI profile.



Choose Device: Please Select...

3. Click Save to add the profile. The new profile is in inactive state and will not be applied to devices.


Switch CLI
CLI Configuration Precautions
View CLI Details >
Search Name or Device Name
Apply
+ Create New Device CLI Profile

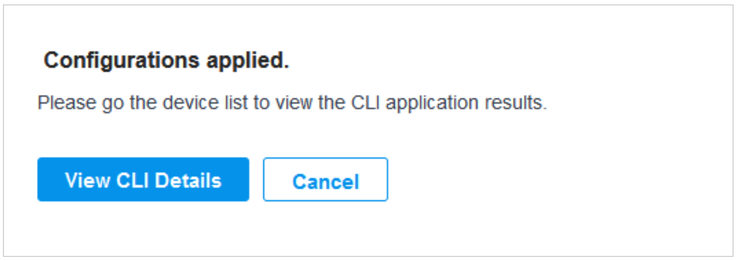
NAME	DEVICE NAME	DESCRIPTION	STATUS	ACTION
Multicast Snooping	Switch	Drop Unknown Groups	● Inactive	Apply

Showing 1-1 of 1 records < 1 > 10 / page Go To page: Go

4. Click Apply to apply the CLI. The profile will change to active state and apply configurations to the devices you selected.

Note:

Once the profile becomes active, you will be unable to edit it.



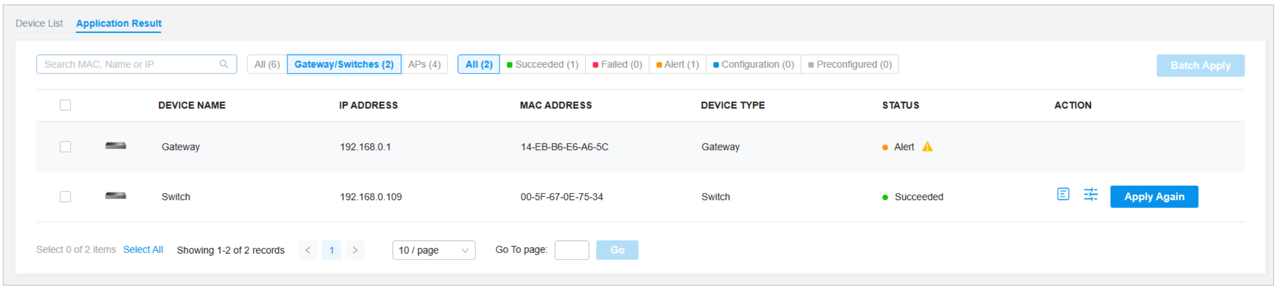
Configurations applied.

Please go the device list to view the CLI application results.

To check whether the profile is successfully applied to devices and takes effect, click View CLI Details to view the configuration results on the Devices > Application Result page.

Note:

Deleting a CLI profile will not take effect on existing configurations on devices. To delete the configurations, use the "no" command.



□	DEVICE NAME	IP ADDRESS	MAC ADDRESS	DEVICE TYPE	STATUS	ACTION
□	Gateway	192.168.0.1	14-EB-B6-E6-A6-5C	Gateway	● Alert ⚠	
□	Switch	192.168.0.109	00-5F-67-0E-75-34	Switch	● Succeeded	Apply Again

Select 0 of 2 items Select All Showing 1-2 of 2 records < 1 > 10 / page Go To page: Go