User Guide

Fusion Gateway

 1900002697 REV1.0.0

About this Guide

This User Guide provides information for using the Fusion gateway. Please read this guide carefully before operation.

Intended Readers

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

Conventions

When using this guide, notice that:

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

In this guide, the following conventions are used:

Fusion Gateway/Fusion System/Gateway/Controller	Stands for the Fusion gateway.
Switch	Stands for the Omada/Omada Campus Switch.
AP/EAP	Stands for the Omada/Omada Campus AP.
Note	The note contains the helpful information for a better use of the controller.
Configuration Guidelines	Provide guidelines for the feature and its configurations.

More Resources

Main Site	https://www.omadanetworks.com/
Video Center	https://support.omadanetworks.com/video/
Documents	https://support.omadanetworks.com/document/
Product Support	https://support.omadanetworks.com/product/
Technical Support	https://support.omadanetworks.com/contact-support/

For technical support, the latest software, and management app, visit https://support.omadanetworks.com/.

CONTENTS

6.Manage Switches

7.Manage APs

8.Manage Clients

9.Upgrade Device Firmware

10.Monitor the Network

11.Configure General Network Settings

12.Configure WAN Networks

13.Configure LAN Networks

14.Configure Wireless Networks

15.Configure VPN Networks

16.Configure Network Security

17.Configure Traffic Management Settings

18.Configure Network Authentication

19.Configure Network Profiles

20.Configure the SD-WAN

21.Configure the Hotspot

22.Maintain the Network

23.Manage Accounts

24.Configure Controller Settings

Chapter 1

Product Overview

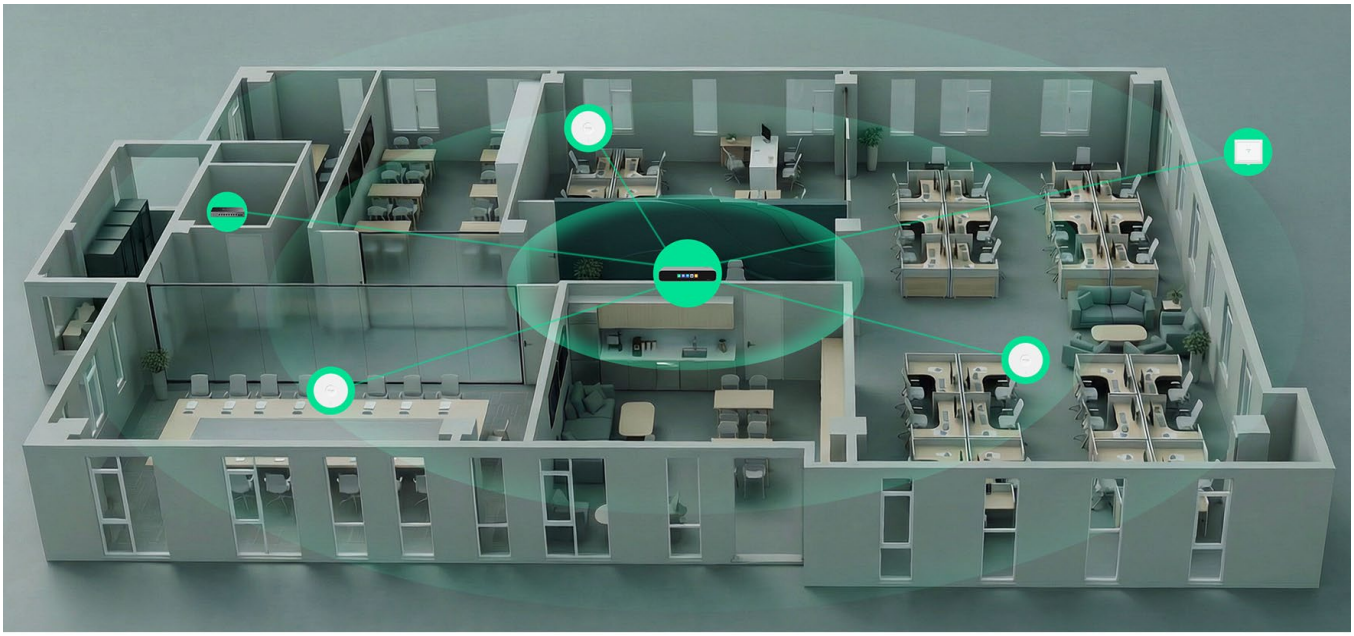
The Fusion gateway delivers an all-in-one solution for networking and centralized management on a single device, featuring a built-in controller for the entire Omada ecosystem. It is ideal for small businesses across single or multiple sites.

The chapter includes the following sections:

1. 1 Overview

Omada Fusion Gateway is an all in one solution that integrates a gateway and controller into a single device. Positioned at the center of the Omada networking ecosystem, it unifies networking and centralized management with license free cloud control straight out of the box. Bluetooth based setup simplifies deployment, cuts installation time, and reduces on site visits through touchscreen based troubleshooting — helping increase profitability while delivering projects more efficiently.

- License Free Cloud Management for Multi Site Work
- Simplified Setup with Auto Device Detection via Bluetooth and One-Tap Bulk Device Adoption
- Enterprise Grade Performance
- Quick Troubleshooting via Touchscreen, Less On-Site Work
- Secure Remote Network Access — One Click Away with Omada Lightlink VPN
- Advanced Software Capabilities: App-Based ACL, One-Click Auto QoS, Full Mesh SD-WAN, Content Filtering



1. 2 Key Features

Fusion gateways are FCC Class A certified products with various advanced software capabilities, primarily used in business, industrial, or office environments.

- Multi-Site Networking and Management: Features an enterprise-grade SD-WAN for multi-site networking in business scenarios (e.g., chain supermarkets and chain restaurants) and Cloud Portal for managing multiple sites.
- Centralized Management: Facilitates unified management of all network devices (including enterprise-grade L3 switches, APs, etc.) within the enterprise network.
- Enterprise Network Stability Assurance: Supports multi-WAN and failover functionality between multi-WANs.
- Enterprise-Grade Device Configuration: Supports professional Command Line Interface (CLI) configuration, batch port configuration across switches, and the SNMP management protocol.
- Enterprise-Grade Operation and Maintenance Management: Features enterprise-grade network packet capture for exporting various network traffic reports with audit logs.
- Commercial-Grade Access/Authentication Methods*: Offers external Portal/Voucher/RADIUS authentication, supports (Private Pre-Shared Key (PPSK), 802.1x/MAC-Based Authentication, and professional enterprise-grade L3 layer network features.
- Management of Professional Enterprise-Grade L3 Network Features: Supports management of enterprise-grade L3 switches.

*These features refer to functions supported by the devices adopted by the Fusion gateway and can be configured through it.

Chapter 2

Get Started with Fusion Gateway

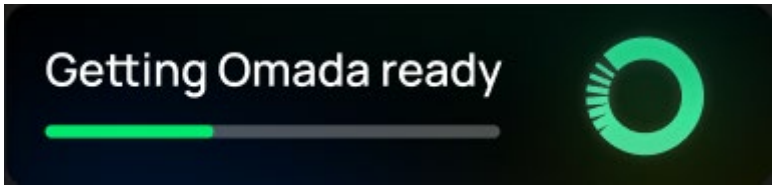
This chapter guides you on how to get started with Fusion gateway to configure the network. You can get started with the Fusion gateway with its management page. It can also be set up via the Omada app easily.

2. 1 Set Up Fusion Gateway via Omada App

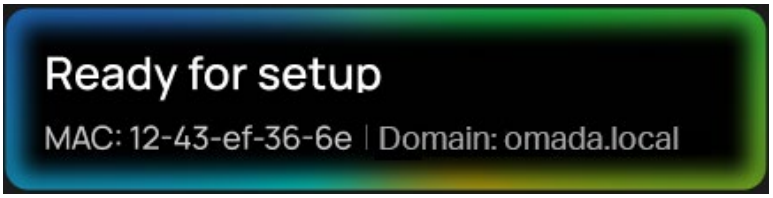
The Fusion gateway can be easily set upvia Bluetooth using the Omada App. Automatically discover and batch adopt all other Omada networking devices at once, saving time and simplifying IT deployment.

To set up the Fusion gateway via Omada app, follow the step:

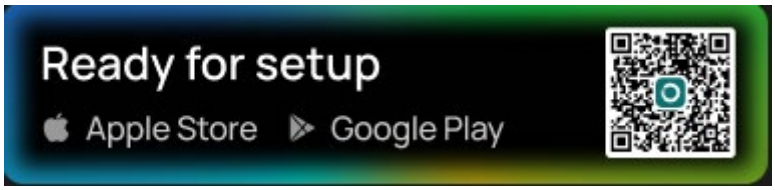
1. Power on your Fusion Gateway, connect the WAN port to the internet using an Ethernet cable. Wait for the device to finish booting up.



2. After the screen starts up, it shows the gateway's MAC and domain name. MAC is used to identify the gateway, and the domain can be used to log in to the gateway's web management page .



3. Once the device has finished booting up, the screen will display "Ready for setup". Scan the QR code on the right side of the screen to download and install the latest Omada app.

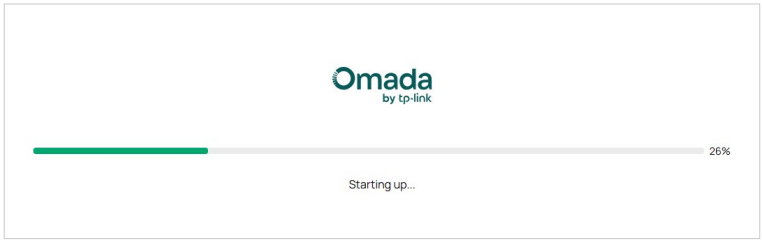


4. Enable Bluetooth on your mobile phone.
5. After the gateway boots up, enter the Omada app, and it will automatically detect the Omada Fusion Gateway nearby that is waiting to be initialized. Select your Fusion system (gateway), tap it and follow the app instructions to configure the internet settings, bind the gateway to your TP-Link ID for cloud access and other network settings.

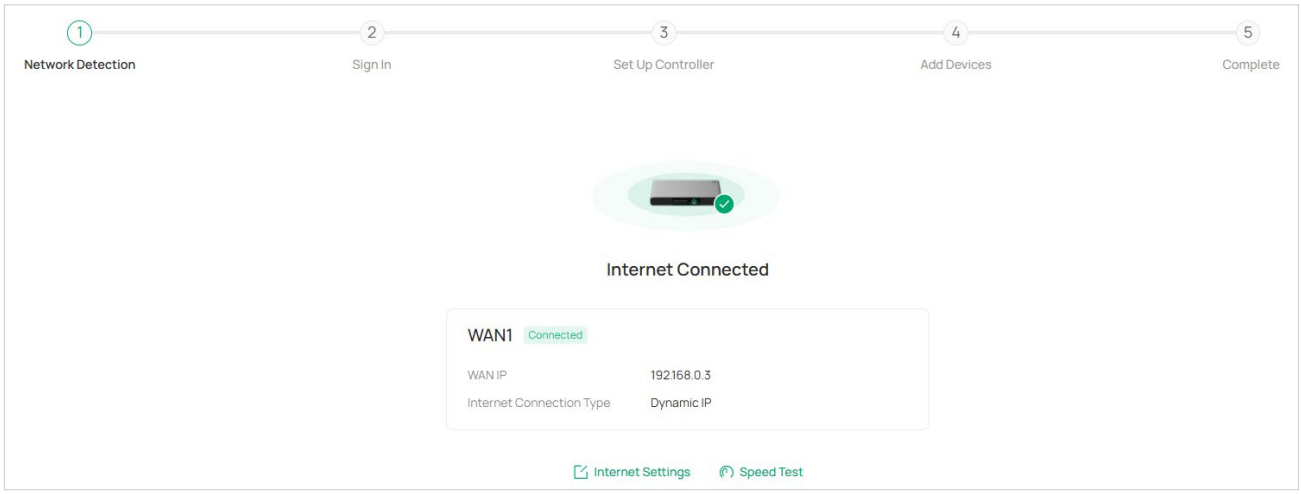
2. 2 Set Up Fusion Gateway via Local Web

Follow the steps below to enter the management interface of the Fusion gateway:

1. Connect a computer to a LAN port of the Fusion gateway with an RJ45 port properly. If your computer is configured with a fixed IP address, change it to obtain an IP address automatically.
2. Launch a web browser and type the default management address https://omada.local or 192.168.188.1 in the address bar, then press **Enter** (Windows) or **Return** (Mac). The management interface will start up.

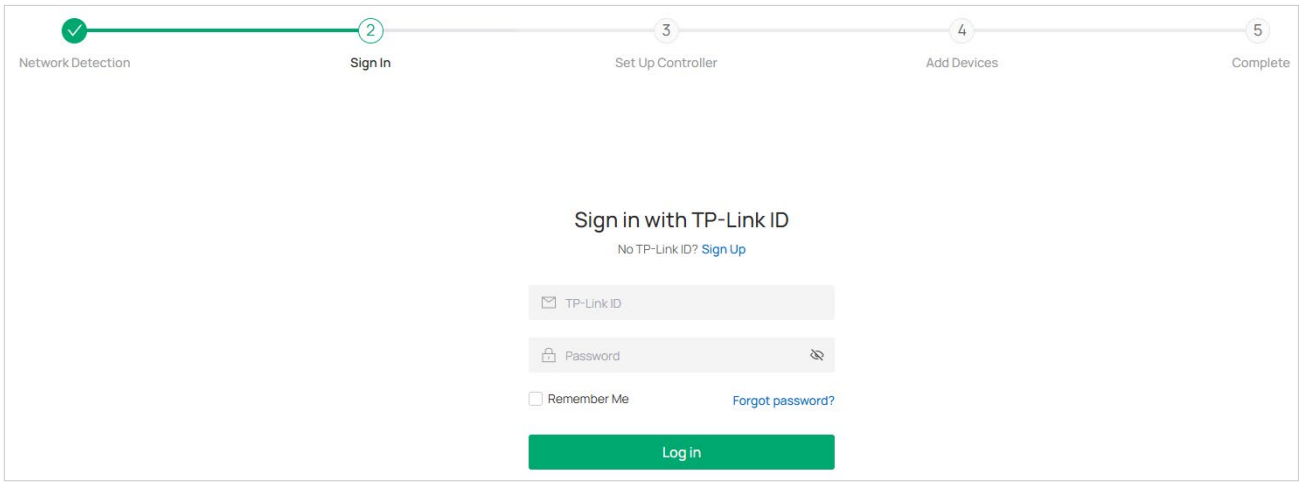


3. After the Gateway boots up, check the WAN port status here. By default, the Omada Fusion Gateway dials up via DHCP. If you need to use a different dial-up method or configure VLAN ID/DNS Server/ MAC Clone, click Internet Settings.

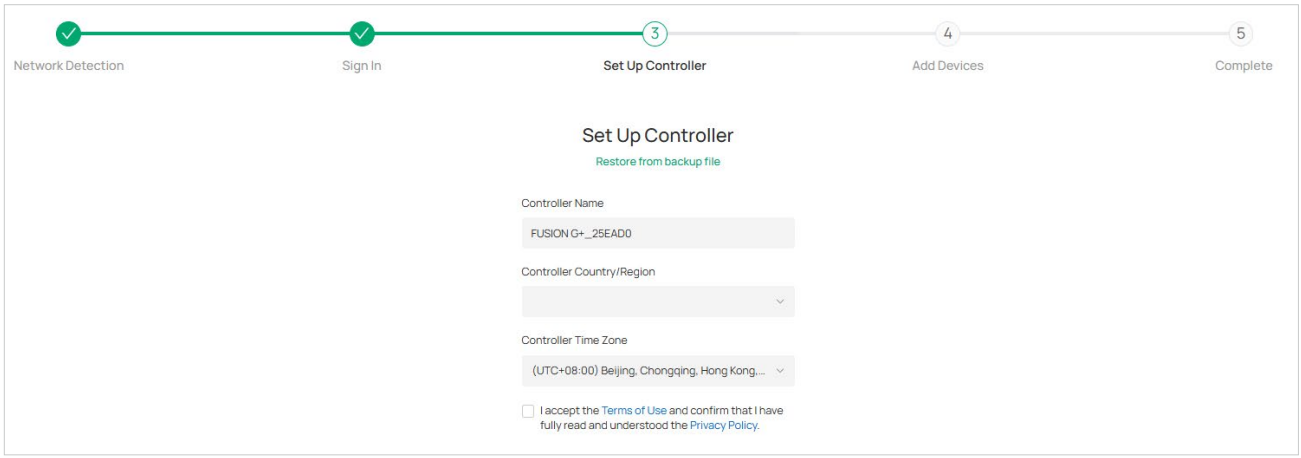


Note: Besides Dynamic IP (DHCP), the Fusion Gateway also supports Static IP, PPPoE, MAP-E, and DS-Lite. Refer to Configure WAN Networks for detailed instructions.

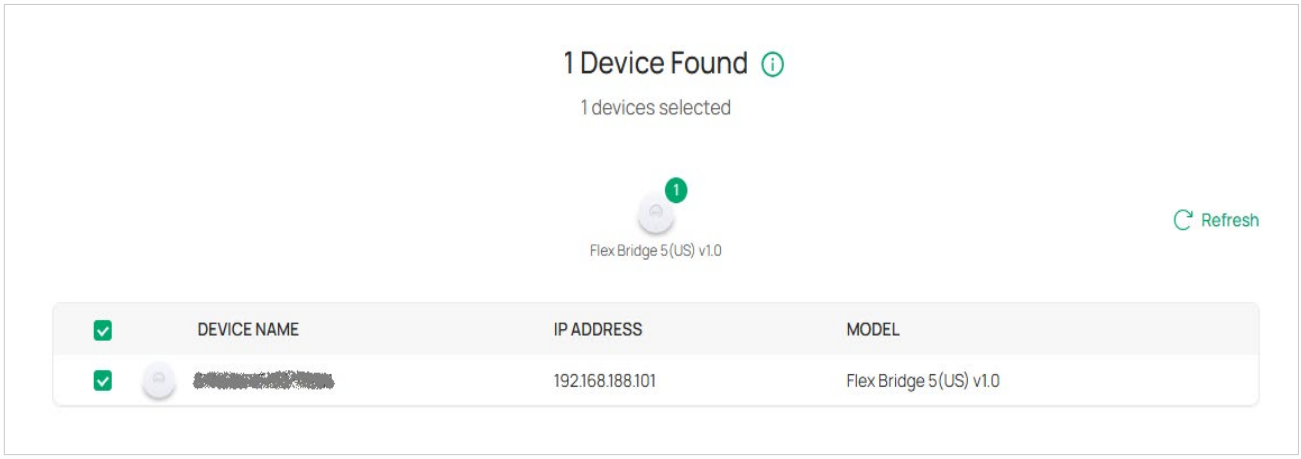
4. Once the Fusion Gateway successfully connects to the network, you are able to click Speed Test to measure your internet speed here.
5. To enable Omada Cloud Management and unlock more features, it is recommended to bind the Fusion Gateway to your TP-Link ID.



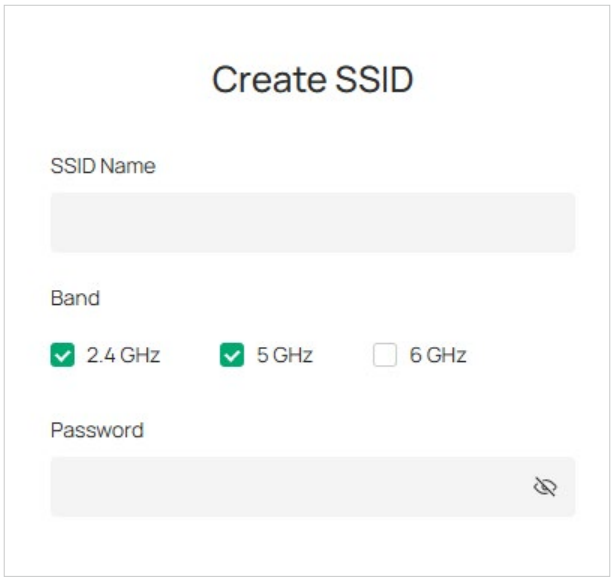
6. Next, name your Fusion Gateway and select the country/region and time zone. Read and agree to the Terms of Use. Click Next



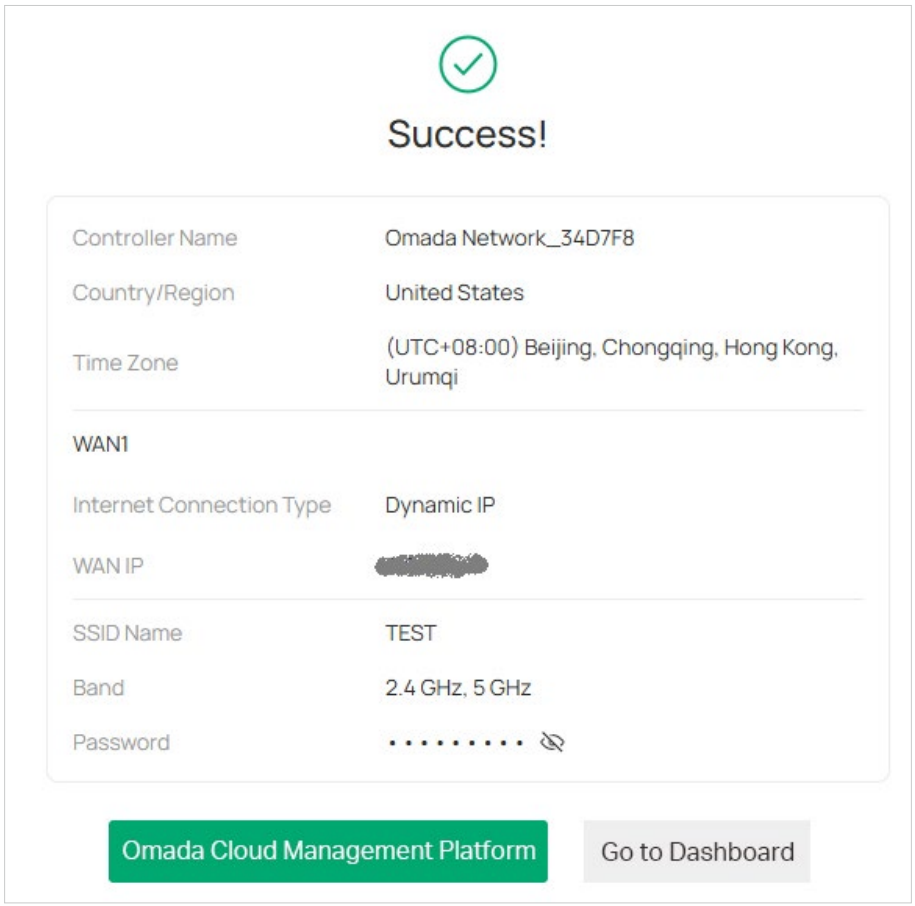
7. If you have already connected other Omada switches or wireless access points in factory mode to the Fusion gateway, you will be able to find and add them here. If not, click Skip, and you can adopt devices by referring to Adopt Devices after the setup wizard is complete.



8. If you have added one or more Omada wireless access points, you can create an SSID that uses a simple password.



9. Done. You can review the configuration summary. Click Go to Dashboard to configure more settings as needed. If you sign in with a TP-Link ID, you will see the Omada Cloud Management Platform button and you can click it to go to the cloud portal to configure and manage the device.

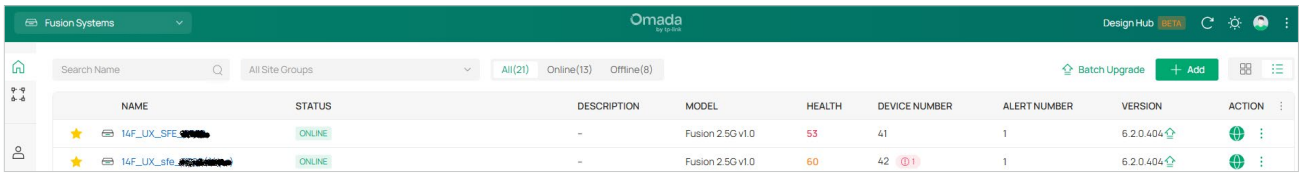


2. 3 Access Fusion Gateway via Cloud Portal

You can access and manage your Omada devices via Omada cloud portal remotely.

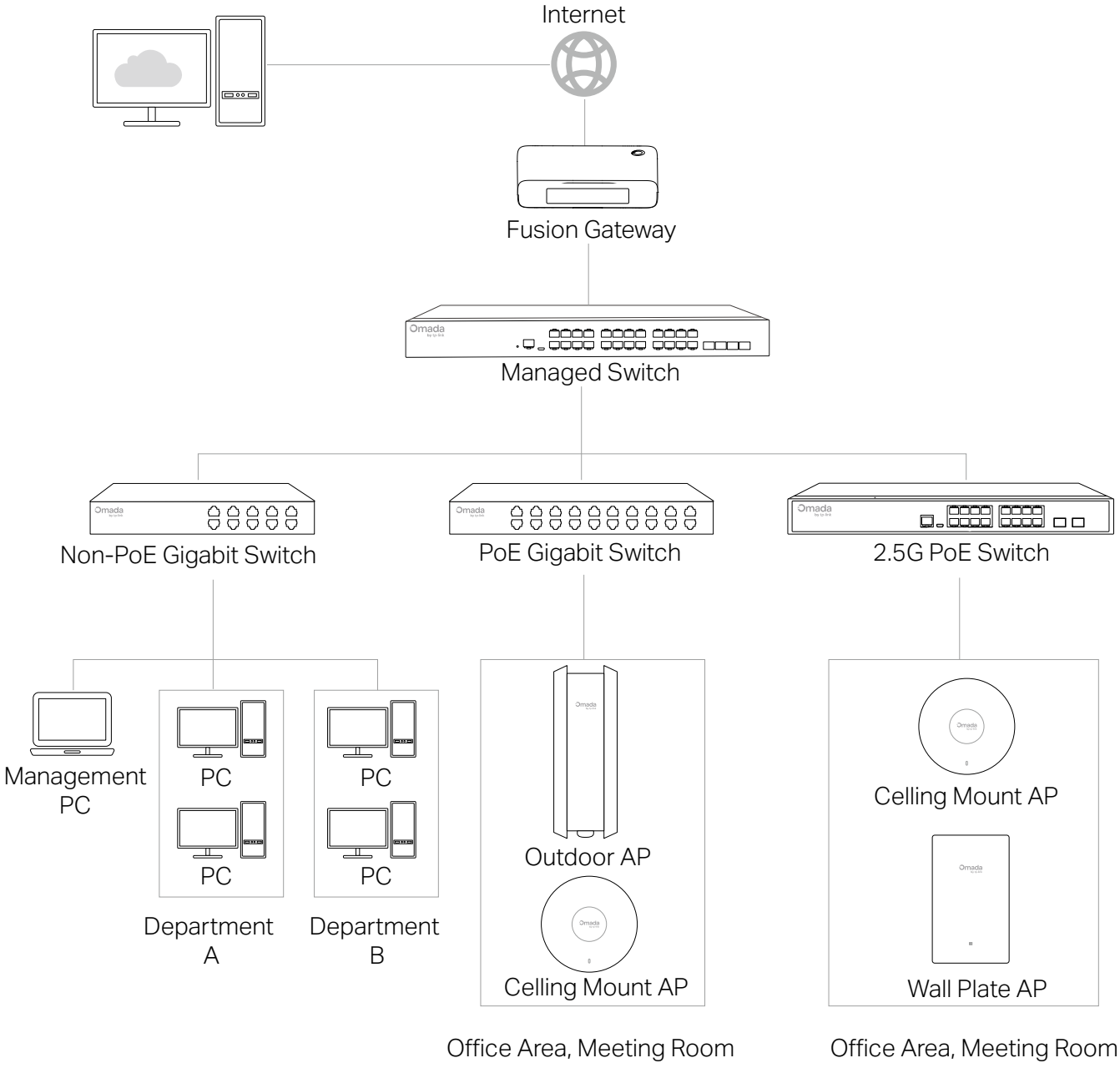
To access the Fusion gateway via cloud portal, follow the steps below:

1. Enable Cloud Access on the Settings page on the gateway and bind a TP-Link ID to your gateway. If you have configured this in the setup wizard, skip the step.
2. Launch a web browser and enter https://omada.tplinkcloud.com in the address bar.
3. Enter your TP-Link ID and password to log in. A list of Fusion gateways that have been bound with your TP-Link ID will appear in the Fusion Systems page. Then you can launch your device to further configure the gateway.

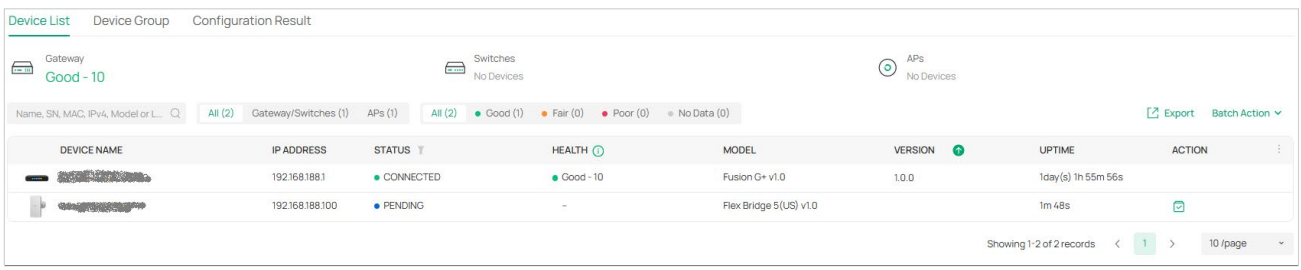


2. 4 Adopt Devices

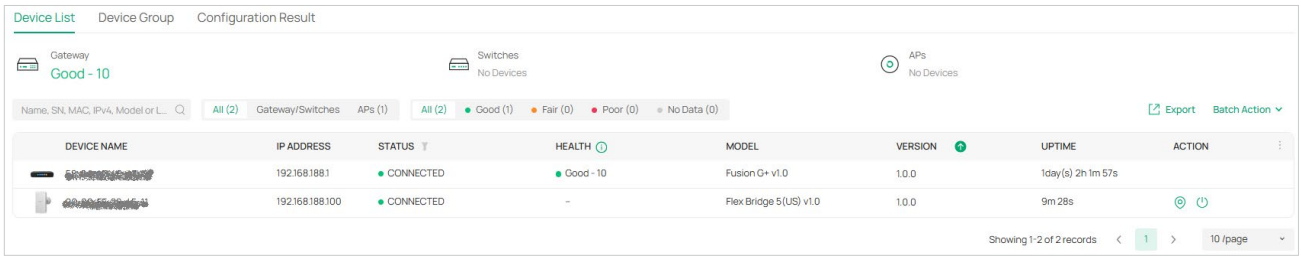
Connect your Omada switches or wireless access points in factory mode to the same network as the Fusion gateway, you will be able to find and add them in the Device List.



1. Go to Devices > Device List, all connected Omada devices (in factory mode) in the same network will display.



2. Select a device and click Adopt and wait until the device's STATUS changes from Pending to CONNECTED.



For more information about STATUS, refer to Manage Network Devices.

2. 5 Navigate the UI

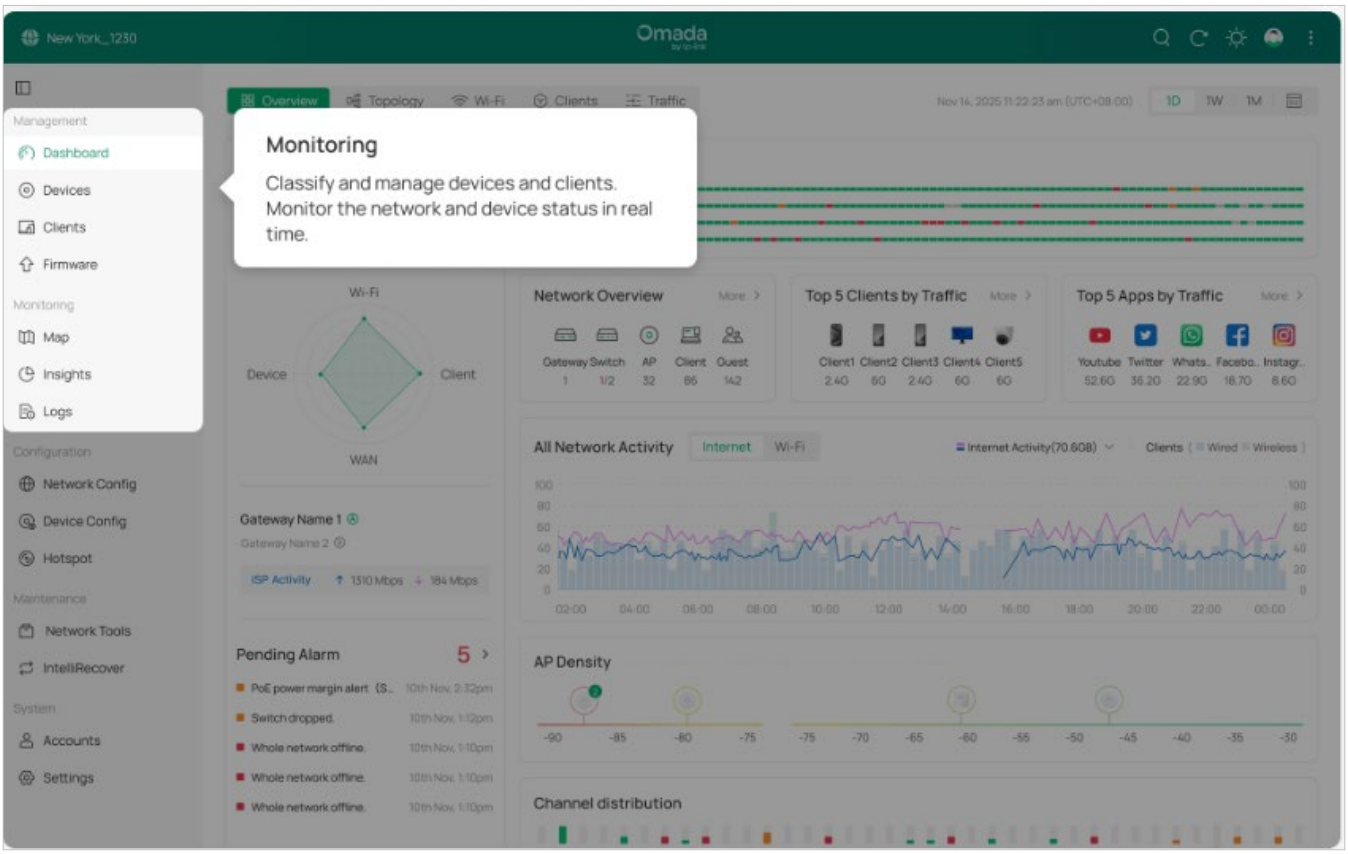
As you start using the management interface of the Fusion gateway (Controller) to configure and monitor your network, it is helpful to familiarize yourself with the Controller UI.

Note: Features available in the Omada Fusion gateway may vary due to your region, controller type and version, and device model.

Know your network status at a glance, gain insights, and manage devices all from the Omada platform. Visualized data brings key information onto a single screen, helping you quickly understand your network conditions and business trends.

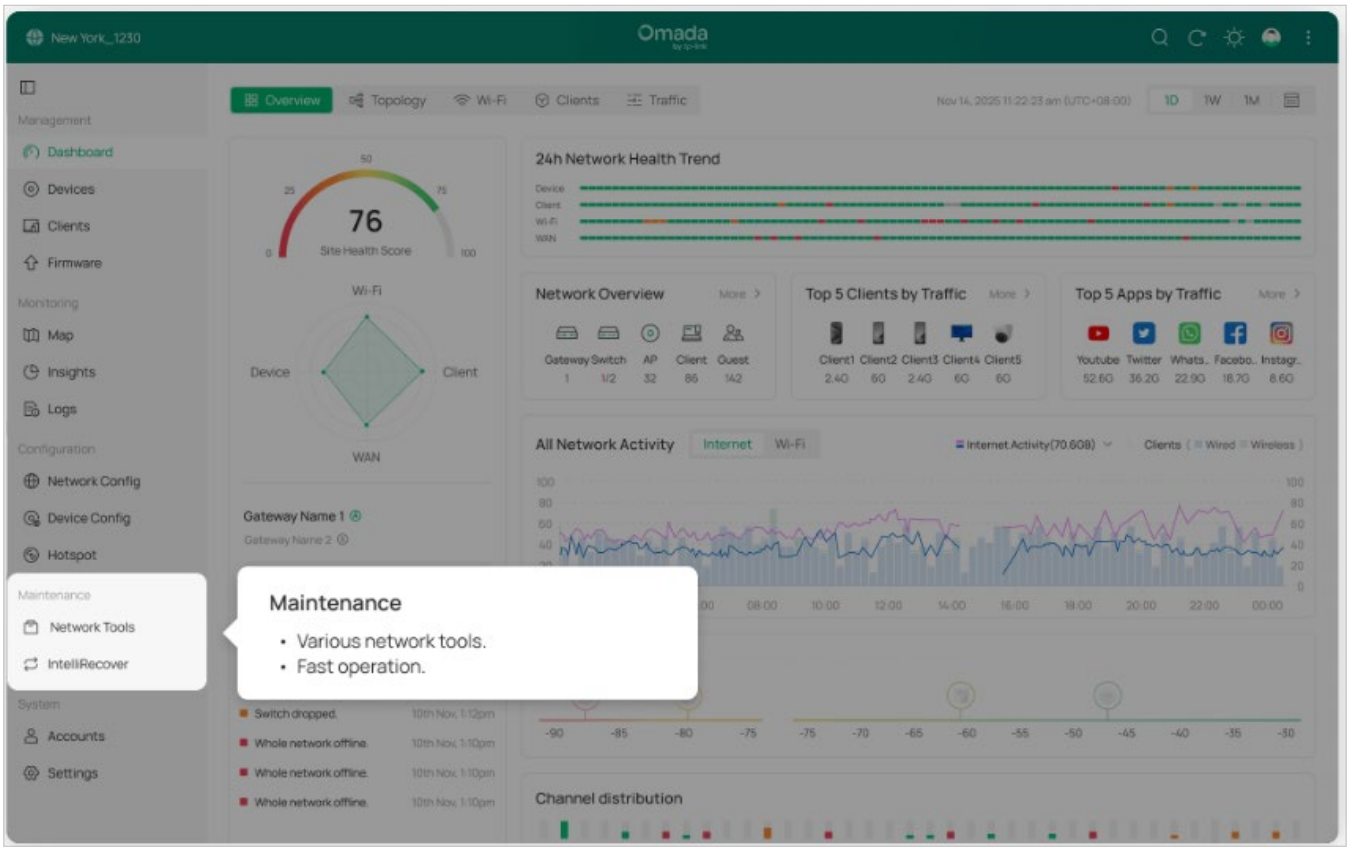
- **Management & Monitoring**

  Network administrators can monitor the status of all network devices and clients in real time. The system provides detailed connection statuses, data usage, and alert logs, ensuring the stability and security of network operations.



- **Maintenance**

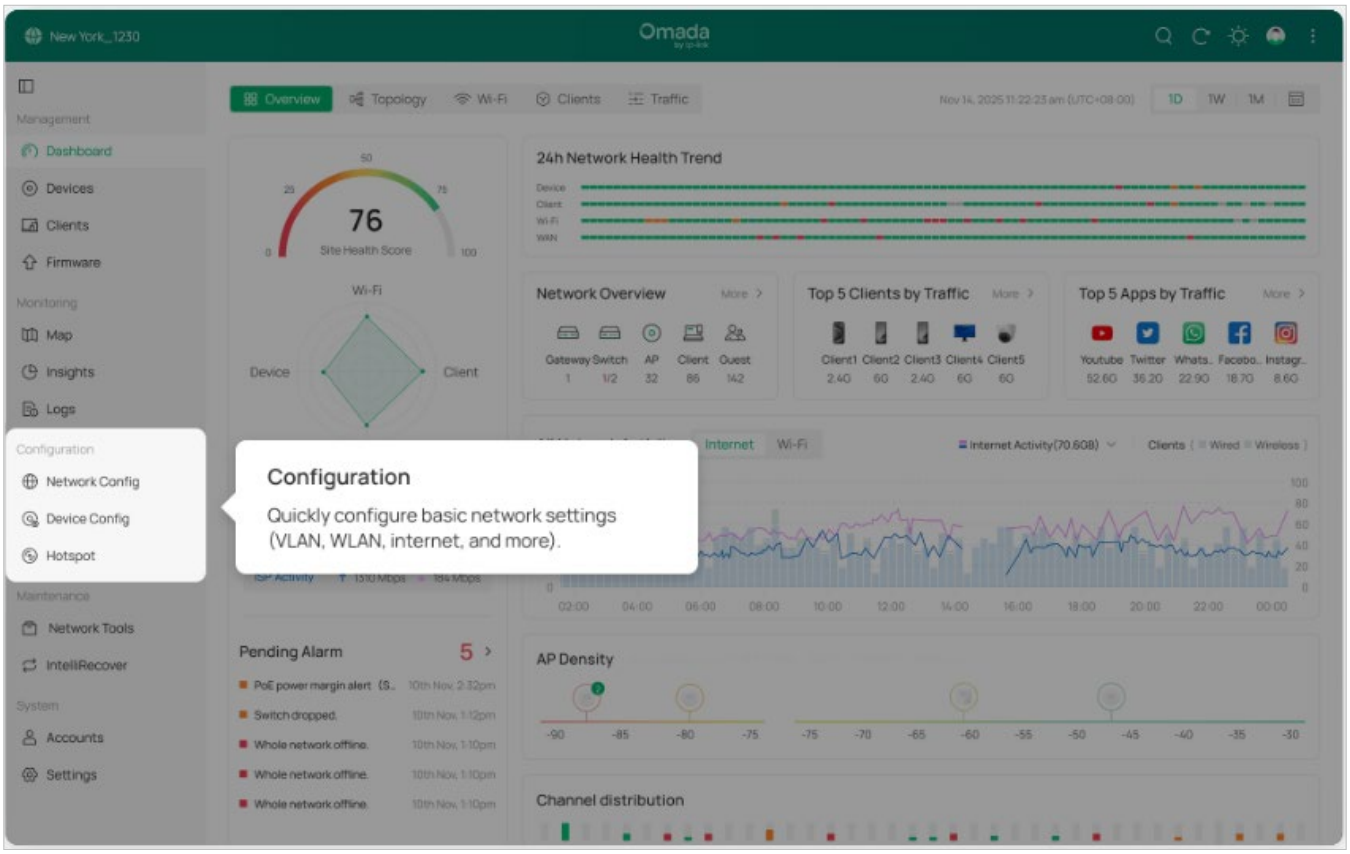
  Provides various network tools for you to test the device connectivity, capture packets for troubleshooting, open Terminal to execute CLI or Shell commands, and perform cable tests.



- **Configuration**

  Set up and manage network, device, and authentication configurations for the optimal overall network performance.

  - **Network Config** — Manage and optimize network configurations to ensure efficient and secure network connections.
  - **Device Config** — Centrally set up and manage device configurations by device type, improving device performance and stability.



- **System**

  Manage the accounts and configure the Fusion gateway's general settings.

The Controller UI is grouped into task-oriented menus. These menus are located in 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.

- **Elements in top right corner**

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

Global Search Feature	Click the Search icon 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.
Refresh Page	Click the Refresh icon to refresh the page.
Theme Settings	Change theme settings to light mode, dark mode, or system theme to improve your overall screen experience.
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 the More icon for more settings. **Feedback**: Click to send your feedback to us. **About**: Click to display the controller info. **Tutorial**: Click to view the quick Getting Started guide which demonstrates the navigation and tools available for the controller.

- **Navigation bar in the left**

  The left-hand navigation bar provides access to:

Dashboard	Displays a summarized view of the network status through different visualizations. The dashboard is a powerful tool that arms you with real-time data for monitoring the network.
Devices	Displays the devices 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 for device details and settings.
Firmware	Allows you to update the firmware of network devices in a one-time or periodic manner.
Clients	Displays a list view of wired and wireless clients, IPCs, and NVRs that are connected to the network. This list view can change depending on your monitoring need through customizing the columns. You can click any entry on the list for more detailed information and settings.
Map	Displays the geographic locations of devices in Device Map. You can also upload images of your location for a visual representation of your network in Heat Map.
Insights	Displays the statistics of various network indicators and their changes over time in Reports and detailed traffic information in Application Analytics.
Logs	Records the activities of the system, devices, users and administrators. 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.
Network Config	Allows you to manage and optimize network configurations to ensure efficient and secure network connections.
Device Config	Allows you to centrally set up and manage device configurations by device type, improving device performance and stability.
Hotspot	Allows you to centrally monitor and manage the clients authorized by portal authentication.
Network Tools	Provides various network tools for you to test the device connectivity, capture packets for troubleshooting, open Terminal to execute CLI or Shell commands, and perform cable tests.
IntelliRecover	Allows you to monitor the status of PoE devices, automatically repairing abnormal devices.
Accounts	Create and manage user accounts for controller access.
Settings	Configure the Fusion gateway's general settings.

Chapter 3

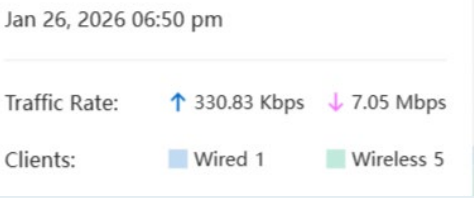
Dashboard

This chapter introduces Dashboard, which is designed for a quick real-time monitor of the network. This chapter includes the following sections:

3. 1 Overview

The Overview page provides a high-level summary of network health, client traffic, and hardware status. Use this dashboard to monitor real-time performance and identify potential bottlenecks at a glance.

■ Interactive Elements & Navigation

Element	Function
	Switch between Overview, Topology, Wi-Fi, Clients, and Traffic views.
	Filter data by 1D (Day), 1W (Week), or 1M (Month).
	Select More > on widgets like Network Overview or Top 5 Clients to view detailed lists.
	Hover over data points in the Activity graph to view specific traffic rates and client counts at a precise timestamp.
	Click the (i) icon (e.g., next to 24h Network Health Trend) to view the calculation logic for that metric.

■ Monitoring Health

To assess the current state of your network, follow these steps:

1. Check the Health Score: Locate the semicircular gauge on the left. A score of 100 indicates optimal performance across Wi-Fi, Device, WAN, and Client categories.
2. Review the 24h Network Health Trend: Scan the green grid. Each block represents a time interval; look for color shifts (e.g., yellow or red) which indicate historical outages or performance dips.
3. Test WAN Port Speed: Run a speed test on a single WAN port and the results will be available in a few seconds. You can also view historical speed test results.
4. Analyze Traffic Spikes: Observe the Activity chart. Compare the blue shaded area (Internet Activity) against the purple line (Clients) to see if high traffic correlates with specific user surges.
5. Identify High-Bandwidth Users: Consult the Top 5 Clients by Traffic and Top 5 Apps by Traffic cards to see which devices or applications (e.g., BitTorrent, NetEase) are consuming the most resources.
6. Evaluate Radio Environment: Scroll to AP Density and Channel Utilization to ensure your access points are operating on clear channels with minimal interference.

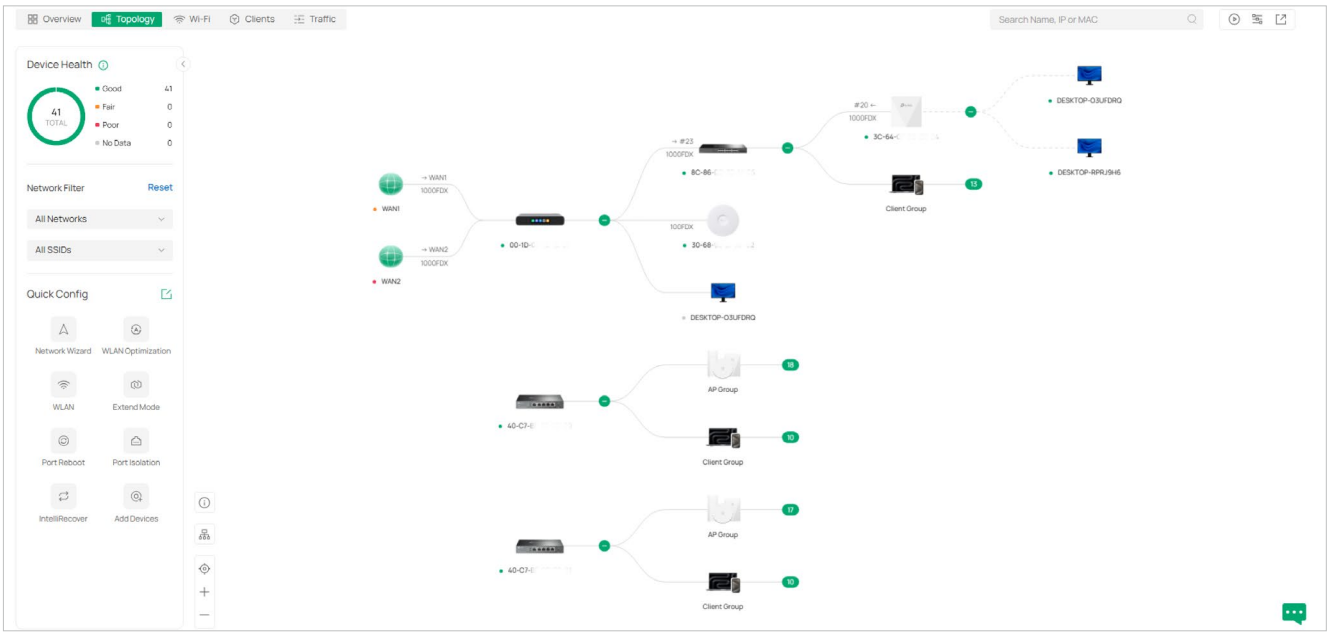
Note:

- You can quickly identify hardware failures in the Network Overview widget. If a device count (e.g., AP or Switch) appears lower than your known inventory, click the icon to jump directly to the device management page for troubleshooting.
- The ISP Activity metrics on the left sidebar show real-time throughput. If the Load Balancing Weight is set to 1:1, the controller is distributing traffic equally across multiple WAN ports.

- The dashboard automatically preserves your workspace preferences, including chart filter selections and table pagination settings. These core configurations persist after you leave the page, ensuring that your previous edits are automatically reloaded upon your next visit to eliminate repetitive setup.

3. 2 Topology

The Topology page provides a real-time map of your network's physical and logical connections. Use this view to visualize device relationships, monitor port speeds, and identify configuration redundancies like MLAG or VRRP.



In the diagram, you can:

- Use the (+) or (-) icons on connection branches to expand or collapse sub-trees.
- Click the icon of the client group to view clients connected to the same device.
- Click any device or client icon to open its Overview window for granular monitoring and configuration.
- Hover your cursor over any device icon to reveal a quick-view summary of its status and hardware information.

In the lower left:

Adjust the size of the topology, change the horizontal/vertical orientation of the topology, and view the legends.

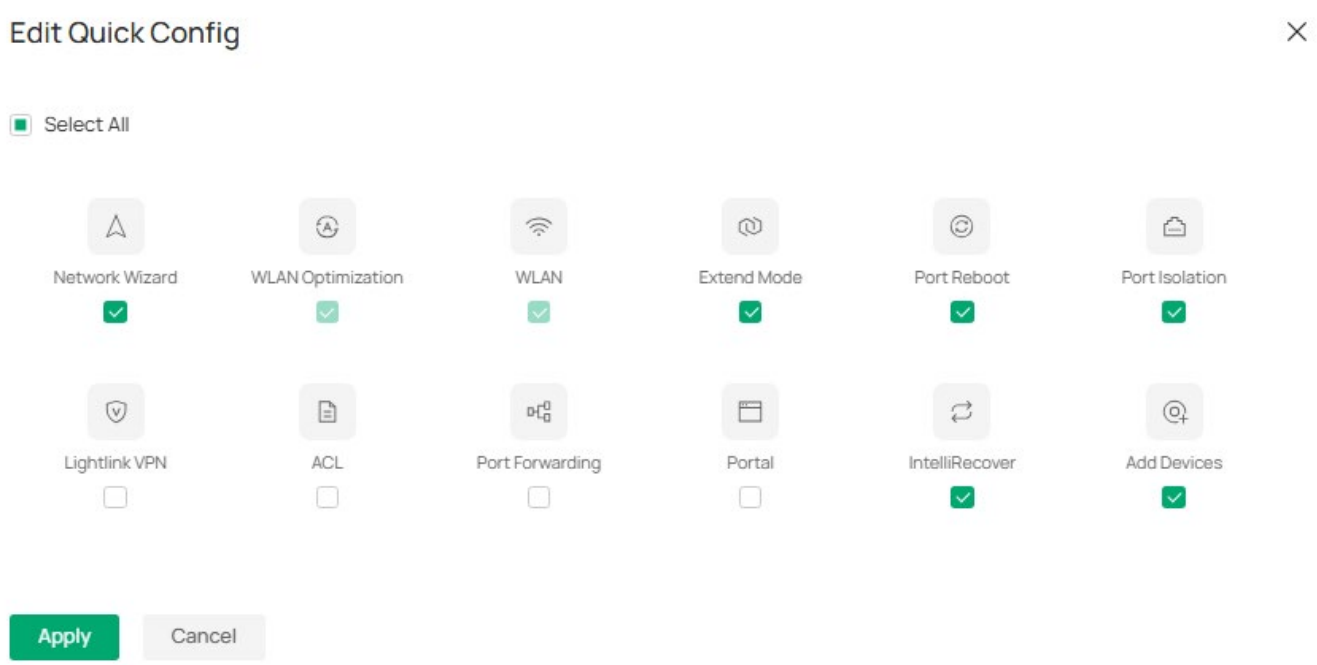
In the upper right:

- When Traffic ( ) is enabled, the map displays the communication rate between devices. If using a third-party gateway, manually select your root node to ensure correct connectivity logic.
- Use the Network Filter ( ) in the left panel to isolate specific LAN or wireless networks (SSIDs) within the visual map.

The left-side panel of the Topology page provides the device statistics chart, Network Filter, and Quick Config.

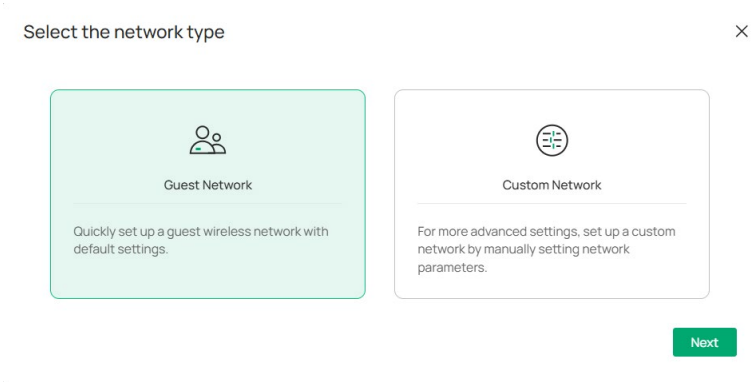
In Network Filter, you can filter the LAN and wireless network to display.

In Quick Config, you can click a configuration icon to quickly configure your network. To customize this section, you can click the edit icon and select the configuration icons to display.



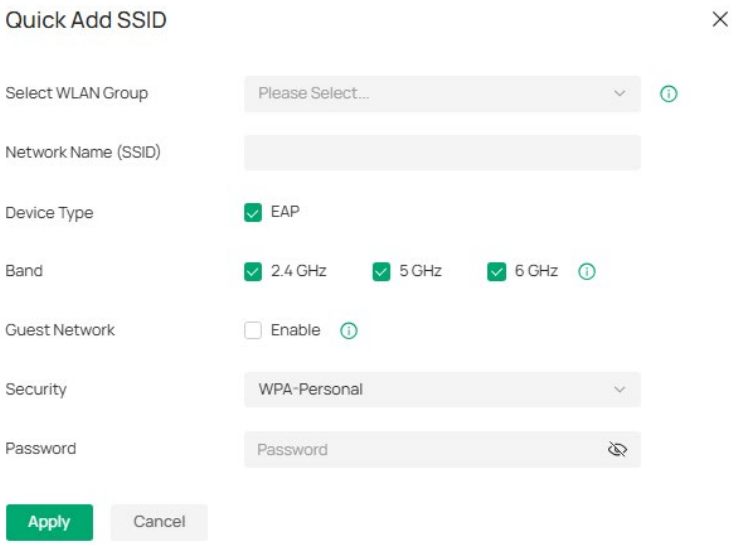
- Network Wizard

In Network Wizard, you can quickly set up a guest wireless network with default settings or a custom network by manually setting network parameters.



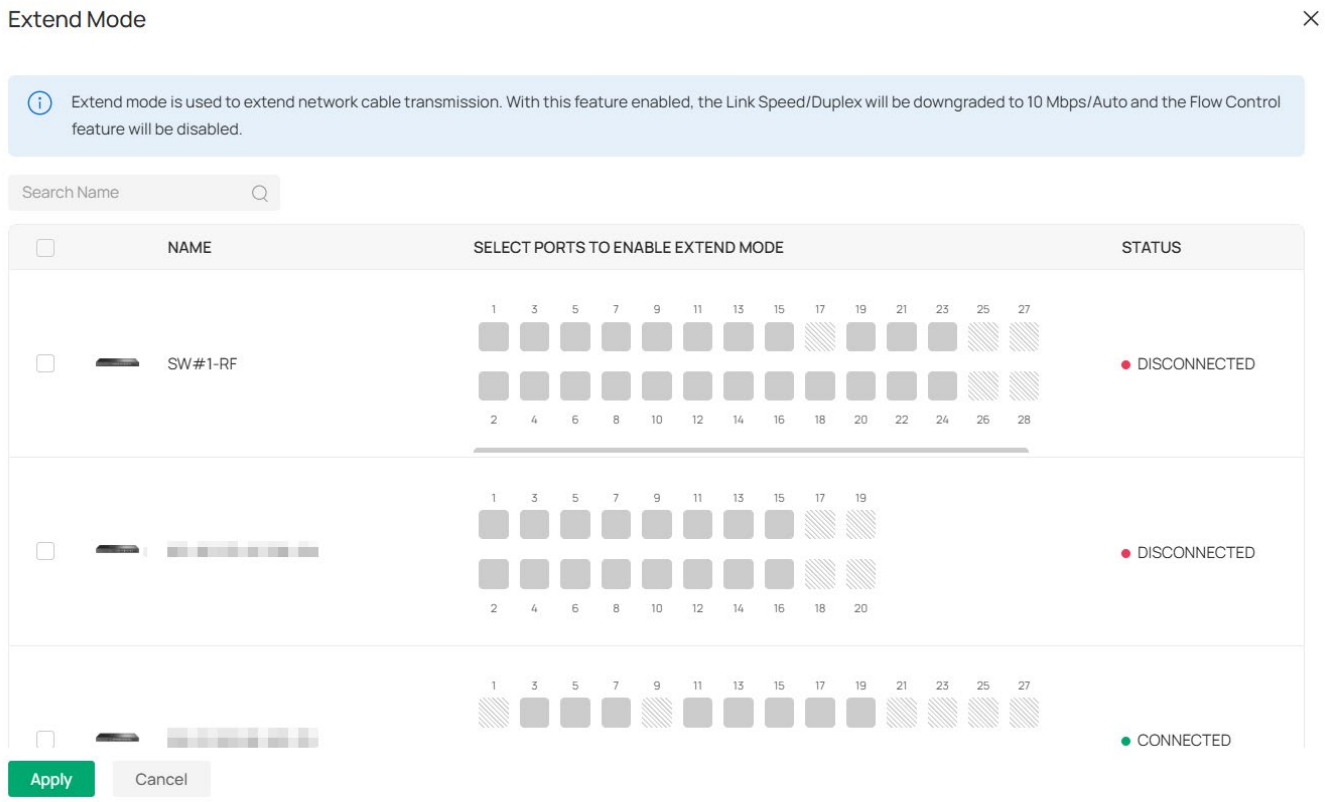
- WLAN

In WLAN, you can quickly create an SSID and set up a basic wireless network.



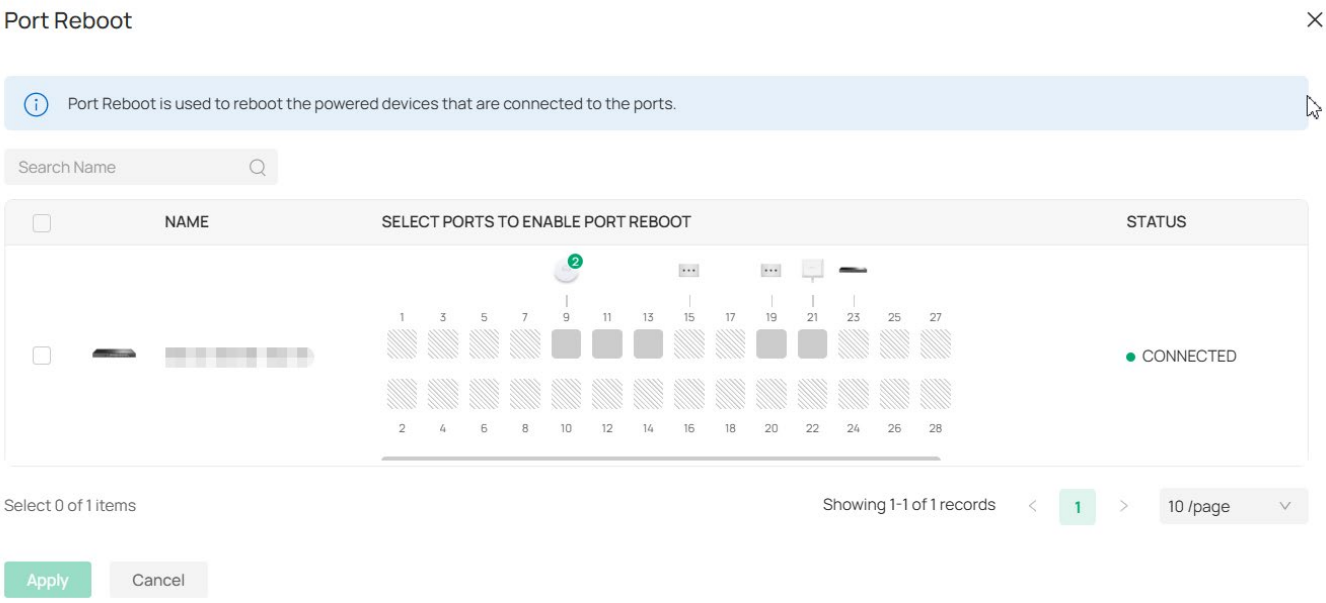
- Extend Mode

In Extend Mode, you can quickly extend network cable transmission for switch ports. With this feature enabled, the Link Speed/Duplex will be downgraded to 10 Mbps/Auto and the Flow Control feature will be disabled.



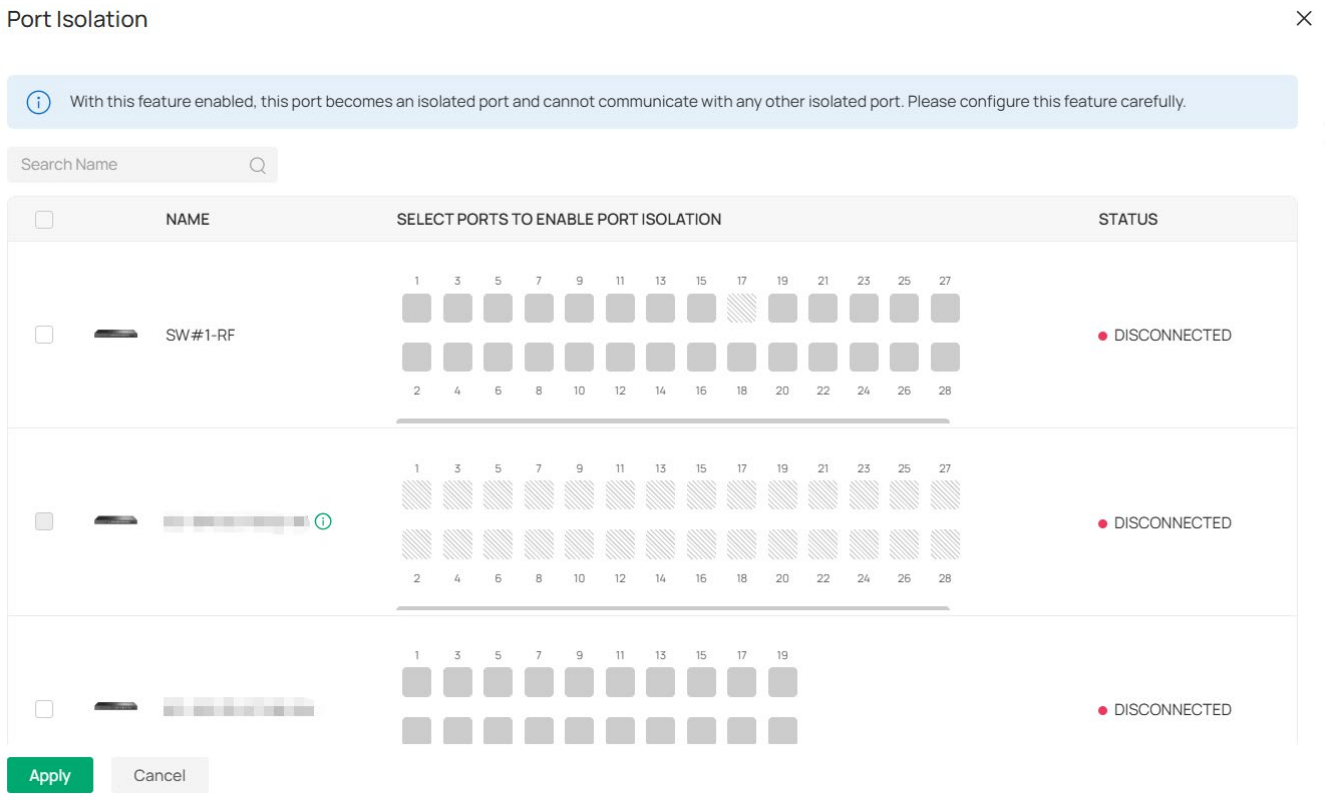
■ Port Reboot

In Port Reboot, you can quickly reboot the powered devices that are connected to the switch ports.



■ Port Isolation

In Port Isolation, you can quickly isolate the selected ports so that the ports cannot communicate with any other isolated port.

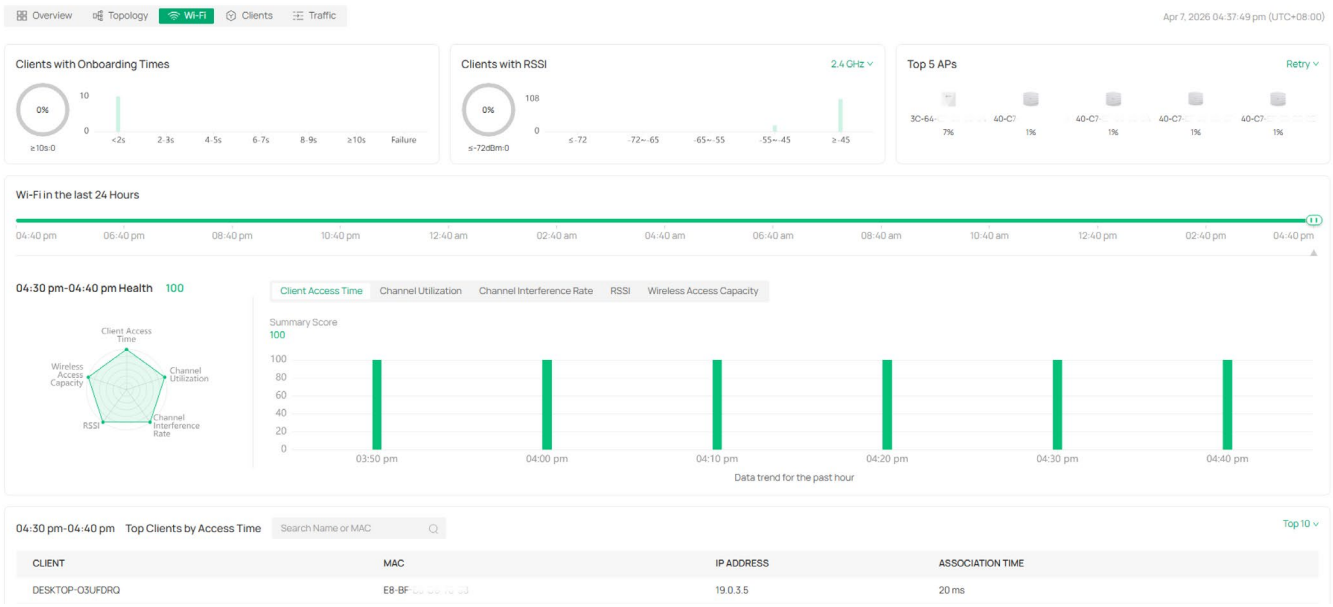


- Others

Other Quick Config functions, including WLAN Optimization, VPN, ACL, Port Forwarding, Portal, and IntelliRecover, will guide you to the configuration page. Refer to the corresponding chapter in this manual for detailed guidance.

3. 3 Wi-Fi

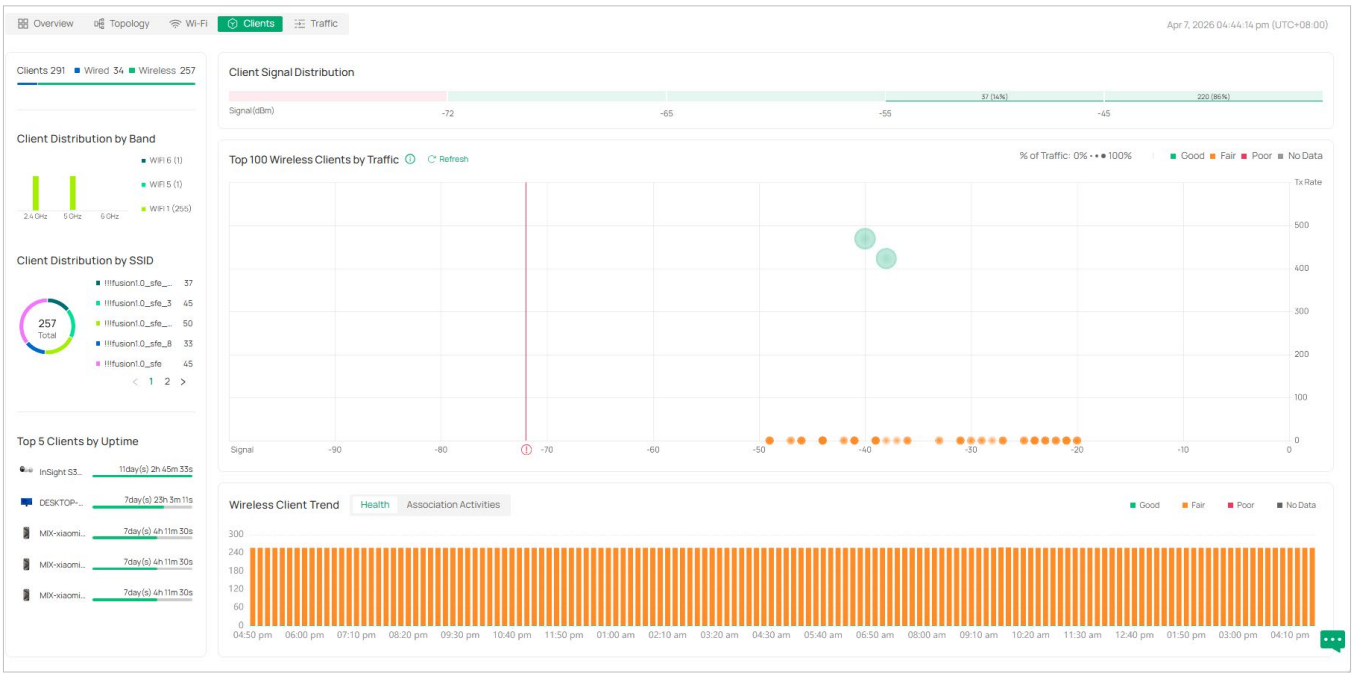
The Wi-Fi page offers a specialized overview of the wireless environment, highlighting connection efficiency, signal strength distribution, and radio resource management.



Widget	Function
Clients with onboarding times	Tracks how long wireless clients take to connect. Metrics are categorized from <2s to ≥10s or Failure.
Clients with RSSI	Displays the distribution of signal strength across the network. Filterable by frequency band (2.4GHz, 5GHz, or 6GHz).
Top 5 APs	Identifies the most active Access Points based on client load or traffic percentage.
Wi-Fi in the last 24 Hours	A chronological health timeline. Use the playback/pause controls to review performance at specific time intervals.

3. 4 Clients

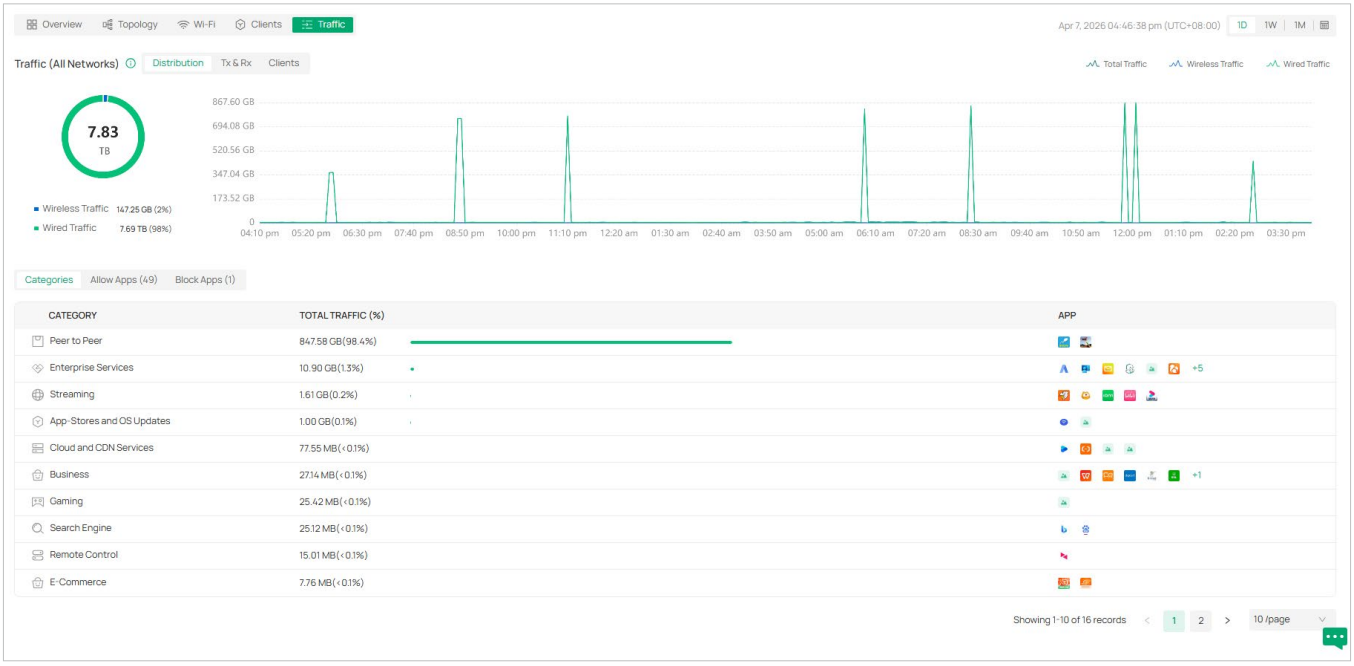
The Clients dashboard provides a comprehensive view of all devices connected to the network. Use this page to monitor client health, track signal distribution, and identify high-bandwidth users across both wired and wireless segments.



Element	Function
Clients Summary	Displays the total number of active clients, with a breakdown of Wired vs. Wireless connections.
Top 5 Clients by Uptime	Lists devices with the longest continuous connection to the network.
Wireless Client Trend	Switches the historical view between Health status and Association Activities.
Distribution	View visualizations for Client Distribution by Band and Client Distribution by SSID.

3. 5 Traffic

The Traffic page provides a deep-dive analysis of network usage, categorized by application type, client device, and connection medium. Use this dashboard to identify bandwidth-heavy applications and monitor data distribution between wired and wireless networks.



Element	Function
Primary Metric Tabs	Switch between Distribution, Tx&Rx, and Clients views to change the primary graph's data focus.
App Control Tabs	Access Allow Apps and Block Apps lists to manage application-specific network permissions.
Pagination Control	Navigate through multiple pages of records or change the rows displayed per page.

Chapter 4

Manage Network Devices

This chapter guides you on how to configure and monitor network devices via the Fusion gateway, including the gateway, switches, and APs. You can configure the devices individually or in batches to modify device configurations. The chapter includes the following sections:

4. 1 Manage the Device List

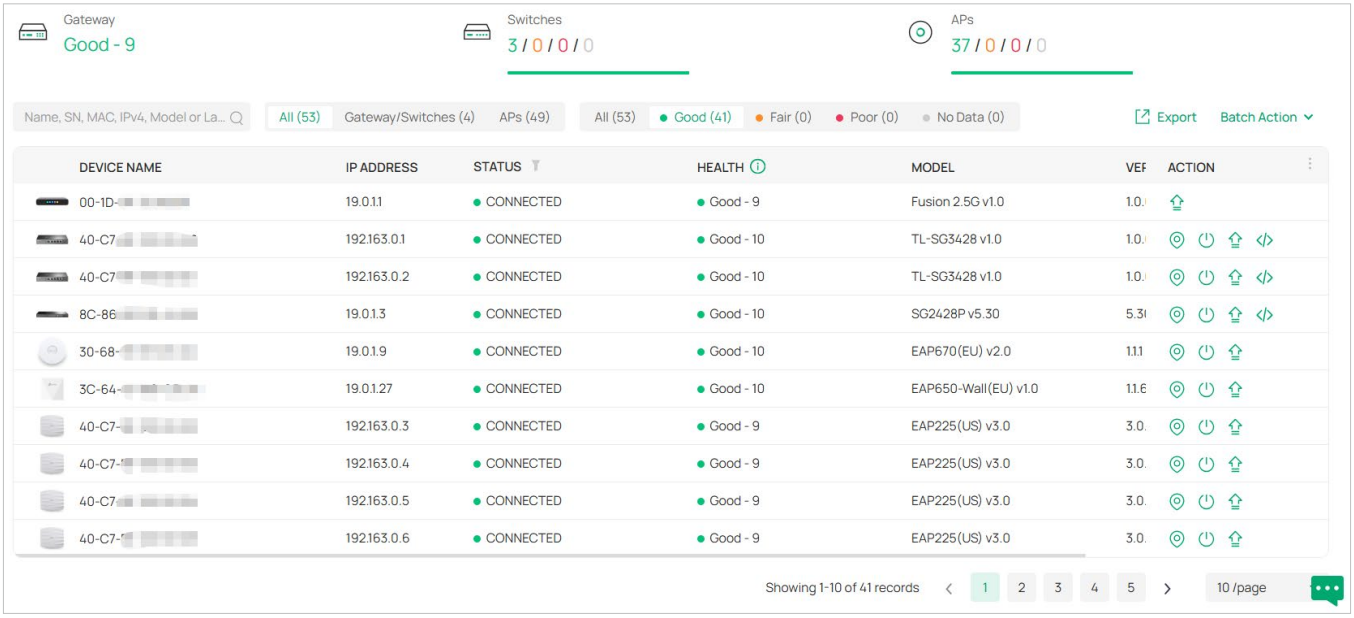
Overview

The Fusion gateway provides 100% centralized management of Omada network devices, including the gateway, switches, and APs.

To manage network devices, go to Devices > Device List.

You can manage the network devices in the list and manage each device in its Properties window and Device Management window.

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



Device Overview

On the top of the device list, get an overview of the types, quantity, and health scores of managed devices. Hover over a device type to view health statistics.

Monitor Device Health

The Health column displays the health scores of devices, indicating how well they are performing.

Good (8 - 10)	The device is operating at or near its optimal performance.
Fair (4 - 7)	The device is functional.
Poor (1 - 3)	The device may have encountered some issues.
No data	No data has been obtained.

Monitor Connection Status

The Status column explains the connection status of devices.

PENDING	The device is in Standalone Mode or with factory settings, and has not been adopted by the controller. To adopt the device, click the Adopt icon in the Action column, and the controller will use the default username and password to adopt it. When adopting, its status will change from Adopting, Provisioning, Configuring, to Connected eventually.
ISOLATED	(For APs in the mesh network) The AP once managed by the controller via a wireless connection now cannot reach the gateway. You can rebuild the mesh network by connecting it to a wireless device in the Connected status, then the isolated AP will turn into a connected one.
CONNECTED	The device has been adopted by the controller and you can manage it centrally. A connected device will turn into a pending one after you forget it.
MANAGED BY OTHERS	The device has already been managed by another controller. You can reset the device or provide the username and password to unbind it from another controller and adopt it in the current controller.
HEARTBEAT MISSED	A transition status between Connected and Disconnected. Once connected to the controller, the device will send inform packets to the controller in a regular interval to maintain the connection. If the controller does not receive its inform packets in 30 seconds, the device will turn into the Heartbeat Missed status. For a heartbeat-missed device, if the controller receives an inform packet from the device in 5 minutes, its status will become Connected again; otherwise, its status will become Disconnected.
DISCONNECTED	The connected device has lost connection with the controller for more than 5 minutes.
ADOPTED FAILED	The device has failed to be adopted.
	(For APs in the mesh network) When this icon appears with a status icon, it indicates the AP with mesh function and no wired connection is detected by the controller. You can connect it to an uplink AP through Mesh.
	When this icon appears with a status icon, it indicates the device in the Connected, Heartbeat Missed, Isolated, or Disconnected status is migrating. For more information, refer to the Migration section of this guide.

Customize the Column

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

To change the list order, click the upside-down triangle icon next to the column head, which indicates the ascending or descending order.

Filter the Devices

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

To search for devices, enter the text in the search box.

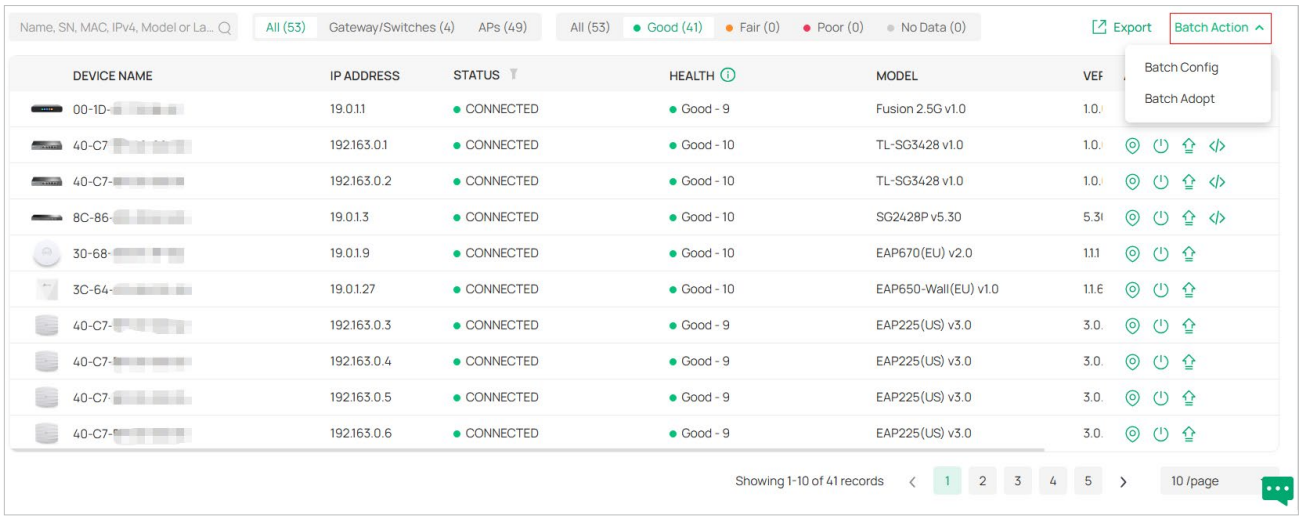
To filter the devices, a tab bar is above the table to filter the devices by device type. You can also filter the devices by their status by clicking the filter icon in the Status column.

Quick Operations

Click the icons in the table header or the Action column to quickly operate the device.

	Click to check if there is new firmware for the managed devices.
	(For pending devices) Click to adopt the device.
	(For connected APs and Switches) Click this icon and the device's LEDs and the peer switch port's LED will flash to indicate the device's location. The LEDs will keep flashing for 10 minutes, or you can click the  icon to stop the flashing.
	(For connected devices) Click to reboot the device.
	Click to upgrade the device's firmware version. This icon appears when the device has a new firmware version.
	Displays the current running configuration. Operators or Administrators or local user group members with execution rights for this command.
	(Only for the Main AP) Click to change the AP's role to a Client AP.

Batch Action



- **Batch Adopt**

  You can adopt devices in batches. Batch Adopt is available only for the devices in the Pending/Managed By Others state.

  To batch adopt devices, click Batch Action > Batch Adopt, select devices, and click Adopt. If the selected devices are all in the Pending state, the controller will adopt them with the default username and password. If not, enter the username and password manually to adopt the devices.

- **Batch Config**

  You can configure the same type of devices in batches. Batch Config is available only for the devices in Connected/Disconnected/Heartbeat Missed/Isolated state.

  To batch configure devices, click Batch Action > Batch Config, select devices, and click an action. You can batch configure device settings, perform custom upgrade, or forget them.

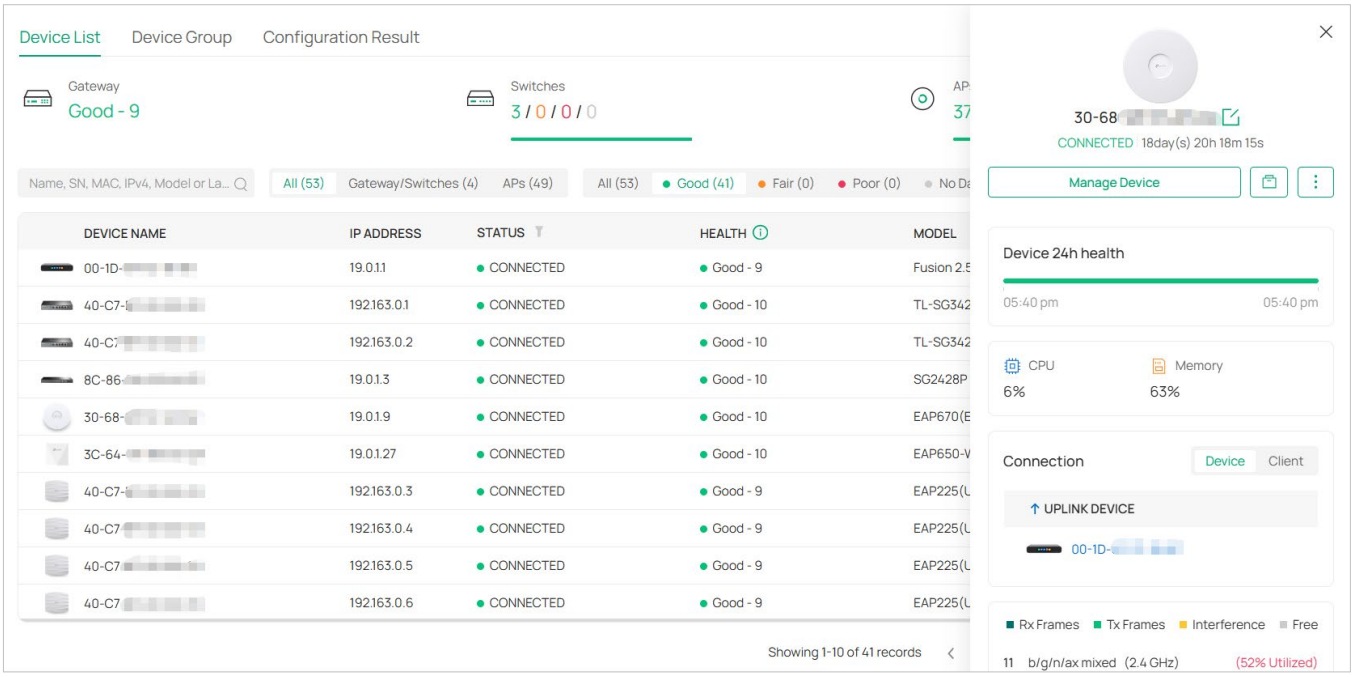
4. 2 Manage a Device

Go to Devices > Device List. In the device list, click a device, then you can monitor and manage it in the Properties window and Device Management window.

4. 2. 1 Properties Window

The Properties window displays the device's basic information, port status, health status, connection information, and more.

Note: The available functions in the window may vary by device type, model, and status.



Quick Operations

Click the ⋮ icon and choose an operation to quickly operate the device.

Note: The available functions may vary by device type, model, and status.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. After upgraded, the device will reboot and be readopted by the controller.
Copy Configuration	Select another device to copy its configurations. **Note:** Only devices of the same model as the current device will be displayed.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.
Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.

Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.
IntelliRecover	(Only for the AP directly connected to the PoE switch) Click to enable the IntelliRecover function for the device so that it can be added to the IntelliRecover monitoring list. IntelliRecover can help you monitor the status of PoE devices, automatically repairing abnormal devices.

Network Tools

Click the  icon and choose a network tool to analyze the network.

Note: The available tools may vary by device type, model, and status.

Network Check	Test the device connectivity via ping or traceroute.
Terminal	Open Terminal to execute CLI or Shell commands.
Cable Test	Perform cable test to check cable issues.
Packet Capture	Capture packets for network troubleshooting.
Link Speed Test	(Only for Bridge APs supporting link speed test and already form a bridge group) Click to test the link speed between the Main AP and Client AP.

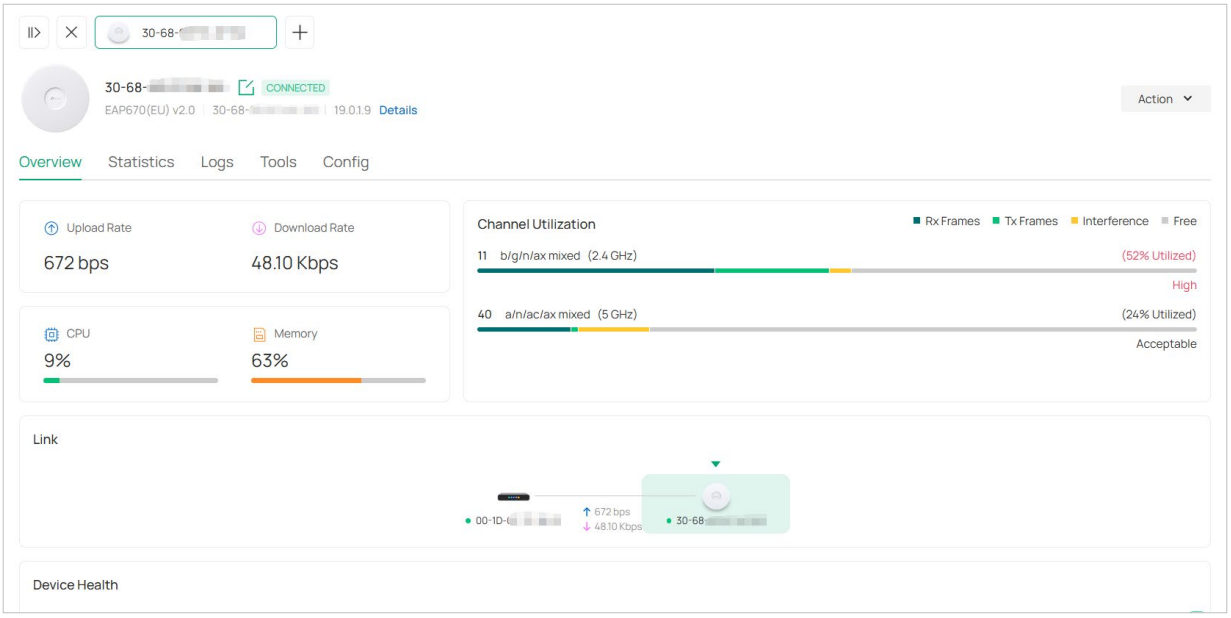
4. 2. 2 Device Management Window

Click Manage Device to open the Device Management window to view more device details and change device settings.

In the management window, you can click + and select one or more devices to open new management windows, click the icon in the top left to minimize the windows to the  icon in the right side, and click the  icon to reopen the minimized windows.

You can also click each tab to monitor and manage the device.

Note: The available tabs and configurations may vary by device type, model, and status.



For instructions about how to manage each type of devices via the Fusion gateway, refer to the relevant chapters:

- Manage the Gateway
- Manage Switches
- Manage APs

4. 3 Create and Manage Bridge Groups

4. 3. 1 Introduction to Bridge

Outdoor Bridge easily builds point-to-point and point-to-multi-point long range wireless connections. In practical application, it can help users to conveniently deploy APs over long range.

In a bridge system, the APs can be categorized mainly into two roles:

- Main AP

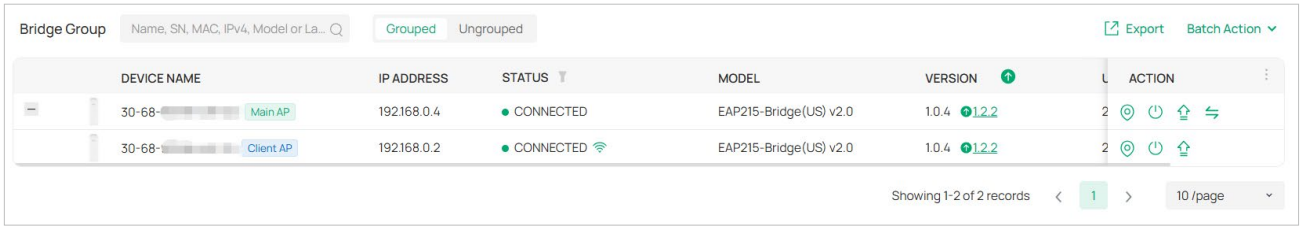
  The Main AP connects to your gateway for network access. A bridge system generally has only one Main AP.

- Client AP

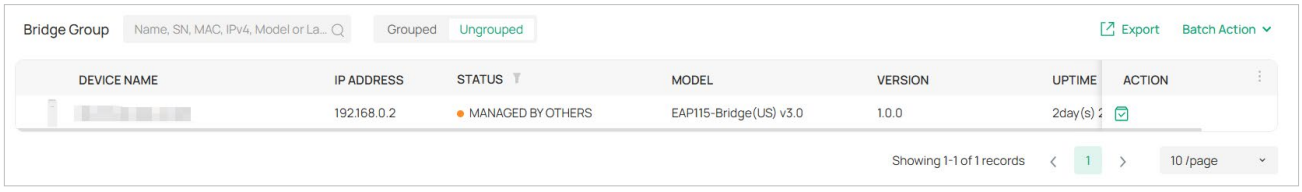
  Client APs connect to the Main AP via wireless bridge. A bridge system may have one or several Client APs.

4. 3. 2 Create a Bridge Group

1. Obtain bridge APs and set up a bridge network by referring to the relevant AP Installation Guide.
2. Go to Devices > Device Group > Bridge Group. The controller will detect the bridge APs and show them in the Grouped list.

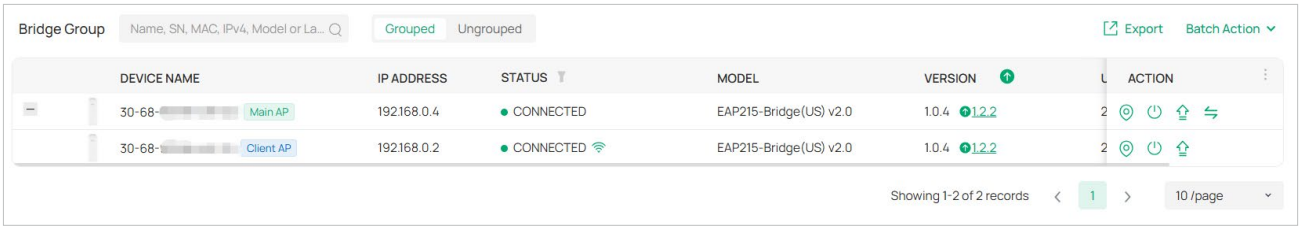


If you have ungrouped bridge APs, locate the AP in the Ungrouped list and click the Adopt icon to adopt it.



4. 3. 3 Configure and Monitor the Bridge Group

In the grouped bridge group list, you can configure and monitor the APs in the group.



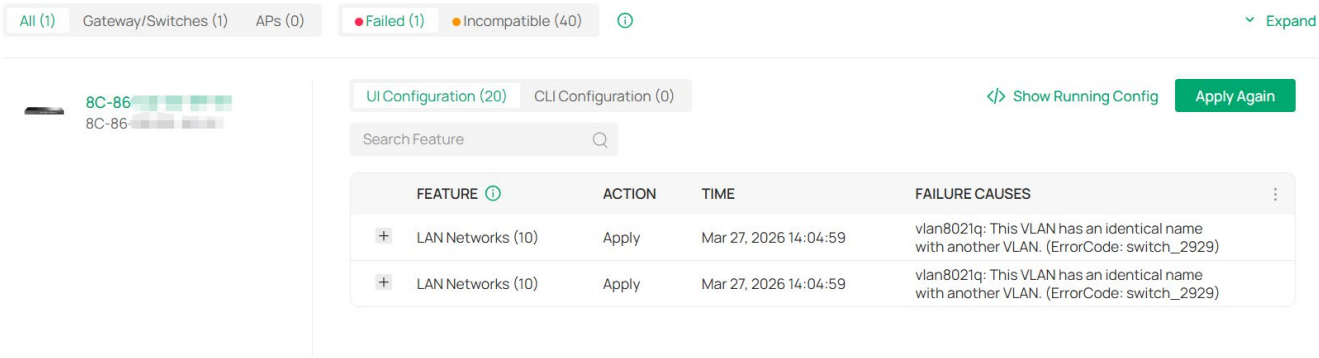
	(For connected APs) Click this icon and the device's LEDs and the peer switch port's LED will flash to indicate the device's location. The LEDs will keep flashing for 10 minutes, or you can click the icon to stop the flashing.
	(For connected devices) Click to reboot the device.
	Click to upgrade the device's firmware version. This icon appears when the device has a new firmware version.
	(Only for the Main AP) Click to change the AP's role to a Client AP.

Click the AP in the bridge group, then you can configure and monitor it in a similar way as configuring and monitoring a common AP. For details, refer to Manage APs.

4. 4 View the Configuration Result

The Configuration Result page displays abnormal configuration results for devices. If a device's configuration is entirely successful, it will not be displayed.

Go to Devices > Configuration Result.



You can switch tabs based on the device type (All Devices, Gateway/Switches, and APs) or configuration result (Failed and Incompatible).

- **Failed:** The configuration is not delivered. For the failure cause of device response timeout, force provision the configuration or restart the device. For other failure causes, check the failed configuration, correct and save it, then deliver it to the device. If the problem still exists, contact our technical support.
- **Incompatible:** The configuration is not supported by the current device's firmware.

You can click Expand on the right to search by Device Name and MAC Address.

Click on a device in the device list on the left to display its detailed configuration and failure causes. Click Show Running Config to display the running configuration.

Click Apply Again to apply the configuration again.

Chapter 5

Manage the Gateway

This chapter provides information for managing the Fusion gateway. The chapter includes the following sections:

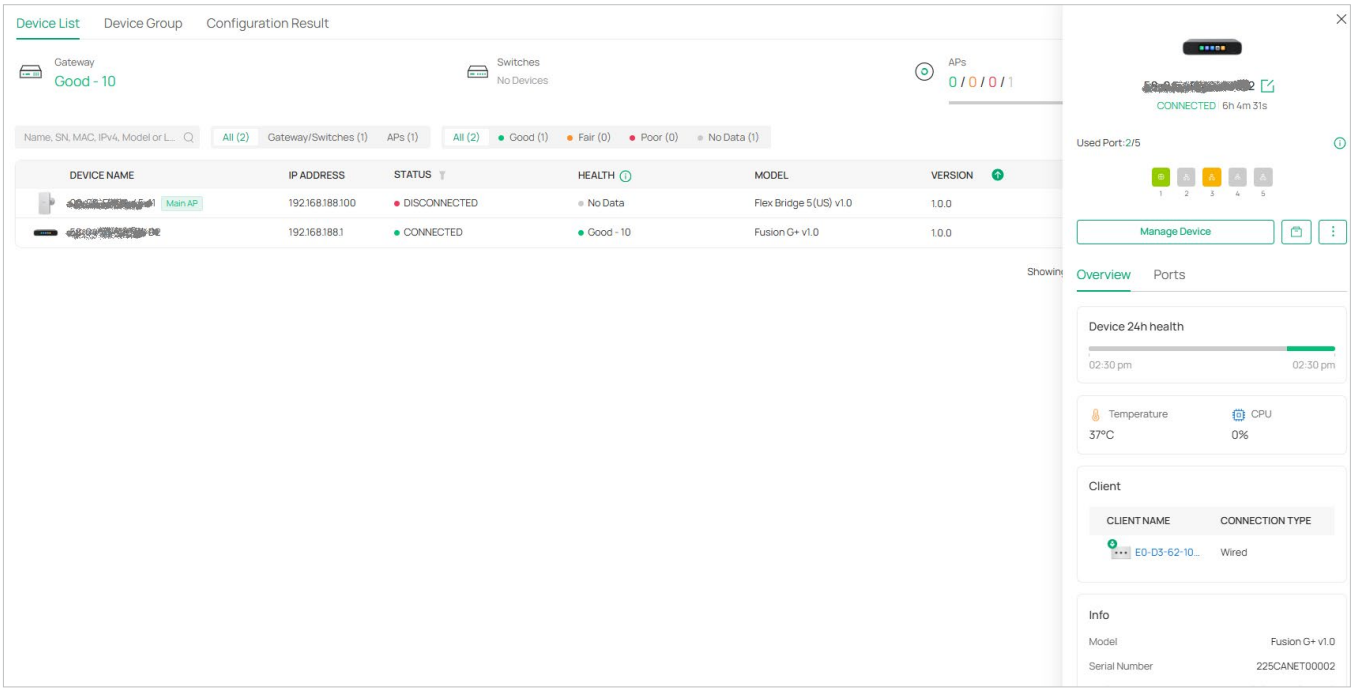
5. 1 Manage the Gateway

Go to Devices > Device List. In the device list, click the gateway, then you can monitor and manage it in the Properties window and Device Management window.

5. 1. 1 Properties Window

The Properties window displays the device's basic information, port status, health status, connection information, and more.

Note: The available functions in the window may vary by device type, model, and status.



Quick Operations

Click the ⋮ icon and choose an operation to quickly operate the device.

Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.
Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.

Network Tools

Click the icon and choose a network tool to analyze the network.

Network Check	Test the device connectivity via ping or traceroute.

Packet Capture	Capture packets for network troubleshooting.
Terminal	Open Terminal to execute CLI or Shell commands.

5. 1. 2 Device Management Window

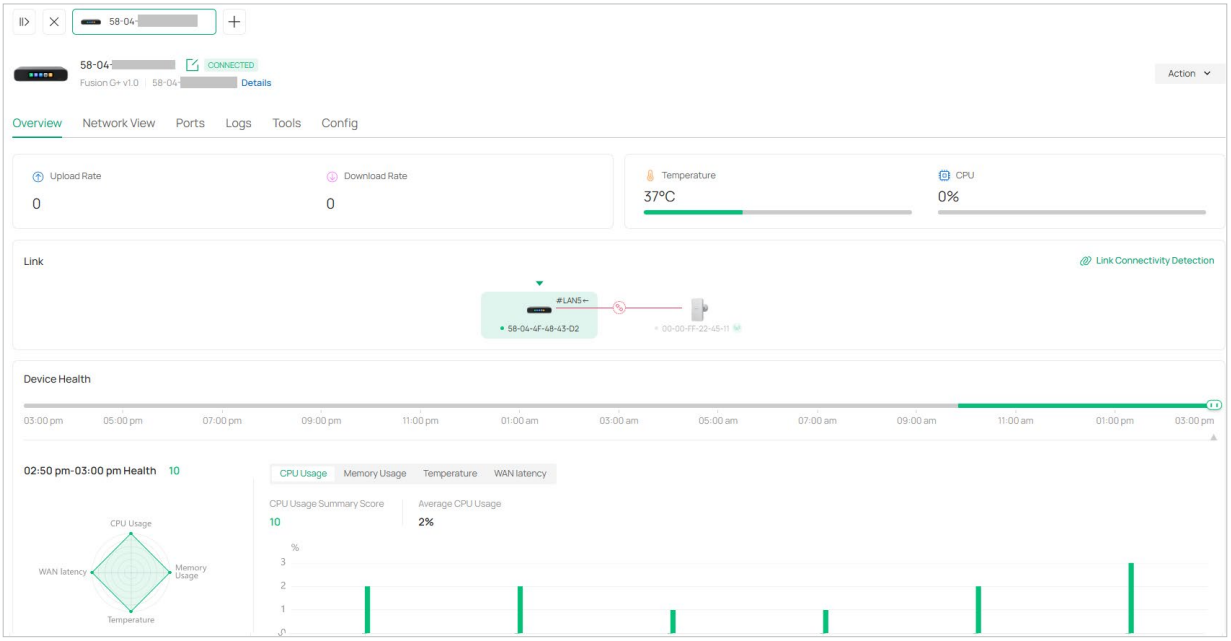
Click Manage Device to open the Device Management window to view more device details and change device settings.

In the management window, you can click + and select one or more devices to open new management windows, click the icon in the top left to minimize the windows to the icon in the right side, and click the icon to reopen the minimized windows.

You can also click each tab to monitor and manage the device. The tabs available may vary by model.

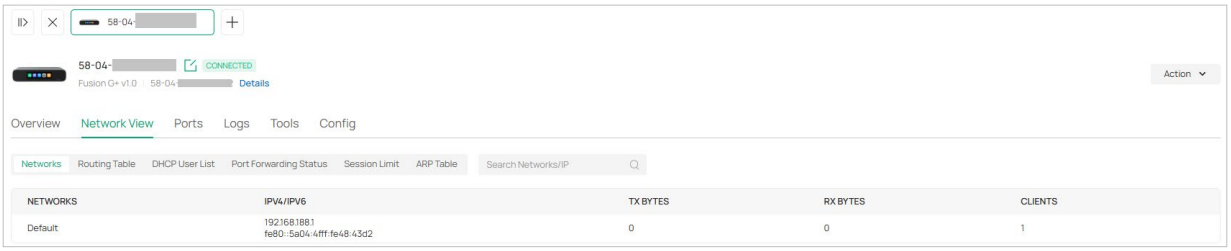
Overview

In Overview, you can get an overview of the device, such as device status, link status, online time, current clients, and more.



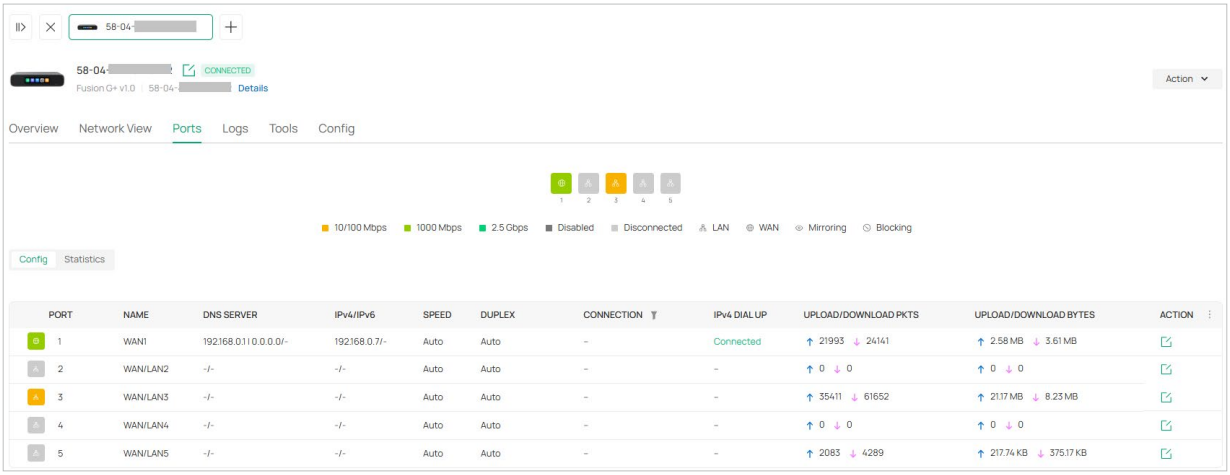
Network View

In Network View, you can check the network information of the device, such as configured networks, routing table, port forwarding status, and more.



Ports

In Ports, you can view the port status and statistics and edit port settings.



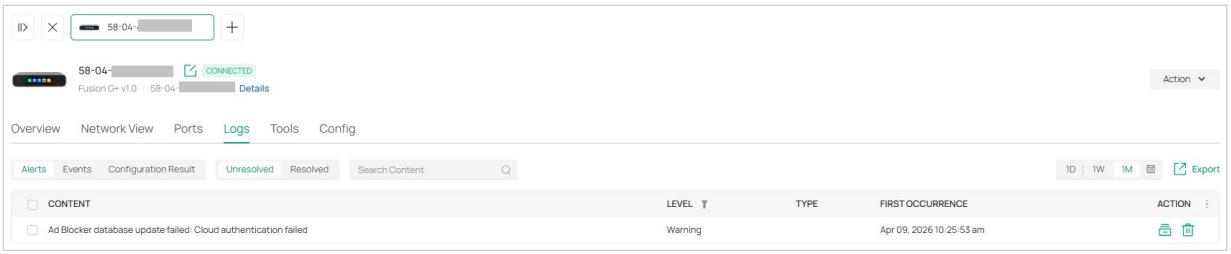
To configure a port, click the edit icon in the Action column. Port settings may vary by port type.

Status	Check the box to enable the port.
PoE Mode	(Only for PoE models) Select the PoE mode: Off or 8.2.3at/af.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Mirroring	Mirroring is used to analyze network traffic and troubleshoot network problems. With Mirroring configured, the gateway will sends a copy of traffics passing through the specified mirrored ports to the current port. To use this function, enable this option to set the current port as the mirroring port, specify one or multiple mirrored ports, and specify the directions of the traffic to be mirrored in the Mirror Mode: Ingress and Egress: Both the incoming and outgoing packets through the mirrored ports will be copied to the mirroring port. Ingress: The packets received by the mirrored ports will be copied to the mirroring port. Egress: The packets sent by the mirrored ports will be copied to the mirroring port.
Native VLAN	Select the Port VLAN Identifier (PVID) for the port.
Port Isolation	When enabled, this port becomes an isolated port and cannot communicate with any other isolated port. Please configure this feature carefully.
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.

Bandwidth Control	When enabled, you can select Rate Limit or Storm Control to control the traffic rate or the percentage of total bandwidth used on each port, and set traffic thresholds to ensure network performance (the Kbps value entered must be a multiple of 64).

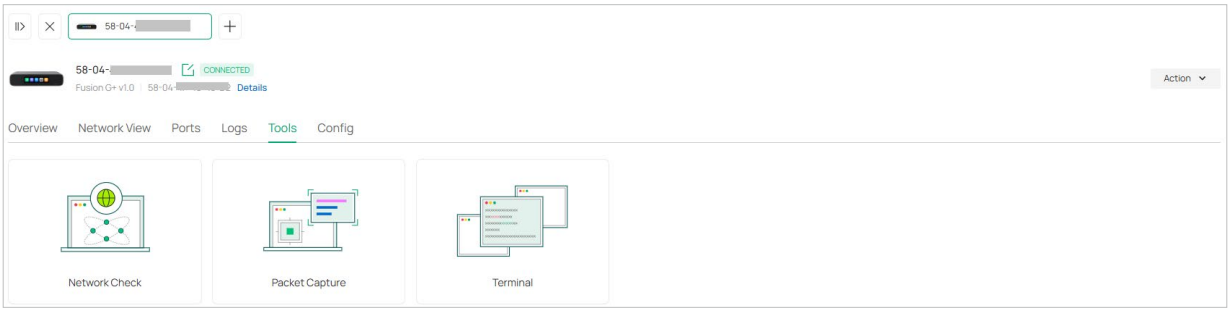
Logs

In Logs, you can check the logs of the device, such as alerts, events, and configuration result.



Tools

In Tools, you can use network tools to test the device connectivity and open Terminal to execute CLI or Shell commands.

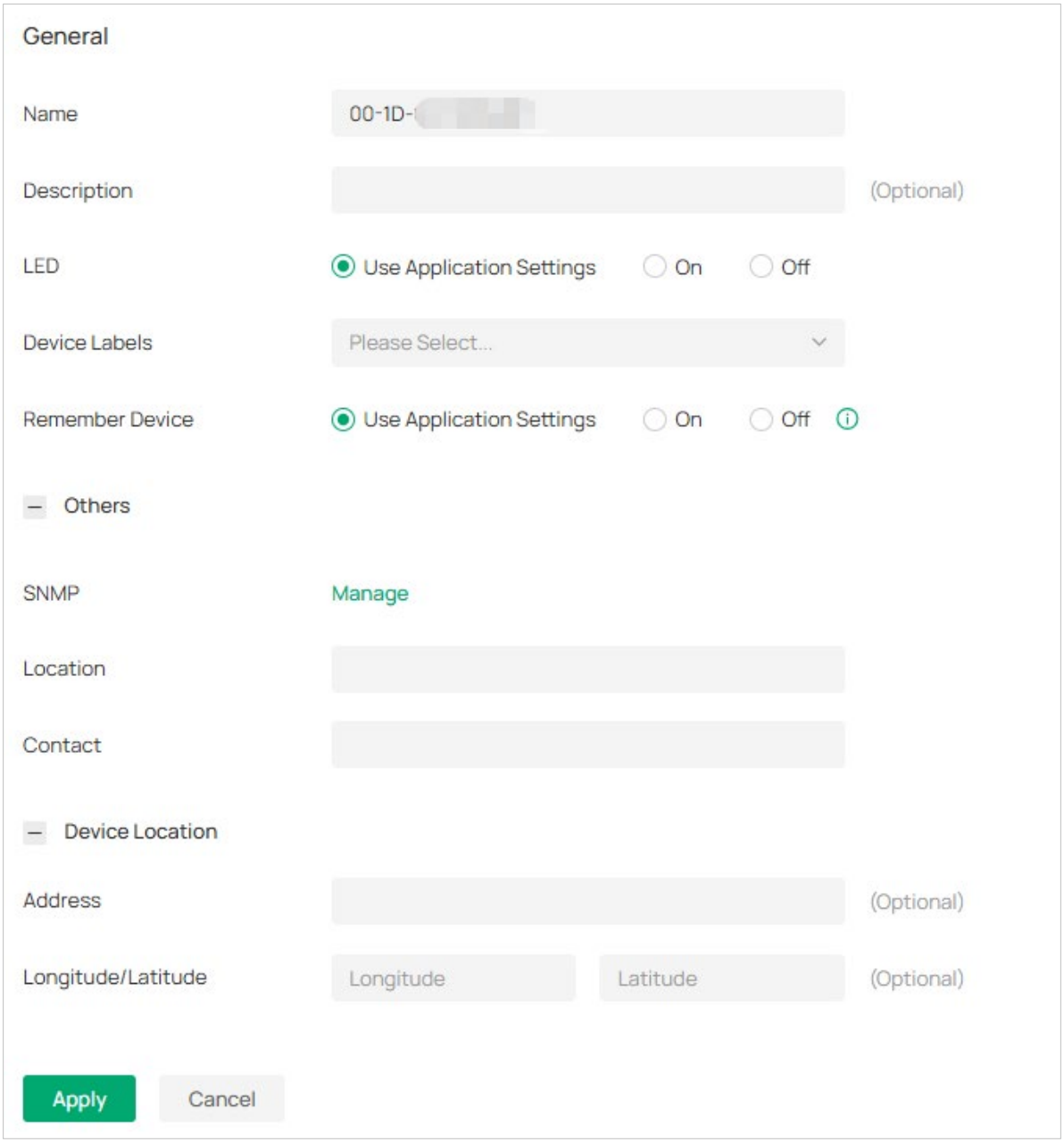


5. 2 Configure General Settings

In General Settings, you can specify the device name, control the LED, configure the device address, and more.

To configure general settings of a gateway, follow the steps below:

1. Go to Devices > Device List. In the device list, click a gateway, click Manage Device and go to Config > General.
2. Configure the parameters.



Name	Specify a name of the device.
Description	(Optional) Enter a description for identification.

LED	Select the way that device's LEDs work. Use Application Settings: The device's LED will work following the settings of the application. On/Off: The device's LED will keep on/off.
Device Labels	Select a label from the drop-down list or create a new label to categorize the device.
Remember Device	With this function, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.
SNMP	Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Network Config > General Settings > SNMP.
Device Location	Configure the address, longitude, and latitude according to where the device is located. These fields are optional.

5. 3 Traffic Management

For configuration instructions, refer to Configure Traffic Management Settings.

ACL	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.
Routing	You can configure the following routing functions for the device. 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.
Gateway QoS	Gateway QoS allows you to define service entries that will appear as matching conditions for you to choose when configuring the rules of related modules like QoS.
NAT	You can configure the following NAT functions for the device. Port Forwarding: 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. Disable NAT: Disable NAT allows internal devices to obtain public IP addresses.
MAC Filtering	MAC Filtering can drop or allow packets from certain devices passing through the router based on the MAC address of the devices. After the MAC filtering policy and MAC filtering list are configured, the router will apply the filter policy to the packets matching the MAC address, and thus limit network traffic and manage network access behaviors.
IP-MAC Binding	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 gateway checks whether it matches any of the IP-MAC Binding entries. If not, the gateway will ignore the ARP packets. In this way, the gateway maintains the correct ARP table.
Session Limit	Session Limit optimizes network performance by limiting the maximum sessions of specific sources.

5. 4 Network Security settings

For configuration instructions of the following functions, refer to Configure Network Security in this guide.

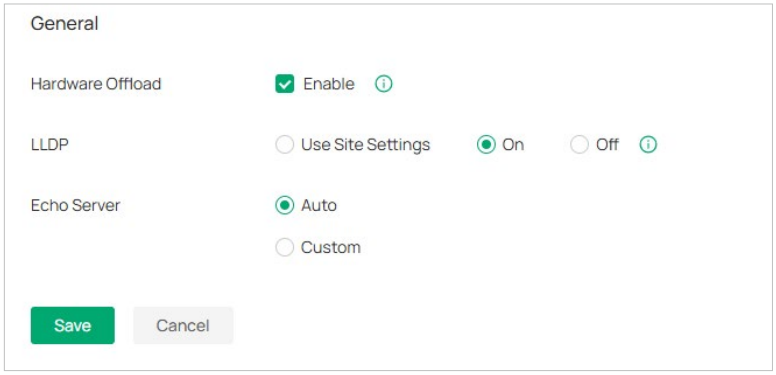
Content Filtering	Content Filtering allows you to control access to websites and online content based on security and usage policies. It protects your network from web-based threats, restricts inappropriate content, and can also block online ads for a better browsing experience.
Application Control	DPI (Deep Packet Inspection) helps you identify, analyze, and control the traffic at the application layer in the network. DPI engine includes the latest application identification signatures to track which applications are using the most bandwidth. You can better manage and distribute network traffic usage through DPI.
IDS/IPS	IDS/IPS is a security mechanism that detects intrusions based on attack characteristics. It can detect malware, Trojan horses, worms, ActiveX and other attacks to protect the network security of users.
Secure DNS	Secure DNS 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.
Firewall	Firewall is used to enhance the network security.

5. 5 Configure Advanced Settings

5. 5. 1 General

You can configure advanced settings to make better use of network resources.

1. Go to Devices > Device List. In the device list, click a gateway, click Manage Device and go to Config > Advanced > General.
2. Configure the parameters.



Hardware Offload	With this feature enabled, packet forwarding performance will be improved and CPU utilization will be reduced. Note that this feature cannot take effect if the QoS is enabled.
LLDP	LLDP (Link Layer Discovery Protocol) can help discover devices..
Echo Server	Echo Server is used to test the connectivity and monitor the latency of the network automatically or manually. If you click Custom, enter the IP address or hostname of your custom server.

5. 5. 2 Dynamic DNS

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. For detailed instructions, refer to Configure Dynamic DNS section in Configure WAN Networks chapter.

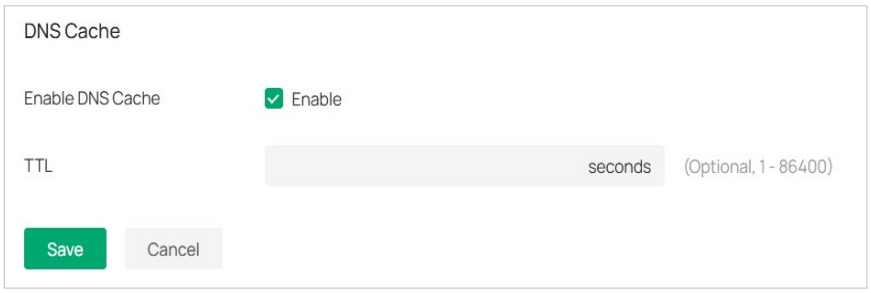
5. 5. 3 DNS Cache

Overview

DNS caching further speeds up domain name translation/resolution by handling it for recently visited addresses before the request is sent to the internet. Even if your network can use a large number of public DNS servers for translation/resolution, it's still faster to have a local copy.

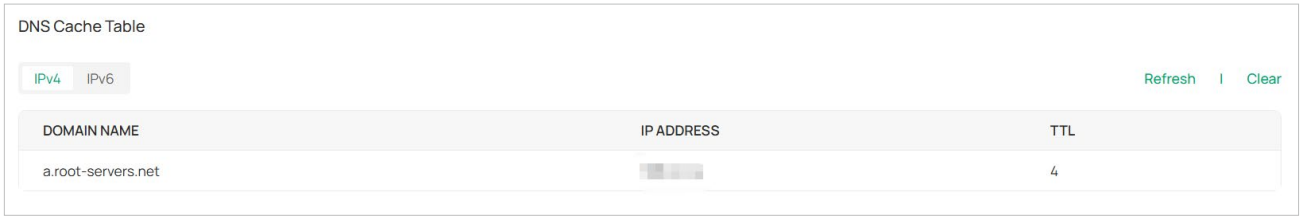
Configuration

1. Go to Devices > Device List, and in the device list, click a gateway, click Manage Device and go to Config > Advanced > DNS > DNS Cache for a specific gateway.
2. Enable DNS Cache and set a TTL value according to your needs. Then save the settings.



TTL	Specify the time to live (TTL) value in seconds. When the life cycle of the DNS entry exceeds the TTL value, the DNS cache will be automatically cleared. The range is 1-86400. If it's not specified, the system will use the default TTL value of each DNS message.

3. Refresh the DNS Cache Table and check the DNS cache status. You can clear the cache information if necessary.



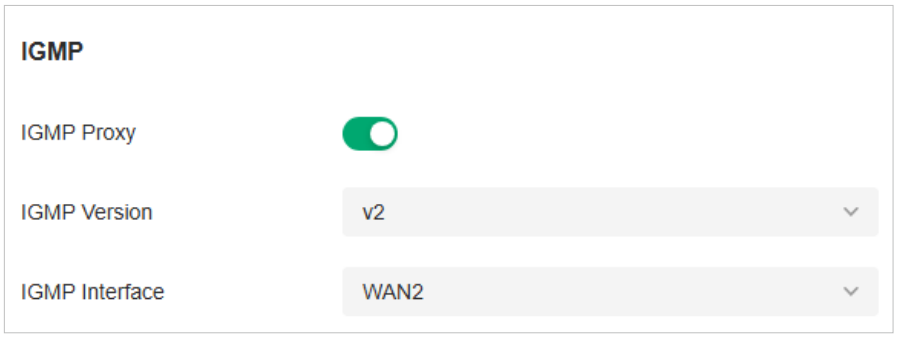
5. 5. 4 IPTV

Overview

IPTV includes three sections: IGMP, MLD 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. In MLD settings, you can enable MLD Proxy to allow the local network devices to receive multicast data from the IPv6 Internet. This feature can be used to detect whether there is any IPv6 multicast member connected to the LAN ports. IPTV settings allow you to enable Internet/IPTV/Phone service provided by your ISP.

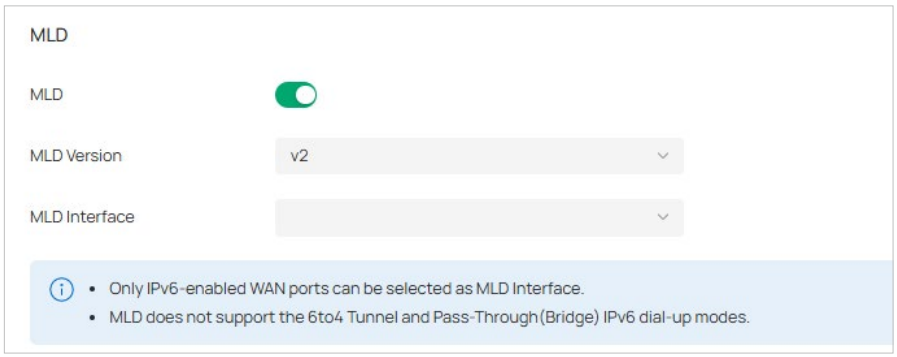
Configuration

1. Go to Device Config > Gateway > IPTV or go to Devices > Device List, and in the device list, click a gateway, click Manage Device and go to Config > Advanced > IPTV.
2. Enable IGMP Proxy and configure the parameters.



IGMP Proxy	Toggle on the switch to 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.

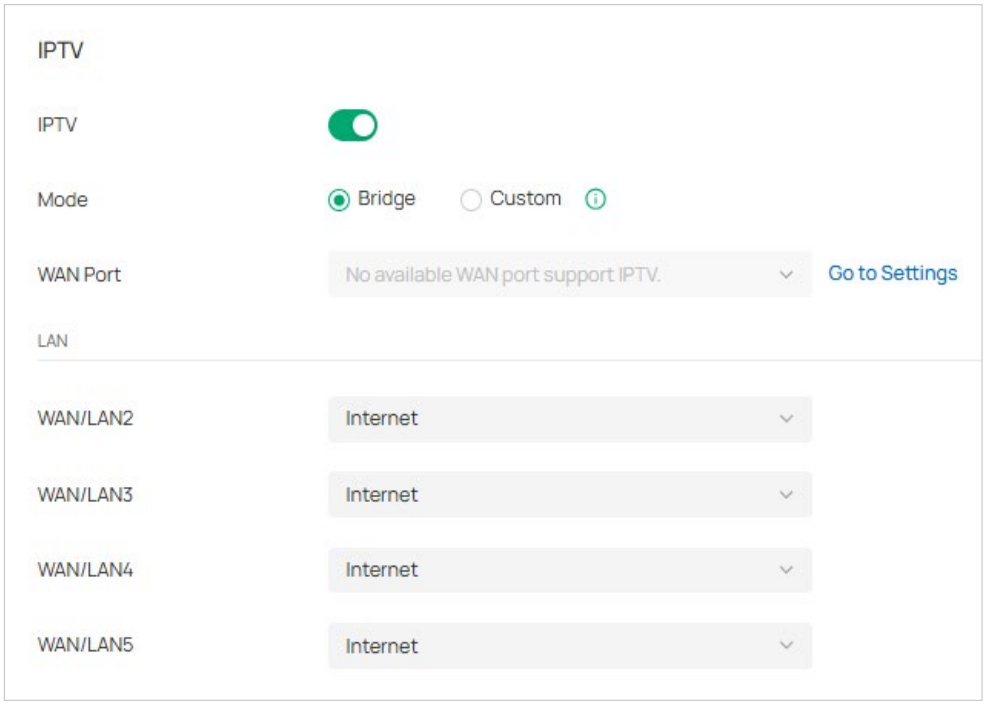
3. If you want the local network devices to receive multicast data from the IPv6 Internet, check the box to enable MLD. This feature is used to detect whether there is any IPv6 multicast member connected to the LAN ports.



MLD	Toggle on the switch to enable MLD. If you want the local network devices to receive multicast data from the IPv6 Internet, check the box to enable MLD Proxy. This feature is used to detect whether there is any IPv6 multicast member connected to the LAN ports.
MLD Version	Configure the MLD version as V1 or V2 according to your ISP.
MLD Interface	Select the IPv6 interface on which MLD takes effect.

4. If you want to configure the IPTV settings, enable IPTV and choose the mode as Bridge or Custom according to your ISP. Then configure the corresponding parameters.

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



IPTV	Toggle on the switch to 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.

5. Click Save.

Chapter 6

Manage Switches

This chapter guides you on how to manage switches via the Fusion gateway. You can configure the devices individually or in batches to modify the configurations of certain devices. The chapter includes the following sections:

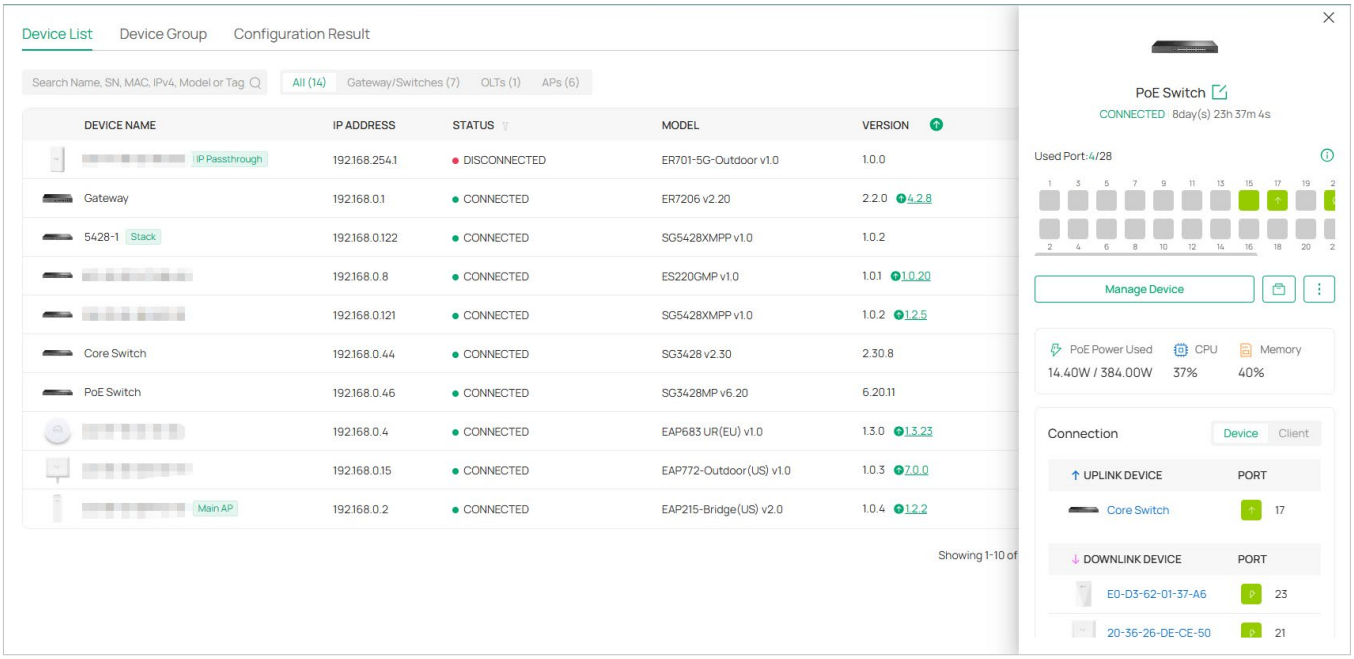
6. 1 Manage the Switch

Go to Devices > Device List. In the device list, click a switch, then you can monitor and manage it in the Properties window and Device Management window.

6. 1. 1 Properties Window

The Properties window displays the device status, port status, connection information, and other device information.

Note: The available functions in the window may vary by device model and status.



Quick Operations

Click the ⋮ icon and choose an operation to quickly operate the device.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. After upgraded, the device will reboot and be readopted by the controller.
Copy Configuration	Select another device to copy its configurations. **Note:** Only devices of the same model as the current device will be displayed.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.
Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.

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

Network Tools

Click the icon and choose a network tool to analyze the network.

Network Check	Test the device connectivity via ping or traceroute. Ping: Sends ICMP echo request packets to a destination to verify basic reachability and measure round-trip time. Traceroute: Maps the path data takes to a destination, identifying each "hop" and pinpointing where delays or packet loss occur in the route. DNS Lookup: Verifies that the switch can correctly resolve domain names to IP addresses, which is essential for cloud connectivity. ARP Table: Displays the Address Resolution Protocol table, showing the mapping between IP addresses and physical MAC addresses of devices directly connected to the switch.
Packet Capture	Capture and analyze real-time network packets for diagnostics.
Terminal	Open Terminal to execute CLI or Shell commands.
Cable Test	Perform cable test to check cable issues.

6. 1. 2 Device Management Window

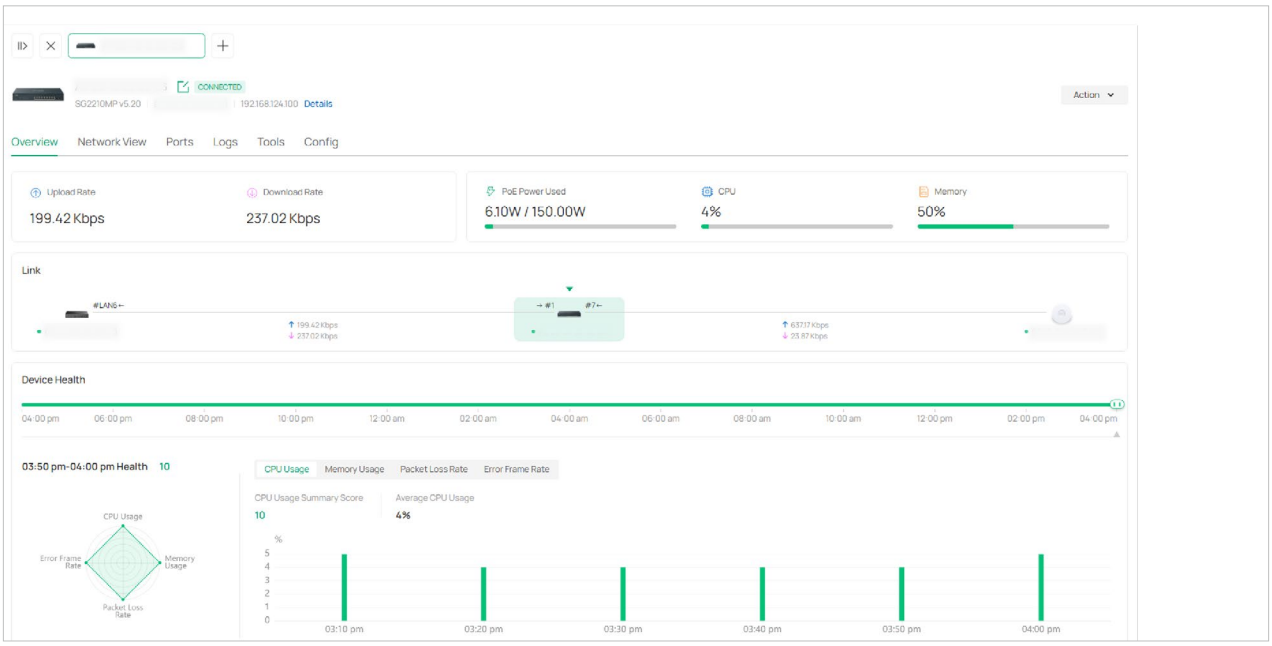
Click Manage Device to open the Device Management window to view more device details and change device settings.

In the management window, you can click + and select one or more devices to open new management windows, click the icon in the top left to minimize the windows to the icon in the right side, and click the icon to reopen the minimized windows.

You can also click each tab to monitor and manage the device. The tabs available may vary by model.

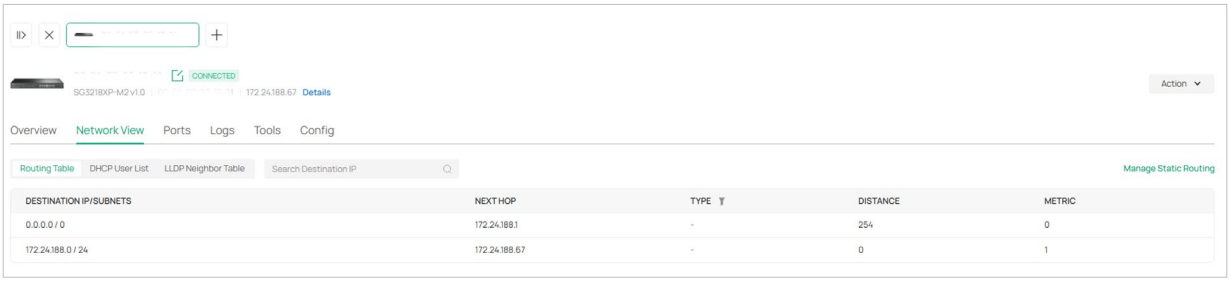
Overview

In Overview, you can get an overview of the device, such as device status, link status, online time, current clients, and more.



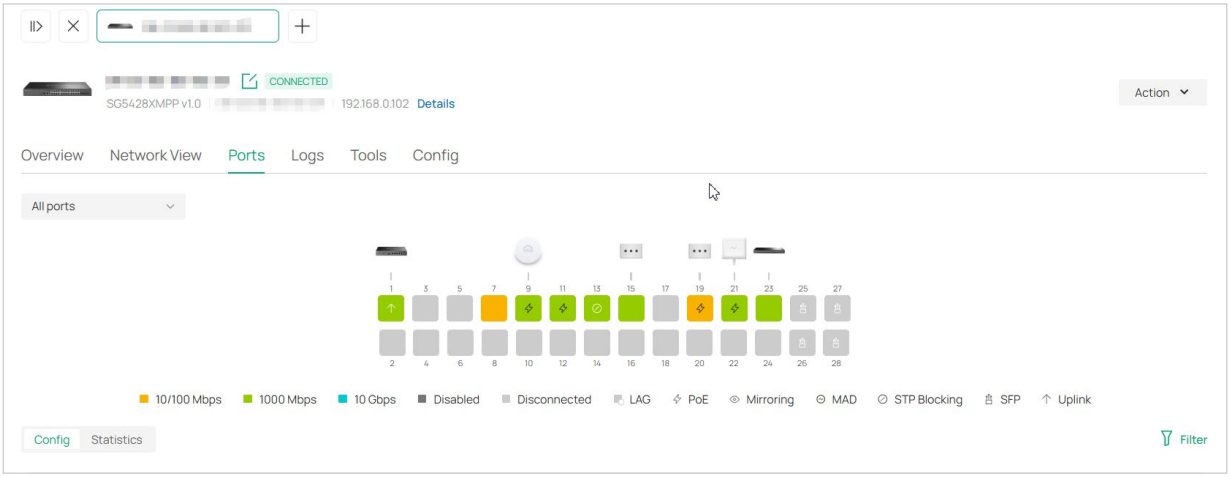
Network View

In Network View, you can check the network information of the device, such as routing table and DHCP User List.



Ports

In Ports, you can view the port status and statistics and edit port settings.

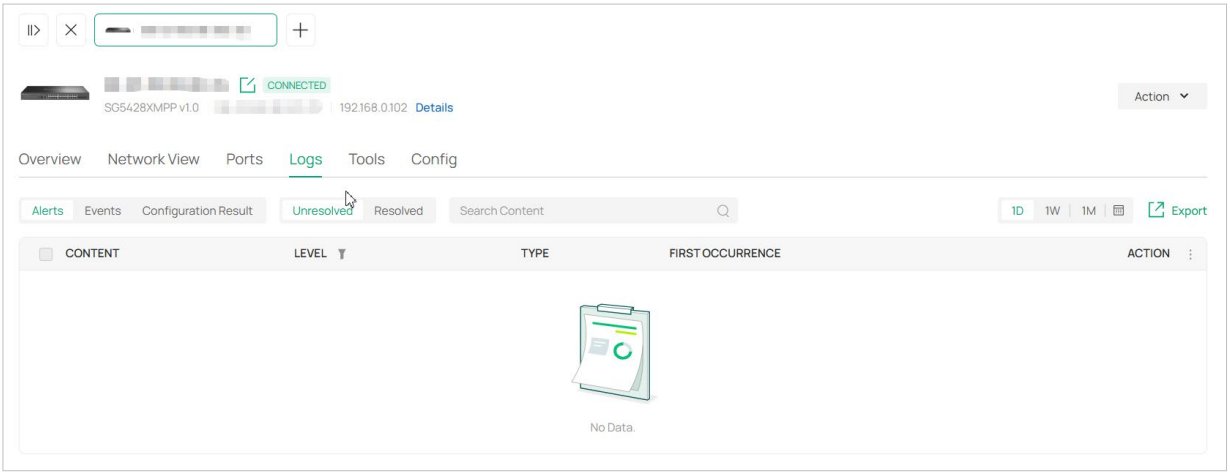


To configure a port, click the edit icon in the Action column. Port settings may vary by port type.

For configuration instructions, refer to Port Settings.

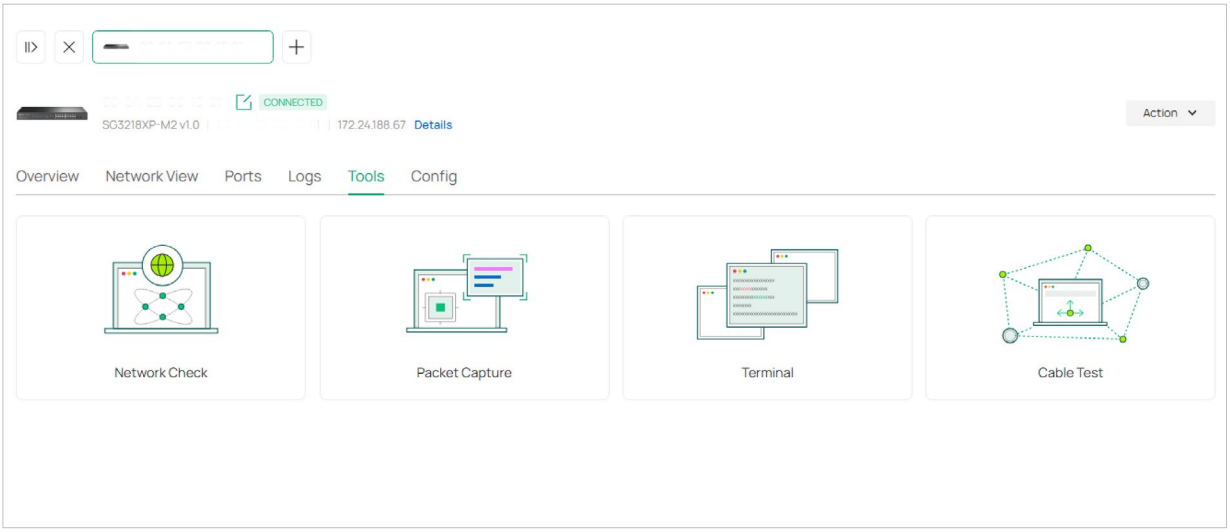
Logs

In Logs, you can check the logs of the device, such as alerts, events, and configuration result.



Tools

In Tools, you can use network tools to test the device connectivity, Open Terminal to execute CLI or Shell commands, and perform cable test to check cable issues.

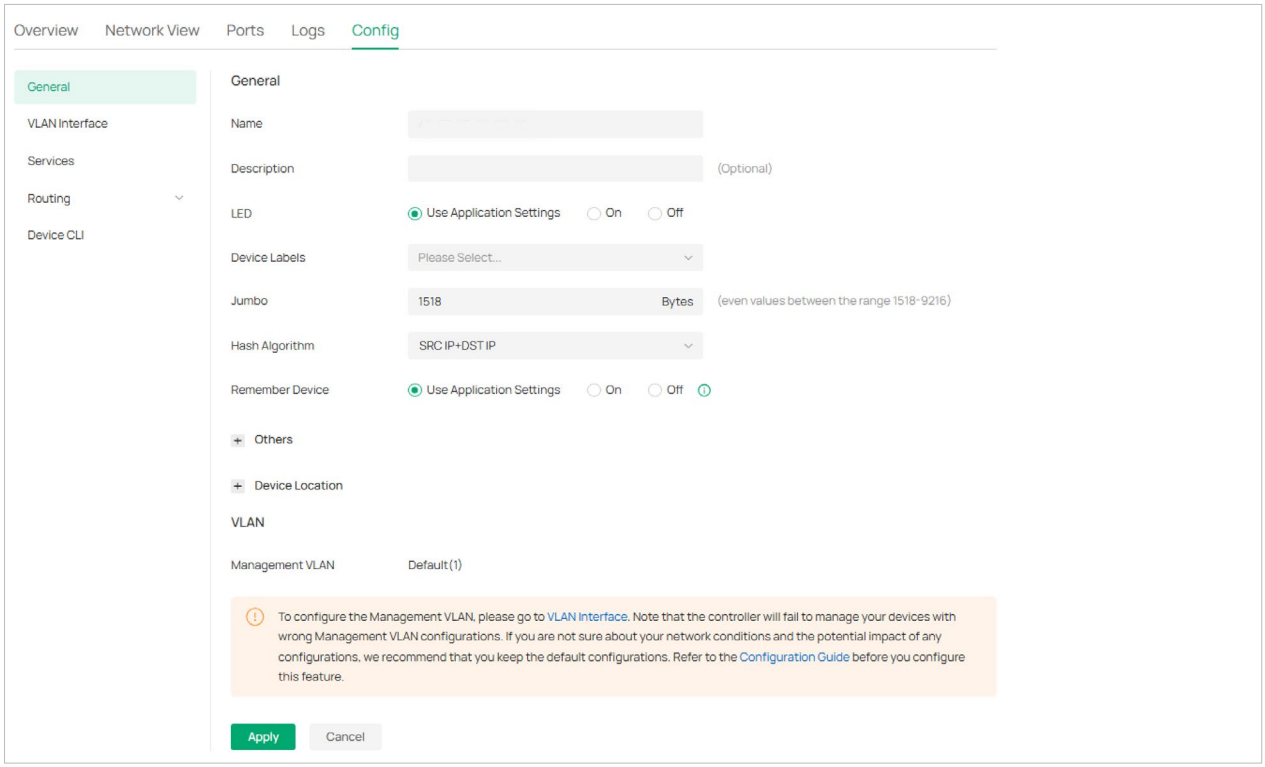


6. 2 Configure General Settings

In General Settings, you can specify the device name, control the LED, configure the device address, and more.

To configure general settings of a switch, follow the steps below:

1. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > General.
2. Configure the parameters.

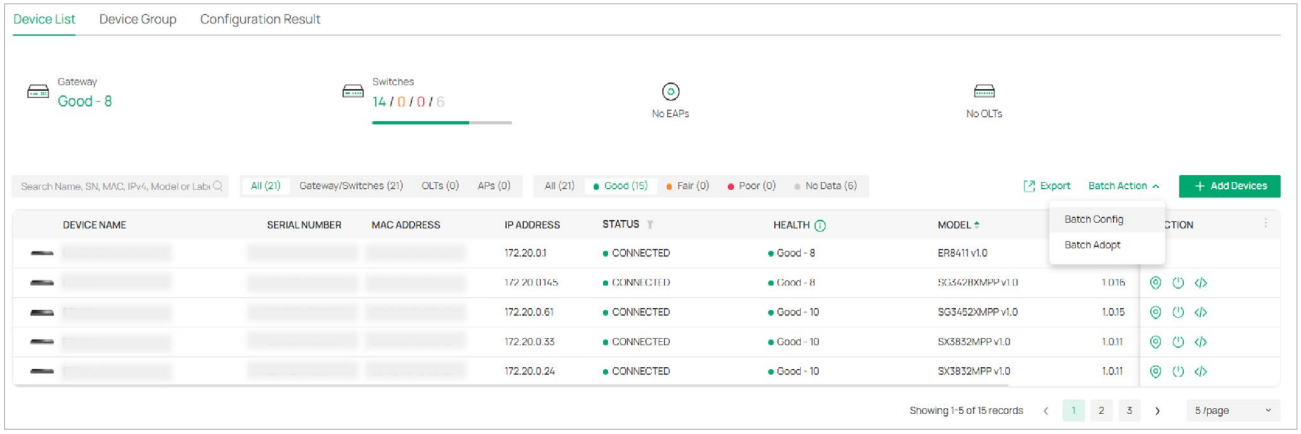


Name	Specify a name of the device.
Description	(Optional) Enter a description for identification.
LED	Select the way that device's LEDs work. Use Application Settings: The device's LED will work following the settings of the application. On/Off: The device's LED will keep on/off.
Device Labels	Select a label from the drop-down list or create a new label to categorize the device.
Jumbo	Configure the size of jumbo frames. By default, it is 1518 bytes. Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1518 bytes. If you want the switch supports to transmit frames of which the MTU size is greater than 1518 bytes, you can configure the MTU size manually here.

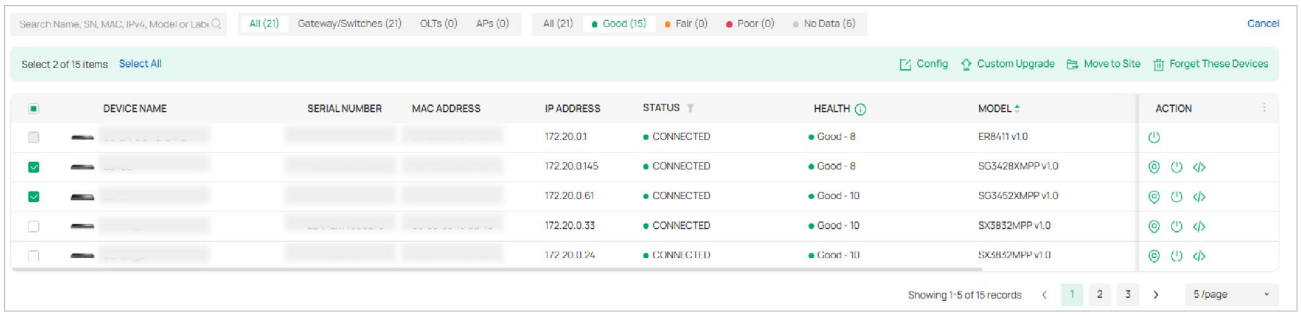
Hash Algorithm	Select the Hash Algorithm, based on which the switch can choose the port to forward the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing. SRC MAC: The computation is based on the source MAC addresses of the packets. DST MAC: The computation is based on the destination MAC addresses of the packets. SRC MAC+DST MAC: The computation is based on the source and destination MAC addresses of the packets. SRC IP: The computation is based on the source IP addresses of the packets. DST IP: The computation is based on the destination IP addresses of the packets. SRC IP+DST IP: The computation is based on the source and destination IP addresses of the packets.
Remember Device	With this function, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.
SNMP	Configure SNMP to write down the Location and Contact detail. You can also click Manage to jump to Network Config > General Settings > SNMP.
SDM Template	Modify the entry limit for the corresponding functions by adjusting the switch's SDM template.
Management VLAN	Display the name of the current Management VLAN. To configure the Management VLAN, go to Config > VLAN Interface. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the Management VLAN Configuration Guide before you configure this feature.

To configure general settings in batches, follow the steps below:

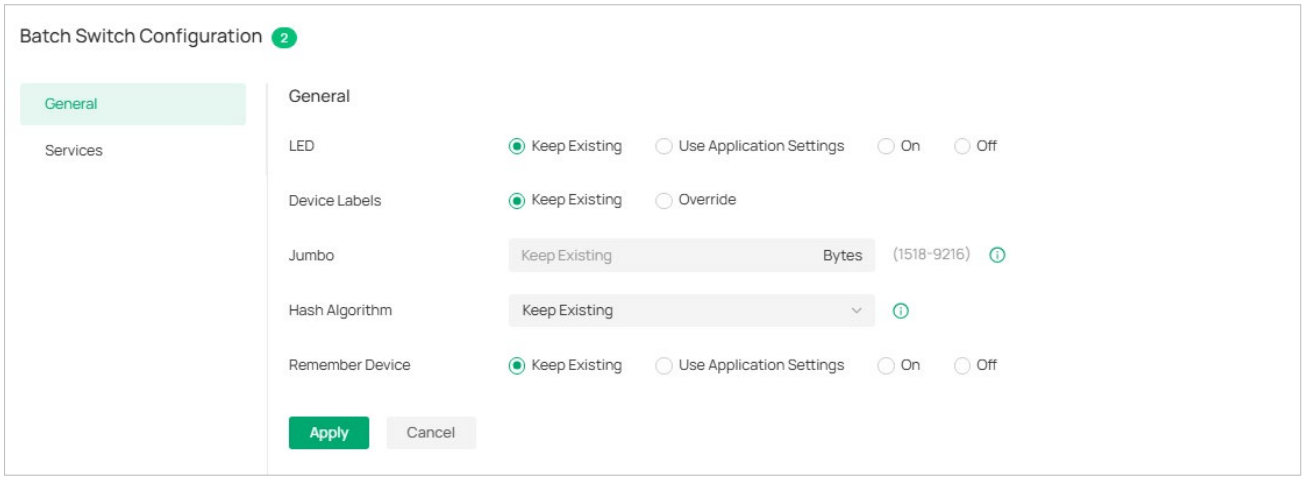
1. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.



2. Select the switches for batch configuration and click Config.



3. Configure the parameters.



LED	Select the way that device's LEDs work. Keep Existing: Keep the existing LED settings. Use Application Settings: The device's LED will work following the settings of the application. On/Off: The device's LED will keep on/off.
Device Labels	Keep Existing: Keep the existing LED settings. Override: Select a label from the drop-down list or create a new label to categorize the device.
Jumbo	Configure the size of jumbo frames. If not set, the jumbo frame will keep the existing value. By default, it is 1518 bytes. Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1518 bytes. If you want the switch supports to transmit frames of which the MTU size is greater than 1518 bytes, you can configure the MTU size manually here.

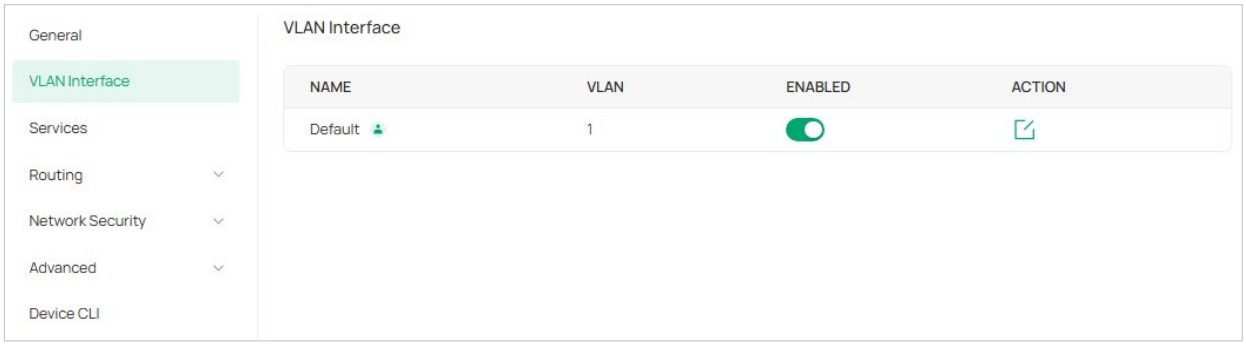
Hash Algorithm	Select the Hash Algorithm, based on which the switch can choose the port to forward the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing. Keep Existing: Keep the existing Hash Algorithm settings. SRC MAC: The computation is based on the source MAC addresses of the packets. DST MAC: The computation is based on the destination MAC addresses of the packets. SRC MAC+DST MAC: The computation is based on the source and destination MAC addresses of the packets. SRC IP: The computation is based on the source IP addresses of the packets. DST IP: The computation is based on the destination IP addresses of the packets. SRC IP+DST IP: The computation is based on the source and destination IP addresses of the packets.
Remember Device	With this function, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it. Keep Existing: Keep the existing Remember Device settings. Use Application Settings: The Remember Device settings will work following the settings of the application. On/Off: The Remember Device settings will keep on/off.
SDM Template	Modify the entry limit for the corresponding functions by adjusting the switch's SDM template.

6. 3 Configure VLAN Interface Settings

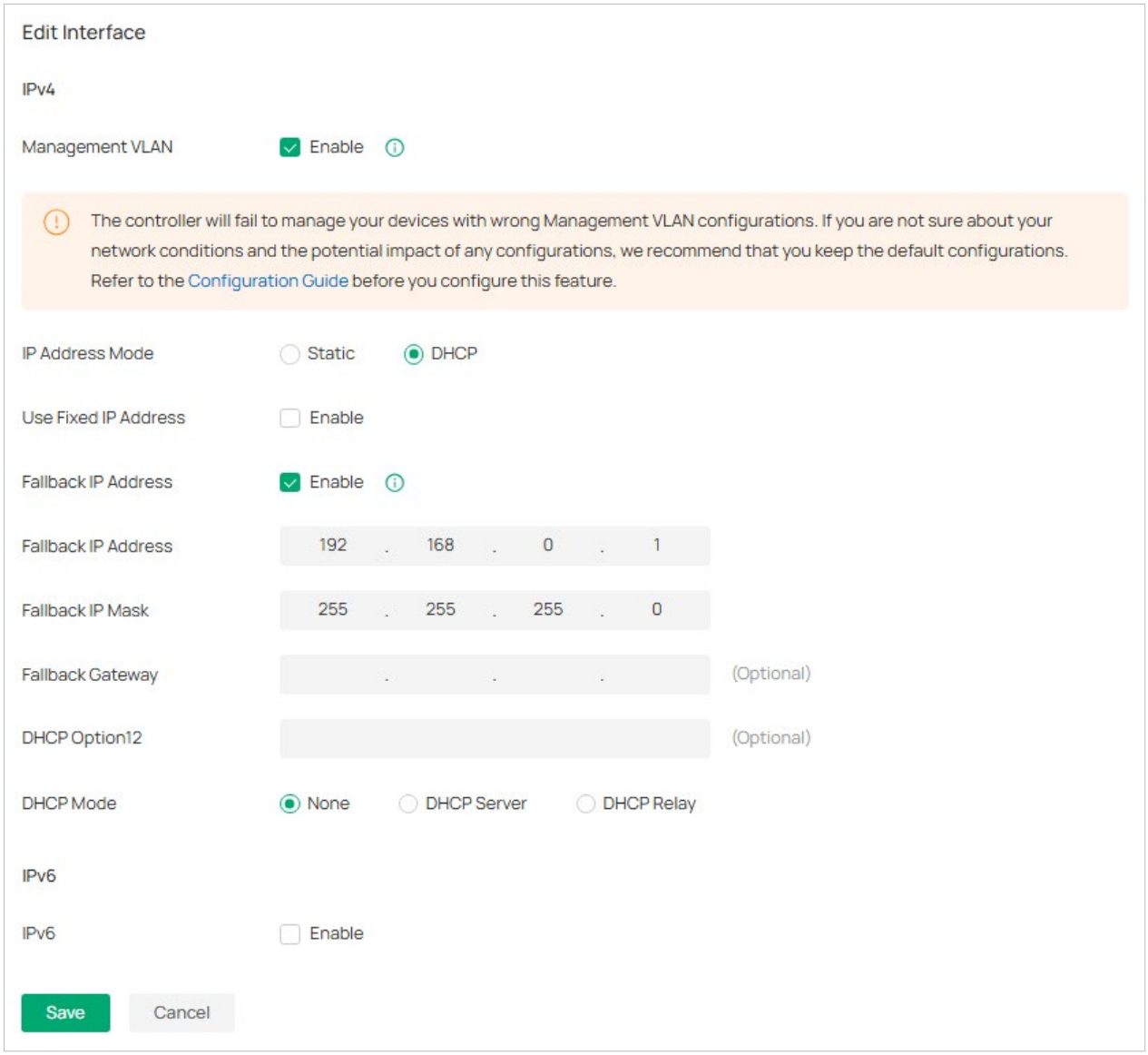
In VLAN Interface, you can enable and edit the VLAN interface.

To configure the VLAN interface of a switch, follow the steps below:

1. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > VLAN Interface.



2. Click the Configure the parameters to edit the VLAN interface.



Management VLAN	Click the checkbox if you want to use the VLAN interface as Management VLAN. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the Management VLAN Configuration Guide before you configure this feature.
IP Address Mode (when Management VLAN enabled)	Select a mode for the interface to obtain its IP address, and the VLAN will communicate with other networks including VLANs with the IP address. Static: Assign an IP address to the interface manually, specify the IP Address and Subnet Mask for the interface. When the VLAN interface is set as the Management VLAN, it is optional for you to specify the Default Gateway and Primary/Secondary DNS for the interface. DHCP: Assign an IP address to the interface through a DHCP server. When you want to let device use a fixed IP address, enable Use Fixed IP Address and specify the Network and IP Address based on needs. When the VLAN interface is set as the Management VLAN, you can further enable Fallback IP Address, and specify the Fallback IP Address, Fallback IP Mask, and Fallback Gateway (optional). If the VLAN interface fails to get an IP address from the DHCP server, the fallback IP address will be used for the interface.
DHCP Option 12	When DHCP is selected as the IP Address Mode, you can specify the hostname of the DHCP client in the field. The DHCP client will use option 12 to tell the DHCP server their hostname.
DHCP Mode	Select a mode for the clients in the VLAN to obtain their IP address. None: Do not use DHCP to assign IP addresses. DHCP Server: Assign an IP address to the clients through a DHCP server. When DHCP Server is selected, you can specify the DHCP Range, and the IP addresses in the range can be assigned to the clients in the VLAN. Also, it is optional for you to specify the DHCP Option 138, Primary/Seconday DNS, Default Gateway, and Lease Time. DHCP Option 138 informs the DHCP client of the controller's IP address when the client sends a request to the DHCP server, and specify Option 138 as the controller's IP address here. Lease Time decides how long the client can use the assigned IP address. You can also click Custom Option and specify the DHCP Option code, type and value to add other DHCP Options. DHCP Relay: It allows clients in the VLAN to obtain IP addresses from a DHCP server ion different subnet. When DHCP Relay is selected, specify the IP address of the DHCP server in Server Address. Devices with the latest firmware support specifying multiple server IP addresses.
IPv6	Enable this option if you want to set up an IPv6 interface.

IPv6 Mode	Select the IPv6 mode. Dynamic IP (SLAAC/DHCPv6): In this mode, determine whether to Get Dynamic DNS or use the specified DNS addresses. Static: In this mode, set the IP address, prefix length, gateway, and DNS server for the static address.
DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually. Get Dynamic DNS: The DNS address will be automatically assigned by the ISP. Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

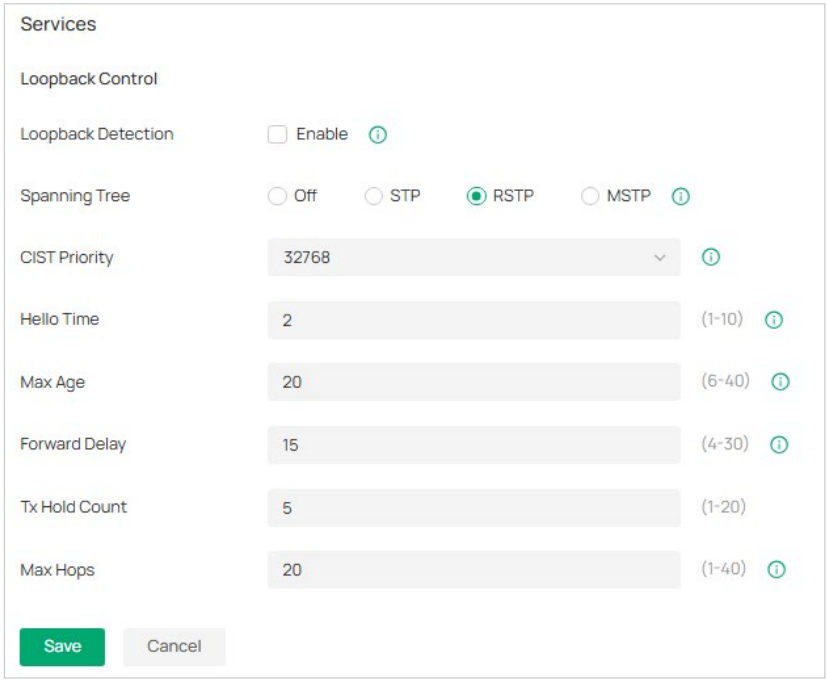
6. 4 Configure Service Settings

6. 4. 1 Loopback Control

In Services, you can configure Loopback Control for the switch.

To configure the Loopback Control settings of a switch, follow the steps below:

1. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Services.
2. Configure the parameters.

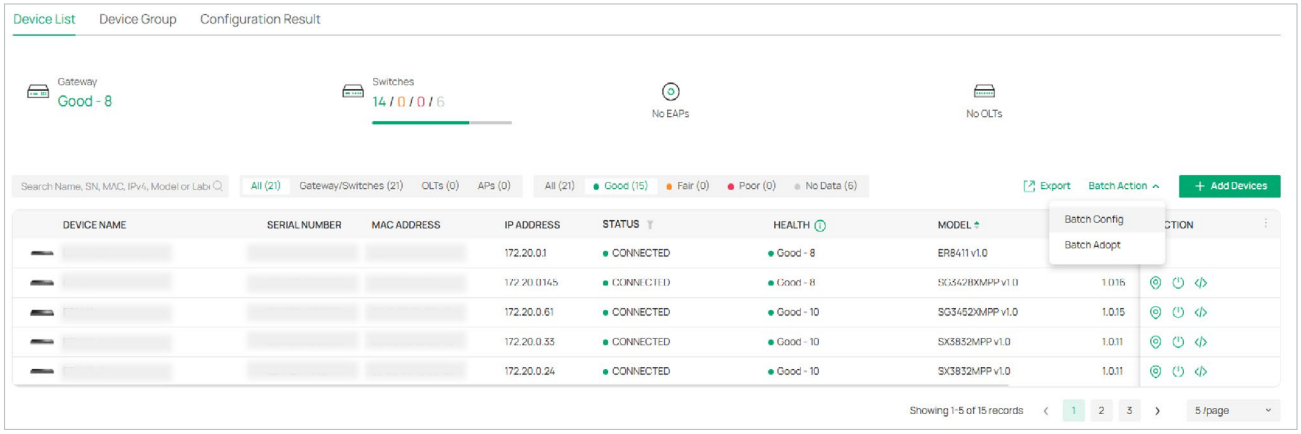


Loopback Detection	When enabled, the switch checks the network regularly to detect the loopback. Note that Lopback Detection and Spanning Tree are not available at the same time.
Spanning Tree	Select a mode for Spanning tree. This feature is available only when Loopback Detection is disabled. Off: Disable Spanning Tree on the switch. STP: Enable STP (Spanning Tree Protocal) to prevent loops in the network. STP helps to block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. RSTP: Enable RSTP (Rapid Spanning Tree Protocal) to prevent loops in the network. RSTP provides the same features as STP with faster spanning tree convergence. MSTP: Enable MSTP (Multiple Spanning Tree Protocal) to prevent loops in the network. MSTP is the extension of STP and RSTP.

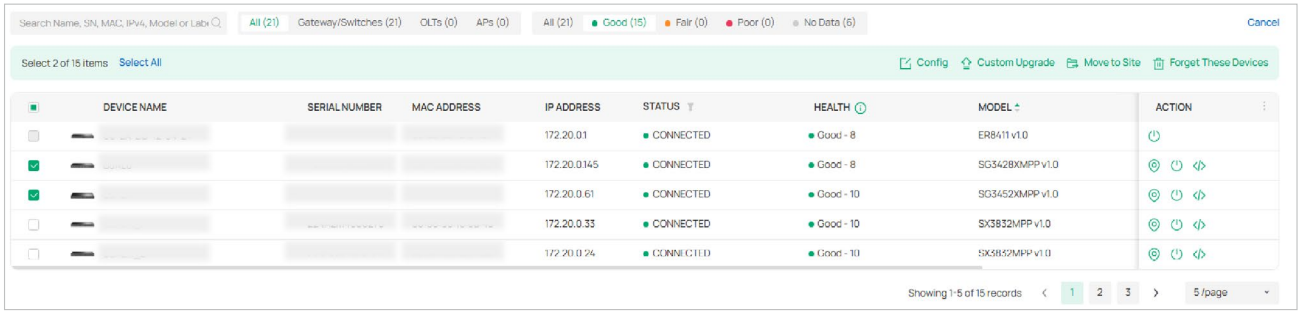
CIST Priority	Specify the CIST priority for the switch. It determines the root bridge election in the spanning tree. A smaller value indicates higher priority, and the switch with the highest priority will be elected as the root bridge.
Hello Time	Specify the interval for sending BPDUs to detect link failures. It works with Max Age to monitor link status and maintain the spanning tree.
Max Age	Specify the aging time of BPDU (Bridge Protocol Data Unit) packets, which refers to the maximum duration a switch will wait to regenerate a new spanning tree if no BPDUs are received.
Forward Delay	When a link failure triggers spanning tree recalculation, the new configuration messages generated from the recalculation cannot propagate throughout the network immediately. After a delay of twice the Forward Delay interval, this latency ensures that new configuration messages have fully propagated across the network, thus preventing the formation of temporary loops.
Tx Hold Count	Specify the maximum number of BPDU that can be sent in a second.
Max Hops	BPDUs are discarded when their hop count reaches zero. This value controls the scale of the spanning tree in an MST region. Switches decrement the hop count by 1 before forwarding BPDUs.

To configure the Loopback Control settings in batches, follow the steps below:

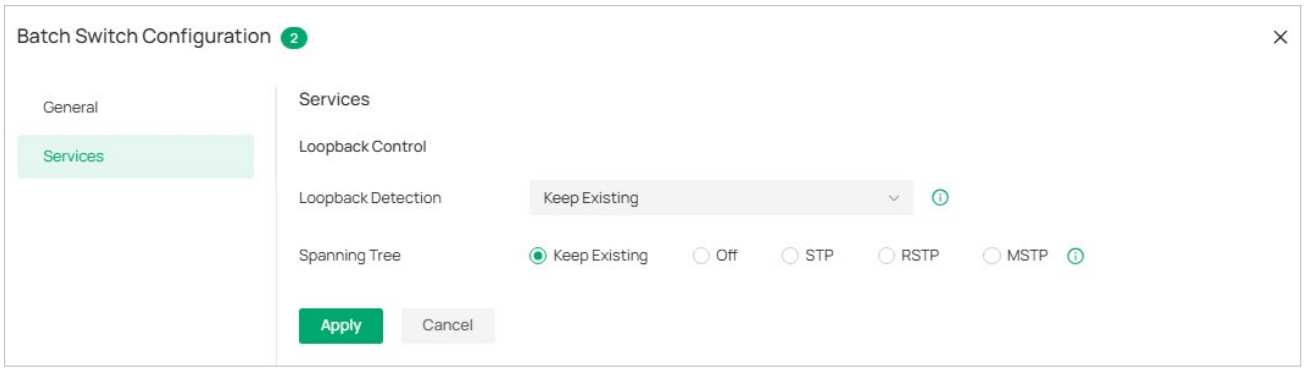
1. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.



2. Select the switches for batch configuration and click Config.



3. Configure the parameters.



Loopback Detection	When enabled, the switch checks the network regularly to detect the loopback. Keep Existing: Keep the existing Spanning Tree mode. Enable: Enable Loopback Detection on the switch. Disable: Disable Loopback Detection on the switch. Note that Lopback Detection and Spanning Tree are not available at the same time.
Spanning Tree	Select a mode for Spanning tree. This feature is available only when Loopback Detection is disabled. Keep Existing: Keep the existing Spanning Tree mode. Off: Disable Spanning Tree on the switch. STP: Enable STP (Spanning Tree Protocal) to prevent loops in the network. STP helps to block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. RSTP: Enable RSTP (Rapid Spanning Tree Protocal) to prevent loops in the network. RSTP provides the same features as STP with faster spanning tree convergence. MSTP: Enable MSTP (Multiple Spanning Tree Protocal) to prevent loops in the network. MSTP is the extension of STP and RSTP.

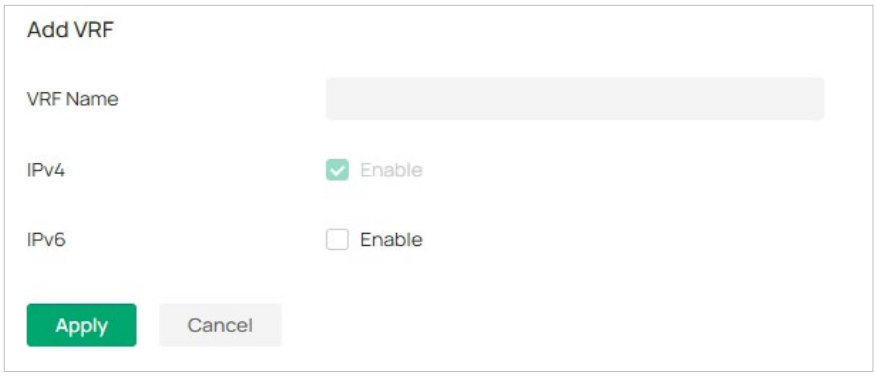
6. 4. 2 VRF (Only for certain models)

In Services, you can add VRF instances to enhance functionality by enabling the division of network paths without requiring multiple devices, effectively transforming one physical router into multiple virtual routers.

To add a VRF instance, click Add and configure the parameters.

To configure the VRF settings of a switch, follow the steps below:

1. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Advanced > VRF.
2. Click Add to add a VRF instance and configure the parameters.



VRF Name	Specify the VRF instance name.
IPv4	Check the box to enable IPv4 for the instance.
IPv6	Check the box to enable IPv6 for the instance.

6. 5 Configure Routing Settings

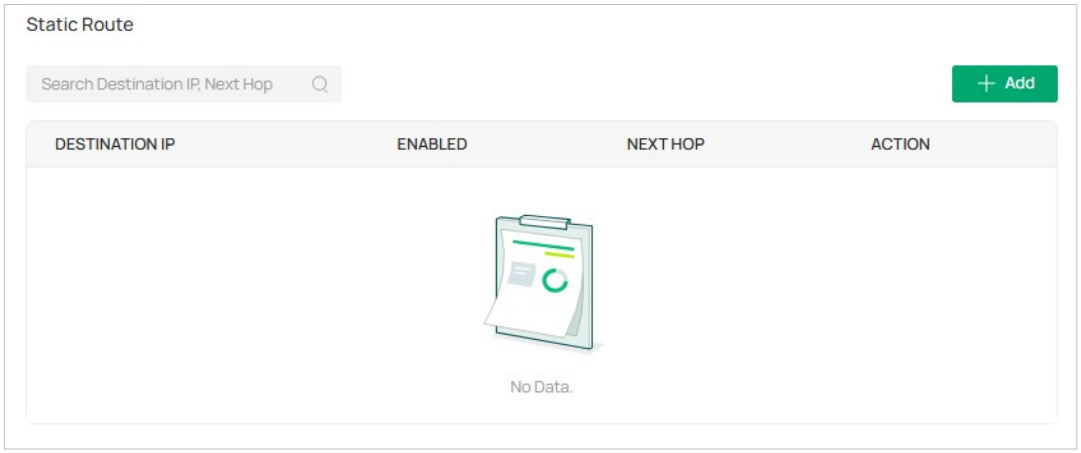
6. 5. 1 Static Route

In Routing, you can configure the Static Route of the switch.

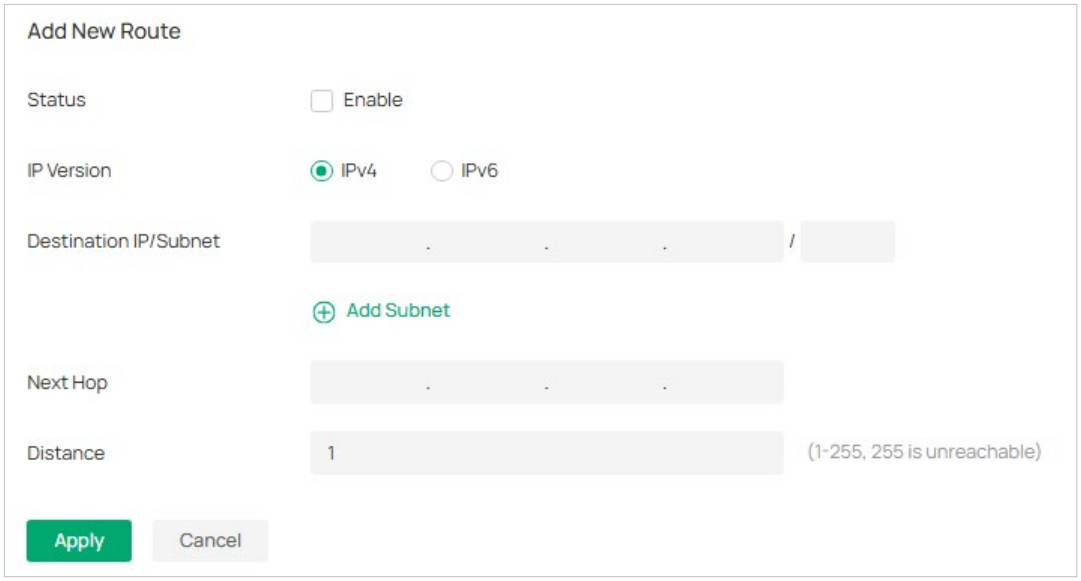
Network traffic is oriented to a specific destination, and Static Route designates the next hop or interface where to forward the traffic.

To configure the Static Route settings of a switch, follow the steps below:

1. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Routing > Static Route.



2. Click Add to add a new route and configure the parameters.



Status	Click the checkbox to enable the static route entry.

IP Version	Specify the IP version. With IPv4 selected, specify the Destination IP/Subnet of the network traffic. The traffic will be forwarded to the specified destination. With IPv6 selected, specify the Destination IP/Prefix Length of the network traffic. The traffic will be forwarded to the specified destination.
Next Hop	Specify the IP address as the next hop. The device will forward the corresponding network traffic to the specific IP address.
Distance	Specify the distance. It ranges from 1 to 255, and 255 is unreachable.

6. 5. 2 OSPF (Only for certain models)

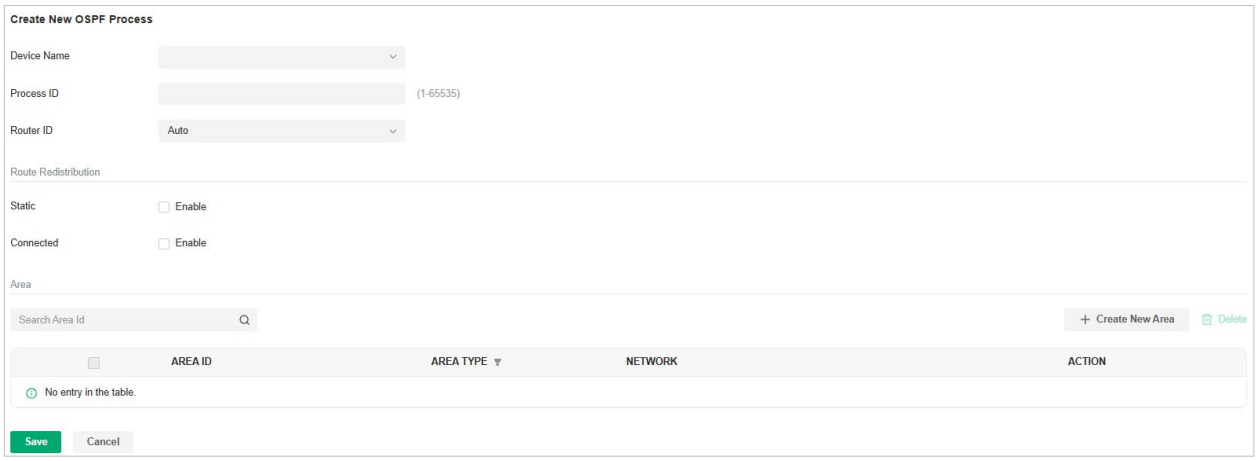
In Routing, you can configure the OSPF of the switch.

The OSPF protocol (Open Shortest Path First) is a link-state-based dynamic routing protocol that uses Dijkstra's SPF (shortest path first) algorithm to calculate routes within a single AS (autonomous system). OSPF establishes a link state database by advertising the state of network interfaces between routers, and generates shortest path trees. Other OSPF routers in the area use these shortest paths to construct routes.

To configure the OSPF settings of a switch, follow the steps below:

1. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Routing > OSPF.

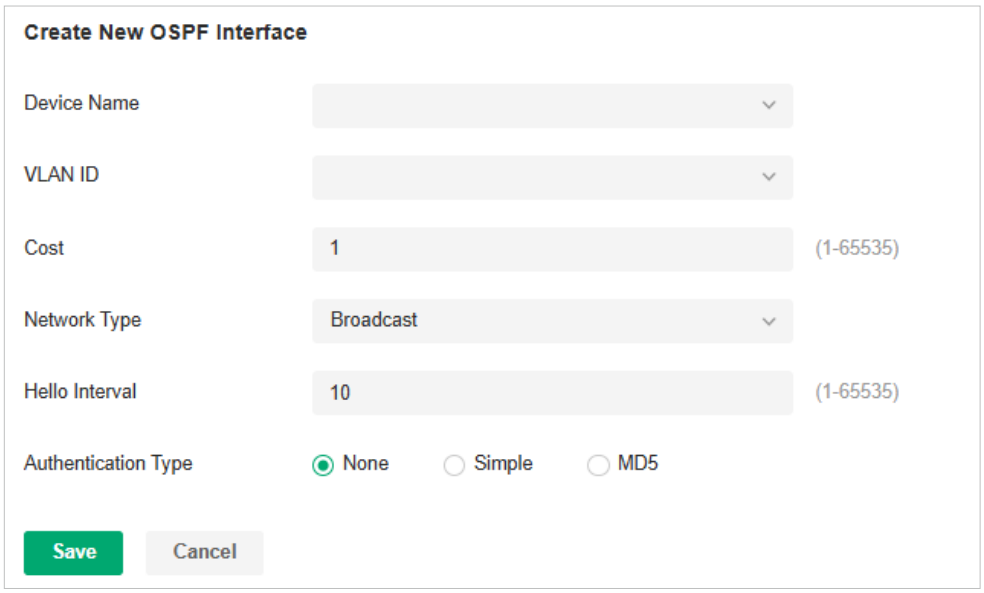
   In OSPF Process, you can add an OSPF process and configure the following parameters:



Process ID	Enter a number between 1 and 65535 to identify the OSPF process locally on the router.
Router ID	Specify the identity of the router. The selection priority order is manually configured interface, loopback interface, then physical interface.

Static	Check the box to enable static route. With this option selected, configure the following parameters: Metric: Specify the path cost when importing external routes. Metric Type: Specify the cost calculation type. Type 1 calculates internal cost and external cost. Type 2 calculates external cost only. The default value is type 2.
Connected	Check the box to enable direct route.
Area	Configure the OSPF areas.

In OSPF Interface, you can add an OSPF interface and configure the following parameters:



VLAN ID	Specify the ID of the VLAN.
Cost	Specify the interface overhead.
Network Type	Specify the network type of the OSPF interface.
Hello Interval	Specify the interval between Hello packets sent on the interface.
Dead Interval	Set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down.
Authentication Type	Specify the interface area verification method. None: No authentication. Simple: Simple authentication mode. The key is transmitted with clear texts. With this option selected, specify the Simple Key for authentication. MD5: MD5 authentication mode. The key and key ID are transmitted through MD5 encryption. With this option selected, specify the MD5 Key ID and MD5 Key for authentication.

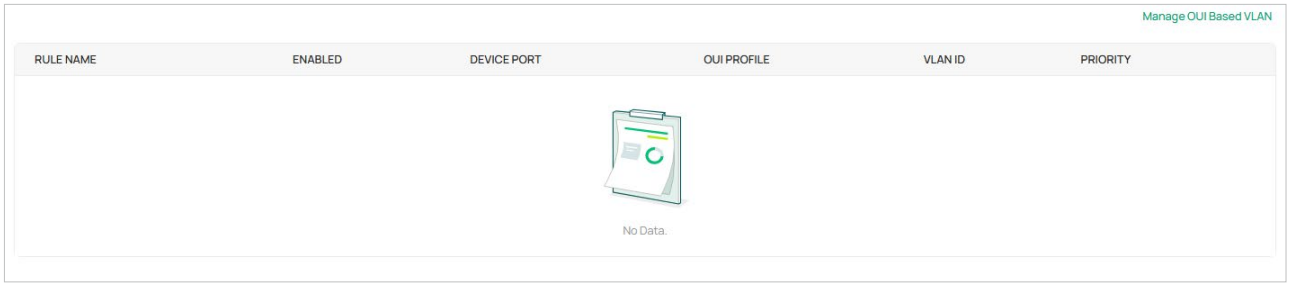
6. 6 Configure Advanced Settings

In Advanced settings, you can view the OUI Based VLAN of the switch.

The OUI Based VLAN function can perform VLAN and priority division and processing on device data packets starting with specific MAC addresses based on OUIs.

To configure the OUI Based VLAN rules of a switch, follow the steps below:

1. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Advanced > OUI Based VLAN.



2. Click Manage OUI Based VLAN to redirect to the OUI Based VLAN page to create and edit switch rules. For detailed instructions about OUI Based VLAN, refer to the relavant chapter.

6. 7 Configure Device CLI Settings

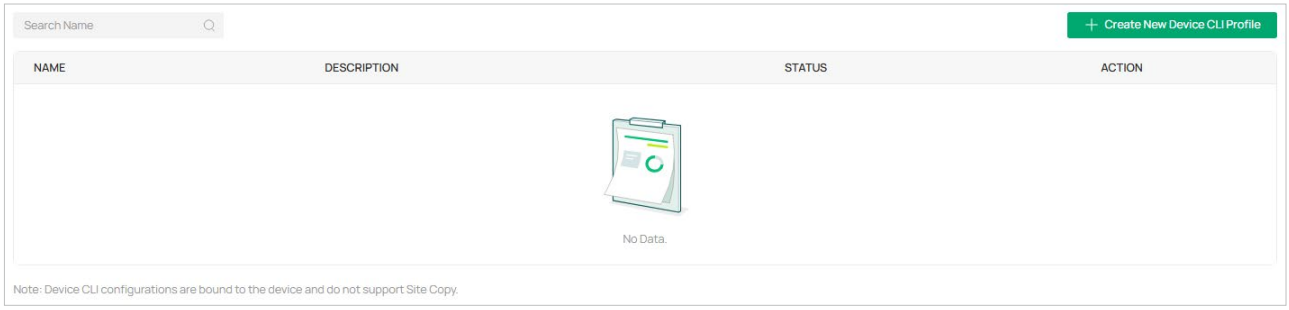
In Device CLI, you can configure the Device CLI settings of the switch.

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.

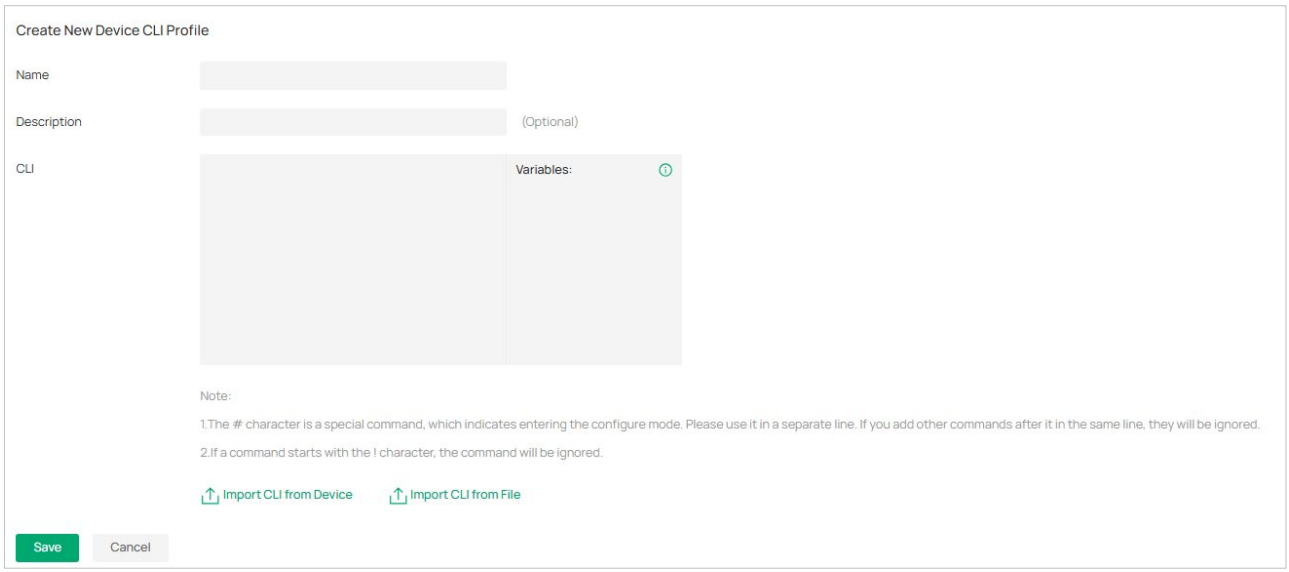
To configure the Device CLI settings of a switch, follow the steps below:

1. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Device CLI.

   Note: Device CLI configurations are bound to the device.



2. Click Create New Device CLI Profile and create a CLI profile according to your needs. Click Save to create the profile. The new profile is in inactive state and will not be applied to the device.



Note:

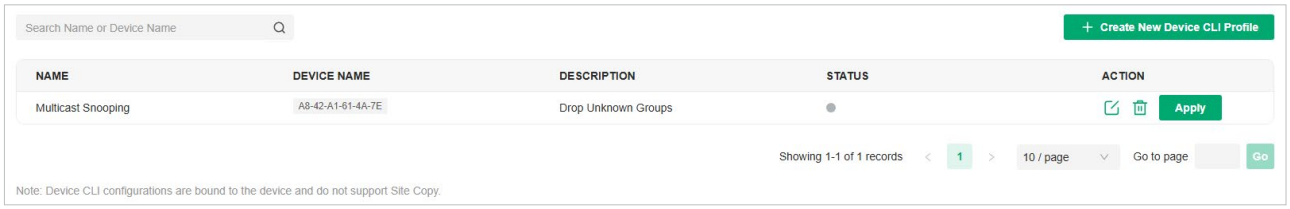
• The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.

• 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.

3. Click Apply to apply the CLI. The profile will change to active state and apply configurations to the device.



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

4. 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.

6. 8 Configure Switch Ports

6. 8. 1 Port Profile

The Switch Port Profile allows you to create port configuration profiles for fast, bulk configuration of switch port parameters.

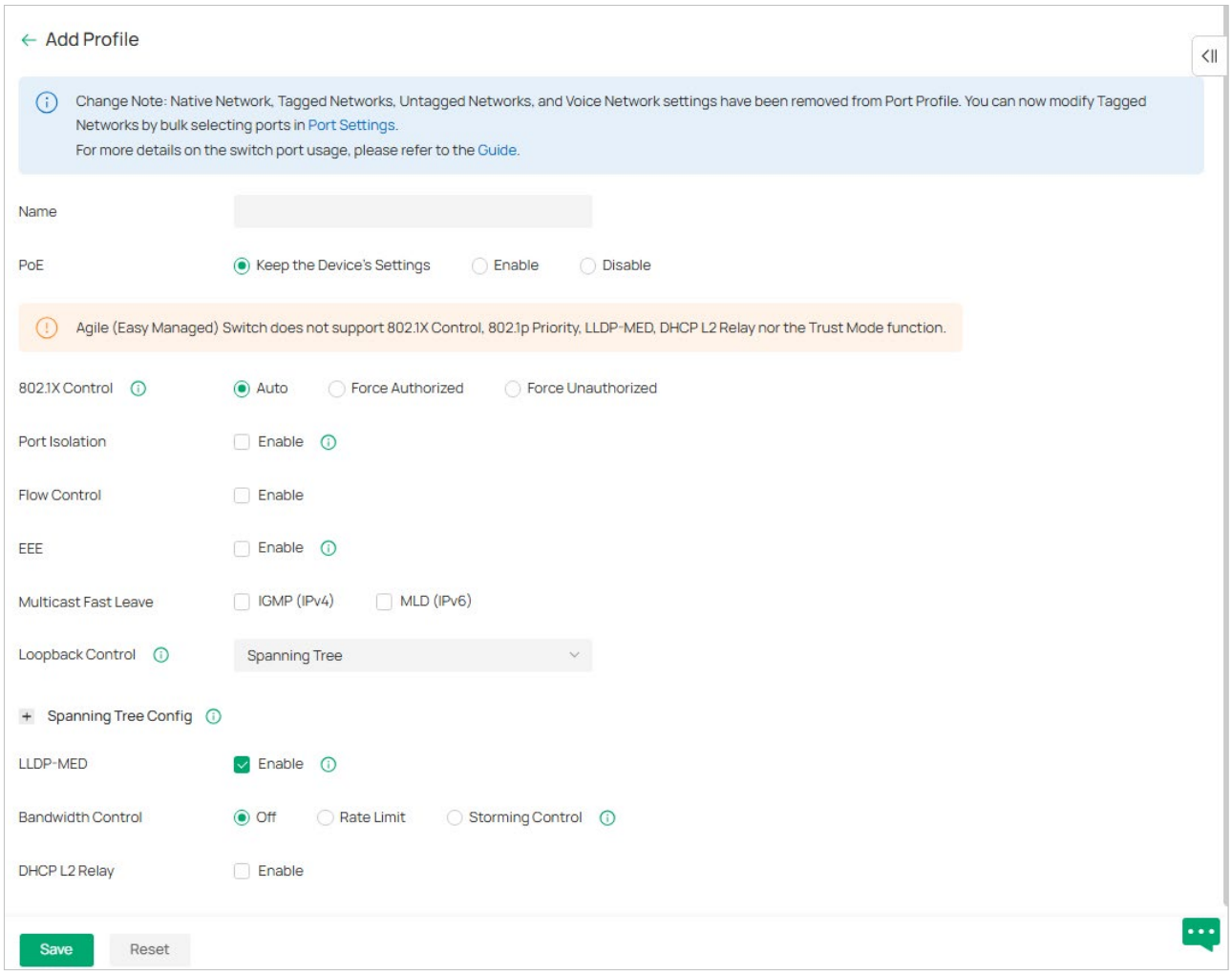
Note: The port network configurations previously included in the Switch Port Profile have been removed. To configure these settings, please go to Port Settings or switch's Properties Window > Manage Device > Ports.

To configure the Port Profile of a switch, follow the steps below:

1. Go to Device Config > Switch > Switch Ports > Port Profile.

   Three port profiles are preconfigured on the controller: Default, Disable, and All. You can click the view icon to check the Disable profile, or click the edit icon to view and edit the Default or All profile.

2. If you want to create a profile, click Add Profile and configure the parameters.



Name	Enter a name to identify the port profile.
PoE	Select the PoE mode for the ports. Keep the Device's Settings: PoE keep enabled or disabled according to the switches' settings. By default, the switches enable PoE on all PoE ports. Enable: Enable PoE on PoE ports. Disable: Disable PoE on PoE ports.
802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to Network Config > 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.
Multicast Fast Leave	After selecting the corresponding protocol, the multicast fast leave feature can be enabled for the port. This allows the switch to immediately stop forwarding multicast traffic to a port when detecting that the last multicast receiver has left the group, improving network bandwidth utilization.
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 current port will be removed from the VLAN. 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.

Spanning Tree Config	If you set Loopback Control to Spanning Tree, configure the following parameters: Priority: Set the port priority. A smaller value indicates higher priority, reducing the likelihood of the port being blocked. Path Cost: Enter the value of the external path cost and internal path cost. External Path Cost determines the root port selection (lowest cost path to the root bridge). Internal Path Cost is used in MSTP to select the root port within an IST (Internal Spanning Tree). Edge Port: Select Enable to set the port as an edge port. Edge ports transition directly from blocking to forwarding during topology changes. Configure ports connected to end devices (e.g., PCs) as edge ports. P2P Link: Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. By default, it is Auto. • Auto: The switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. • Open(Force): A port is set as the one that is connected to a P2P link. You should check the link first. • Close(Force): A port is set as the one that is not connected to a P2P link. You should check the link first. STP Security: STP Security prevents the loops caused by wrong configurations or BPDU attacks. It contains the following options: • Loop Protect: Ports with Root/Alternate/Backup roles enter error-disabled blocking if no BPDUs are received. Automatically recovers when BPDUs resume. Enable this on Root/Alternate/Backup ports. • Root Protect: Ports enter error-disabled blocking upon receiving superior BPDUs. Automatically recovers when superior BPDUs stop. Enable on Designated ports; avoid enabling on Root/Alternate/Backup ports (may cause device unmanageability). • TC Guard: When enabled, ports do not flush MAC address tables upon receiving TC (Topology Change) notifications. • BPDU Protect: Manually configured edge ports enter error-disabled blocking upon receiving BPDUs. Requires manual recovery. Enable on Edge Ports. • BPDU Filter: When enabled, ports neither send nor process BPDUs, disabling loop prevention. Use only on network-edge ports with no loop risk. Enabling on Root/Alternate/Backup ports risks broadcast storms. • BPDU Forward: BPDU Forward will take effect only when the Spanning Tree is disabled for the entire device.
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. Storming Control: With this feature enabled, Omada switches can control the traffic rate or the percentage of total bandwidth used on each port, and set traffic thresholds to ensure network performance (the Kbps value entered must be a multiple of 64).
Ingress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limitv	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Rate Mode	Specifies the rate threshold measurement for storm control. Kbps: Sets an absolute rate threshold in kilobits per second. Ratio: Sets a relative threshold as a percentage of total bandwidth.
Broadcast Threshold	When Storming 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 Storming 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.
Unknown Unicast Threshold	When Storming 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 Storming Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: The port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: The port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.
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 will be added to the profile list.

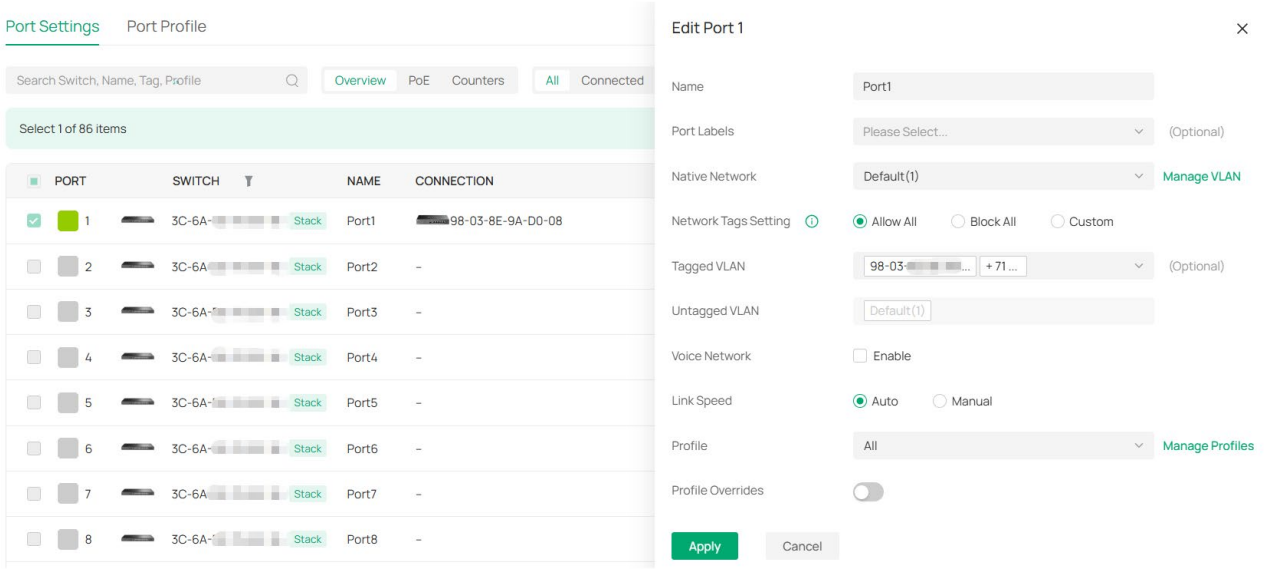
6. 8. 2 Port Settings

The Port Settings page allows you to monitor and manage the ports of all adopted switches.

To configure the Port Settings of a switch, follow the steps below:

1. Go to Device Config > Switch > Switch Ports > Port Settings.
2. Switch between Overview, PoE, and Counters to view the general, PoE-related, and traffic-related information of the ports.
3. To configure a single port, click the edit icon of the port entry. To configure ports in batches, click the checkboxes and then click Edit Selected.

Note: When configuring ports in batches, only common configuration items can be configured and all settings are Keep Existing by default.

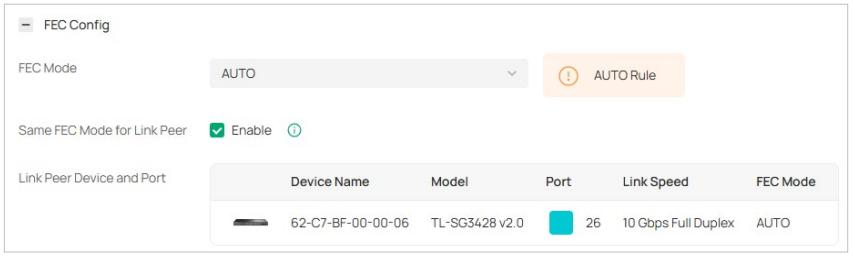


Name	Specify the name of the port.
Port Labels	Set a user-defined label for port identify.
Native Network	Select the native network from all networks. The native network determines the Port VLAN Identifier (PVID) for switch ports. When a port receives an untagged frame, the switch inserts a VLAN tag 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.

Network Tags Setting	Select a network communication mode for the port. Allow All: The port will be automatically tag the configured VLANS.Any tagged traffic with a non existent VLAN ID will be dropped. Block All: The port will be automatically block all VLAN traffic except for the Native Network(PVID).Any tagged traffic with a other VLAN ID will be dropped. Custom: VLAN Management can be customized to either tag specific VLANS only. If you select Custom, set the following parameters: Tagged VLAN: 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 VLAN: 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	Enable this option and select a network that connects VoIP devices like IP phones as the Voice Network. The Voice Network feature configures IP Phones via the LLDP-MED protocol to ensure their transmitted packets carry a specific VLAN tag, directing voice traffic through the designated VLAN. Enabling this feature will automatically activate LLDP-MED on the port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Profile	Set the switch port configuration file to quickly batch configure switch port parameters.
Profile Overrides	Click the checkbox to override the applied profile if needed. The parameters to be configured vary in Operation modes,

For switch ports supporting FEC (Forward Error Correction), FEC parameters will be displayed.

FEC is a technology used to enhance the reliability of data transmission by adding redundant information to the data being sent. This allows the receiver to detect and correct errors that may have occurred during transmission. FEC is commonly used in environments requiring high reliability, particularly in long-distance fiber optic transmissions or networks with high bit error rates. It helps ensure a stable network and high data transmission quality.

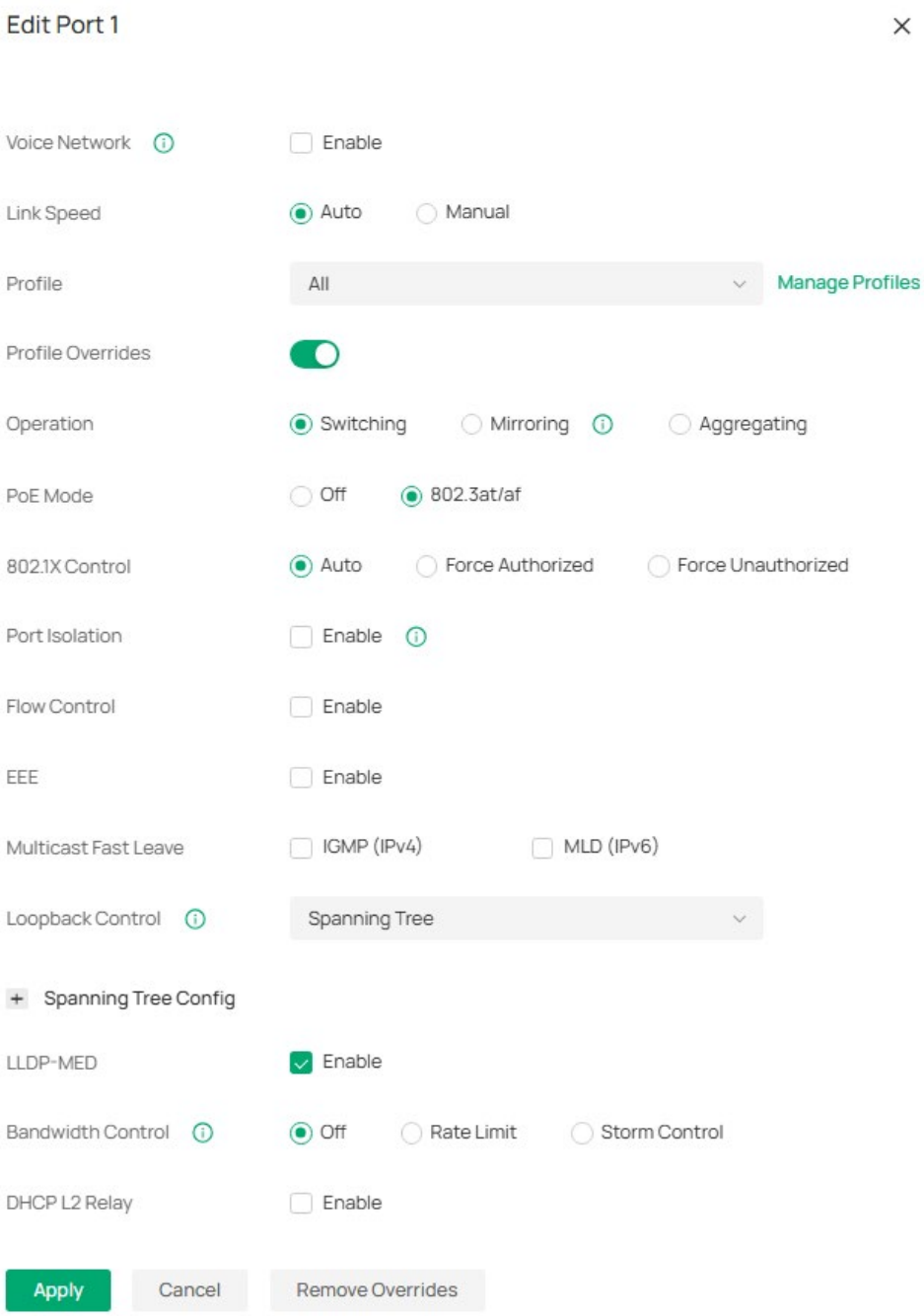


FEC Mode	Select the FEC Mode. By default, the port supporting the FEC function would have FEC Mode as AUTO. **Note:** 1. The function requires both sides using the same FEC mode, otherwise the Link cannot be established. 2. Each Link Speed has a different list of configurable FEC modes, please try changing the link speed manually if can't find desired FEC mode. 3. Ports in the LAG group do not support configuring the FEC mode.
Same FEC Mode for Link Peer	If this option is enabled and the peer is also a managed Omada Switch with firmware supporting FEC report function, it would synchronize local Link speed & FEC configuration to the peer port, show the peer's FEC configuration, and the available options are limited to those supported by both ends for your convenience to adjust accordingly.

4. If you enable Profile Overrides, select an operation mode and configure the parameters.

   • Override the Applied Profile

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



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

802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to Network Config > Authentication > 802.1X. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, and the client connected to the port cannot authenticate with any means. The switch cannot provide authentication services to the client through the port.
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.
Multicast Fast Leave	Select IGMP (IPv4) and/or MLD (IPv6) to allow the port to immediately stop forwarding multicast traffic to a client when it receives an IGMP and/or MLD Leave message, instead of waiting for the next group-specific query. This process improves network efficiency by saving bandwidth and resources, especially in networks with many hosts or frequent group departures.
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 current port will be removed from the VLAN. 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. To make sure Spanning Tree takes effect on the port, go to the Config tab and enable Spanning Tree on the switch.

Spanning Tree Config	If you set Loopback Control to Spanning Tree, configure the following parameters: Priority: Set the port priority. A smaller value indicates higher priority, reducing the likelihood of the port being blocked. Path Cost: Enter the value of the external path cost and internal path cost. External Path Cost determines the root port selection (lowest cost path to the root bridge). Internal Path Cost is used in MSTP to select the root port within an IST (Internal Spanning Tree). Edge Port: Select Enable to set the port as an edge port. Edge ports transition directly from blocking to forwarding during topology changes. Configure ports connected to end devices (e.g., PCs) as edge ports. P2P Link: Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. By default, it is Auto. • Auto: The switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. • Open(Force): A port is set as the one that is connected to a P2P link. You should check the link first. • Close(Force): A port is set as the one that is not connected to a P2P link. You should check the link first. STP Security: STP Security prevents the loops caused by wrong configurations or BPDU attacks. It contains the following options: • Loop Protect: Ports with Root/Alternate/Backup roles enter error-disabled blocking if no BPDUs are received. Automatically recovers when BPDUs resume. Enable this on Root/Alternate/Backup ports. • Root Protect: Ports enter error-disabled blocking upon receiving superior BPDUs. Automatically recovers when superior BPDUs stop. Enable on Designated ports; avoid enabling on Root/Alternate/Backup ports (may cause device unmanageability). • TC Guard: When enabled, ports do not flush MAC address tables upon receiving TC (Topology Change) notifications. • BPDU Protect: Manually configured edge ports enter error-disabled blocking upon receiving BPDUs. Requires manual recovery. Enable on Edge Ports. • BPDU Filter: When enabled, ports neither send nor process BPDUs, disabling loop prevention. Use only on network-edge ports with no loop risk. Enabling on Root/Alternate/Backup ports risks broadcast storms. • BPDU Forward: BPDU Forward will take effect only when the Spanning Tree is disabled for the entire device.
LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP (Voice over Internet Protocol) devices.

Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and specify traffic threshold on each port to make good use of network bandwidth. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storming Control: With this feature enabled, Omada switches can control the traffic rate or the percentage of total bandwidth used on each port, and set traffic thresholds to ensure network performance (the Kbps value entered must be a multiple of 64).
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.
Rate Mode	Specifies the rate threshold measurement for storm control. Kbps: Sets an absolute rate threshold in kilobits per second. Ratio: Sets a relative threshold as a percentage of total bandwidth.
Broadcast Threshold	When Storming 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 Storming 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.
Unknown Unicast Threshold	When Storming 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 Storming Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: The port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: The port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.

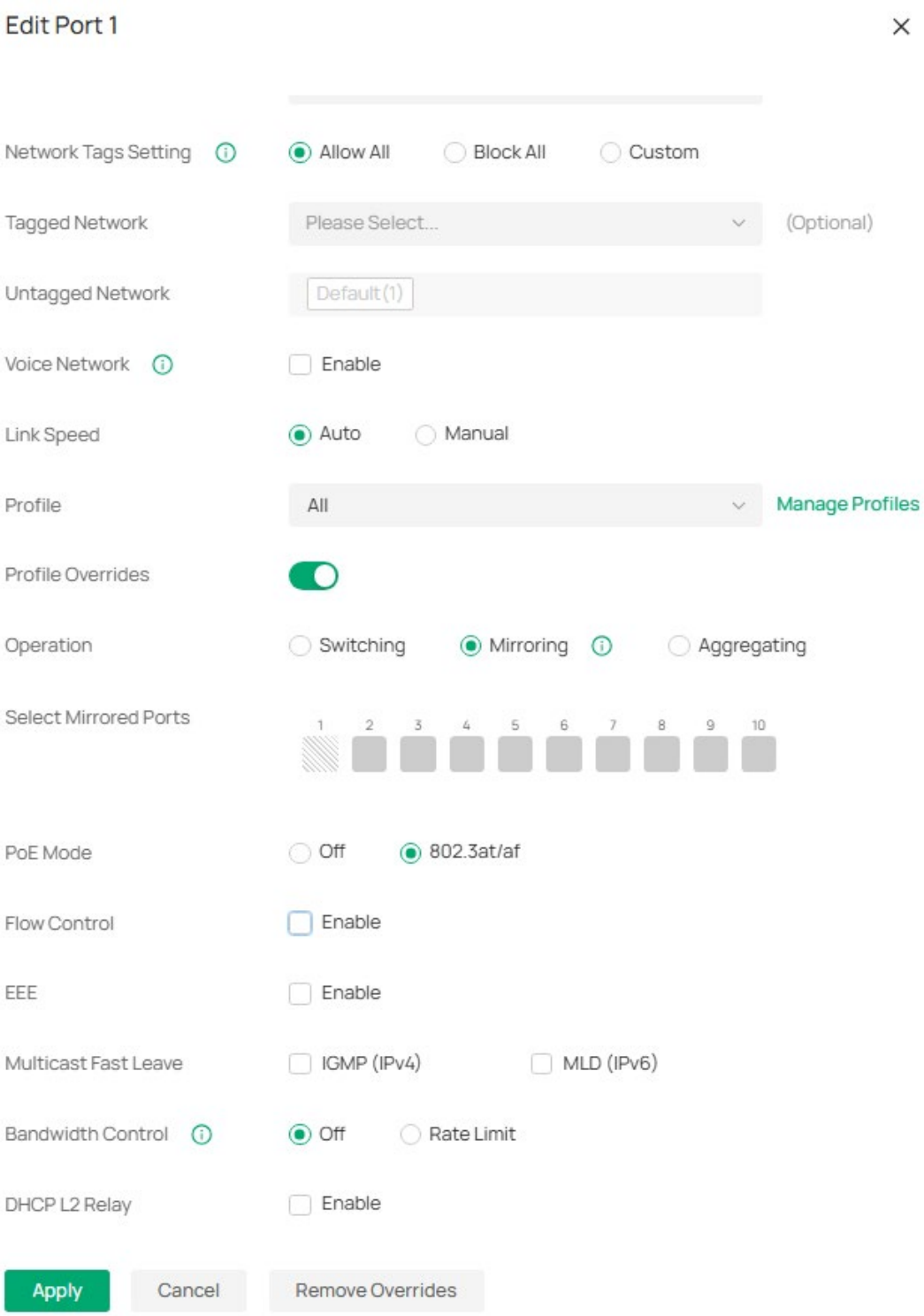
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network, which takes the Layer 2 DHCP communications (Discover, Request, etc.) and forwards them to a specified IP address (your DHCP server). Format: Select the format of option 82 sub-option value field. • Normal: The format of sub-option value field is TLV (type-length-value). • Private: The format of sub-option value field is just value. Circuit ID: Omada switches preset a default Circuit ID in TLV (Type, Length, and Value) format. You can also customize it if needed. Remote ID: Omada switches preset a default Remote ID in TLV (Type, Length, and Value) format. You can also customize them if needed.
802.1p Priority	Specify the port-to-802.1p priority mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p queue mappings.
Trust Mode	Select the trusted priority mode for the desired port. The switch will process the ingress packets according to the trusted priority mode. Untrusted: In this mode, the packets will be processed according to the port priority configuration. Trust 802.1p: In this mode, the packets will be processed according to the 802.1p priority configuration. Trust DSCP: In this mode, the packets will be processed according to the DSCP priority configuration.

• Configure a Mirroring Port

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

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

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

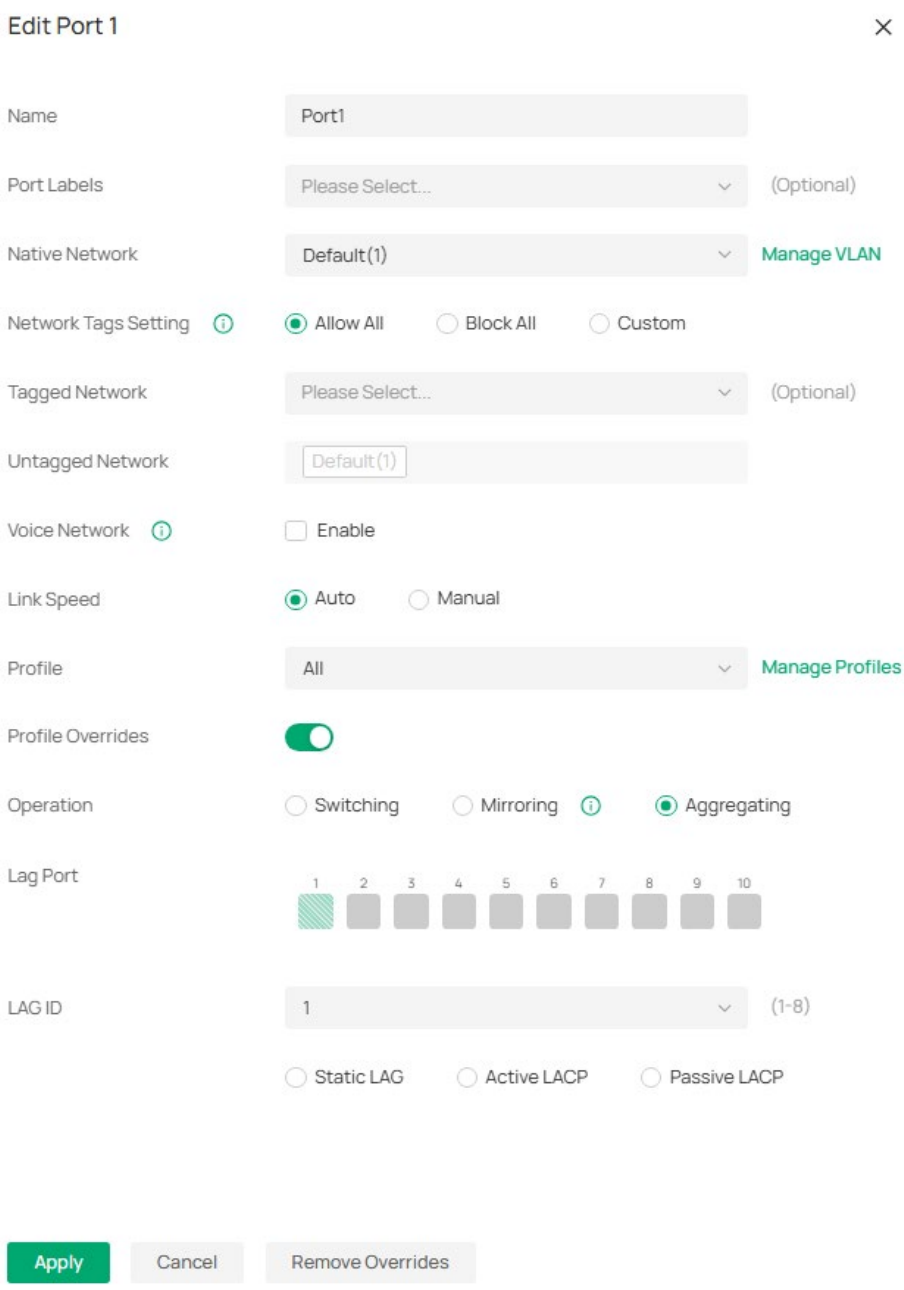


PoE Mode	(Only for PoE ports) Select the PoE mode for the port. Off: Disable PoE on the PoE port. 802.3bt/at/af: Enable PoE on the PoE port.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.

EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Multicast Fast Leave	Select IGMP (IPv4) and/or MLD (IPv6) to allow the port to immediately stop forwarding multicast traffic to a client when it receives an IGMP and/or MLD Leave message, instead of waiting for the next group-specific query. This process improves network efficiency by saving bandwidth and resources, especially in networks with many hosts or frequent group departures.
Bandwidth Control	Bandwidth control optimizes network performance by limiting the bandwidth of specific sources. Off: Disable bandwidth control on the port. Rate Limit: Enable bandwidth control on the port, and you need to specify the ingress and/or egress rate limit.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized.
Egress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network, which takes the Layer 2 DHCP communications (Discover, Request, etc.) and forwards them to a specified IP address (your DHCP server). 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. Circuit ID: Omada switches preset a default Circuit ID in TLV (Type, Length, and Value) format. You can also customize it if needed. Remote ID: Omada switches preset a default Remote ID in TLV (Type, Length, and Value) format. You can also customize them if needed.
802.1p Priority	Specify the port-to-802.1p priority mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p queue mappings.

• Configure a LAG

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


Edit Port 1
Name
Port1
Port Labels
Please Select...
(Optional)
Native Network
Default(1)
Manage VLAN
Network Tags Setting
Allow All
Block All
Custom
Tagged Network
Please Select...
(Optional)
Untagged Network
Default(1)
Voice Network
Enable
Link Speed
Auto
Manual
Profile
All
Manage Profiles
Profile Overrides
Operation
Switching
Mirroring
Aggregating
Lag Port
1 2 3 4 5 6 7 8 9 10
LAG ID
1
(1-8)
Static LAG
Active LACP
Passive LACP
Apply
Cancel
Remove Overrides

Configuration Guidelines:

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

To configure a new LAG, select other ports to be added to the LAG, specify the LAG ID, and choose a LAG type. Click Apply. To discard the modifications, click Remove Overrides and all profile configurations become the same as the applied profile. For other parameters, configure them under the LAG tab.

LAG ID	Specify the LAG ID of the LAG. Note that the LAG ID should be unique. The valid value of the LAG ID is determined by the maximum number of LAGs supported by your switch. For example, if your switch supports up to 14 LAGs, the valid value ranges from 1 to 14.
Static LAG	In Static LAG mode, the member ports are added to the LAG manually.
Active LACP / Passive LACP	LACP extends the flexibility of the LAG configurations. In LACP, the switch uses LACPDU (Link Aggregation Control Protocol Data Unit) to negotiate the parameters with the peer end. In this way, the two ends select active ports and form the aggregation link. Active LACP: In this mode, the port will take the initiative to send LACPDU. Passive LACP: In this mode, the port will not send LACPDU before receiving the LACPDU from the peer end.

Chapter 7

Manage APs

This chapter provides information for centrally managing APs via the Fusion gateway. The chapter includes the following sections:

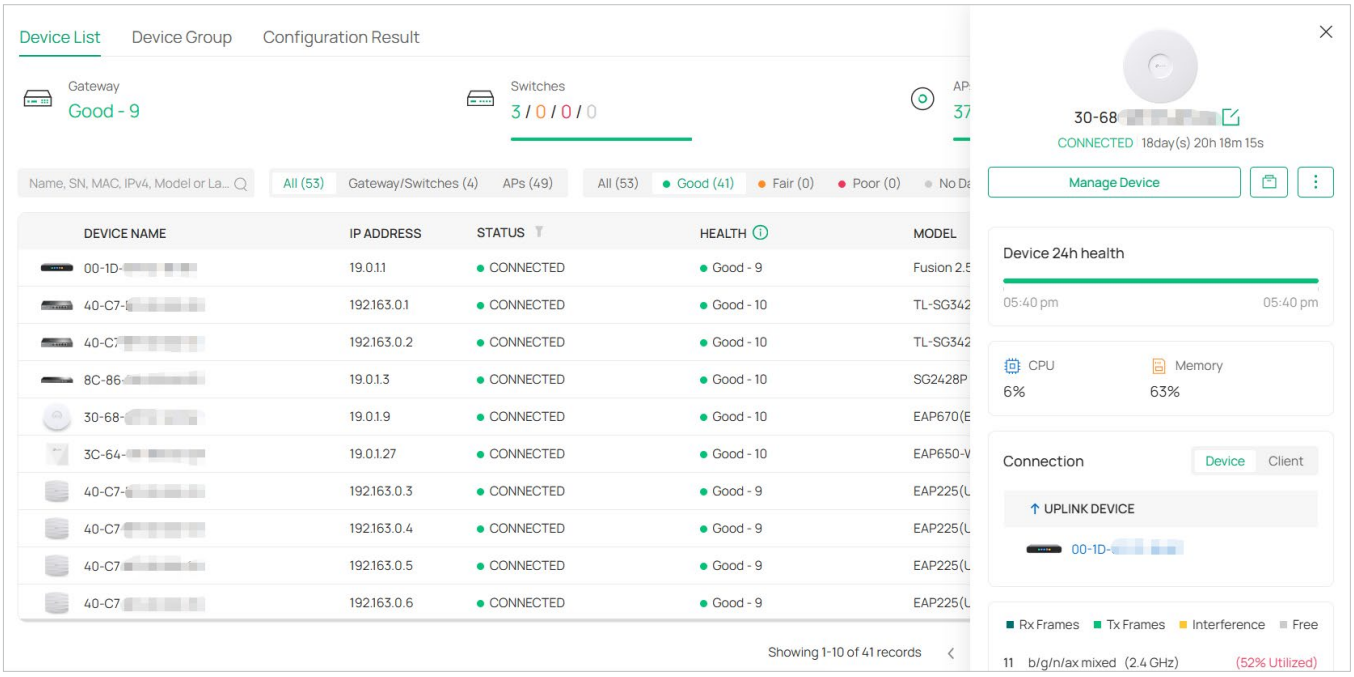
7. 1 Manage the AP

Go to Devices > Device List. In the device list, click an AP, then you can monitor and manage it in the Properties window and Device Management window.

7. 1. 1 Properties Window

The Properties window displays the device's basic information, health status, connection information, and more.

Note: The available functions in the window may vary by device model and status.



Quick Operations

Click the ⋮ icon and choose an operation to quickly operate the device.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. After upgraded, the device will reboot and be readopted by the controller.
Copy Configuration	Select another device to copy its configurations. **Note:** Only devices of the same model as the current device will be displayed.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.
Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.

IntelliRecover	(Only for the AP directly connected to the PoE switch) Click to enable the IntelliRecover function for the device so that it can be added to the IntelliRecover monitoring list. IntelliRecover can help you monitor the status of PoE devices, automatically repairing abnormal devices.
Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.

Network Tools

Click the icon and choose a network tool to analyze the network.

Network Check	Test the device connectivity via ping or traceroute.
Packet Capture	Capture packets for network troubleshooting.
Terminal	Open Terminal to execute CLI or Shell commands.
Link Speed Test	(Only for Bridge APs supporting link speed test and already form a bridge group) Click to test the link speed between the Main AP and Client AP.

7. 1. 2 Device Management Window

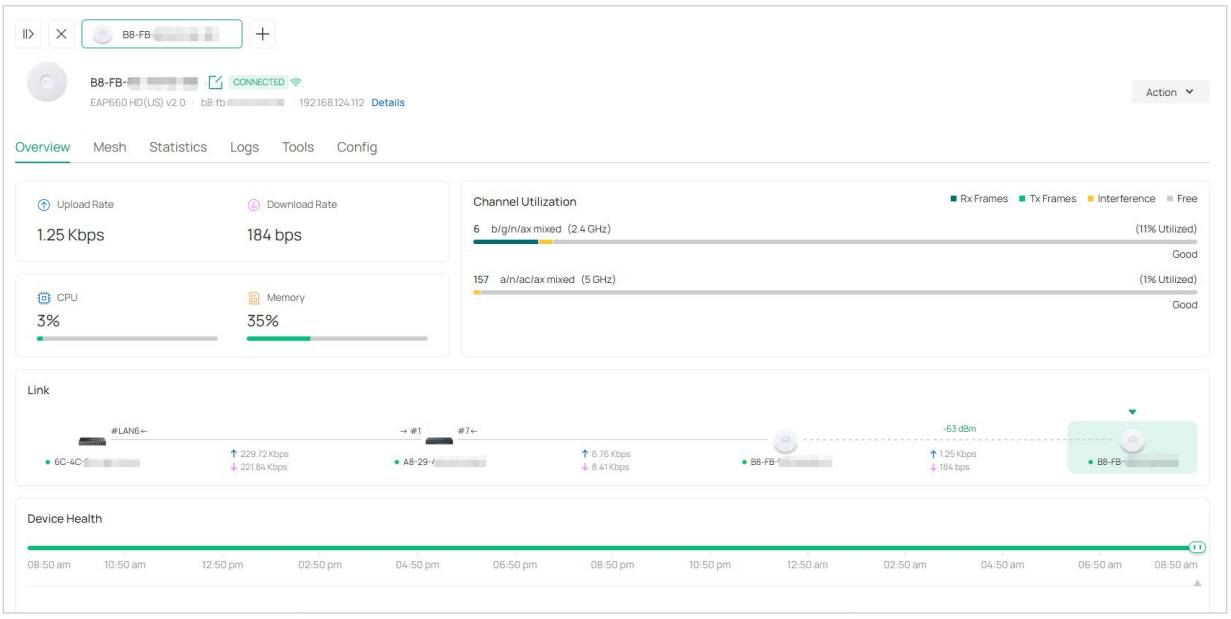
Click Manage Device to open the Device Management window to view more device details and change device settings.

In the management window, you can click + and select one or more devices to open new management windows, click the icon in the top left to minimize the windows to the icon in the right side, and click the icon to reopen the minimized windows.

You can also click each tab to monitor and manage the device. The tabs available may vary by model.

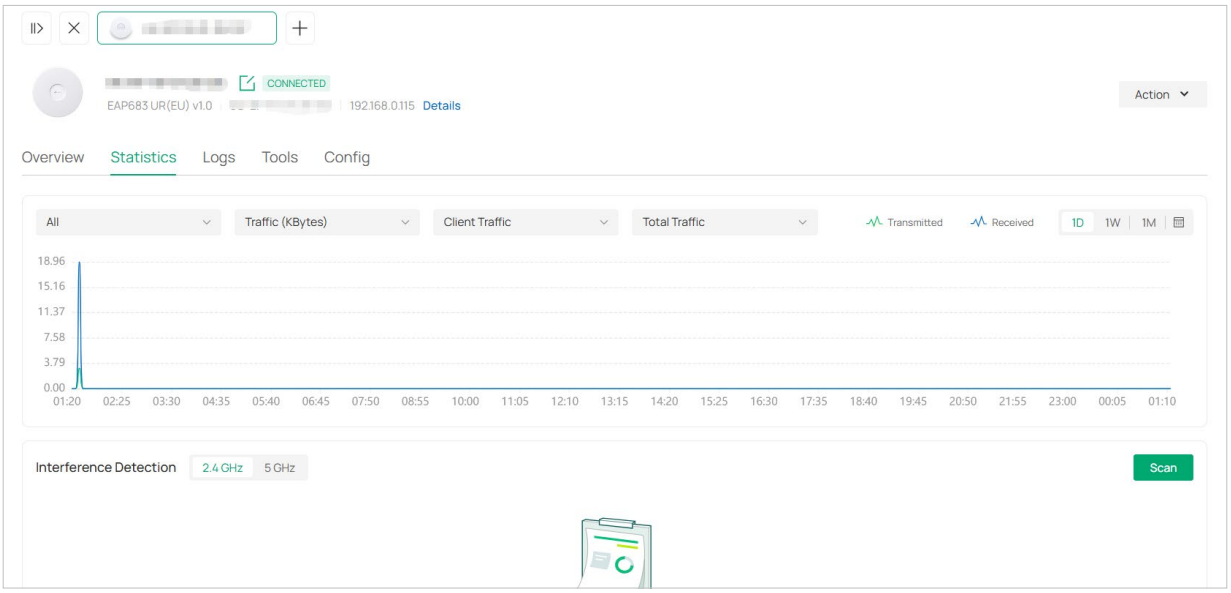
Overview

In Overview, you can get an overview of the device, such as device status, device health, link status, online time, current clients, and more.



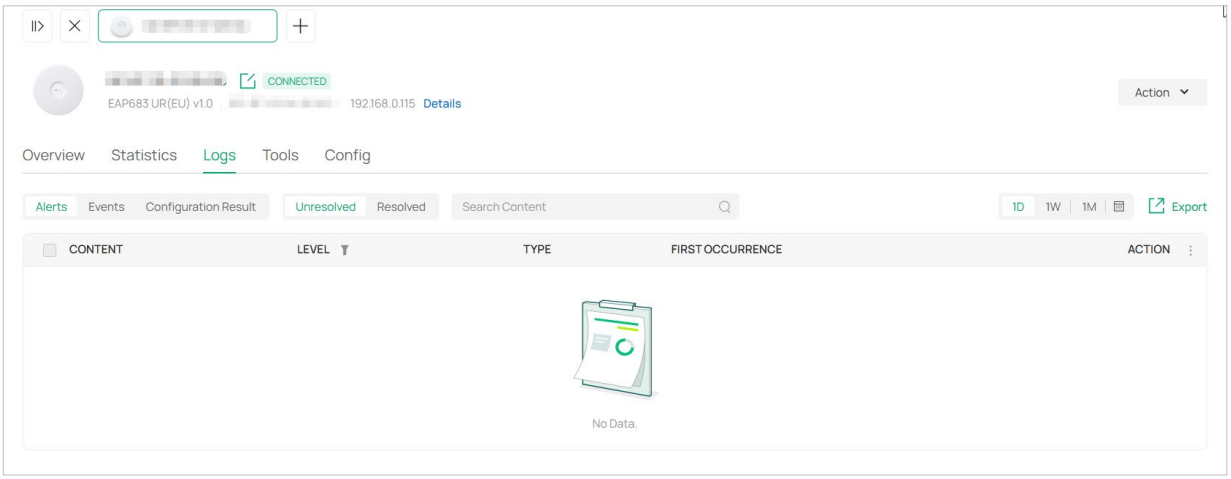
Statistics

In Statistics, you can check the traffic statistics of the device. You can also perform RF Scanning, interface detection, and/or spectral analysis if the device firmware supports these functions.



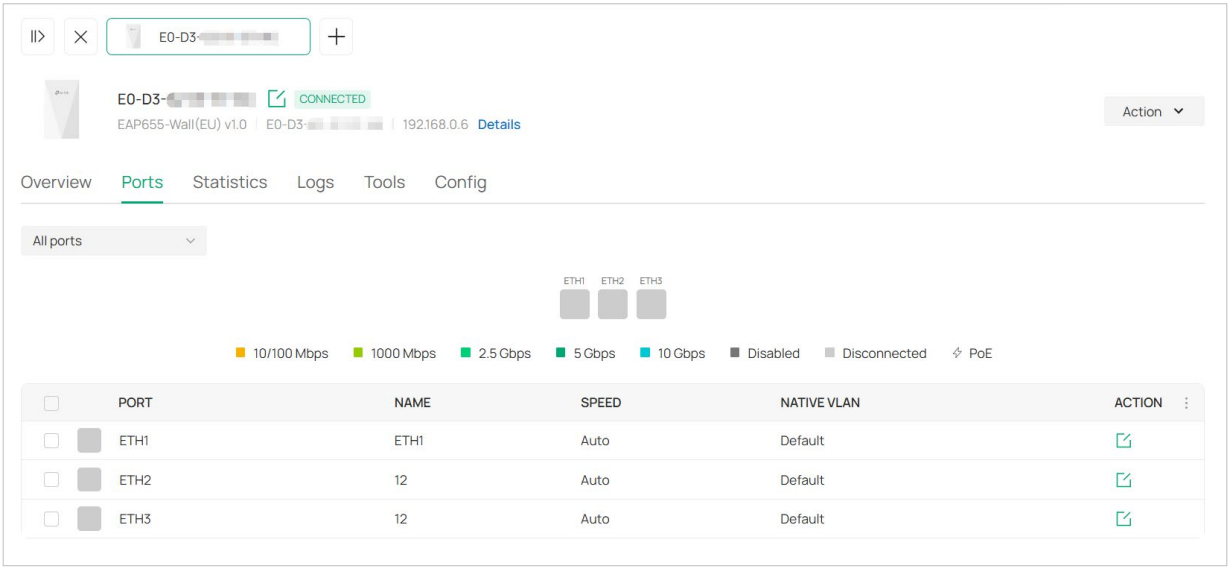
Logs

In Logs, you can check the logs of the device, such as alerts, events, and configuration result.



Ports (Only for APs with multiple LAN ports)

In Ports, you can view the port status and statistics and edit port settings.



To configure a port, click the edit icon in the Action column. Port settings may vary by port type.

Name	Specify the name of the port.
Status	Click the box to enable or disable the port.
VLAN	Configure the uplink port VLAN corresponding to the SSID. Default: Using untagged transmission. Custom: Enter the PVID (Port VLAN Identifier). When a port receives an untagged frame, the AP inserts a VLAN tag to the frame based on the PVID before forwarding it.
PoE Out	(Only for APs with the PoE out port) Enable this function to supply power to the connected device on this port.

Mesh (Only for pending/connected/isolated devices supporting Mesh)

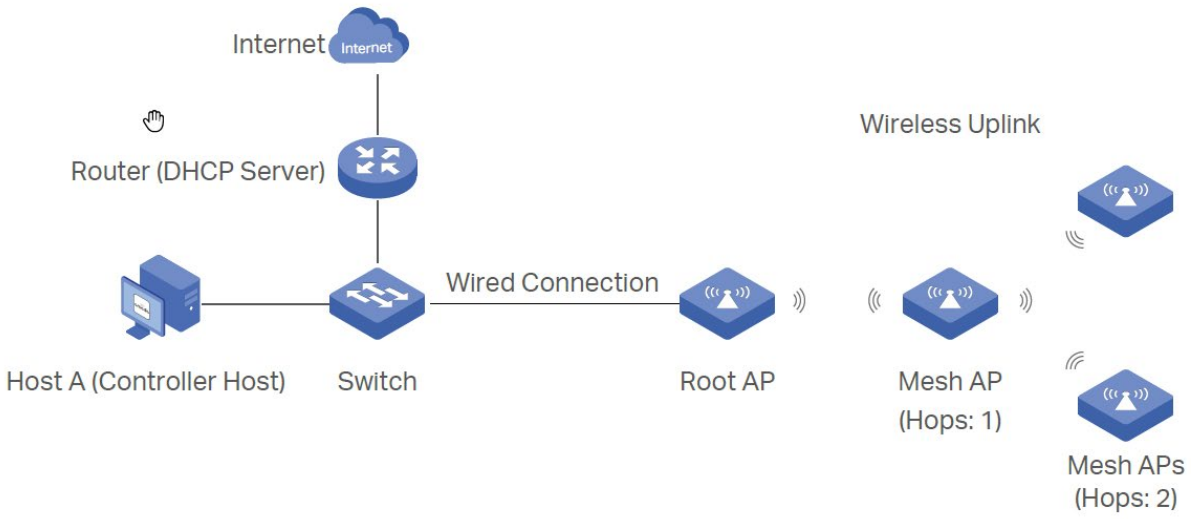
Mesh is used to establish a wireless network or expand a wired network through wireless connection on 5 GHz radio band. In practical application, it can help users to conveniently deploy APs without requiring Ethernet cable. After mesh network establishes, the APs can be configured and managed in the controller in the same way as wired APs. Meanwhile, because of the ability to self-organize and self-configure, mesh also can efficiently reduce the configuration.

Note that only certain AP models support Mesh.

To understand how mesh can be used, the following terms will be introduced:

Root AP	The AP is managed by the Controller with a wired data connection that can be configured to relay data to and from mesh APs (downlink AP).
Isolated AP	When the AP which has been managed by the Controller before connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state.
Mesh AP	An isolated AP will become a mesh AP after establishing a wireless connection to the AP with network access.
Uplink AP/Downlink AP	Among mesh APs, the AP that offers the wireless connection for other APs is called uplink AP. A Root AP or an intermediate AP can be the uplink AP. And the AP that connects to the uplink AP is called downlink AP. An uplink AP can offer direct wireless connection for 4 downlink APs at most.
Wireless Uplink	The action that a downlink AP connects to the uplink AP.
Hops	In a deployment that uses a root AP and more than one level of wireless uplink with intermediate APs, the uplink tiers can be referred to by root, first hop, second hop and so on. The hops should be no more than 3.

A common mesh network is shown as below. Only the root AP is connected by an Ethernet cable, while other APs have no wired data connection. Mesh allows the isolated APs to communicate with pre-configured root AP on the network. Once powered up, factory default or unadopted APs can detect the AP in range and make itself available for adoption in the controller.



After all the APs are adopted, a mesh network is established. The APs connected to the network via wireless connection also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

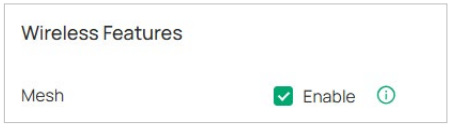
To build a mesh network, follow the steps below:

1) Enable Mesh function.

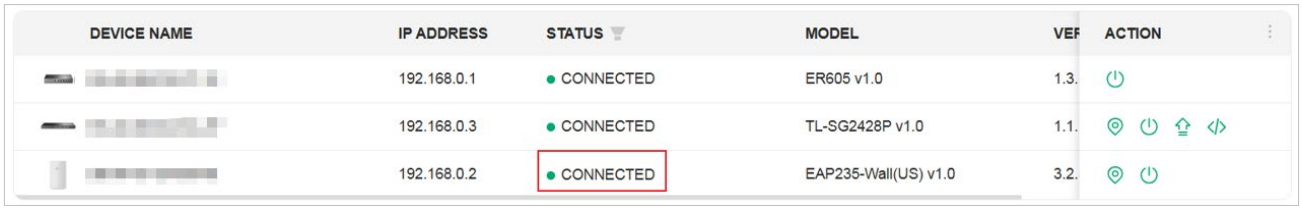
2) Adopt the Root AP.

3) Set up wireless uplink by adopting APs in Pending (Wireless) or Isolated status.

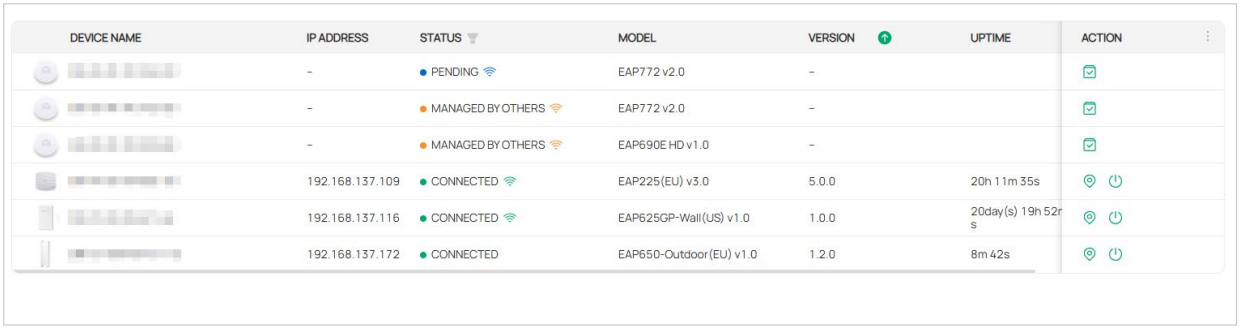
1. Go to Network Config > General Settings > Network Application Settings > Wireless Features and make sure Mesh is enabled.



2. Go to Devices to make sure that the Root AP has been adopted by the controller. The status of the Root AP is Connected.



3. Install the AP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The APs that is waiting for Wireless Uplink includes two cases: factory default APs and APs that has been managed by the controller before. Go to Devices to adopt an AP in Pending (Wireless) status or link an isolated AP.



   1) For the factory default AP, after powering on the device, the AP will be in Pending (Wireless) status. Go to Devices, click Add Devices, choose Auto Find, then click the adopt icon in the Action column to adopt the AP.

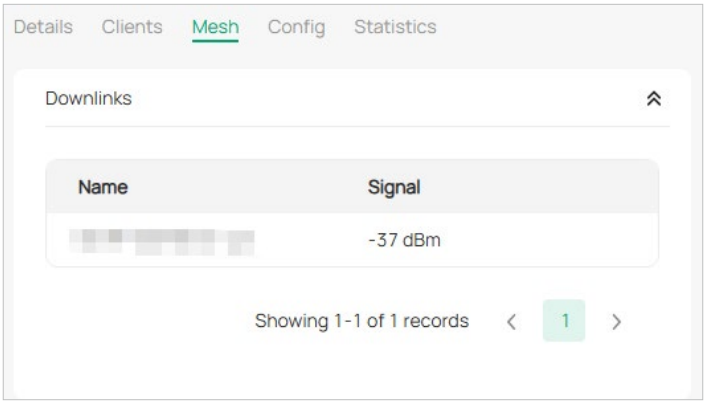
   2) For the AP that has been managed by the Controller before and cannot reach the gateway, it goes into Isolated status in the Devices list when it is discovered by controller again. Click the adopt icon in the Action column to connect the Uplink AP.

Once mesh network has been established, the AP can be managed by the controller in the same way

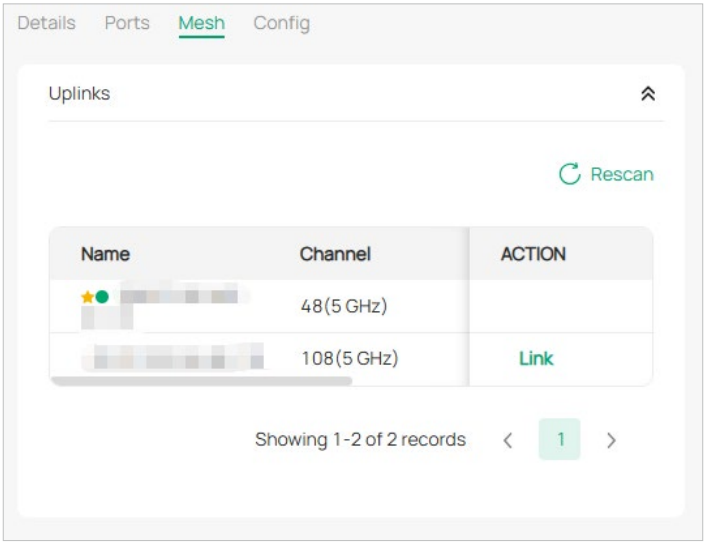
as a wired AP.

To view mesh info, click the mesh AP in the device list, click Manage Device, and go to the Mesh page.

In Mesh, if the selected AP is an uplink AP, this page lists all downlink APs connected to the AP.



If the selected AP is a downlink AP, this page lists all available uplink APs and their channel, signal strength, hop, and the number of downlink APs. You can click Rescan to search the available uplink APs and refresh the list, and click Link to connect the uplink AP and build up a mesh network.

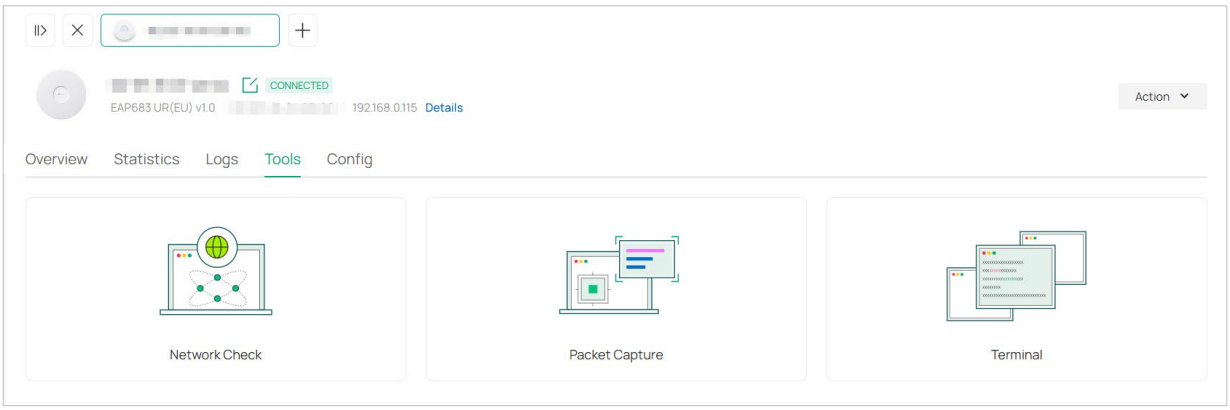


Tips:

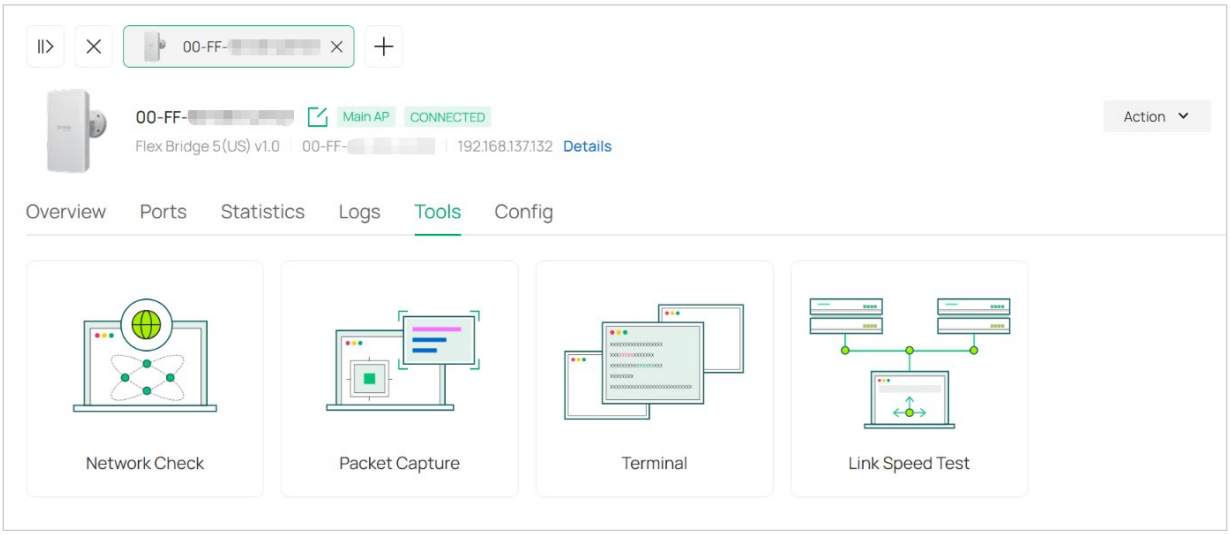
- You can manually select the priority uplink AP that you want to connect in the uplink AP list. To build a mesh network with better performance, we recommend that you select the uplink AP with the strongest signal, least hop and least downlink AP.
- Auto Failover is enabled by default in Network Application Settings, and it allows the controller automatically select an uplink AP for the isolated AP to establish Wireless Uplink. And the controller will automatically select a new uplink AP for the mesh APs when the original uplink fails.

Tools

In Tools, you can use network tools to test the device connectivity or Open Terminal to execute CLI or Shell commands.



For Bridge APs supporting link speed test and already form a bridge group, you can test the link speed between the Main AP and Client AP.

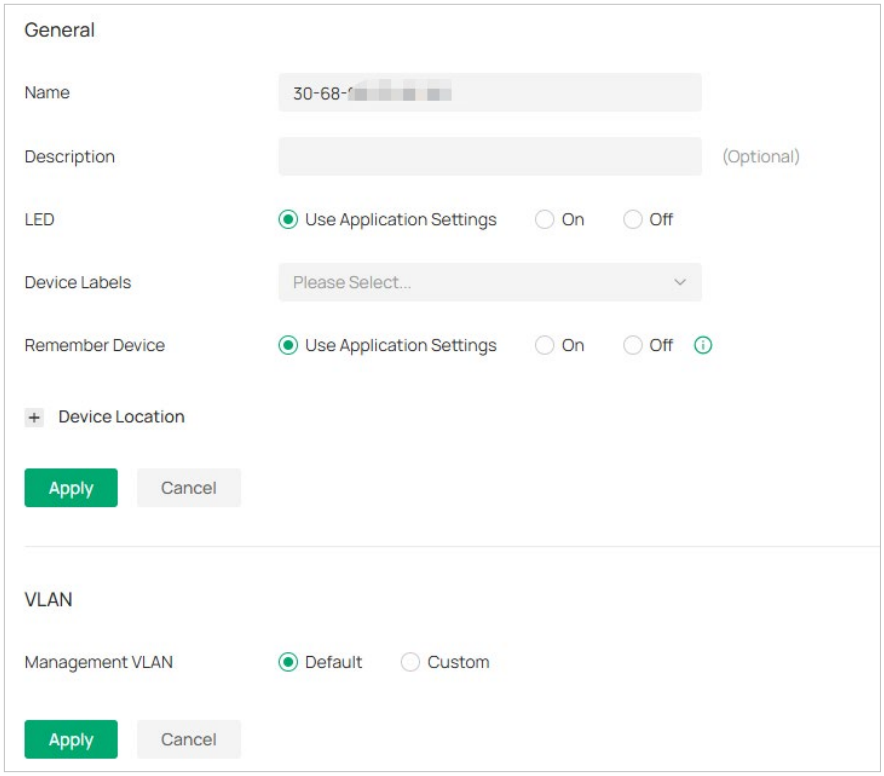


7. 2 Configure General Settings

In General Settings, you can specify the device name, control the LED and Wi-Fi, configure the device address, and more.

To configure general settings of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > General.
2. Configure the parameters.



Name	Specify a name of the device.
Description	(Optional) Enter a description for identification.
LED	Select the way that device's LEDs work. Use Application Settings: The device's LED will work following the settings of the application. On/Off: The device's LED will keep on/off.
Wi-Fi Control	(Only for Certain APs) Enable Wi-Fi Control, and it will take effect only when the LED feature is enabled. After enabling Wi-Fi Control, you can press the LED button on the AP to turn on/off the Wi-Fi and LED at the same time.
Device Labels	Select a tag from the drop-down list or create a new tag to categorize the device.
Remember Device	With this function, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.

Disable Hardware Reset	When enabled, the hardware reset button will be ineffective when the device is managed by the controller, and it will be effective again when the device is disconnected from the controller.
Device Location	GPS Enable: (Only for models with the with GPS chip) When enabled, the device can actively obtain GPS data and update its location. Address/Longitude/Latitude: Configure the parameters according to where the device is located. These fields are optional.
Management VLAN	Specify the VLAN ID of the management VLAN. Only the hosts in the Management VLAN can log in to the AP via the Ethernet port. This provides a safer method to manage the AP. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the Management VLAN Configuration Guide before you configure this feature.

To configure general settings in batches, follow the steps below:

1. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.
2. Select the APs for batch configuration and click Config.
3. In Genral settings, configure the parameters. The parameters are the same as or fewer than those for configuring a single AP. You can keep existing settings or change them according to actual needs.

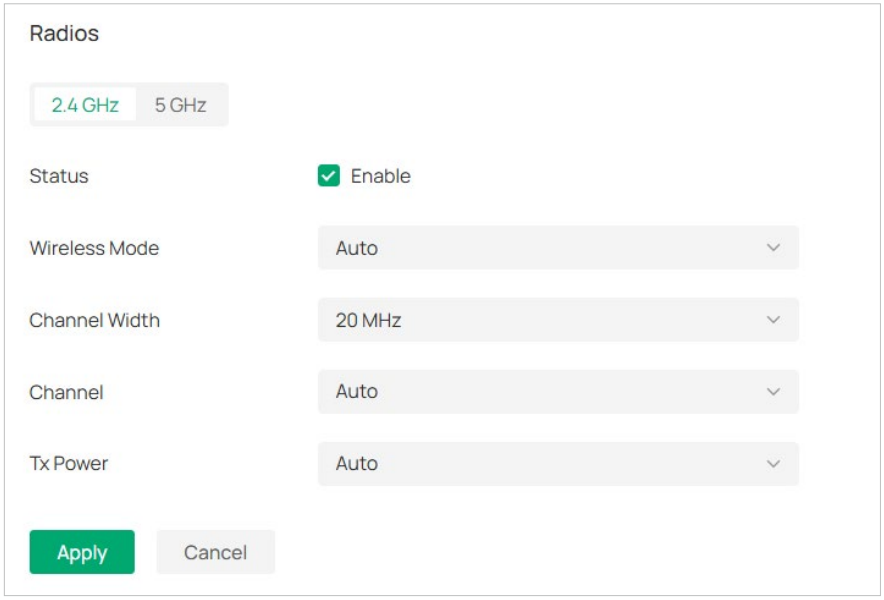
7. 3 Configure Wireless Settings

7. 3. 1 Radio Settings

In Radios, you can control how and what type of radio signals the AP emits.

To configure radio settings of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Wireless > Radios.
2. Select each band and configure the parameters. Different models support different bands.



AFC	(For Wi-Fi 7 APs of US version) Enable this feature to use the 6GHz band normally. The AFC (Automated Frequency Coordination) feature adjusts the transmission power of the 6 GHz band according to your geographic location to meet regulatory requirements.
Installation Type	(For Outdoor APs of non-US versions) Choose the installation mode of the device. Default Mode: In this mode, the device will adjust the Indoor/Outdoor mode of the 5GHz/6GHz band according to local regulations. This mode is recommended. Indoor Mode / Outdoor Mode: If selected, the device will adjust 5GHz/6GHz channel power bandwidth parameters for indoor / outdoor usage.
Status	If you disable the frequency band, the radio on it will turn off.
Wireless Mode	Specify the wireless mode of the band. Different bands have different available options. We recommend using the default value.
Channel Width	Specify the channel width of the band. Different bands have different available options. We recommend using the default value.

Channel	Specify the operation channel of the device to improve wireless performance. If you select Auto for the channel setting, the device scans available channels and selects the channel where the least amount of traffic is detected.
Channel Range	(Only for certain models) Specify the channel range of the device to improve wireless performance.
Tx Power	Specify the Tx Power (Transmit Power) in the 4 options: Low, Medium, High and Custom. The actual power of Low, Medium and High are based on the minimum transmit power (Min. Txpower) and maximum transmit power (Max. TxPower), which may vary in different countries and regions. Low: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (round off the value) Medium: Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (round off the value) High: Max. TxPower Custom: Specify the value manually.

To configure radio settings in batches, follow the steps below:

1. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.
2. Select the APs for batch configuration and click Config.
3. In Wireless > Radios settings, configure the parameters. The parameters are the same as or fewer than those for configuring a single AP. You can keep existing settings or change them according to actual needs.

7. 3. 2 WLAN Settings

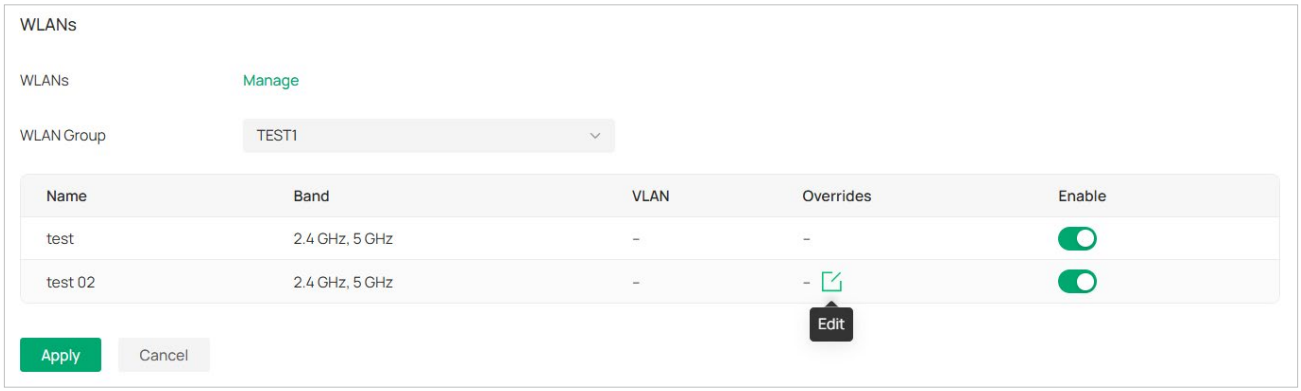
The system has a default WLAN group, and APs adopted will be applied with the default WLAN group by default.

In WLANs, you can change the WLAN group of the AP or specify a different SSID and password to override the SSID in the WLAN group. After that, clients can access the AP's network via the new SSID and password.

To configure WLAN settings of an AP, follow the steps below:

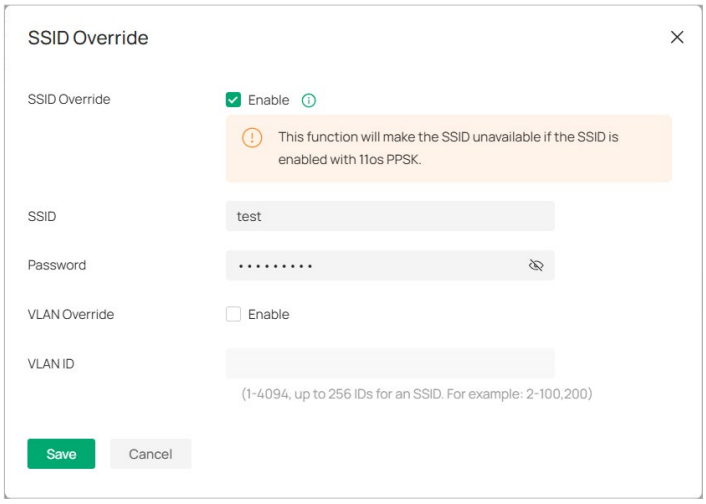
1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Wireless > WLANs.

2. Configure the parameters.



WLANs	Click Manage to redirect to the WLAN group page to create and edit WLAN groups. For detailed instructions about WLAN groups, refer to the relavant chapter.
WLAN Group	Choose a WLAN group to apply its preset wireless network settings to the AP.

If you want to override an SSID of the WLAN group, hover on it, then click the edit icon in the Overrides column. Set the parameters.



SSID Override	Enable or disable SSID Override on the AP. If enabled, specify the new SSID and password to override the current one. Note: If the SSID is enabled with 11os PPSK, the override function will make the SSID unavailable!
VLAN Override	Enable or disable VLAN Override on the AP. If enabled, enter a VLAN ID to override the current one.

To configure WLAN settings in batches, follow the steps below:

1. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.
2. Select the APs for batch configuration and click Config.
3. In Wireless > WLANs settings, configure the parameters. The parameters are the same as or fewer than those for configuring a single AP. You can keep existing settings or change them

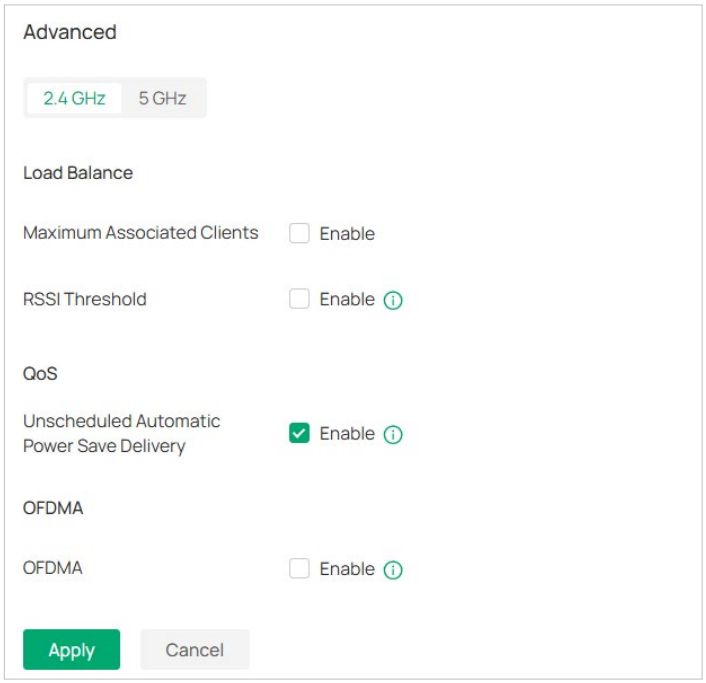
according to actual needs.

7. 3. 3 Advanced Settings

In Advanced, you can configure Load Balance, QoS, and OFDMA to improve network performance.

To configure advanced wireless settings of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Wireless > Advanced.
2. Select each band and configure the parameters. Different models support different bands.



Load Balance	Load Balance controls the clients associated to the device. Max Associated Clients: Enable this function and specify the maximum number of connected clients. If the number of connected clients reaches the specified value, the device will disconnect those with weaker signals to make room for other clients requesting connections. RSSI Threshold: Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If a client's signal strength is weaker than the threshold, the client will lose connection with the device.
QoS	QoS optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media. Unscheduled Automatic Power Save Delivery: Abbreviation as U-APSD, this function greatly improves the energy-saving capacity of clients to extend their battery life, and reduces the latency of traffic flow that is delivered over the wireless media.

OFDMA	(Only for AP supporting 802.11 ax or later standards) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improves speed and efficiency. Note that the benefits of OFDMA can be fully enjoyed only when the clients support OFDMA.

To configure advanced settings in batches, follow the steps below:

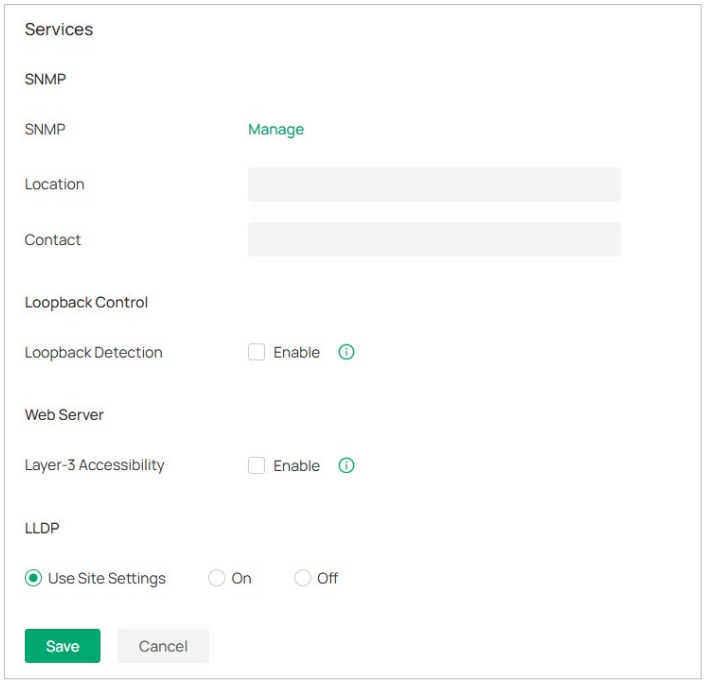
1. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.
2. Select the APs for batch configuration and click Config.
3. In Wireless > Advanced settings, configure the parameters. The parameters are the same as or fewer than those for configuring a single AP. You can keep existing settings or change them according to actual needs.

7. 4 Configure Service Settings

In Services, you can configure SNMP and LLDP for the AP.

To configure service settings of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Services.
2. Configure the parameters.



SNMP	Configure SNMP to write down the Location and Contact detail. You can click Manage to redirect to the SNMP setting page.
Loopback Control	(Only for APs with multiple LAN ports) Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or enable Loopback Detection to help detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked.
Web Server	With the web server, you can access and manage the AP. Layer-3 Accessibility: With this feature enabled, devices from a different subnet can access controller-managed devices.
LLDP	LLDP (Link Layer Discovery Protocol) can help discover devices.

To configure service settings in batches, follow the steps below:

1. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.
2. Select the APs for batch configuration and click Config.
3. In Services settings, configure the parameters. The parameters are the same as or fewer than

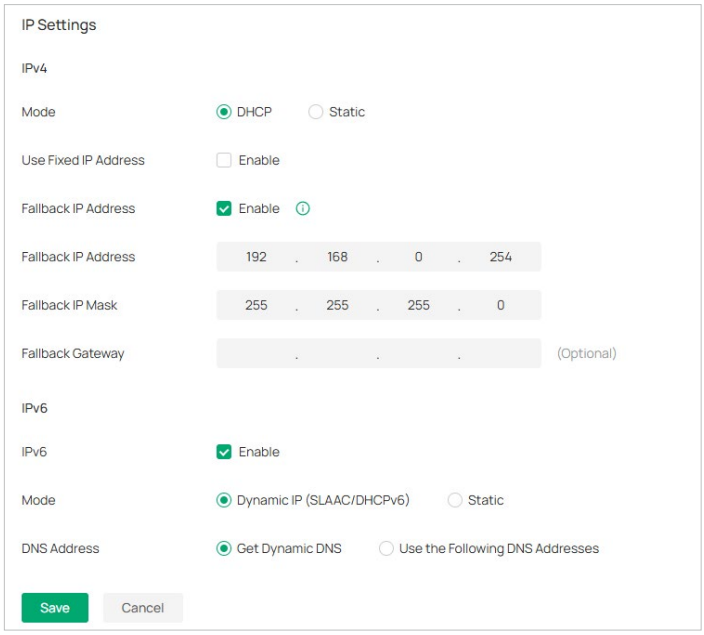
those for configuring a single AP. You can keep existing settings or change them according to actual needs.

7. 5 Configure IP Settings

In IP Settings, you can configure the IP address of the AP.

To configure IP settings of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > IP Settings.
2. Configure the parameters.



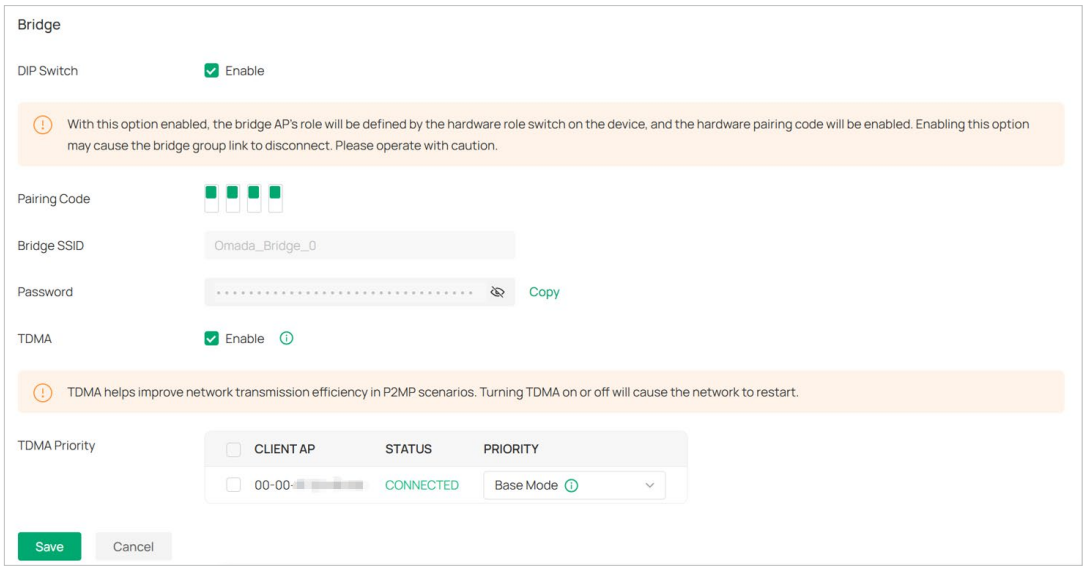
IPv4 Mode	Select an IP mode and configure the parameters for the device. DHCP: In this mode, make sure there is a DHCP server in the network and then the device will obtain dynamic IP address from the DHCP server automatically. If you want to let the device use a fixed IP address, enable Use Fixed IP Address, and set the network and IP address according to actual needs. If you want to hold an IP address in reserve for the situation in which the device fails to get a dynamic IP address, enable Fallback IP Address and set the IP address, IP mask, and gateway. Static: In this mode, set the IP address, IP mask, gateway, and DNS server for the static address.
IPv6	Enable this option if you want to set up an IPv6 address.
IPv6 Mode	Select the IPv6 mode. Dynamic IP (SLAAC/DHCPv6): Select this mode if your ISP uses Dynamic IPv6 address assignment, either DHCPv6 or SLAAC+Stateless DHCP. In this mode, set the DNS Address to determine whether to get dynamic DNS or use the specified DNS addresses. Static: In this mode, set the IP address, prefix length, gateway, and DNS server for the static address.

7. 6 Bridge Settings (Only for Bridge APs)

In Bridge Settings, you can configure bridge settings of the AP.

To configure bridge settings of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Bridge.
2. Configure the parameters.



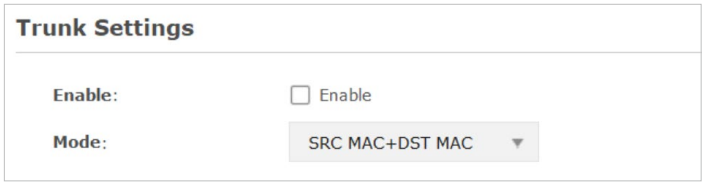
DIP Switch	(Only for APs with the hardware DIP switch) This feature controls hardware DIP switches on the AP, such as the role switch and pairing code switches. When enabled, the bridge AP's role will be defined by the hardware role switch on the device, and the hardware pairing code will be enabled. When disabled, hardware DIP switches will no longer take effect.
Pairing Code	Displays the pairing code indicated by the hardware DIP switches on the AP. Client APs can only be adopted when the pairing code is consistent with that of the main AP.
Bridge SSID / Password	Set the Bridge SSID and password of the AP. APs with the same Bridge SSID and password will form a Bridge network. These fields will be unavailable when the DIP Switch is enabled.
TDMA	TDMA helps improve network transmission efficiency in P2MP scenarios. Turning it on or off will cause the network to restart.
TDMA Priority	Choose the priority level for the client AP: Low Mode, Base Mode, High Mode. The higher the priority, the higher the average throughput of the Client AP and the lower the average latency.

7. 7 Configure Trunk Settings (Only for certain models)

The trunk function can bundle multiple Ethernet links into a logical link to increase bandwidth and improve network reliability.

To configure trunk settings of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Trunk.
2. Enable this function and select the trunk algorithm mode.



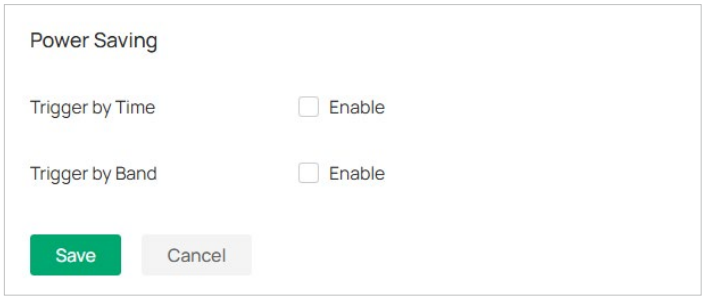
Mode	Select the trunk algorithm mode. Based on the selected algorithm mode, the AP determines which physical port is used to send out the received packet. SRC MAC+DST MAC: The AP determines the outgoing port based on both the source and destination MAC addresses of the packet. DST MAC: The AP determines the outgoing port based on the destination MAC address of the packet. SRC MAC: The AP determines the outgoing port based on the source MAC address of the packet.

7. 8 Configure Power Saving (Only for Certain Models)

Power saving can reduce the AP's power usage.

To configure power saving settings of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Power Saving.
2. Configure the parameters.



Trigger by Time	With this option enabled, you can specify the start and end time to enable power saving every day within the time period.
Trigger by Band	With this option enabled, you can specify the bands and idle duration to enable power saving when there are no connections for the specified duration on the bands.

To configure power saving settings in batches, follow the steps below:

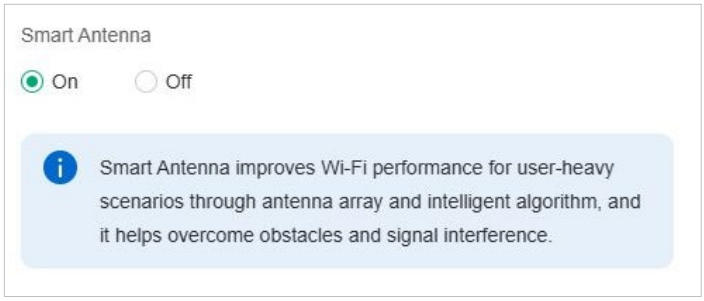
1. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.
2. Select the APs for batch configuration and click Config.
3. In Power Saving settings, configure the parameters. The parameters are the same as or fewer than those for configuring a single AP. You can keep existing settings or change them according to actual needs.

7. 9 Configure Smart Antenna (Only for Certain Models)

Smart Antenna improves Wi-Fi performance for user-heavy scenarios through antenna array and intelligent algorithm. This helps overcome obstacles and signal interference.

To enable or disable Smart Antenna of an AP, follow the steps below:

1. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Smart Antenna.
2. Enable or disable Smart Antenna according to actual needs.



7. 10 Configure EoGRE Tunnel

Overview

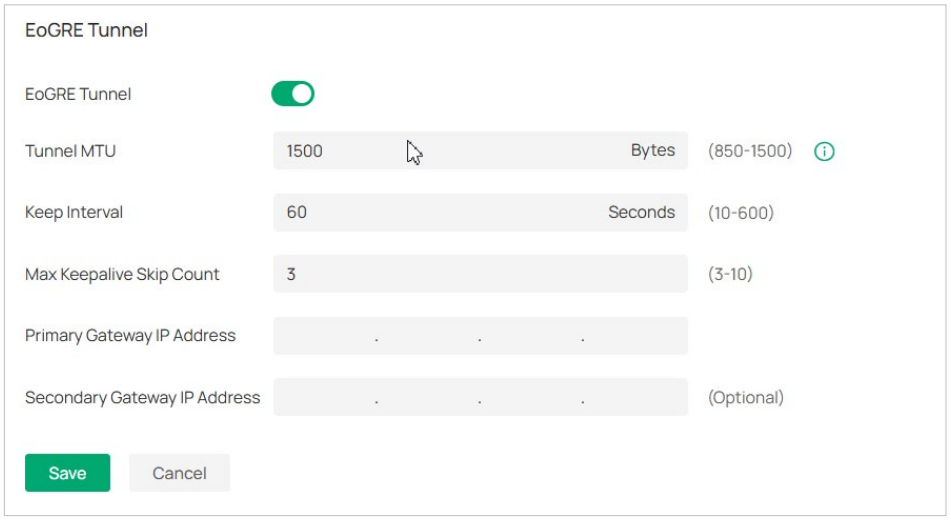
You can configure the EoGRE (Ethernet over GRE) tunnel for APs. Set the IP address to the gateway IP of the peer-end EoGRE Server. Ensure that the topology meets the point-to-point structure and that the two points are connected across Layer 3 wired connections. In this configuration, the following two conditions must be met to make the AP tunnel interface up:

- The function is enabled.
- There is a client connection.

Configuration

To configure the EoGRE tunnel for APs, follow the steps below:

1. Go to Device Config > AP > EoGRE Tunnel.
2. Enable EoGRE Tunnel and configure the parameters.



Tunnel MTU	Specify the MTU (Maximum Transmission Unit) of the tunnel.
Keep Interval	Specify the time interval for the device to send Keepalive packets to confirm the link status.
Max Keepalive Skip Count	Specify the maximum number of times the keepalive message is not replied. If the number of times exceeds this value, the device will consider the peer to be offline.
Primary Gateway IP Address	Specify the Gateway IP address of the peer.
Secondary Gateway IP Address	Specify the secondary Gateway IP address of the peer. This field is optional.

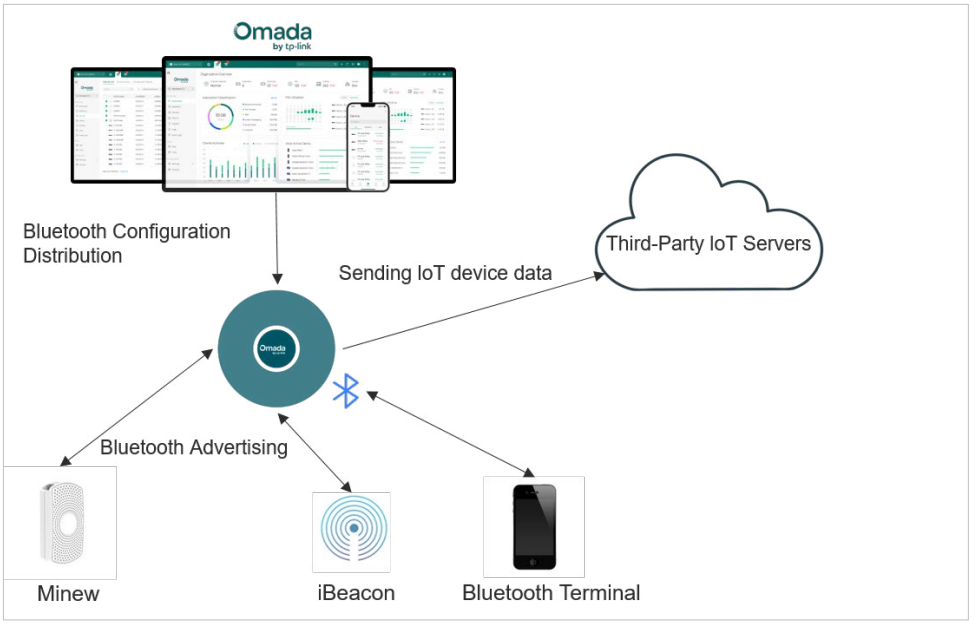
7. 11 Configure Bluetooth Settings

7. 11. 1 Overview

Omada supports Bluetooth settings to provide IoT (Internet of Things) solutions compatible with the AP for applications in healthcare, nursing homes, and more.

The Bluetooth Advertising with iBeacon technology turns the AP into a Bluetooth beacon, enabling location features for iOS apps using the Apple Core Location API.

Bluetooth IoT utilizes the AP Bluetooth module to easily collect Bluetooth data from third-party beacons and sensors, seamlessly connecting to external IoT servers for improved applications.



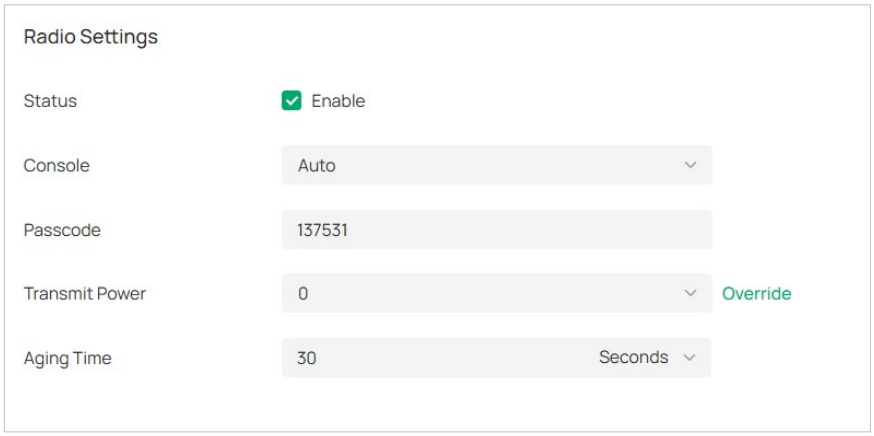
7. 11. 2 Configure Radio Settings

The Radio Settings module allows you to configure the broadcasting and connection behavior of Bluetooth devices. By adjusting these parameters, you can control the effective transmission power of Bluetooth broadcasts, device aging time, and other Bluetooth-related settings to optimize the network performance and connection stability of Bluetooth devices.

To configure radio settings of Bluetooth devices, follow the steps below:

1. Go to Device Config > AP > Bluetooth > Radio Settings.

2. Configure the parameters.



Status	Toggle to enable Bluetooth radio. Configurations on the IoT Transport Streams and Bluetooth Advertising pages are effective only when this option is enabled. When disabled, Bluetooth disables all TX and RX activities.
Console	A Bluetooth Console allows you to communicate with a device over a wireless Bluetooth connection using serial protocols. Set the Bluetooth console mode: Auto: Automatically enables the Bluetooth console if a network error or device disconnection occurs and disables it when the device reconnects normally. On: Always on. Off: Always off.
Passcode	Specify the 6-digit pairing code used to establish a Bluetooth connection.
Transmit Power	Specify the broadcast transmission power (dB).
Aging Time	Set the time in seconds, minutes, or hours to control the aging time of devices. If an AP does not receive the data sent by a device within the aging time, it will delete the device entry and no longer forward it to the IoT application server. If the AP receives the data sent by the device again, it will re-add the device entry and continue to report the Bluetooth data of the device.

7. 11. 3 Configure IoT Transport Streams

IoT Transport Streams allow Bluetooth-enabled APs to scan BLE Advertising frames in its surrounding environment, collect the required BLE data, and then report the data to the designated third-party IoT server. IoT Transport Streams can be divided into two functions: BLE Periodic Telemetry and BLE Data Forwarding.

BLE Periodic Telemetry: The APs will parse the scanned BLE Advertising frames, extract the valid data, and save the data to their BLE device lists. They will populate BLE device list data into the messages at set intervals and report to the designated third-party IoT server.

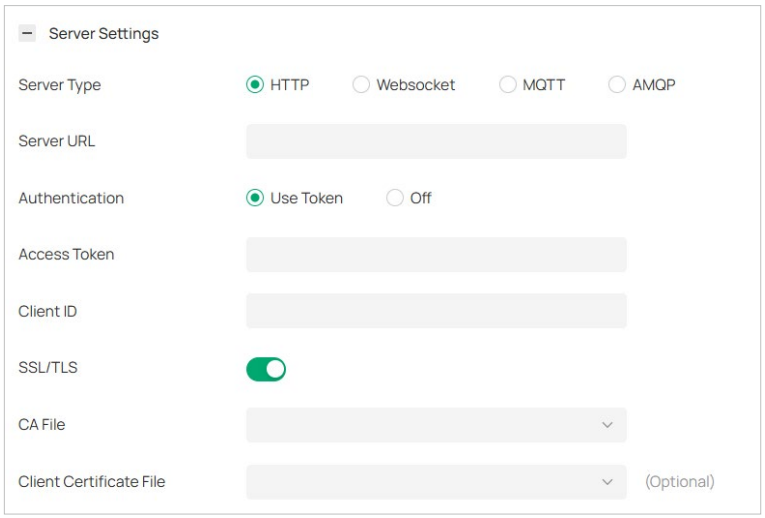
BLE Data Forwarding: The APs will automatically forward the scanned BLE Advertising frames of the specified protocol. The forwarded data is the raw data received by the APs, which is forwarded in real time.

To configure IoT Transport Streams, follow the steps below:

1. Go to Device Config > AP > Bluetooth > IoT Transport Streams.
2. Click Create New Entry to create a new IoT Transport Streams profile.
3. Configure basic information.

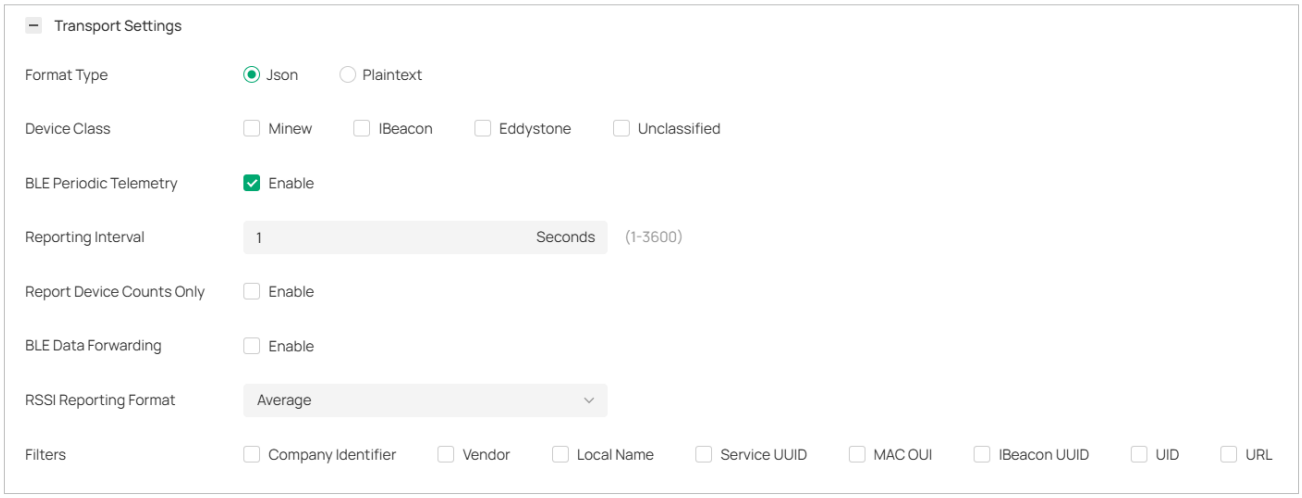
Name	Enter the name of the profile.
Status	Toggle on to enable this profile on Bluetooth-enabled APs.

4. Configure server settings.



Server Type	Specify the type of server receiving IoT data. Available options include HTTP, WebSocket, MQTT, and AMQP.
Server URL	Enter the server address for IoT data reporting. Currently, the URL path with http as the prefix is supported.
Authentication	Specify the authentication method. Currently, token authentication is supported.
Access Token	Specify the token used for identity authentication.
Client ID	Specify the ID used for identity authentication.
SSL/TLS	Specify whether to enable SSL/TLS.
CA File	Upload the certificate from a CA authority or a self-signed certificate.
Client Certificate File	Upload the certificate issued by a CA authority or generated locally, which will be sent to the server to authenticate the client's identity.

5. Configure transport settings.



Format Type	Specify the format type of the reported data. Available options are Json, Plaintext.
Device Class	Specify the vendors and protocols. Currently, only iBeacon, Eddystone, and Minew protocols are supported. More protocols will be supported in the future.
BLE Periodic Telemetry	Toggle on if you want to enable the periodic reporting of the AP.
Reporting Interval	Specify the interval period for the AP to report IoT data.
Report Device Counts Only	When enabled, the AP only reports the number of IoT devices.
BLE Data Forwarding	Toggle on if you want to enable the transparent transmission of the AP data.
RSSI Reporting Format	Specify the signal strength reporting format. Currently, Average, Max, Last, Smooth, and Bulk are supported.
Filters	Specify the custom configuration items that control the AP to filter IoT devices. Currently, Company Identifier, Vendor, Local Name, Service UUID, MAC OUI, iBeacon UUID, UID, and URL are supported.

6. Click Apply. The profile will be added and applied to Bluetooth-enabled APs. You can go to Devices > Configuration Result to check whether the configuration is applied to the corresponding APs successfully.

7. 11. 4 Configure Bluetooth Advertising

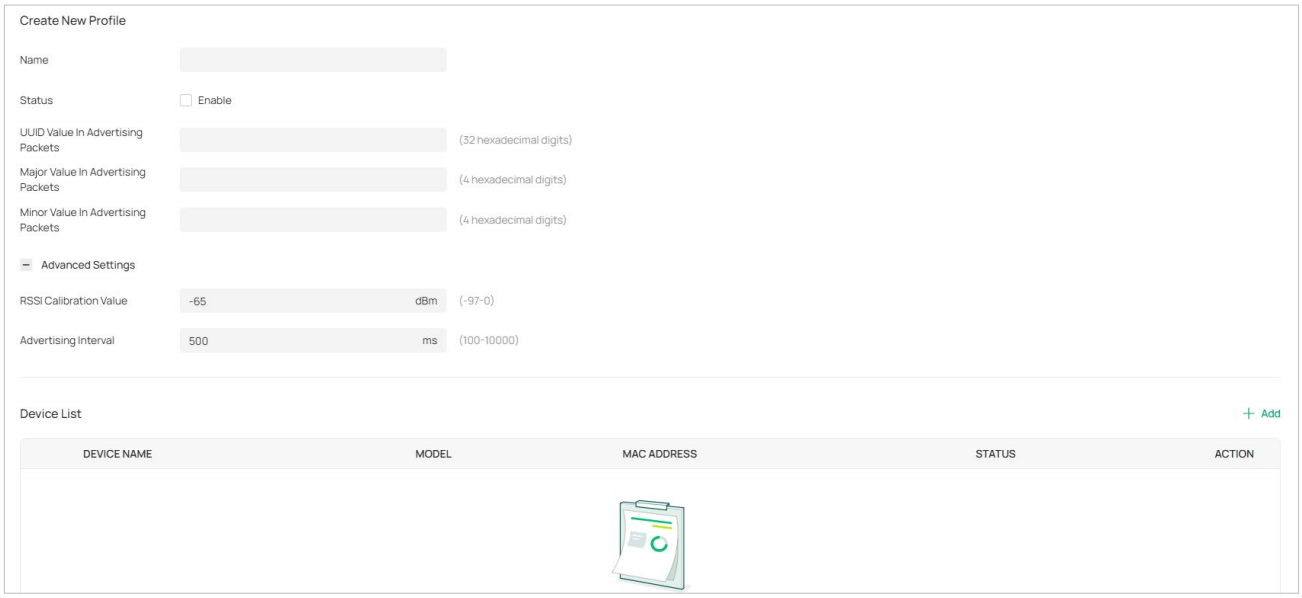
The Bluetooth Advertising function allows Bluetooth-enabled APs to send out specific BLE broadcast frames according to the set configuration. Currently, it only supports broadcasting iBeacon frames, and more protocols will be supported in the future.

There is a default rule in the initial interface, which can be turned off but cannot be deleted.

You can also add Bluetooth Advertising profiles and apply them to specific APs.

To add a Bluetooth Advertising profile, follow the steps below:

1. Go to Device Config > AP > Bluetooth > Bluetooth Advertising.
2. Click Create New Profile to create a Bluetooth Advertising profile. Configure the parameters.



Name	Enter the name of the profile.
Status	Toggle on to enable this profile on Bluetooth-enabled APs.
UUID Value In Advertising Packets	Specify the Universally Unique Identifier (UUID) of the broadcast iBeacon device, which is the unique identifier of the universal device.
Major Value In Advertising Packets	Specify the major value of the broadcast iBeacon device, used to mark larger groups.
Minor Value In Advertising Packets	Specify the minor value of the broadcast iBeacon device, used to mark smaller groups.
RSSI Calibration Value	Specify the RSSI calibration value (dB).
Advertising Interval	Specify the interval of advertising frames.
Device List	Click Add and select devices to apply this profile. Only Bluetooth-enabled APs will be listed for selection. Notes: 1. The default entry does not have this configuration item. Only custom entries support the configuration of specific devices. 2. Currently, a single device is supported to configure a Bluetooth Custom configuration entry for advertising.

3. Click Create. The profile will be added and applied to the Bluetooth-enabled APs you selected. You can go to Devices > Configuration Result to check whether the configuration is applied to the corresponding APs successfully.

Chapter 8

Manage Clients

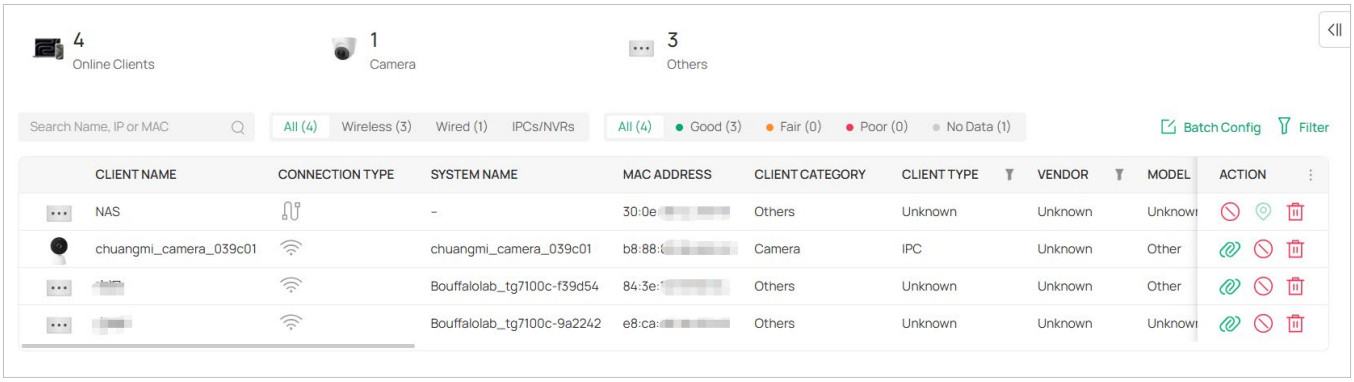
This chapter guides you on how to monitor and manage the clients using the Clients page. This chapter includes the following sections:

8. 1 Manage the Client List

The Clients page offers a straight-forward way to manage and monitor clients. It displays wired and wireless clients and their general information.

To manage clients, go to the Clients page.

You can manage clients in the client list. You can switch pages based on the client status (Online, Offline, Blocked, and All).



Monitor Connection Status

The Status column explains the connection status of clients.

PENDING	The client has not passed the authentication and it is not connected to the internet.
AUTHORIZED	The client has been authorized and is connected to the internet.
CONNECTED	The client is connected to internet via non-portal network.
AUTHENTICATION-FREE	The client does not need to be authorized and it is connected to the internet.
DISCONNECTED BLOCKED	The client is blocked.

Customize the Column

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

To change the list order, click the upside-down triangle icon next to the column head, which indicates the ascending or descending order.

When this icon appears in the Wireless Connection column, it indicates the client is in the power-saving mode.

Filter the Clients

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

To search for clients, enter the text in the search box.

To filter clients, a tab bar is above the table to filter the clients by client type. You can also filter clients by their status, connected SSID, network, AP/port by clicking the filter icons in the table header.

Quick Operations

For quick operations on a single client, click the icons in the Action column. The available icons vary according to the client status and connection type.

	Click to block the client.
	Click to forget the client.
	Click to manually authorize the client that has not passed the authentication.
	(With portal authentication enabled) Click to unauthorize the client that has passed the portal authentication.
	(For wireless clients) Click to reconnect the wireless client to the wireless network.
	(For clients connected to switches) Click this icon and the peer switch port's LED will flash to indicate the client's location. The LED will keep flashing for 10 minutes, or you can click the  icon to stop the flashing.

Batch Config

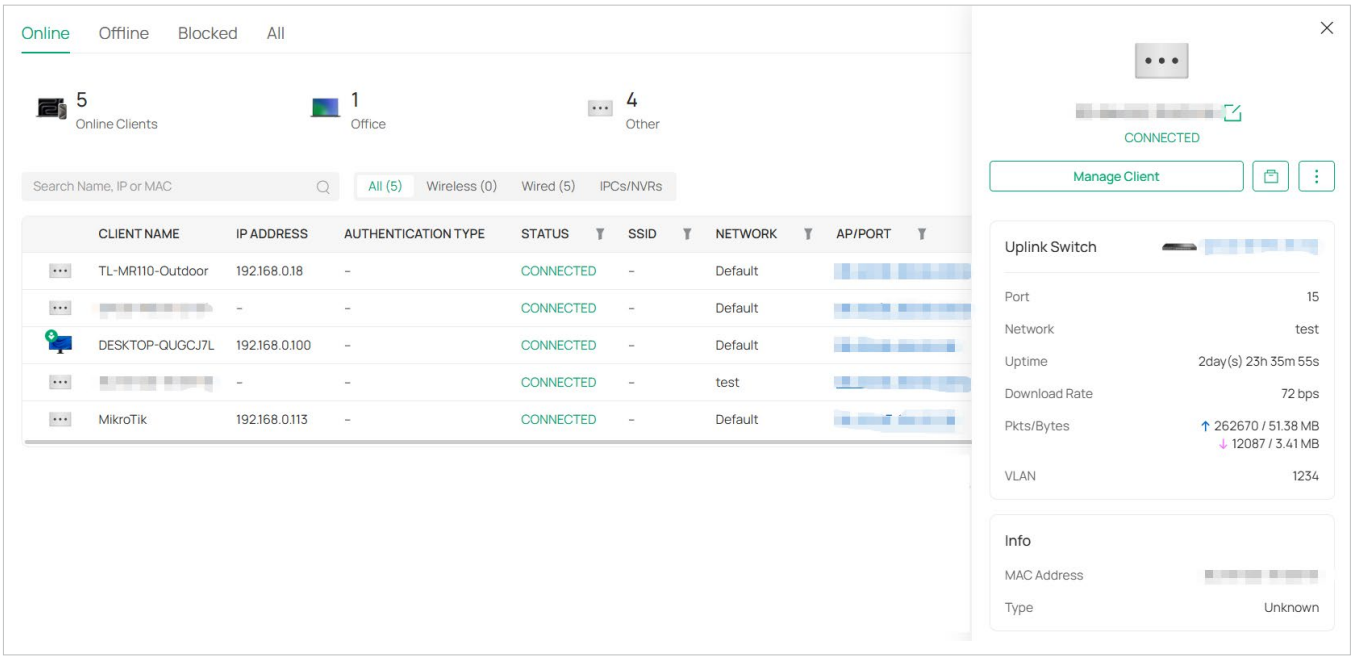
You can configure clients in batches. Click Batch Config, select clients, and click Done. Then you can configure settings for the selected clients in batch.

8. 2 Manage a Client

To manage a client, go to the Clients page. In the client list, click a client, then you can monitor and manage it in the Properties window and Client Management window.

Properties Window

The Properties window displays the basic information of the client. You can click the edit icon to edit the client name and information.



- **Quick Operations**

  Click the ⋮ icon and choose an operation to quickly operate the client.

Block	Click to block the client from accessing the network.
Forget	Click to remove the client from the network. Once forgotten, client settings will be wiped out.
Reconnect	(For wireless clients) Click to reconnect the wireless client to the wireless network.
Authorize	Click to manually authorize the client that has not passed the authentication.
IntelliRecover	(Only for the client directly connected to the PoE switch) Click to enable the IntelliRecover function for the client so that it can be added to the IntelliRecover monitoring list. IntelliRecover can help you monitor the status of PoE devices, automatically repairing abnormal devices.

- **Network Tools**

  Click the icon and choose a network tool to analyze the network.

Network Check	Test the network connectivity via ping or traceroute.

Remote Access	(For clients identified as IPCs/NVRs only) Allows easy access to internal network devices from an external network using adopted Omada devices. To ensure privacy and security, connections are time-limited and expire automatically.

Client Management Window

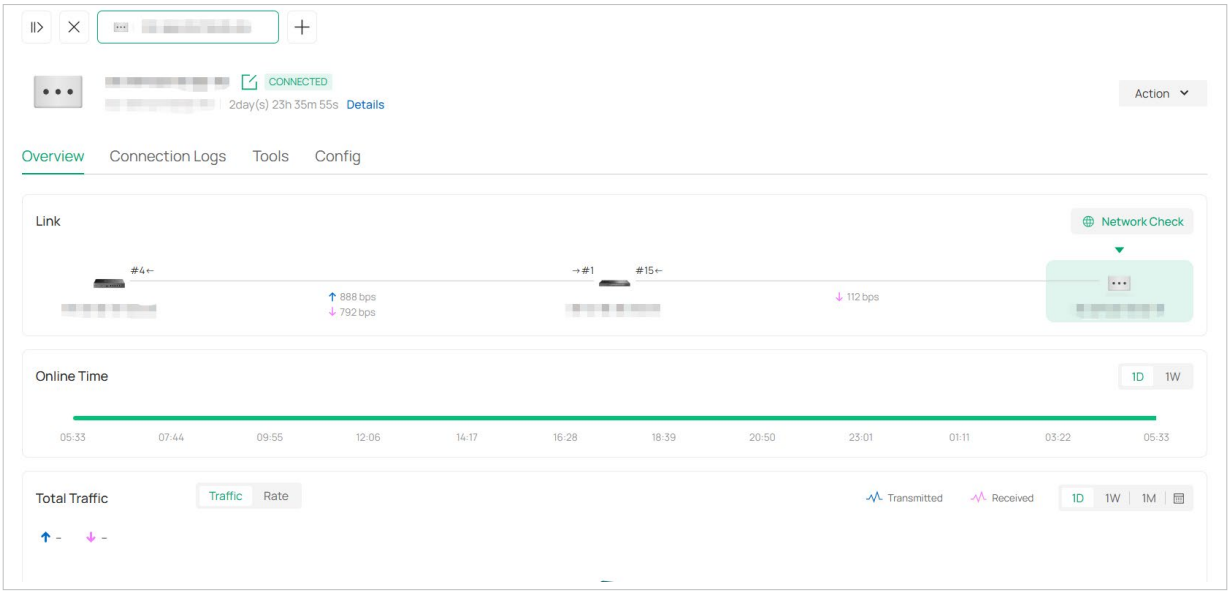
Click Manage Client to open the Client Management window to view more client details and change client settings.

In the management window, you can click + and select one or more clients to open new management windows, click the icon in the top left to minimize the windows to the icon in the right side, and click the icon to reopen the minimized windows.

You can also click each tab to monitor and manage the client.

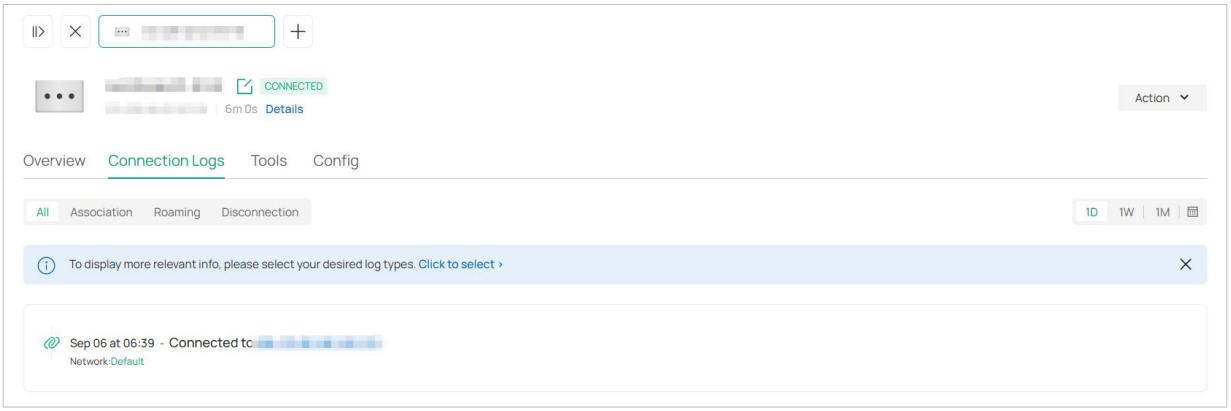
- **Overview**

  In Overview, you can get an overview of the client, such as link status, online time, and more.



- **Connection Logs**

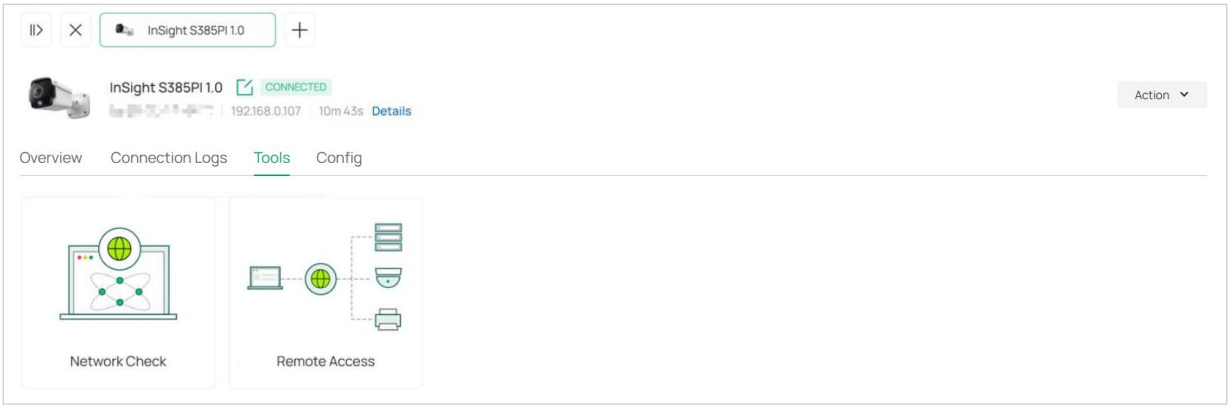
  In Connection Logs, you can check the connection logs of the client, such as association, roaming, disconnection, and more.



Tools

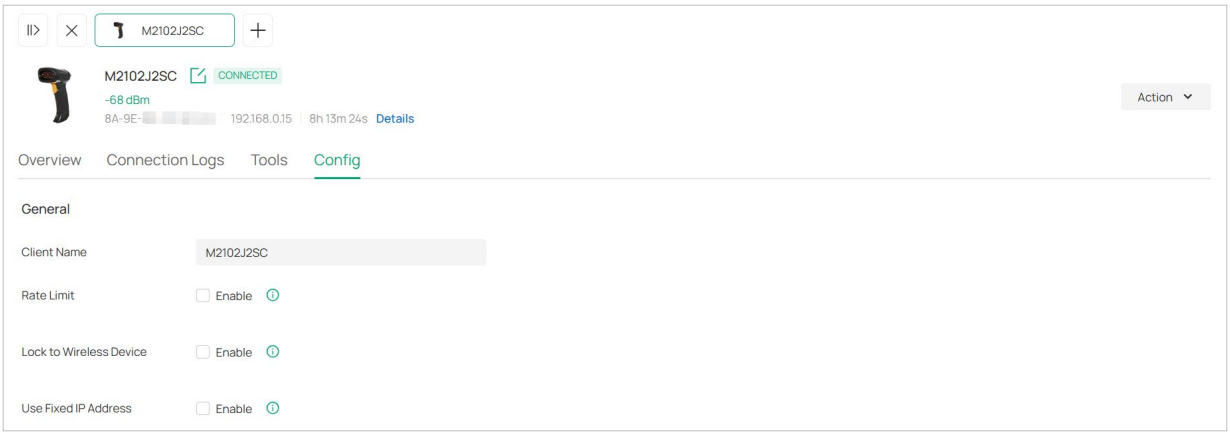
In Tools, you can use the network tool to test the network connectivity. For clients identified as IPCs/NVRs, you can configure Remote Access so you can easily access them from an external network.

For detailed instructions, refer to 22. 1 Maintain the Network with Tools.



Config

In Config, you can edit client settings.



Client Name	Specify the client's name to better identify different clients, and the name is used as the client's username in the table on the Clients page.
Rate Limit	Enable this function if you want to limit the download and upload rate of each client to balance bandwidth usage. When enabled, select an existing rate limit profile, create a new rate limit profile or customize the rate limit. Custom: Specify the Download Limit and Upload Limit based on needs. Note: Rate Limit on this page is only available for the clients connected to the APs. To limit the rate of the clients connected to the gateway or switch, go to the Bandwidth Control page.
Lock to Wireless Device	When enabled, you can lock the device to a specific wireless device for stable connection. To use this function, ensure your device is using the device MAC rather than a random MAC. Otherwise, the function may not take effect. Only 11ac and above products support this function.

Use Fixed IP Address	Click the checkbox to configure a fixed IP address for the client. With this function enabled, select a network and specify an IP address for the client. Note: A gateway is required for this function. Otherwise, you cannot set a fixed IP address for the client.

Chapter 9

Upgrade Device Firmware

This chapter introduces how to upgrade device firmware. It includes the following sections:

9. 1 Introduction

The Omada system relies on a tight handshake between the controller and managed devices. Upgrading device firmware is essential to get new features, optimize performance, patch security vulnerabilities, and fix bugs. It ensures the devices operate efficiently, maintain compatibility with controller updates, and prevents potential system failures, ultimately ensuring network performance and reliability.

Omada offers different firmware updates to meet different needs:

- **Stable Version:**

A fully tested and verified official release version. It is recommended for use in production environments to ensure system reliability and stability.

Available in the Stable channel.

- **Release Candidate:**

A version before the official version is released, which is close to the official released version, but may still have some undiscovered or unresolved issues. It is suitable for users who want to use new features in advance, but not suitable for use in critical business environments.

Available in the Release Candidate channel.

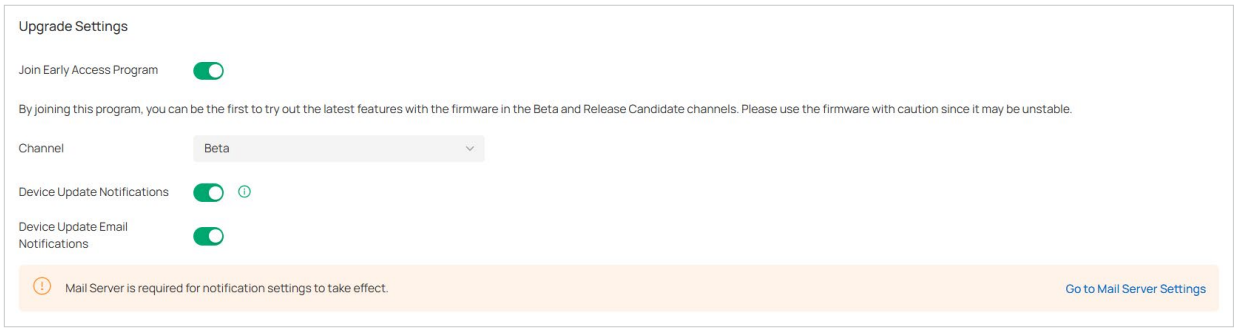
- **Beta Version:**

A preliminary release version, whose functions may not be completely stable yet. It is mainly used for testing and feedback, suitable for users who want to be the first to try out new features and willing to take potential risks. It is not recommended for use in production environments.

Available in the Beta channel.

9. 2 Configure Upgrade Settings

1. Go to Firmware > Overview.
2. In Upgrade Settings, configure the parameters.

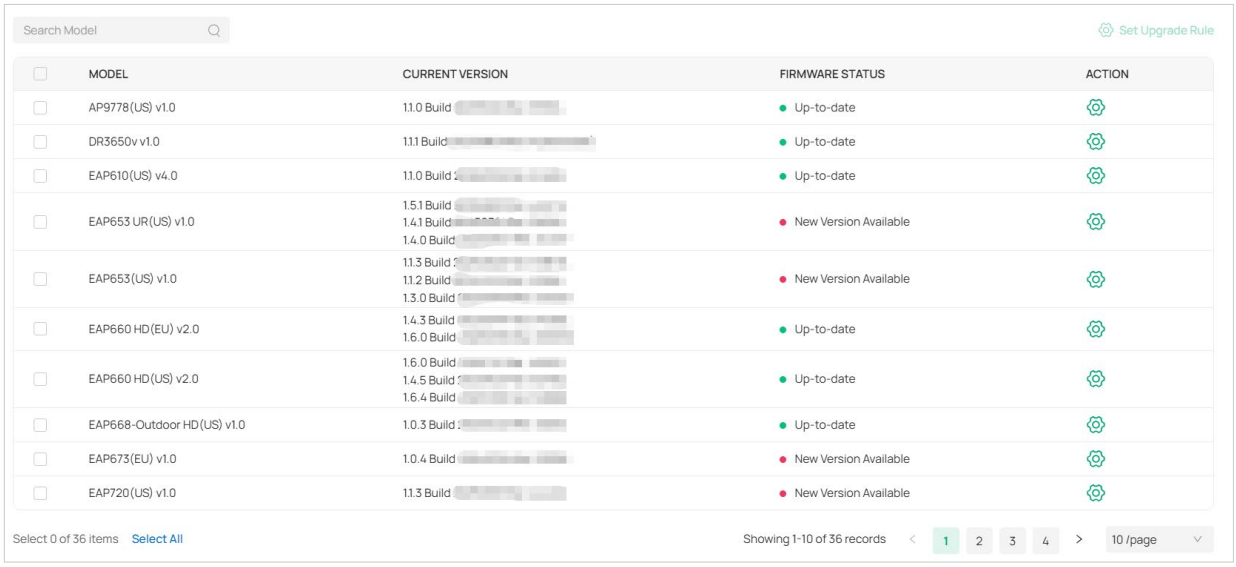


Join Early Access Program	By joining this program, you can be the first to try out the latest features with the firmware in the Beta and Release Candidate channels. Please use the firmware with caution since it may be unstable.
Channel	Select a channel for the early access program: Stable, Beta, or Release Candidate.
Device Update Notifications	With this option enabled, the system will query the cloud for device firmware updates.
Device Update Email Notifications	With this option enabled, the system will send emails to notify the administrators when new device firmware is available in the Stable channel (by default) or the channel selected for the early access program. Mail Server is required for notification settings to take effect. For instructions, refer to the Mail Server section.

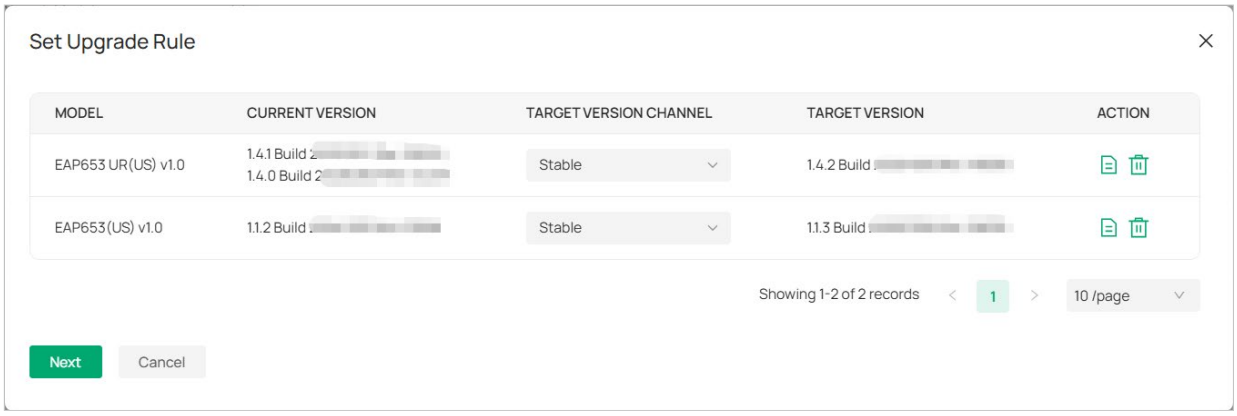
9. 3 Configure One-Time Upgrade

If you want to upgrade device firmware via Omada Cloud for one time only, follow the steps below:

1. Go to Firmware > One-Time Upgrade.
2. In the device model list, locate a device model whose firmware status is “New Version Available” and click the setting icon in the Action column. For batch upgrade, select multiple models and click Set Upgrade Rule.



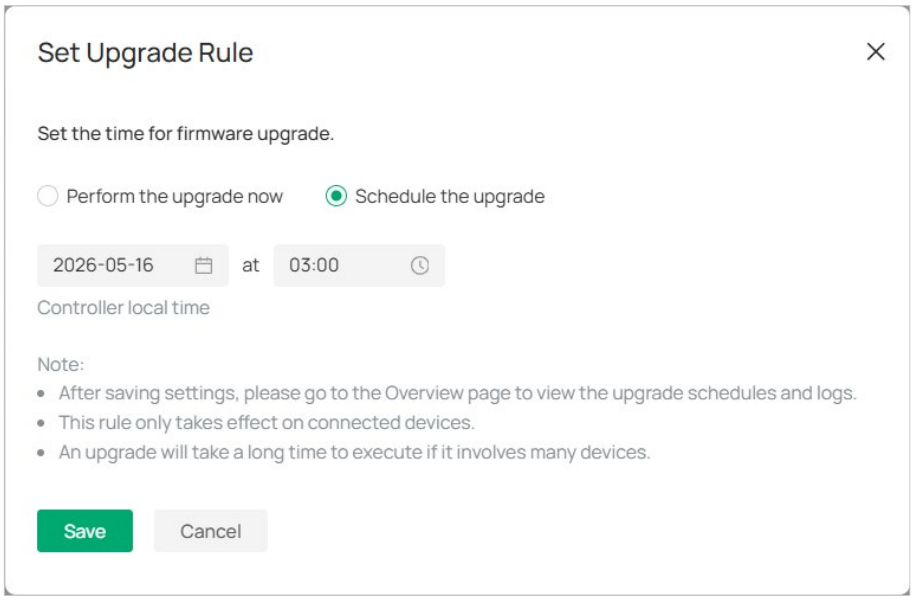
3. Select a channel to get the target version. The Stable channel is recommended for use in production environments. You can click the Release Note icon to view new firmware details. Click Next.



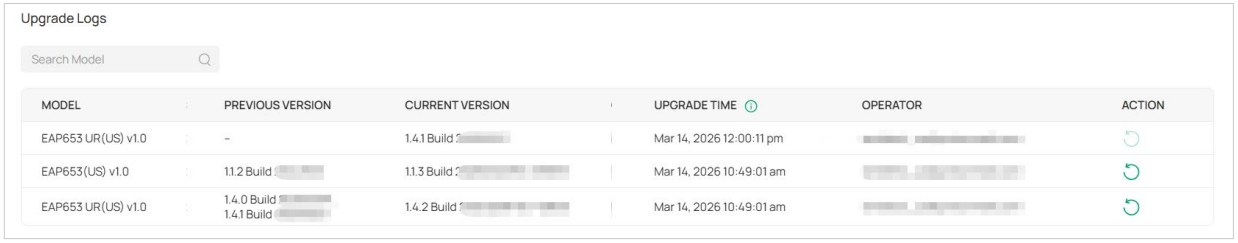
4. Set the upgrade time. It is recommended to schedule the upgrade for a time of lowest traffic.

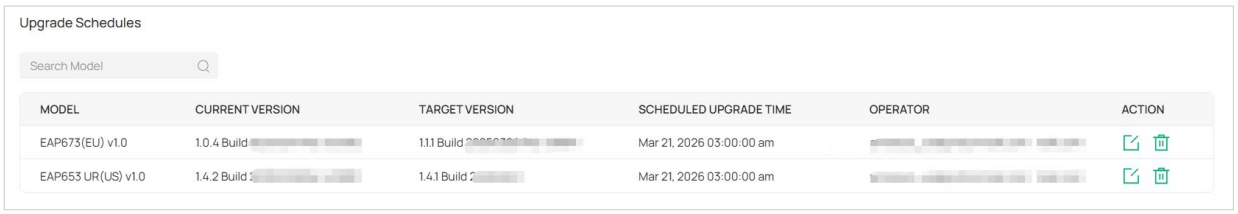
Notes:

- This rule only takes effect on connected devices.
- An upgrade will take a long time to execute if it involves many devices.



5. Save the settings. The devices of the specified model(s) will be upgraded at the time you set. You can go to the Overview page to view the upgrade/rollback schedules and logs.





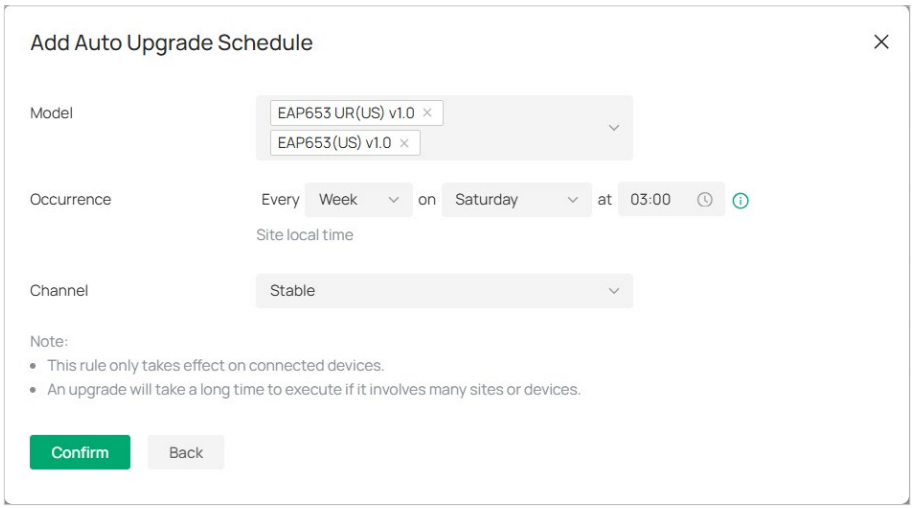
9. 4 Configure Periodic Upgrade

If you want to upgrade device firmware via Omada Cloud periodically, follow the steps below:

1. Go to Firmware > Periodic Upgrade. Click Add Auto Upgrade Schedule.
2. Select your desired models and set the upgrade time. It is recommended to schedule the upgrade for a time of lowest traffic. Select a channel to get the target version. The Stable channel is recommended for use in production environments.

Notes:

- This rule only takes effect on connected devices.
- An upgrade will take a long time to execute if it involves many devices.

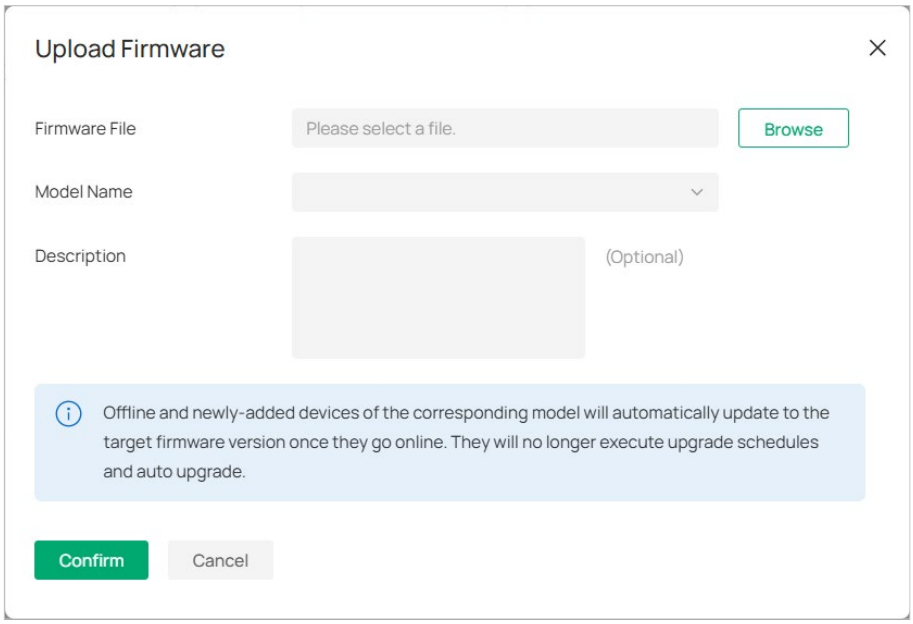


3. Save the settings. The schedule will be added to the list. The devices of the specified model(s) will be upgraded at the time you set.

9. 5 Upload Firmware for Upgrade

If you want to upload firmware for upgrade, follow the steps below:

1. Go to https://support.omadanetworks.com/download/firmware/ and obtain your desired firmware file.
2. Go to Firmware > Upload Firmware for Upgrade. Click Upload Firmware.
3. Upload the firmware file you obtained and select the device model matching the firmware file.

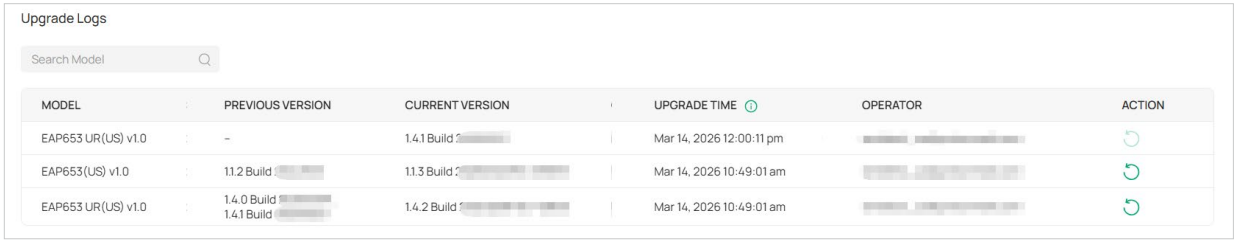


4. Save the settings. The devices of the specified model will be upgraded to the firmware you uploaded.

Note:

Offline and newly-added devices of the corresponding model will automatically update to the target firmware version once they go online. They will no longer execute upgrade schedules and auto upgrade.

You can go to the Overview page to view the upgrade/rollback logs.



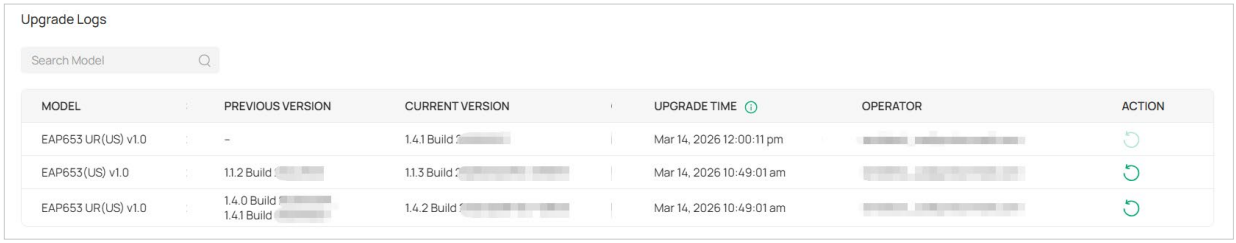
9. 6 Roll Back Device Firmware

In case you want to roll back device firmware after firmware upagrade, follow the steps below:

1. Go to Firmware > Overview.
2. In Upgrade Logs, locate the device model that you want to roll back device firmware, then click the Roll Back icon in the Action column.

Note:

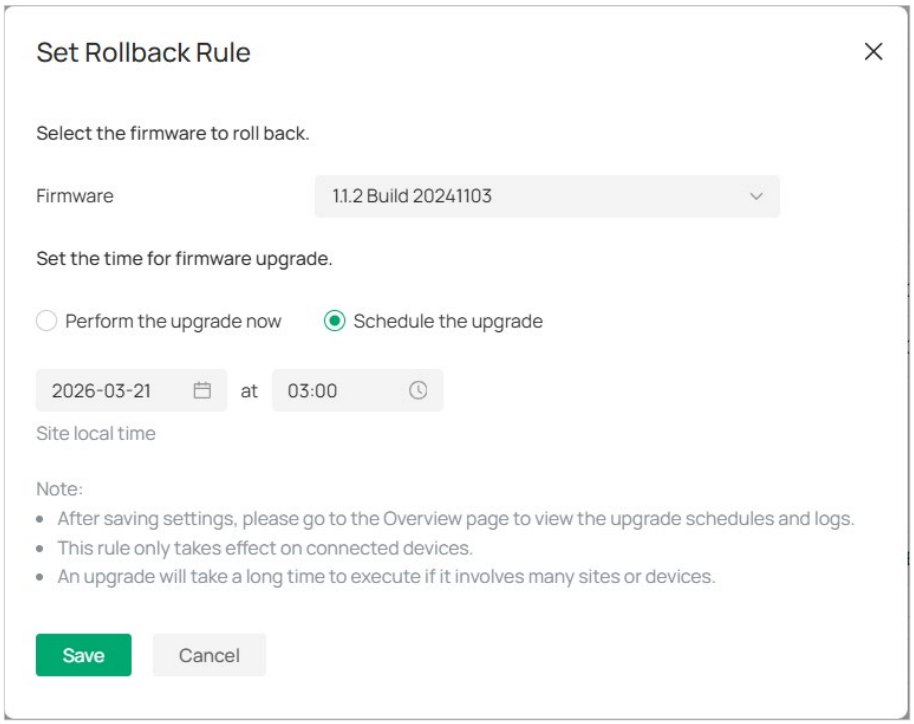
Only the firmware upgraded within 14 days can be rolled back.



4. Select the firmware to roll back and set the rollback time. It is recommended to schedule the rollback for a time of lowest traffic.

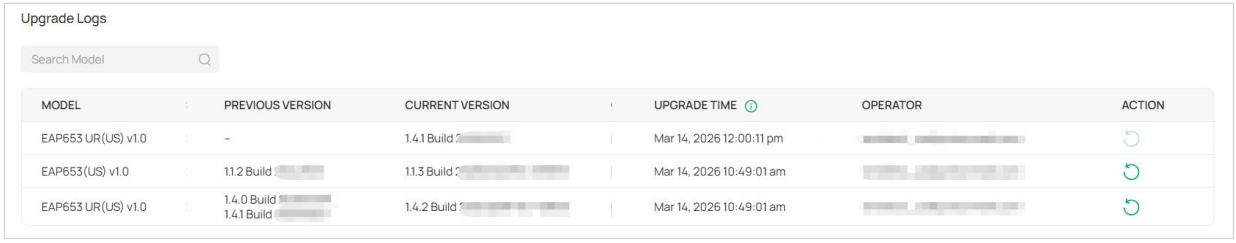
Notes:

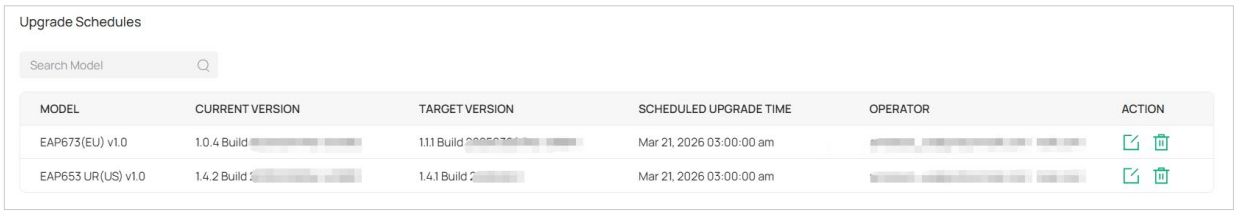
- This rule only takes effect on connected devices.
- An rollback will take a long time to execute if it involves many devices.



5. Save the settings. The devices corresponding to the upgrade log will be rolled back at the time you set.

   You can go to the Overview page to view the upgrade/rollback schedules and logs.





Chapter 10

Monitor the Network

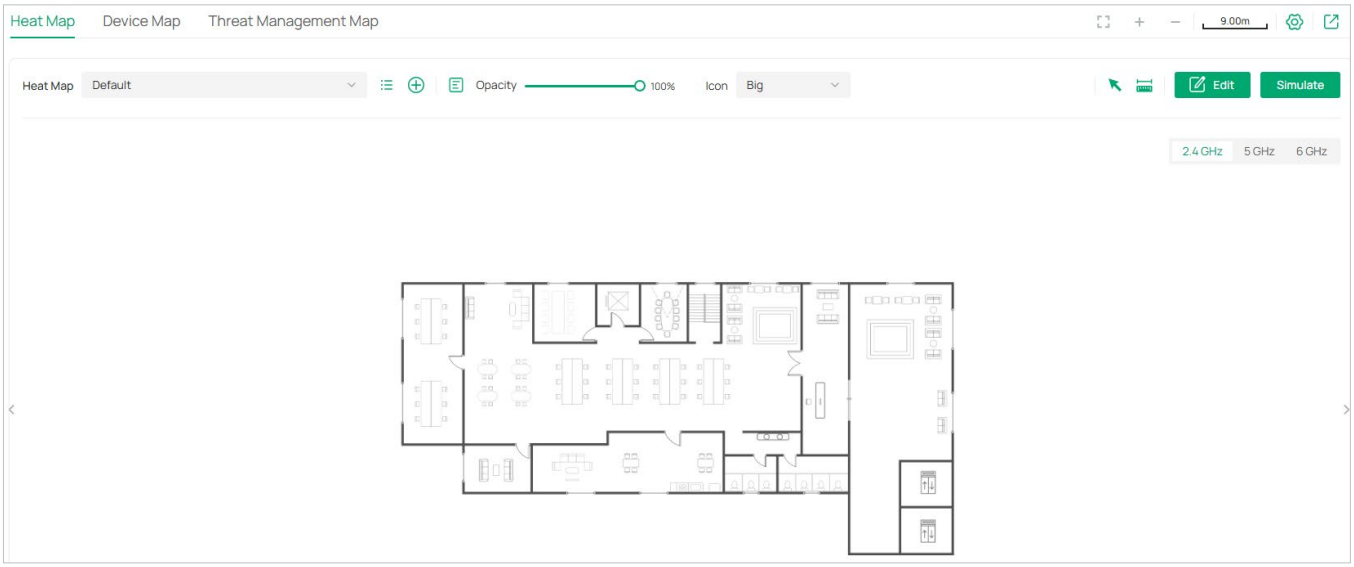
This chapter guides you on how to monitor the network status to ensure the stability and security of network operations. This chapter includes the following sections:

10. 1 Monitor the Network with Map

With the Map function, you can customizes a visual representation of your network in Heat Map and visually display the geographic location of each device in Device Map.

10. 1. 1 Heat Map

Go to Map > Heat Map, and a default map is shown as below. You can upload your local map images and add devices and different types of walls to customize a visual representation of your network.



Click the following icons to add, edit, and select the map. After selecting a map, click and drag in the devices from the Devices list to place it on the map according to the actual locations.

Heat Map Default	Click to select a map from the drop-down list to place the devices.
	Click to edit maps in the pop-up window. Click the edit icon to edit the description and layout of the map. Click the delete icon to delete the map.
	Click to add a map. In the pop-up window, enter the description, select the layout, and upload an image in the .jpg, .jpeg, .gif, .png, .bmp, .tiff format.
Opacity 100%	Adjust the opacity of the map.
Icon Big	Click to select the icon size displayed on the map.
	Click to use the selection tool to select the elements including walls and devices on the map.
	Click to use the measurement tool. Draw a line on the map to measure the actual distance according to the map scale.

Edit	Click to edit the elements including walls and devices on the map.
Simulate	Click to simulate the network heat map. Note: It is required to click Simulate to generate a new heat map after editing elements on the map.
	Click to fit the map to the web page.
	Click to zoom in the map.
	Click to zoom out the map.
9.00m	Click to set the map scale. Draw a line on the map by clicking and dragging, and then define the distance of the line.
	Click to set the default height of the added devices and the information displayed on the map.
	Click to export the network coverage report.

Configuration

To generate a visual representation and heat map of your network, follow these steps:

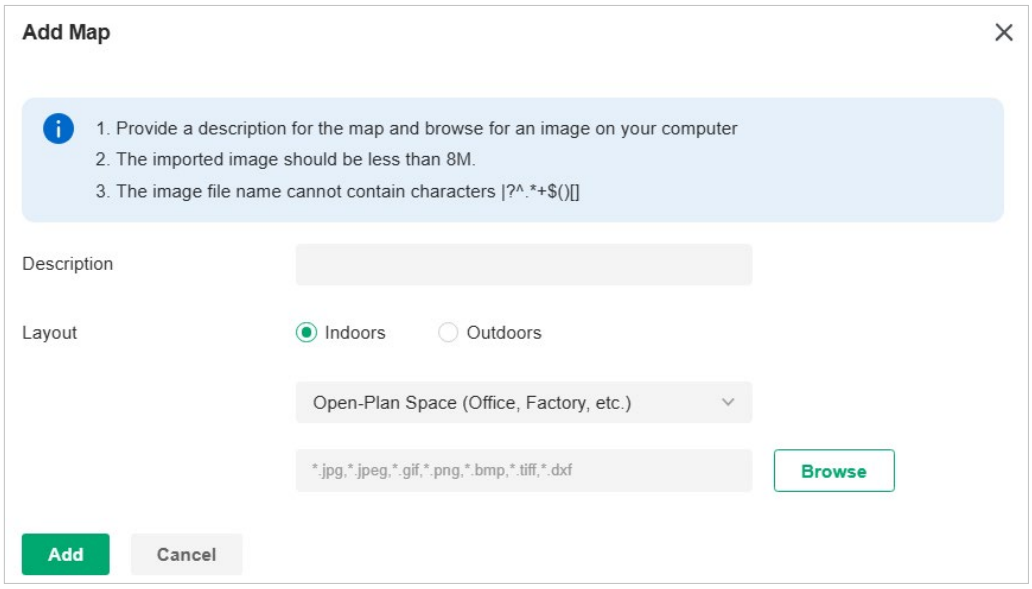
1) Add a map and configure the general parameters for the map.

2) Add devices and walls, and configure the parameters.

3) View simulation results.

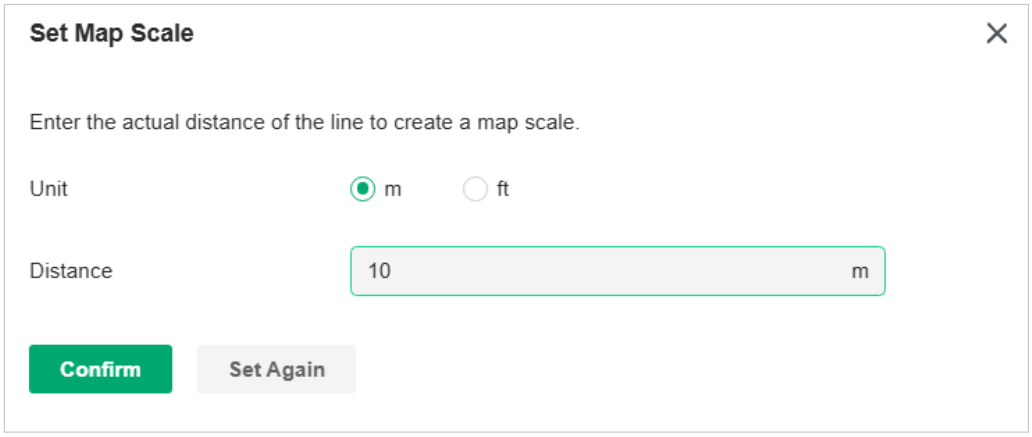
Step 1: Add Map

1. Go to Map > Heat Map and click ⊕ to add a new map. Then click Add.

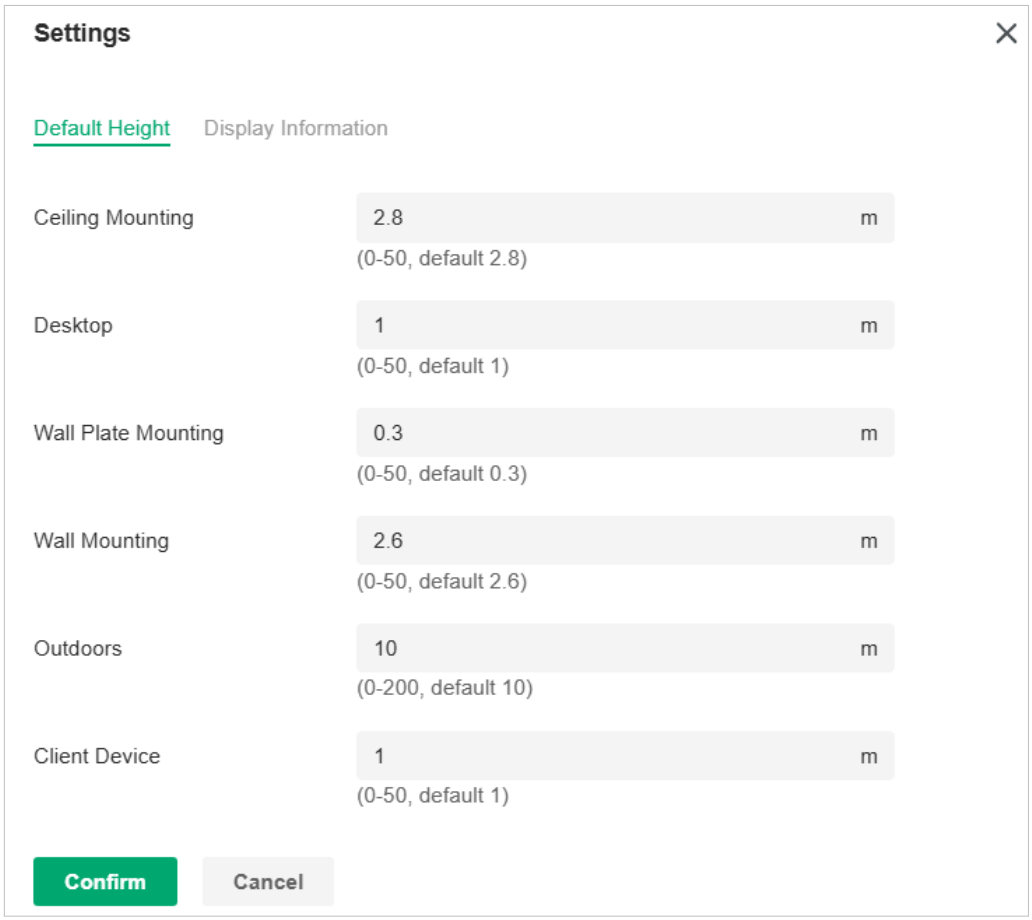


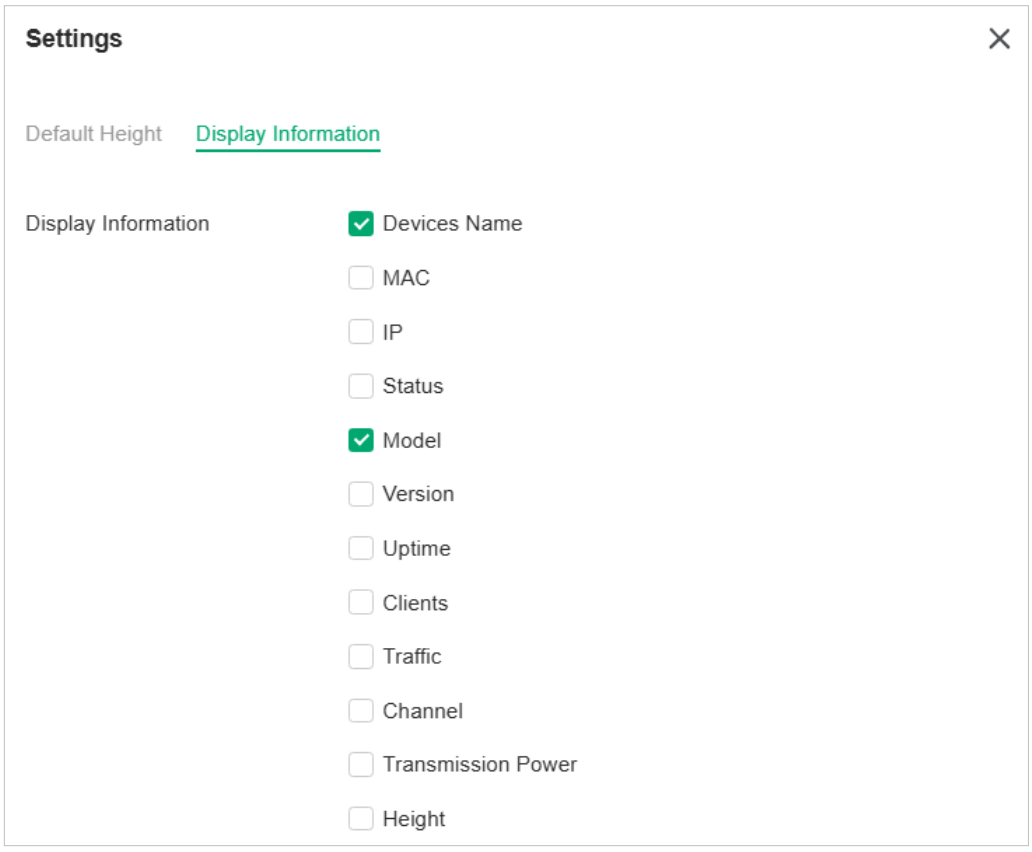
Description	Enter a description for the map.
Layout	Select the general layout of the map, which will make the simulation more accurate and the upload the map in the .jpg, .jpeg, .gif, .png, .bmp, .tiff, .dxf format. **Tip:** You can upload a CAD (.dxf) file, and the Fusion gateway will automatically identify the walls in the layout.

2. Click the scale icon on the upper right to set a map scale. Draw a line on the map by clicking and dragging, and then define the distance of the line.



3. Click the settings icon to set the default height of the added devices and the information displayed on the map. Then click Confirm.

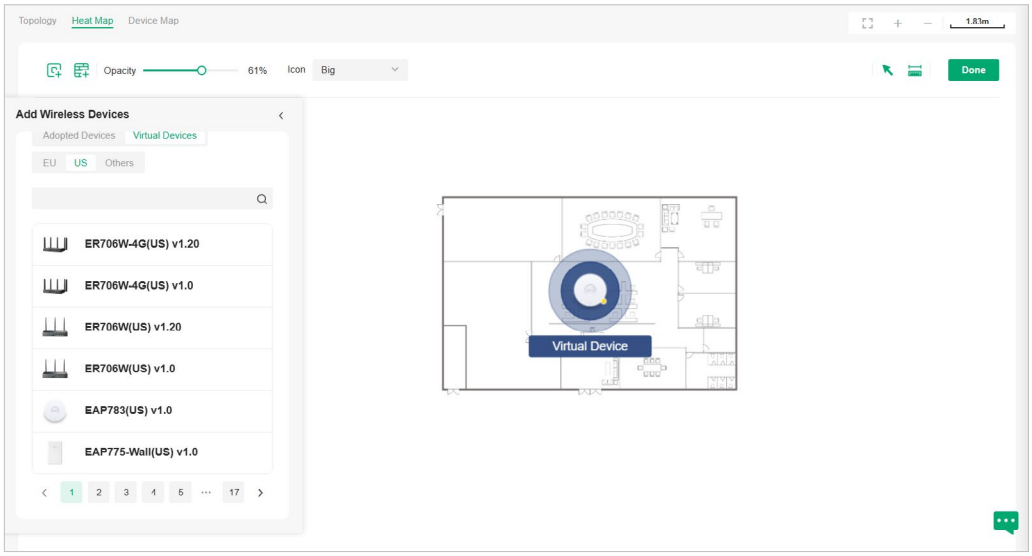

Settings
Default Height
Display Information
Ceiling Mounting
2.8
m
(0-50, default 2.8)
Desktop
1
m
(0-50, default 1)
Wall Plate Mounting
0.3
m
(0-50, default 0.3)
Wall Mounting
2.6
m
(0-50, default 2.6)
Outdoors
10
m
(0-200, default 10)
Client Device
1
m
(0-50, default 1)
Confirm
Cancel


Settings
Default Height
Display Information
Display Information
Devices Name
MAC
IP
Status
Model
Version
Uptime
Clients
Traffic
Channel
Transmission Power
Height

Default Height	Specify the default height for devices. You can change the height for individual device later.
Display Information	Select the information you want to see on the map.

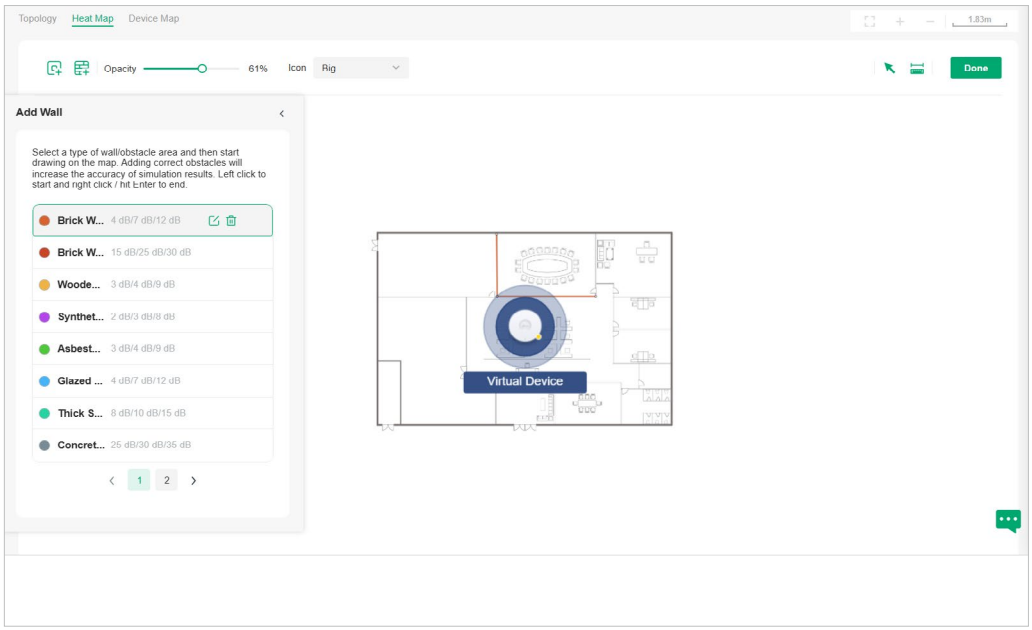
Step 2: Add Devices and Walls

1. Click the Edit icon to enter the editing status of the map.
2. Click the Add Wireless Devices icon on the upper left, and the list of adopted devices and virtual devices will appear. Drag the devices to the desired place on the map.



3. Click the Add Wall icon on the upper left. Select a type of wall/obstacle area and then start drawing on the map. Left click to start and right click / hit Enter to end.

   You can also edit the details parameters of the walls and obstacles, delete, and add walls. Adding correct obstacles will increase the accuracy of simulation results.



4. Click the Done icon to exit the editing status of the map.

Step 3: View and Export Results

It is required to click Simulate to generate a new heat map after editing elements on the map.

1. Click the Simulate icon to generate the heat map. You can adjust the receiver sensitivity, show signal strength, and view the simulation results according to your needs.

Show Signal Strength	Enable the feature, and you can move the cursor to view the signal strength of a specific location.
Show Simulation	Enable or disable the display of simulation results on the map.
2.4 GHz 5 GHz-1 5 GHz-2 6 GHz	Select 2.4GHz or 5GHz to view the simulation results of the band.
	Click and follow the instruction to specify an area to view the signal strength and the corresponding percentage.
Strong Receiver sensitivity -75 dBm Weak	Adjust the receiver sensitivity, and the new settings will take effect after refreshing the simulation.

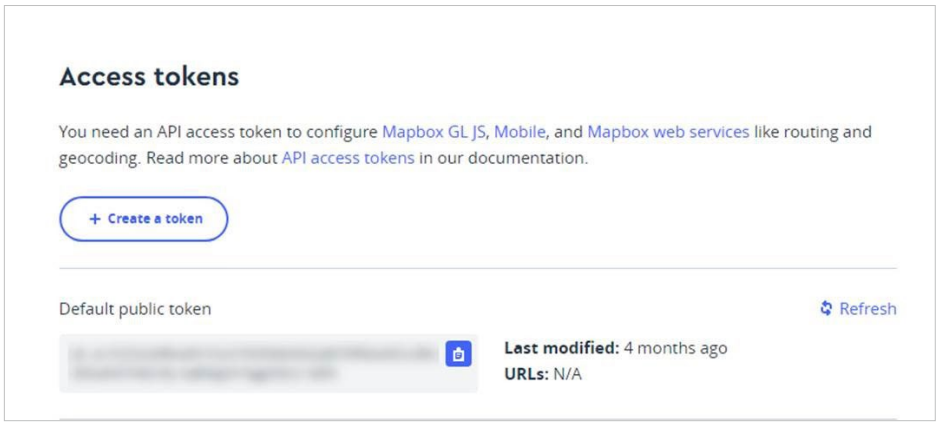
2. (Optional) If you want to export a network coverage report, click the Export icon on the upper right to export a report in .docx format.

10. 1. 2 Threat Management Map

Prerequisite

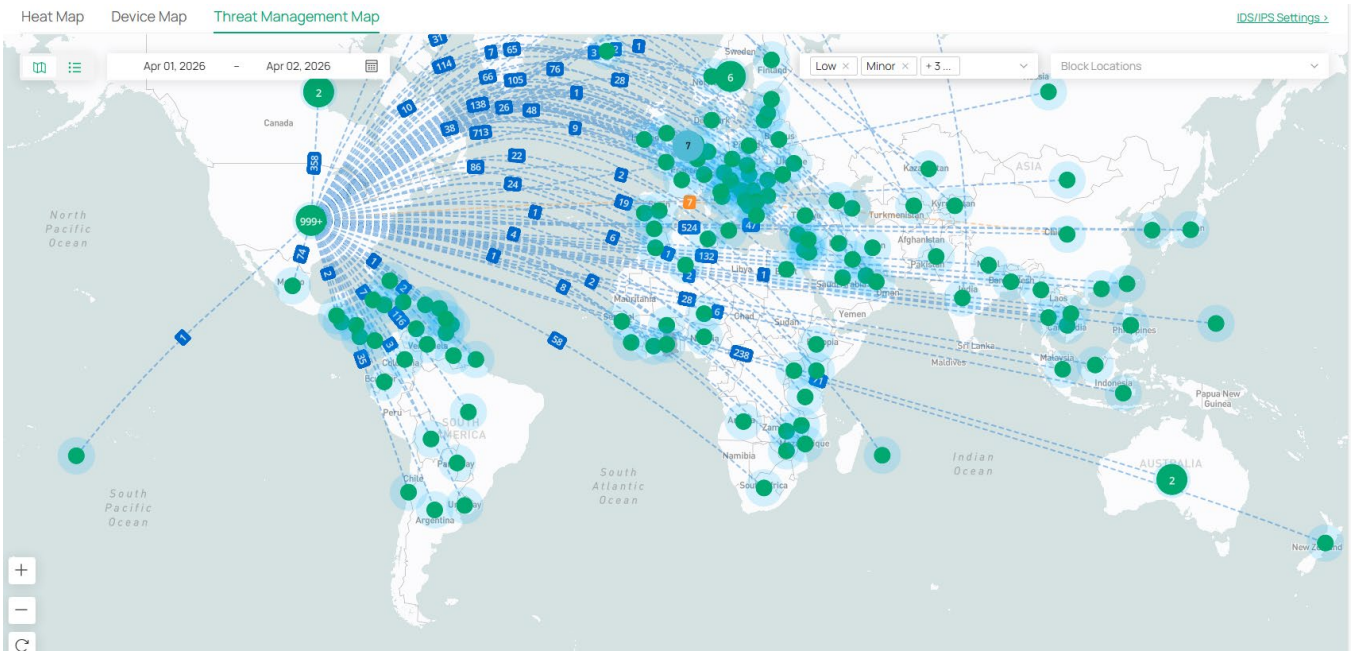
In Threat Management, you can view the threat logs of the IPS/IDS module, figure out the features of the detected threats, and set the actions to counteract the threats. To use Threat Management, please enable IDS/IPS first: click Go to Config, enable IDS/IPS and configure the parameters referring to 16. 3 Configure IDS/IPS for Threat Management.

A valid Mapbox API Access Token is required to use the Device Map function. Visit https://www.mapbox.com, register an account, and obtain the default token on the account page.

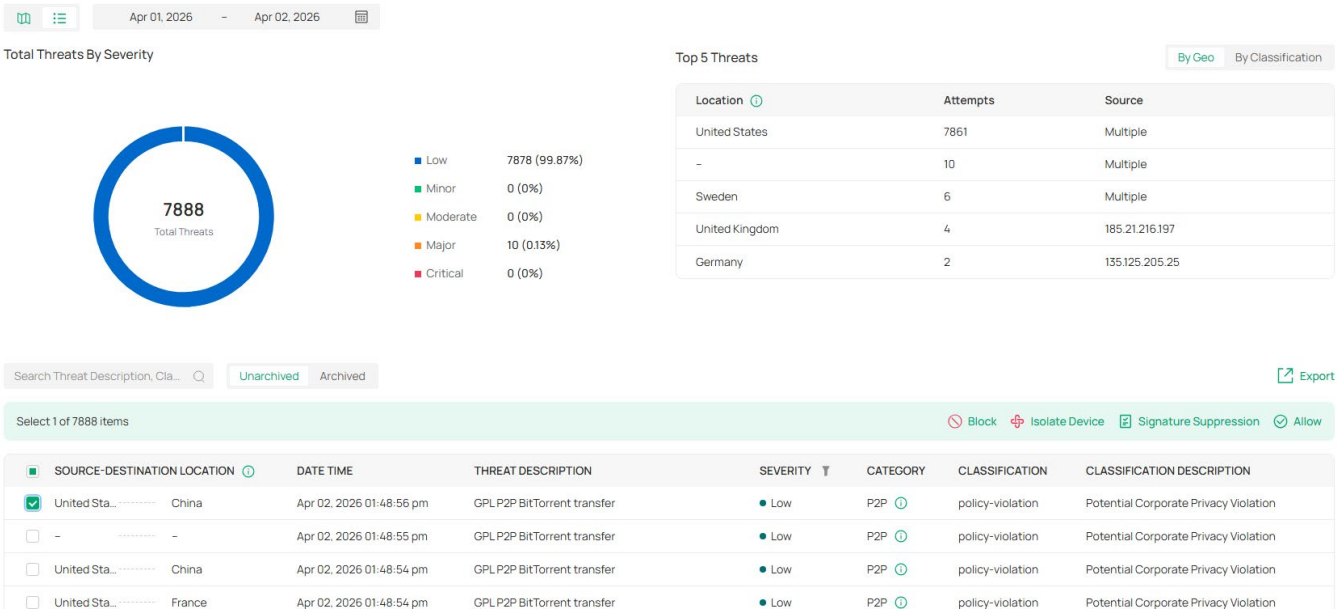


Configuration

1. Go to Map > Threat Management Map.
2. You can right-click a location to block its attack events and manage the Block Locations list at the upper riight corner. If excessive attacks have been detected, you can choose specific severity levels to display.



3. You can click ☰ to view the Threat Management List. In the Threat Management List, you can check top threats by severity, locations of top threats, and unarchived and archived threats. In the unarchived threat list, click an entry, then you can choose a specified response strategy for the corresponding attack IP: Block, Isolate Device, Signature Suppression, or Allow.



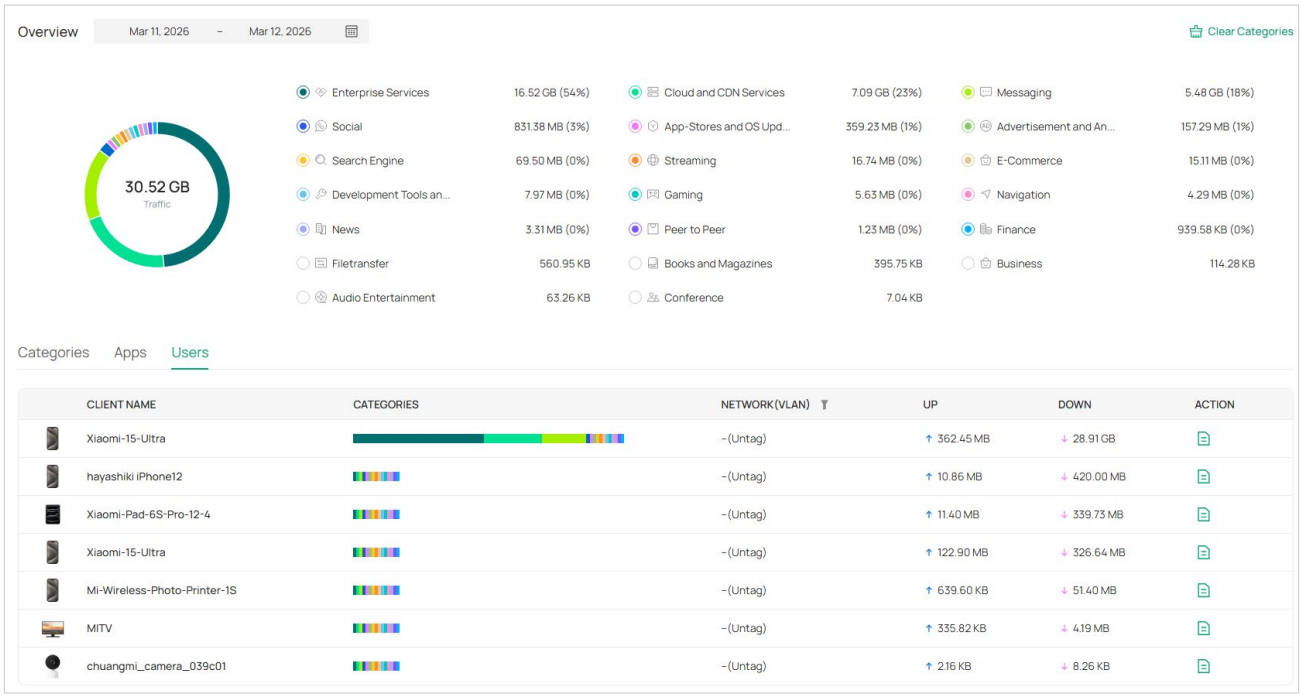
Block	Drop traffic to/from the external IP address and the specific internal IP address. If you block an entry, it will be added to the Block List at Network Config > Security > IDS/IPS.
Isolate Device	Drop traffic to/from the external IP address and any internal IP address.
Signature Suppression	Mute the alerting on certain signatures. This will also disable blocking on traffic matching the designated suppression rule. If you suppress the signature of an entry, it will be added to the Signature Suppression list at Network Config > Security > IDS/IPS.
Allow	Trust the IP address so that the traffic, depending on the direction selected, will not get blocked to or from the identified IP address. If you allow an entry, it will be added to the Allow List at Network Config > Security > IDS/IPS.

10. 2 Monitor the Network with Insights

10. 2. 1 Application Analytics

You can view detailed traffic information if you have adopted a gateway that supports DPI and enabled DPI in Application Control.

Go to Insights > Application Analytics, then you can monitor the network traffic at the application layer.



10. 2. 2 Reports

Network Report shows the statistics of various network indicators and their changes over time, helping network administrators to intuitively and comprehensively understand the current and historical operating status of their network. Thus, it facilitates network administrators to decide whether the Fusion gateway and devices needs to be upgraded and optimized. It also provides network administrators and SI with data support for reporting network conditions.

Go to Insights > Reports, then you can view the connection data of the devices in the topology and the statistics of various network indicators and their changes over time.

Click the tabs on the top to view the statistics of specific section of the network.

Summary	Includes the Health Score (radar chart for Wi-Fi, Client, WAN, and Device), Total Device counts by category, and Client Connection Trends. It also features a Traffic overview showing the ratio of Tx (Transmit) vs. Rx (Receive) traffic across the entire network. You can click the edit icon next to the tab name to customize the statistics to display.
Wired	Tracks Gateway Utilization (CPU/Memory), ISP Load (Throughput vs. Latency), and Switch Health Trends. It monitors hardware status through the Switch Status (Connected/ Disconnected) and Average PoE Utilization widgets. You can click the edit icon next to the tab name to customize the statistics to display.
Wireless	Focuses on Wireless Traffic distribution across 2.4 GHz, 5 GHz, and 6 GHz bands. Key parameters include AP Health Trends, AP Status, and traffic-based rankings for Top 5 APs and Top 5 SSIDs. You can click the edit icon next to the tab name to customize the statistics to display.
Client & Application	Monitors Clients Association Activities (time-stamped logs), Clients with Onboarding Time (connection speed distribution), and a breakdown of Application Categories (e.g., Enterprise Services, Messaging, Peer-to-Peer) by total byte consumption. You can click the edit icon next to the tab name to customize the statistics to display.

Behind the tabs, you can click the + icon to add new tabs and click the setting icon to configure tab settings.

In the upper right, you can click the time control to specify the time period of data to display and click Export to save the network report.

Note: For Linux system, please install Chromium before exporting the network report and make sure you can run Chromium as root.

10. 3 Monitor the Network with Logs

The Fusion gateway uses logs to record the activities of the system, devices, users and administrators, which provides powerful supports to monitor operations and diagnose anomalies.

Different logs can be classified from the following aspects.

- **Notifications**

  Two categories in notifications are Event and Alert, and you can classify the logs into them by yourself.

- **Severities**

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

- **Contents**

  Four types in contents are Operation, System, Device, and Client, which indicate the log contents relating to.

10. 3. 1 Manage Alerts

Alerts are the logs that need to be noticed and archived specially.

To configure logs as Alerts, go to Logs > Alerts. All the logs configured as Alerts are listed under the Alerts tab for you to search, filter, and archive.

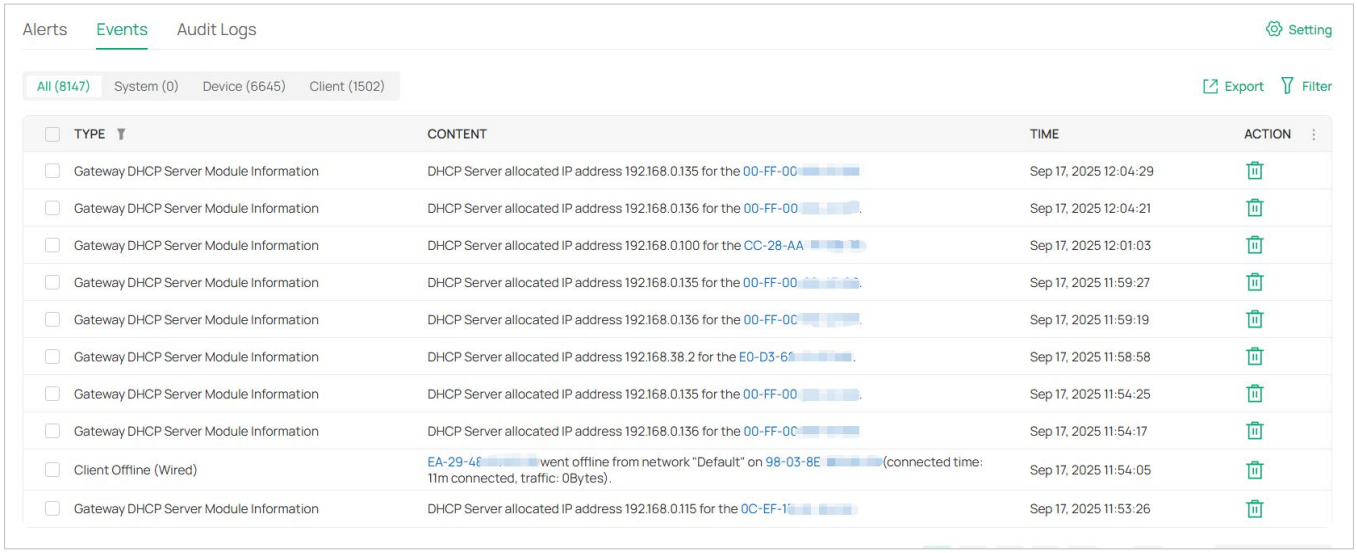
Export	Click to export the logs in .CSV or .XLSX format.
Filter	Click the filter the logs to display.
 	Click to change the view mode for a better overview.  : Displays the logs in a table.  : Displays the logs in graphs.
	Click the tab to filter the unresolved and resolved logs. You can click the Resolved icon or Batch Resolved to resolve a single log and all, respectively.
	Click All to display all types of logs. Click System or Device to display the corresponding type of logs only.
Batch Resolved	Click to resolve the logs in batches.

Batch Delete	Click to delete the logs in batches.
	Click to resolve the log entry.
	Click to delete the log entry. Once deleted the logs cannot be recovered.

10. 3. 2 Manage Events

Events are the logs of state or activity changes within the system.

To configure logs as Events, go to Logs > Events. All the logs configured as Events are listed under the Events tab for you to search and filter.



All (59) System (0) Device (59) Client (0)	All/System/Device/Client: Click All to display all types of logs. Click System or Device or Client to display the corresponding type of logs only.
Export	Click to export the logs in .CSV or .XLSX format.
Filter	Click the filter the logs to display.
Batch Delete	Click to delete the logs in batches.
	Click to delete the corresponding event logs.

10. 3. 3 Manage Audit Logs

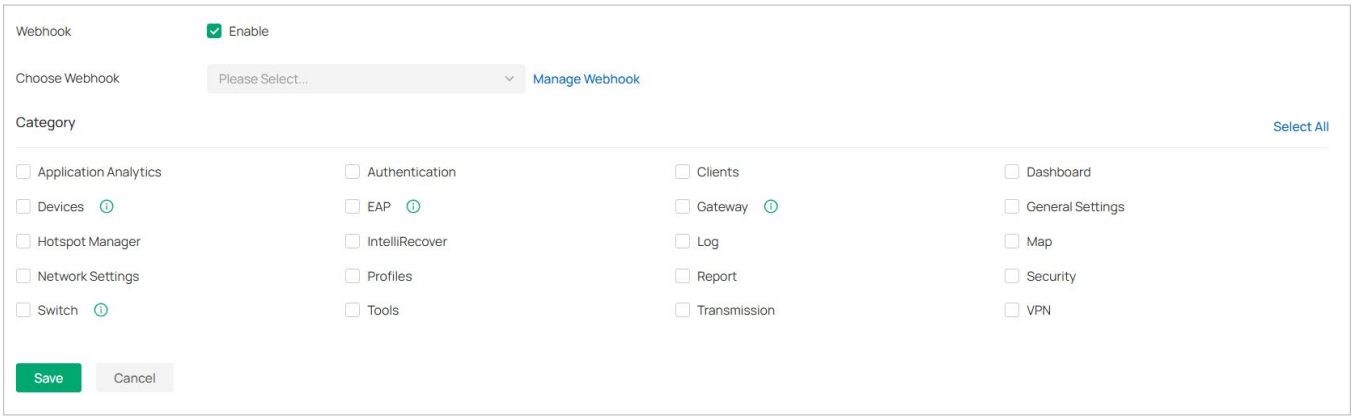
Audit log records information about which accounts have accessed the system, and what operations they have performed during a given period of time.

Step 1: Create Webhooks

Go to Settings > Platform Integration > Webhooks and create webhooks. For detailed configuration, refer to the Webhooks section.

Step 2: Enable Webhook for Audit Logs

1. Go to Logs, click the Setting icon in the upper right, then go to the Audit Logs page.
2. Enable Webhook and choose webhooks.
3. Specify which categories will be sent to the corresponding log server via Webhook.



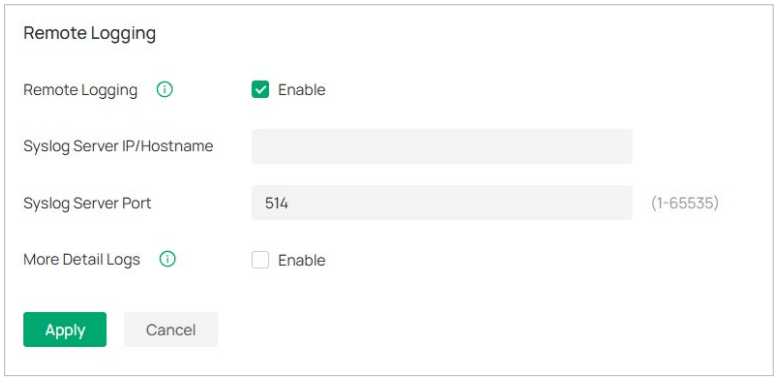
4. Save the settings.

10. 3. 4 Configure Remote Logging

With Remote Logging configured, the Fusion gateway will send the system logs to the specified log server once it is generated.

To configure Remote Logging, follow the steps below:

1. Go to Logs > Alerts, click the Setting icon in the upper right, then go to the Advanced page.
2. Enable Remote Logging and configure the parameters.



Syslog Server IP/ Hostname	Enter the IP address or hostname of the log server.
Syslog Server Port	Enter the port of the server.

More Detail Logs	With the feature enabled, the logs of AP clients and switch system will be sent to the Syslog Server.

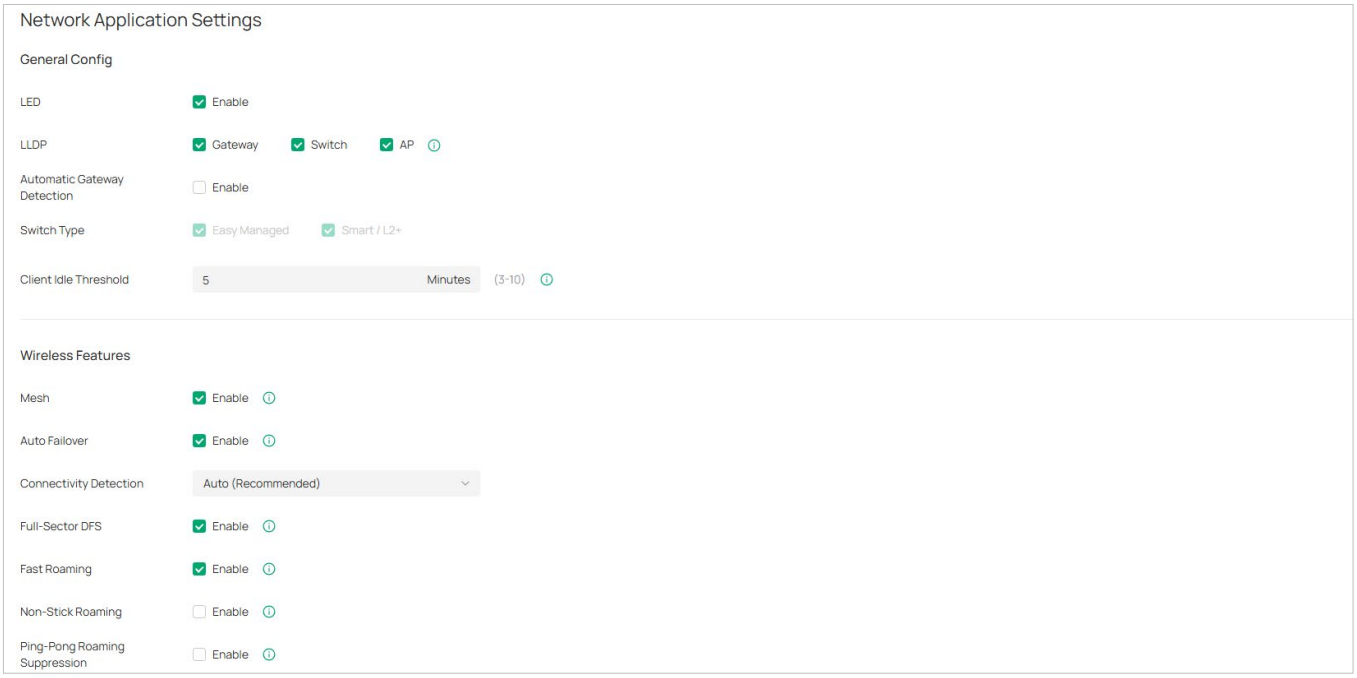
Chapter 11

Configure General Network Settings

This chapter guides you on how to configure general network settings with the Fusion gateway. The chapter includes the following sections:

11. 1 Configure Network Application Settings

1. Go to Network Config > General Settings > Network Application Settings.



2. Configure the parameters according to actual needs.

- General Config

In General Config, you can control the LED status of devices, configure the Fusion gateway to send generated system logs to the log server.

LED	Enable or disable LEDs of all devices.
LLDP	This feature ensures accurate topology recognition.
Automatic Gateway Detection	When enabled, the device can automatically detect gateway changes for IP update. This prevents prolonged failure to refresh and obtain a valid IP due to an unexpired lease, thereby avoiding disruptions to normal operations.
Switch Type	Select the switch types supported for management.
Client Idle Threshold	The Fusion gateway will consider a client offline (thus disconnect it) when it is idle for longer than the specified threshold. If the specified threshold is too short, clients may be disconnected frequently.

- Wireless Features

Wireless features include Mesh, Auto Failover, Connectivity Detection, Full-Sector DFS, EAP LLDP, Fast Roaming, Non-Stick Roaming, AI Roaming, Band Steering, Multicast/Broadcast Rate Limit and Beacon Control. They are applicable to wireless devices. With these wireless features configured properly, you can improve the network's stability, reliability and communication efficiency.

Wireless 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 Wireless Features as their default configurations.

Mesh	With this feature enabled, wireless devices that support Mesh can establish the mesh network at the Fusion gateway.
Auto Failover	Auto failover is used to automatically maintain the mesh network. When enabled, the Fusion gateway will automatically select a new wireless uplink for the Wireless Device if the original uplink fails.
Connectivity Detection	Specify the method of connection detection when mesh is enabled. In a mesh network, the wireless devices can send ARP request packets to a fixed IP address to test the connectivity. If the link fails, the status of these wireless devices will change to Isolated status. Auto (Recommended): Select this method and the mesh wireless devices will send ARP request packets to the default gateway to test the connectivity. Custom IP Address: Select this method and specify a desired IP address. The mesh wireless devices 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 Wireless Device will use IP address of the default gateway for the detection.
Full-Sector DFS	With this feature enabled, when radar signals are detected on current channel by one Wireless Device, the other wireless devices in the mesh network will be also informed. Then all wireless devices in the mesh network will switch to an alternate channel.
Fast Roaming	When enabled, clients supporting 802.11k/v can improve fast roaming experience when moving among different wireless devices.
Non-Stick Roaming	This feature helps disconnect “sticky clients” receiving weak signals from their suboptimal Wireless Device, allowing them to switch to a superior Wireless Device and improve network efficiency. Note that this may cause temporary disconnections or hinder re-association in rare cases.
Ping-Pong Roaming Suppression	This feature prevents clients from frequently roaming between two APs in areas where weak signals overlap, improving connection stability. In rare cases, clients may be unable to connect to certain APs, and AP transmit power may be adjusted dynamically.
AI Roaming	When enabled, Wireless Device will adjust the roaming behaviors based on the current typology and network environment. In this way, AI Roaming will facilitate Fast Roaming and improve roaming experience of the clients that support 802.11k/v.
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, dual-band clients will be steered to the 5 GHz and 6 GHz bands 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. Disable: Turn off Band Steering. Prefer 5 GHz/6 GHz: Choose a specific preferred band. Balance: Balance traffic on all bands.
Multicast/Broadcast Rate Limit	With rate limit configured for Other Multicast, multicast services such as multicast video will be affected.

Management Frame Control	Beacons are transmitted periodically by the Wireless Device to announce the presence of a wireless network for the clients. The beacon control is configured separately for 2.4 GHz, 5 GHz and 6 GHz bands. Beacon Interval: Specify how often the APs send a beacon to clients. DTIM Period: Specify how often the clients check for buffered data that are still on the Wireless Device awaiting pickup. The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the EAP has buffered data for client devices. The DTIM period indicates how often the clients connected with the wireless devices should check for buffered data still on the Wireless Device awaiting pickup. The default value is 1, indicating clients check for buffered data on the Wireless Device at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend that you keep the default interval. RTS Threshold: Specify the threshold value, when 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. RTS (Request to Send) can ensure efficient data transmission by avoiding the conflict of packets. 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. We recommend that you keep the default threshold, which is 2347. Airtime Fairness: When enabled, each client connecting to the Wireless Device 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 in multi-rate wireless networks. Probe Response Maximum Retransmission: Set the maximum number that the AP retransmits probe responses if it does not receive a client acknowledgment. When a client sends a probe request to detect the network, the AP responds with a probe response. However, factors like interference, long distance, or mobile devices (such as passing clients) may cause response loss and trigger retransmissions. Frequent invalid retransmissions in high-density scenarios will occupy wireless channel resources. It is recommended to keep the default value of 1 to balance reliability and efficiency. Probe Response Threshold: When enabled, the AP will filter probe requests with signal strength below the set threshold and stop responding, which may affect weak signal terminals from discovering the network. It is recommended to enable this feature only in high-density scenarios and select the Auto mode to optimize efficiency. In Auto mode, the AP dynamically calculates the threshold based on historical coverage data to avoid wasting wireless resources for devices in non-target areas. In Custom mode, you need to set the threshold manually.

- Device Account

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

Username / Password	Enter a username and password for devices. The new username and password will be applied to all the managed devices. For newly adopted devices, once they are adopted by the Fusion gateway, their username and password becomes the same as settings in device account.

11. 2 Configure SSH Settings

Overview

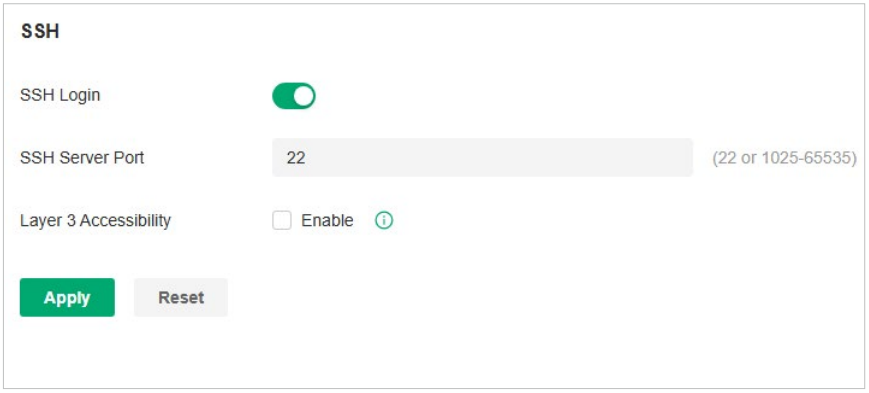
SSH (Secure Shell) provides a method for you to securely configure and monitor network devices via a command-line user interface on your SSH terminal.

Note:

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

Configuration

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



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

11. 3 Configure Schedule Settings

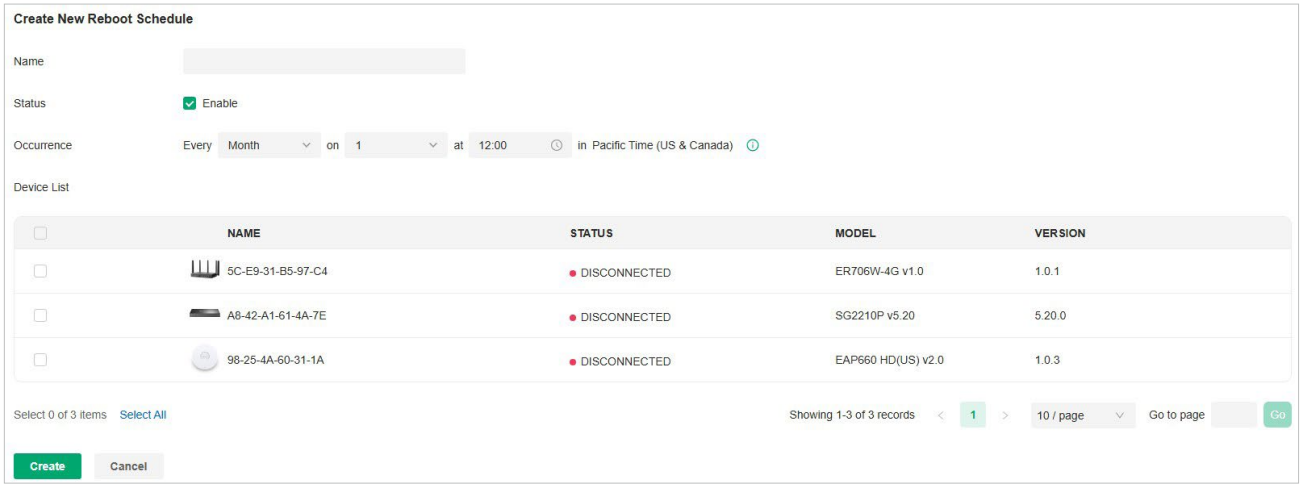
Overview

In Reboot Schedule, you can set schedules to reboot the connected devices periodically based on needs. You can configure the reboot schedule flexibly by creating multiple entries.

In Port Schedule, you can set schedules to control the PoE feature of the PoE switch or control the on/off behavior of the switch port. PoE Schedule has two types: scheduling the PoE supply or the PoE reboot. When the PoE feature is disabled, the PoE switches will not supply power to the connected PoE devices during the specified time period, but the switches can still transmit data; when the Port feature is disabled, please check your topology and related configurations to avoid network problems. You can configure PoE or Port Schedule flexibly by creating multiple entries.

11. 3. 1 Configure Reboot Schedule

1. Go to Network Config > General Settings > Schedule > Reboot Schedule.
2. Click Create New Reboot Schedule to load the following page and configure the parameters.



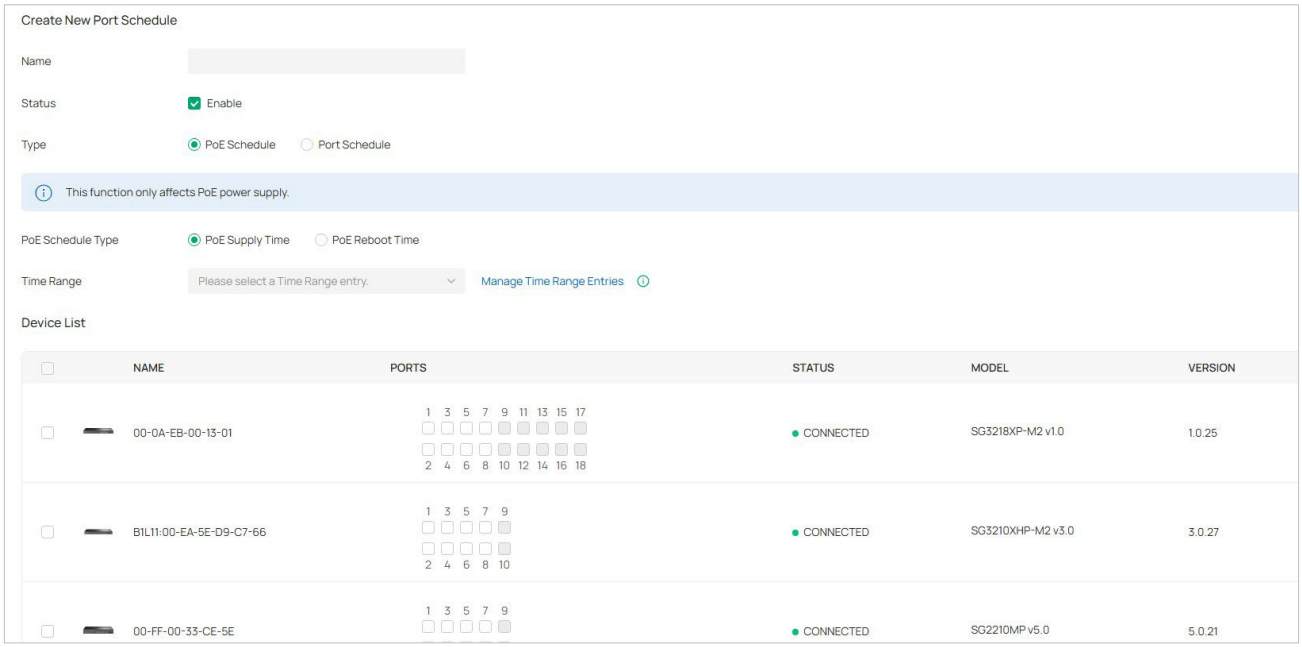
Name	Enter the name to identify the Reboot Schedule entry.
Status	Enable or disable the Reboot Schedule entry.
Occurrence	Specify the date and time for the devices to reboot.
Devices List	Select the devices which the Reboot Schedule applies to.

3. Click Create. The new Reboot Schedule entry will be added to the table.

11. 3. 2 Configure Port Schedule

1. Go to Network Config > General Settings > Schedule > Port Schedule.

2. Click Create New Port Schedule to load the following page and configure the parameters.



Name	Enter a name to identify the PoE or Port schedule entry.
Status	Click the checkbox to enable the PoE or Port schedule entry.
Type	Specify the schedule type.
Time Range	When the Type is PoE Schedule, select the time range when the PoE switches will supply power to the powered devices; when the Type is Port Schedule, select the time range when the switches will turn on the designated ports. You can create a Time Range entry by clicking from the drop down list.
Occurrence	Specify the date and time for the ports to reboot the PoE function.
Devices List	When Type is PoE Schedule, select the PoE switch and PoE port to apply the schedule; when Type is Port Schedule, select the switch and port to apply the schedule.

3. Click Create to save the PoE or Port schedule entry.

Note: Port schedule settings can be applied to devices only when the devices are bound with the device templates specified in port schedule settings

11. 4 Configure mDNS Settings

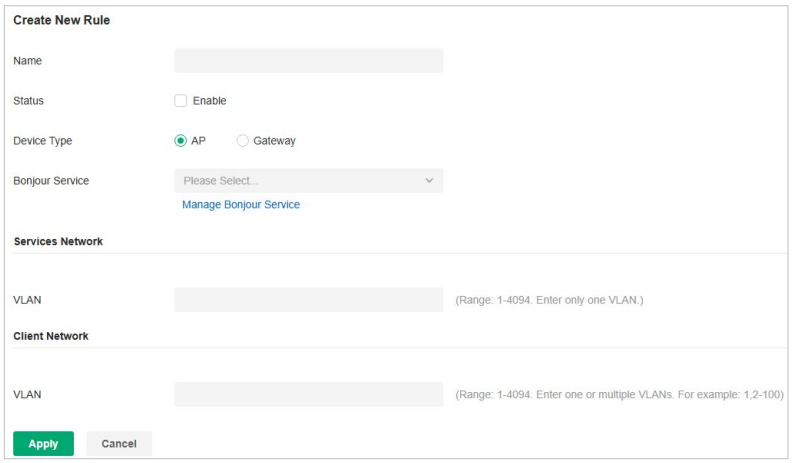
Overview

mDNS (Multicast DNS) Repeater can help forward mDNS request/reply packets between different VLANs. With this function, you can create a forwarding rule to allow the devices in the specified Client VLAN to discover the mDNS service in the specified Service VLAN. You can also specify the services to be forwarded.

The Bonjour service is a zero-configuration network protocol developed by Apple based on the mDNS (Multicast DNS) service. It defines how to use mDNS packets to transmit service information within a VLAN.

11. 4. 1 Configure mDNS Settings

1. Go to Network Config > General Settings > mDNS.
2. Click Create New Rule. Configure the parameters.

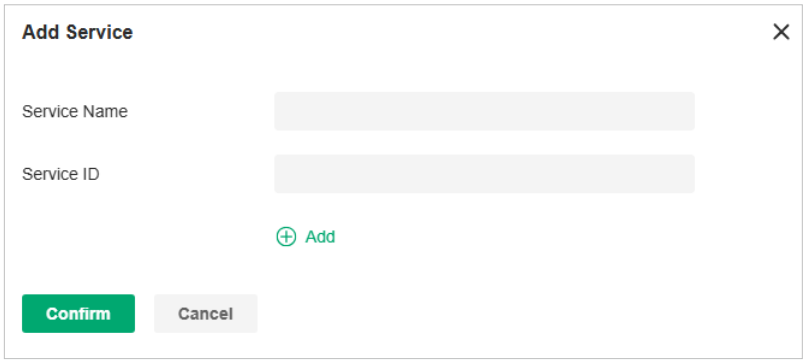


Name	Specify the rule name for identification.
Status	Enable or disable this rule.
Device Type	Specify the device type for which the rule takes effect.
Bonjour Service	Specify the services to be forwarded.
Services Network	VLAN: Specify the VLANs where the mDNS services are located. You can enter VLAN ranges or VLAN IDs separated by comma. Network: Specify the networks where the mDNS services are located.
Client Network	VLAN: Specify the VLANs where the Client devices are located. You can enter VLAN ranges or VLAN IDs separated by comma. Network: Specify the networks where the Client devices are located.

3. Apply the settings.

11. 4. 2 Configure Bonjour Service Settings

1. Launch the Fusion gateway and access a site.
2. Go to Network Config > General Settings > mDNS > Bonjour Service.
3. Click Create New Bonjour Service to add a new profile .



4. Configure the parameters.

Service Name	Specify the profile name for identification.
Service ID	Specify the domain name corresponding to the mDNS service. It is used to identify and filter mDNS packets.

5. Click Confirm to save the profile.

11. 5 Configure VoIP Settings

VoIP (Voice over Internet Protocol) allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

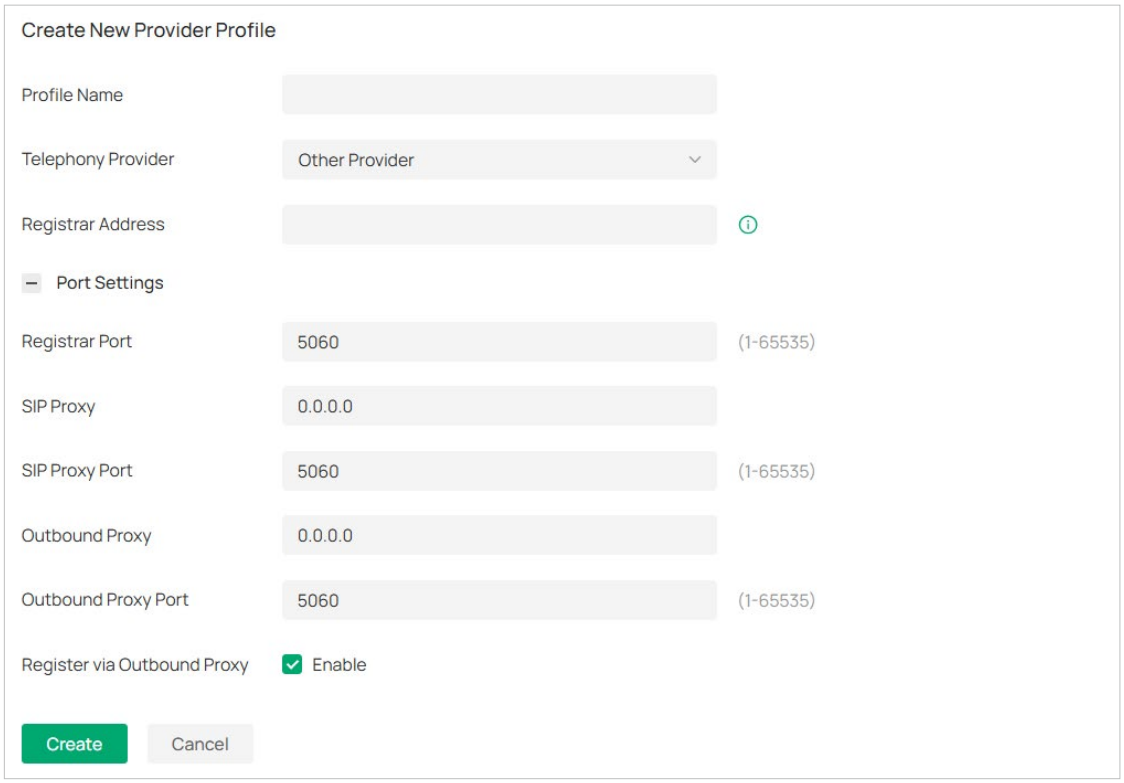
11. 5. 1 Call Settings

Overview

You can create telephony provider profiles, digit map profiles, call blocking profiles, and emergency number settings to facilitate telephony configurations.

Configuration

1. Go to Network Config > General Settings > VoIP > Call Settings.
2. Click Create New Provider Profile. Configure the parameters and click Create.



Profile Name	Enter a name to identify the profile.
Telephony Provider	Choose your telephony provider, then enter the parameters specified by your provider. The parameters differ according to your selection. If your provider is not listed, choose Other Provider, then refer to the following to configure the parameters:

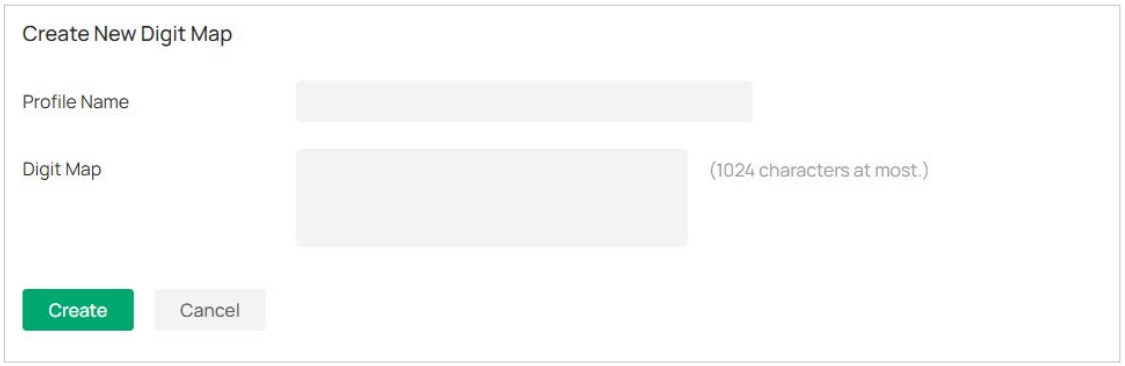
Registrar Address	Specify the registrar address specified by your provider. Usually it is a domain name, if not, an IP address.
Registrar Port	Specify the registrar port. Typically 5060, unless your provider specifies a different port.
SIP Proxy	Specify the IP address or URL of the SIP proxy server.
SIP Proxy Port	Specify the SIP proxy port. Typically 5060, unless your provider specifies a different port.
Outbound Proxy	Specify the IP address or URL of the outbound proxy server.
Outbound Proxy Port	Specify the outbound proxy port. Typically 5060, unless your provider specifies a different port.
Register via Outbound Proxy	When enabled, the connected VoIP devices will use the specified Outbound Proxy for SIP registration. When disabled, the connected VoIP devices will use the Registrar Address above for SIP registration.

3. Configure other call settings according to actual needs.

- Digit Map

A digit map can be used to match digits to control phone numbers from being dialed. A phone number can be dialed out only when its digit sequence matches the digit map.

Click Create New Digit Map. Configure the parameters and click Create.

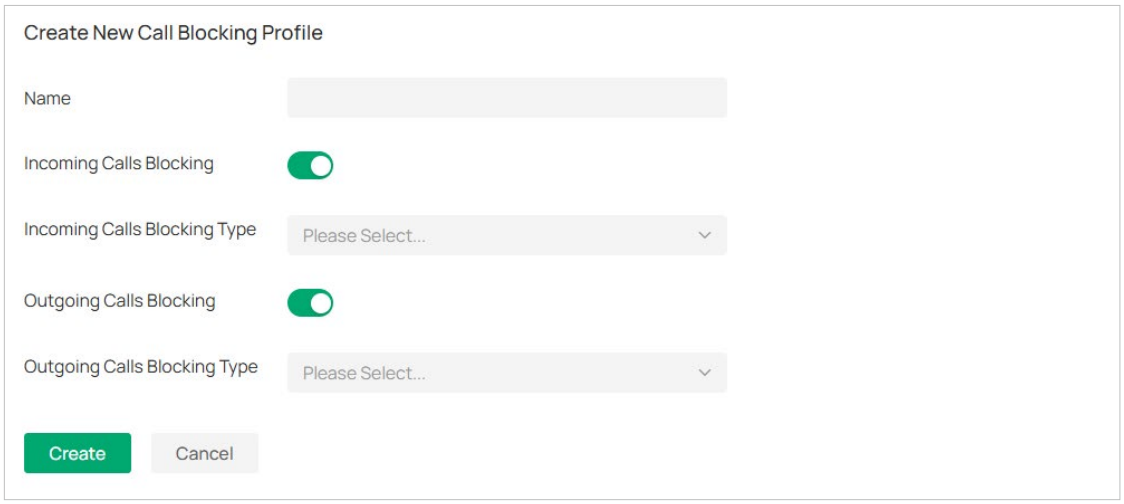


Profile Name	Enter a name to identify the profile.
Digit Map	Enter a digit map by referring to the setting examples.

- Call Blocking

Call Blocking allows the connected VoIP devices to block unwanted incoming and outgoing calls.

Click Create New Call Blocking Profile. Configure the parameters and click Create.



Profile Name	Enter a name to identify the profile.
Incoming Calls Blocking	Enable this option to block unwanted incoming calls.
Incoming Calls Blocking Type	Specify the types of incoming calls to block. Specific Number: Specify one or more phone numbers to block incoming calls from them. Anonymous Number: Block all unknown incoming calls.
Outgoing Calls Blocking	Enable this option to block unwanted outgoing calls.
Outgoing Calls Blocking Type	Specify the types of outgoing calls to block. Mobile: Block outgoing calls to mobile numbers. Landline: Block outgoing calls to landline numbers. Long Distance: Block outgoing calls to long-distance numbers. International: Block outgoing calls to international numbers. Calls with specific number prefix: Specify one or more number prefixes to block outgoing calls to phone numbers with the prefixes.

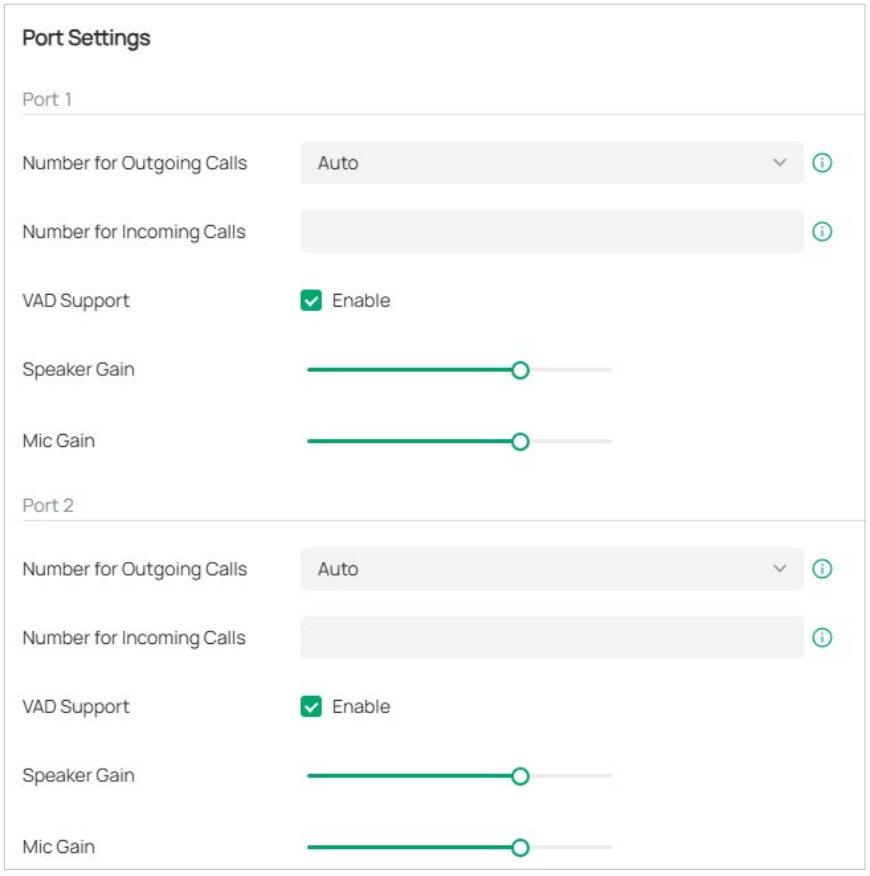
11. 5. 2 VoIP Devices

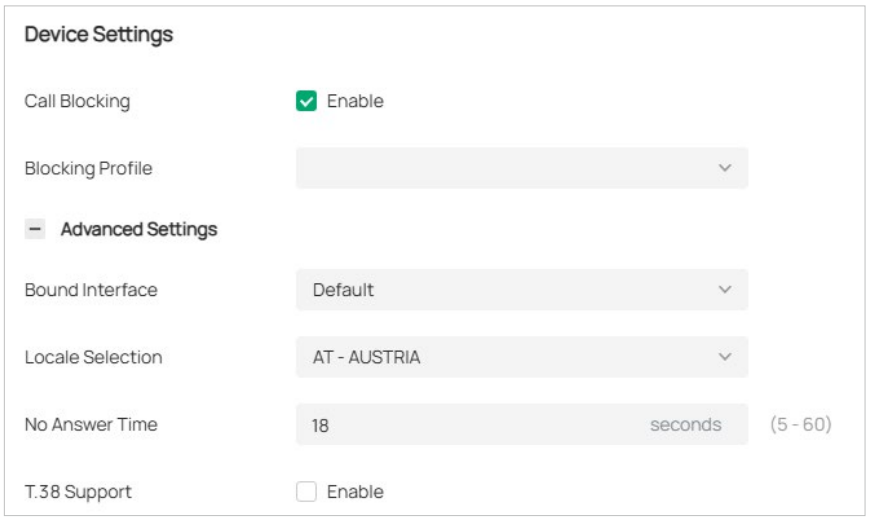
Overview

In VoIP Devices, you can configure and manage the connected VoIP devices.

Configuration

1. Go to Network Config > General Settings > VoIP > VoIP Devices.
2. Click the Telephony Settings icon. Configure the parameters and click Apply.





Number for Outgoing Calls	Select the phone number used by your telephony device to make outgoing calls. The default is Auto, which means the device will automatically select an available phone number to make calls.

Number for Incoming Calls	Select the phone numbers used by your telephony device to receive incoming calls. The default is all registered numbers, which means the device can use all registered numbers to receive calls.
VAD Support	VAD (Voice Activity Detection) saves bandwidth consumption by avoiding transmission of silence packets. It also ensures that the bandwidth is reserved only when voice activity is activated.
Speaker Gain	Adjust the slider to control the speaker sound.
Mic Gain	Adjust the slider to control the microphone sound.
Call Blocking	Enable this function to block unwanted calls.
Blocking Profile	Select a blocking profile to block unwanted calls.
Digit Map Profile	Select a digit map profile to control phone numbers from being dialed. A phone number can be dialed out only when its digit sequence matches the digit map.
Locale Selection	Select your location. The system is embedded with the default location-based parameters such as ring tones.
DSCP for SIP / DSCP for RTP	DSCP (Differentiated Services Code Point) is the first 6 bits in the ToS (Type of Service) byte. DSCP marking allows you to ensure preferential treatment for higher-priority traffic on the network based on the DSCP value. Select DSCP for the SIP (Session Initiation Protocol) and RTP (Real-time Transport Protocol) respectively. If you are unsure, please keep the default value.
DTMF Relay Setting	Select a protocol for DTMF relay setting. If you are unsure of which one to select, please keep the default value.
Registry Expiration Time	Enter the expiration time of the SIP registration.
Registry Retry Interval	Enter the time duration for which the system sends a request to retry registering automatically prior to the Registry Expiration Time. If you are unsure, please keep the default value.
T.38 Support	Select the check box to enable T.38 support that allows fax documents to be transferred in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. This function is only effective between two T.38-enabled terminals.
End with #	Select the check box to use the pound sign (#) as an end-of-dialing.

11. 5. 3 VoIP Phone Number

Overview

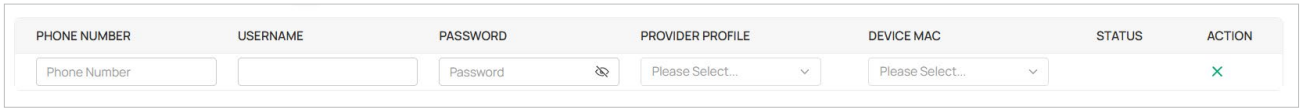
On this page, you can configure phone numbers for VoIP-enabled devices.

Configuration

1. Go to Network Config > General Settings > VoIP > VoIP Phone Number.
2. Choose a method to add phone numbers:

- Add phone numbers separately

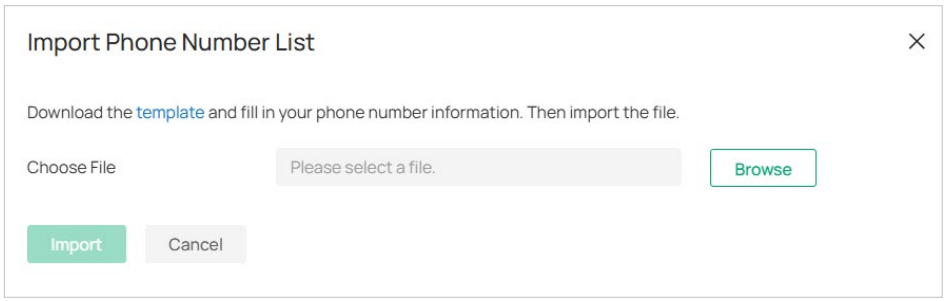
  Click Add. Configure the parameters and click Save.



PHONE NUMBER	The number used to make calls. This number cannot be reused across different devices.
USERNAME	The account name used to register the phone number. Please enter it according to the registration server configuration.
PASSWORD	The authentication password used to register the phone number. Please enter it according to the registration server configuration.
PROVIDER PROFILE	Specify the provider profile associated with the phone number. The phone number will be registered on the corresponding server.
DEVICE MAC	Specify the VoIP device associated with the phone number. Up to eight phone numbers can be added to a device.
STATUS	Displays the phone number's registration status.
ACTION	Edit or delete an added phone number.

- Import phone numbers in batches

  Click Import. Download the template and fill in your phone number information. Then import the file.



- Export phone numbers

  Click Export to export the number file.

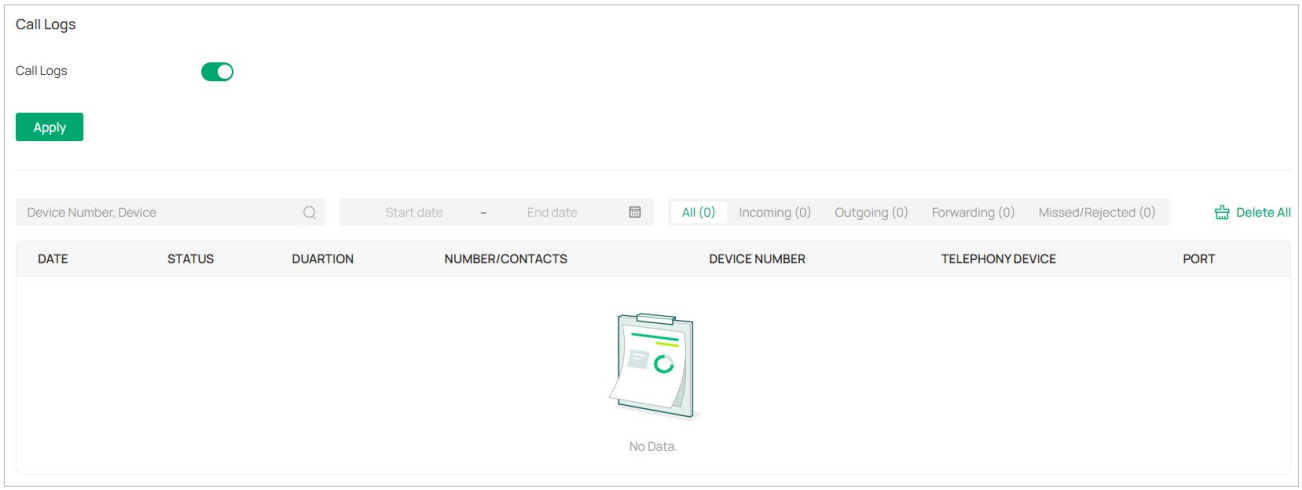
11. 5. 4 Call Log

Overview

In Call Log, you can record the details of incoming calls and outgoing calls.

Configuration

1. Go to Network Config > General Settings > VoIP > Call Log.
2. Enable Call Logs and click Apply. The calls will be recorded in the table below.



11. 5. 5 Advanced Settings

Overview

In Advanced Settings, you can configure Telephone Book,Emergency Number, DND (Do Not Disturb), and Call Forwarding.

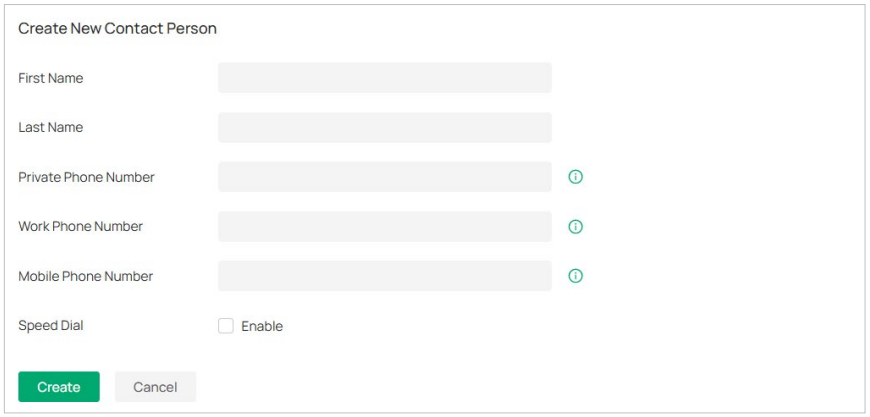
Configuration

1. Go to Network Config > General Settings > VoIP > Advanced Settings.
2. Configure the functions according to actual needs.

- Telephone Book

  In Telephone Book, you can save contact details and assign a speed dial number to the contact.

Click Create New Contact Person. Configure the parameters and click Create.

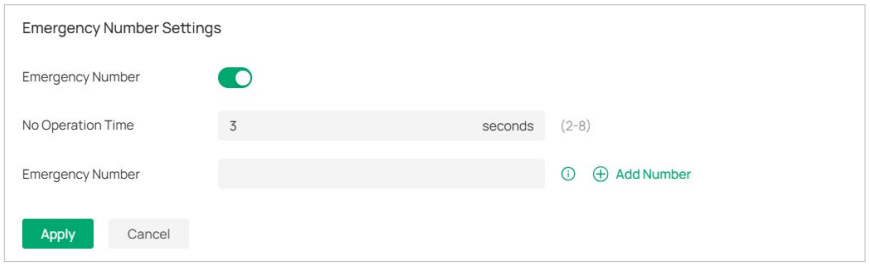


First Name / Last Name	Enter the last name and first name of your contact.
Private Phone Number	Enter the private phone number of your contact.
Work Phone Number	Enter the work phone number of your contact.
Mobile Phone Number	Enter the mobile phone number of your contact.
Speed Dial Number Type	Select the type of number for speed dial. Speed Dial allows you to quickly place a call with fewer numbers to dial.
Speed Dial Number	Set the speed dial number. After saving the settings, you can simply press this number followed by # to place a call.

■ Emergency Number Settings

Emergency number settings can be helpful to make a call for help when emergency occurs.

Enable Emergency Number. Configure the parameters and click Apply.

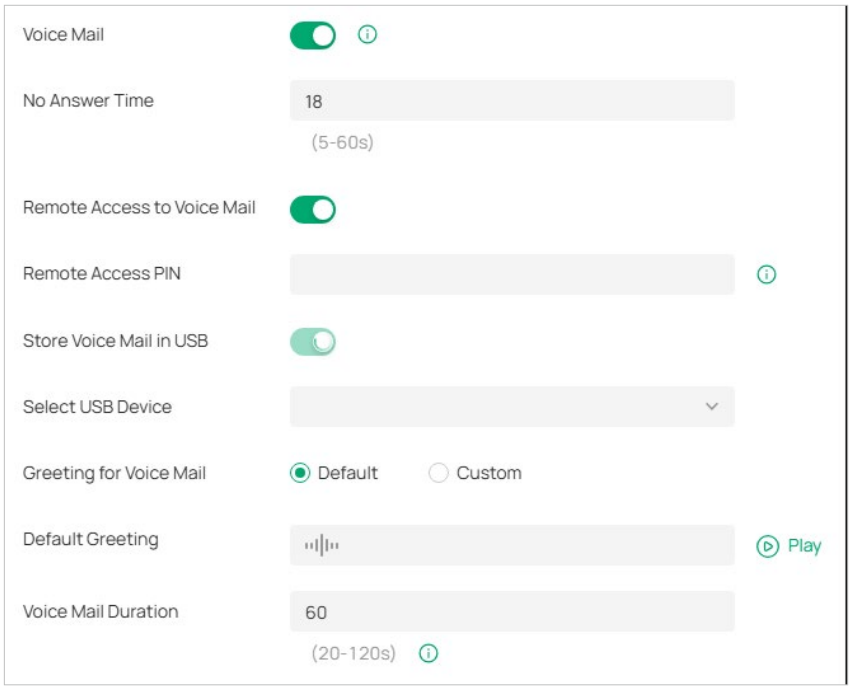


Emergency Number	Enable this function to allow the telephony device to call a specific contact when the handset is picked up but no operation is done within a specific time period.
No Operation Time	Specify the time period before the telephony device makes a call automatically.
Emergency Number	Specify one or more phone numbers for emergency calls. The telephony device will call these numbers in order if the previous call is not answered.

- Voice Mail

Voice Mail allows callers to leave voice messages on an external USB storage device with the appropriate configuration files when calls are not answered. To use this function, plug the USB storage device into the USB port on the gateway. This feature is only available for DSL gateways.

Enable Voice Mail, configure the parameters, and click Apply. The voice mails will be recorded in the Voice Mail List.



No Answer Time	Enter the duration for the incoming calls to go to voicemail or the destination telephone number when there is no response.
Remote Access to Voice Mail	(Optional) If you want to listen to your voice mails remotely, enable Remote Access to Voice Mail.
Remote Access PIN	To access your voice mail remotely, dial the number for incoming calls. When your personal greeting starts, press *. Enter your Remote Access PIN when prompted.
Store Voice Mail in USB	Enable Store Voice Mail in USB. Select a path in the USB storage device to save your voice mail.
Greeting for Voice Mail	Select the Greeting for Voice Mail to use either the default or your custom greeting for the voice mail. You can click the Play icon to play the greeting.
Default Greeting	Click the Play icon to play the greeting.
Voice Mail Duration	Specify the length of each voice mail.

11. 6 Use 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 Fusion gateway supports the following types of CLI configuration:

- **Controller CLI**

  Controller CLI supports batch configuration of devices that support CLI configuration on the controller.

- **Device CLI**

  Device CLI supports batch configuration of selected devices.

- **Model CLI**

  Model CLI simplifies management by targeting configurations at the hardware model level.

Currently, CLI configuration only supports switches. Please refer to the CLI Reference Guide of the correspond Omada switch to understand the CLI commands.

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 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 deliver configurations to the device in the order of GUI, Controller CLI, Model CLI and then Device CLI. If there is a configuration conflict, the configuration delivered last takes effect.
   b. CLI profiles (including Controller CLI profiles and Device CLI profiles) will only be sent to devices once after applied, unless the “Apply Again” button in the Configuration Result is clicked to trigger the full configurations application.
   c. When a device upgrades its firmware, the Controller will deliver the full configurations to the device in the order of GUI, Controller CLI, Model CLI and then Device CLI.
   d. Since the later configuration may overwrite the previous configuration, the running configurations of different devices may be different after the same function has been modified repeatedly through GUI, Controller CLI, Model 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 delivered, 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 through the 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 the GUI, and avoid modifying related configurations via the 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 Fusion gateway.
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.

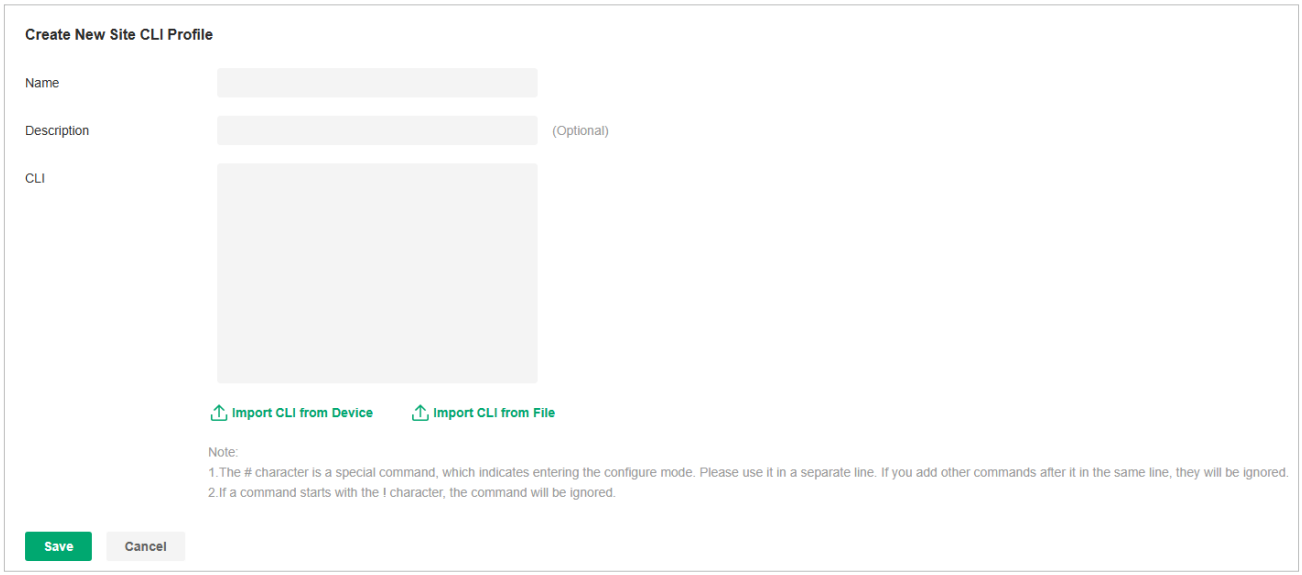
11. 6. 1 Controller CLI

Overview

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

Configuration

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



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.

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 controller.

Note:

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

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.

11. 6. 2 Device CLI

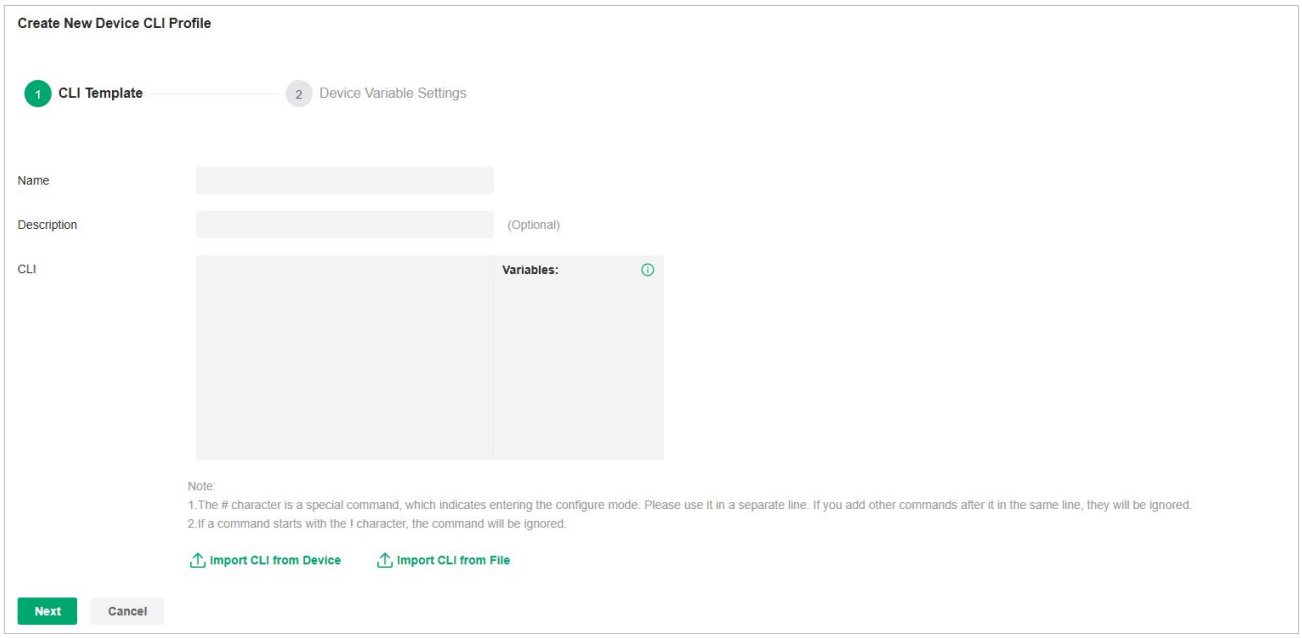
Overview

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 Network Config > General Settings > CLI Configuration > Device CLI. Click Create New Device CLI Profile and create a CLI profile according to your needs.

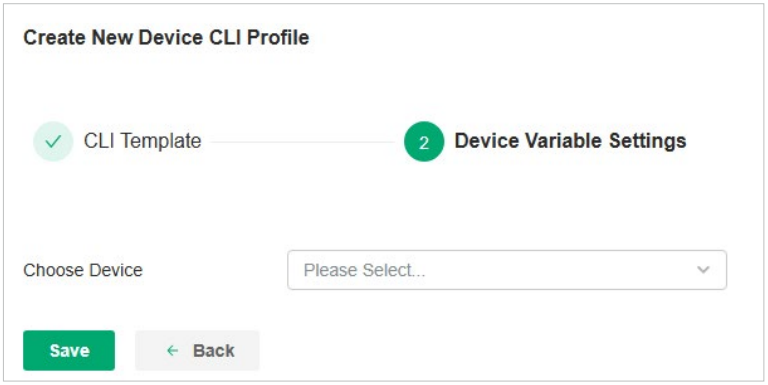


Note:

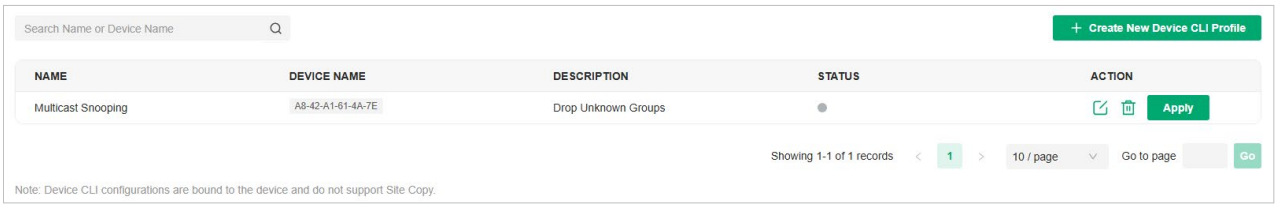
- The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.
- If a command starts with the ! character, the command will be ignored.

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.



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



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.

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.

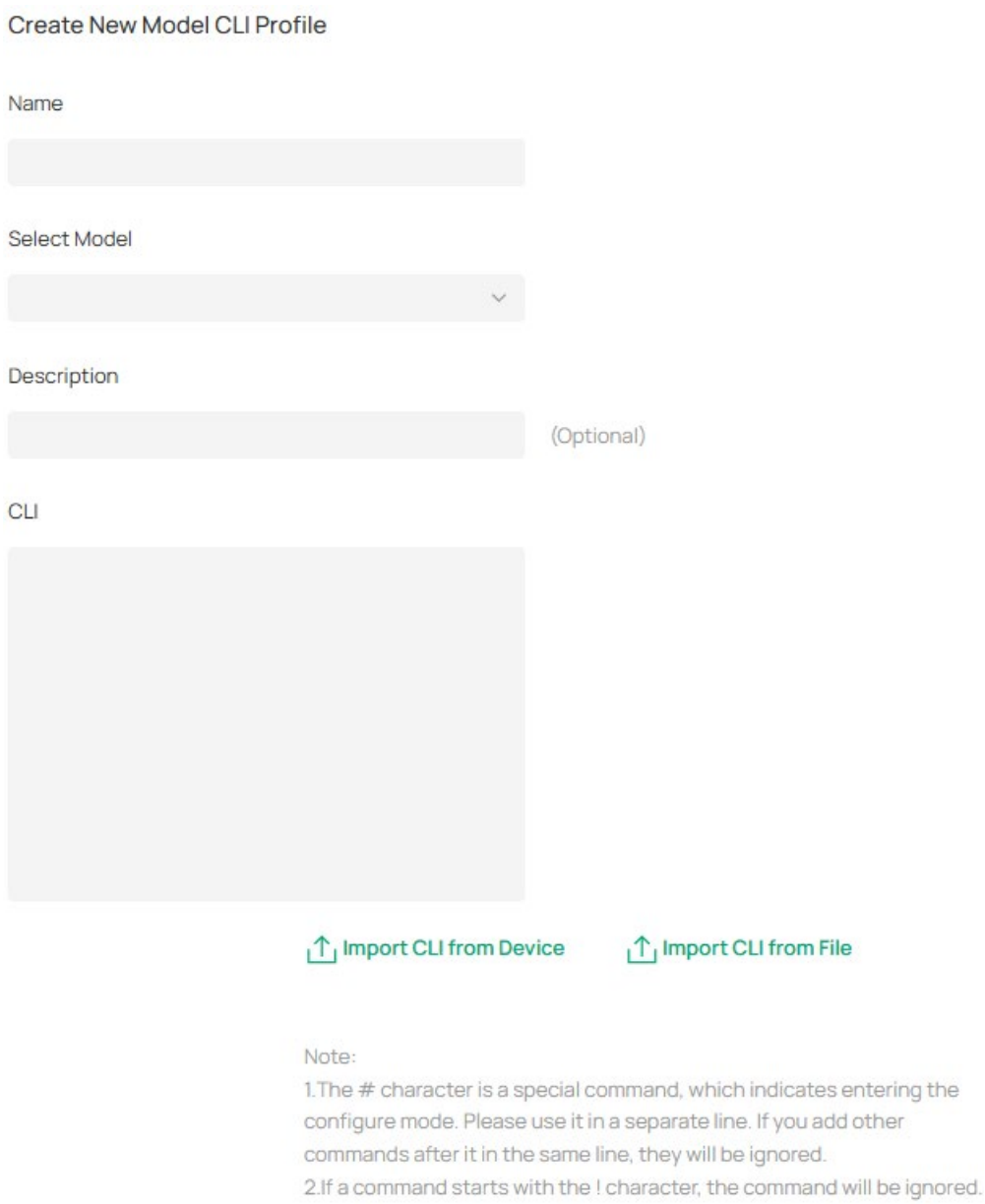
11. 6. 3 Model CLI

Overview

Model CLI allows you to batch configure devices of the same model in the current Controller via the command line.

Configuration

1. Go to Network Config > General Settings > CLI Configuration > Model CLI. Click Create New Model CLI Profile and create a CLI profile according to your needs.



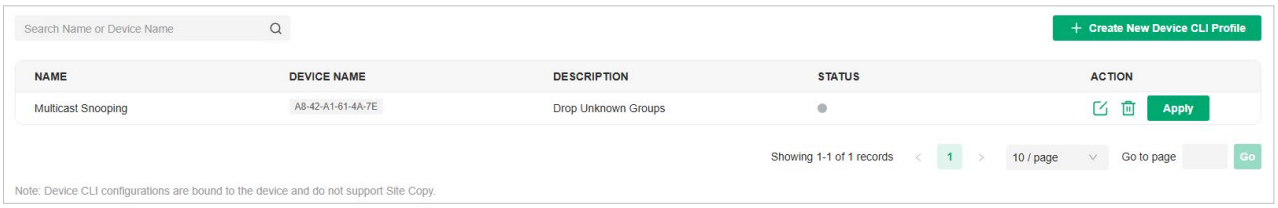
Note:

- 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.
Select Model	Select device model to be configured from the drow-down list.
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 Save to add the profile. The new profile is in inactive state and will not be applied to devices.



3. 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.

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.

11. 7 Configure SNMP Settings

Overview

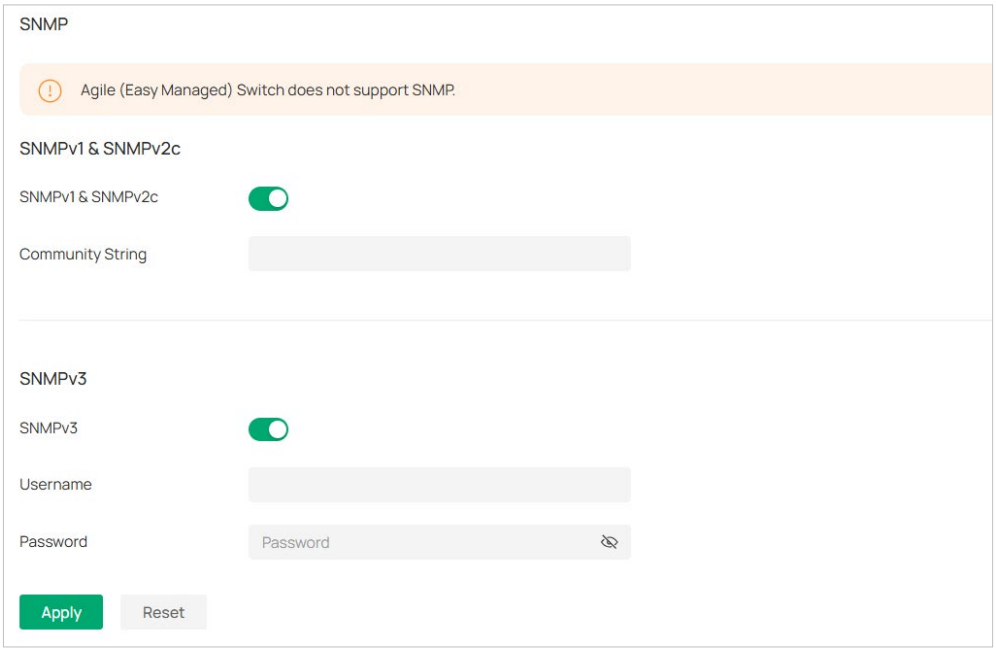
SNMP (Simple Network Management Protocol) provides a convenient and flexible method for you to configure and monitor network devices. Once you set up SNMP for the devices, you can centrally manage them with an NMS (Network Management Station).

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

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

Configuration

1. Go to Network Config > General Settings > SNMP.
2. Configure the parameters. Then click Apply.



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

Chapter 12

Configure WAN Networks

This chapter guides you on how to configure WAN networks with the Fusion gateway. The chapter includes the following sections:

12. 1 Set Up an Internet Connection

Overview

On the WAN page, 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. Virtual WAN allows multiple WAN connections to share one physical WAN port. Each virtual WAN can be configured independently to meet your ISP's requirements. This is useful for separating services, assigning different ISPs, or applying distinct routing and traffic policies without additional hardware.

The parameters of the internet connection for the gateway depends on which connection types you use. For an IPv4 connection, the following internet connection types are available: Dynamic IP, Static IP, PPPoE, L2TP, 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).

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.

Step 1: Select WAN Mode

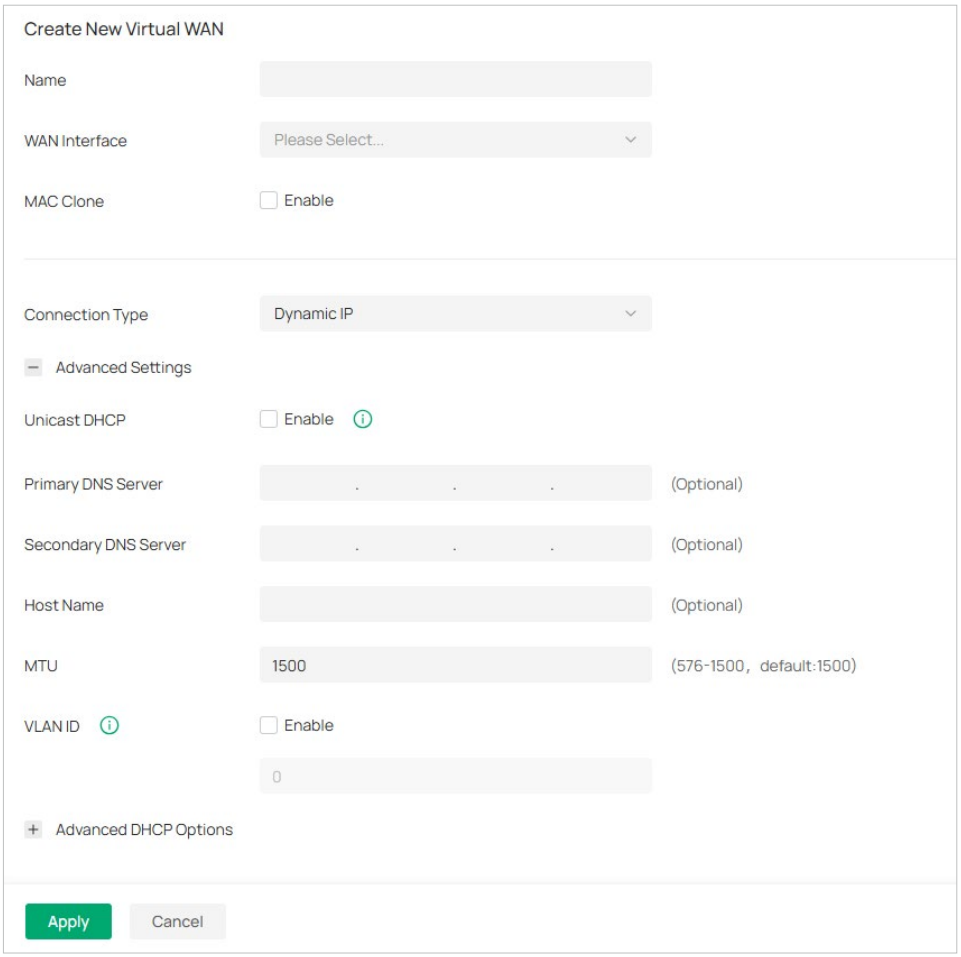
- Configure Physical WAN

Go to Network Config > Network Settings > WAN to load the following page. In the WAN Config > Physical WAN section, toggle the switch on to set the desired ports as WAN ports. You can click the filter icon next to SET AS WAN to filter WAN or LAN ports.

- (Optional) Configure Virtual WAN

Virtual WAN allows multiple WAN connections to share one physical WAN port. Each virtual WAN can be configured independently to meet your ISP's requirements. This is useful for separating services, assigning different ISPs, or applying distinct routing and traffic policies without additional hardware.

Go to Network Config > Network Settings > WAN to load the following page. In the WAN Config > Virtual WAN section, click Create New Virtual WAN to create virtual WAN interfaces as needed and other parameters. Then click Apply.



Name	Enter the name to identify the virtual WAN interface.
WAN Interface	Select the physical WAN interface which the virtual WAN interface is mapped to.
MAC Clone	Enable this option and specify the MAC address of the WAN interface if needed. Typically, this is required when your ISP has bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

Step 2: Configure WAN Connections

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

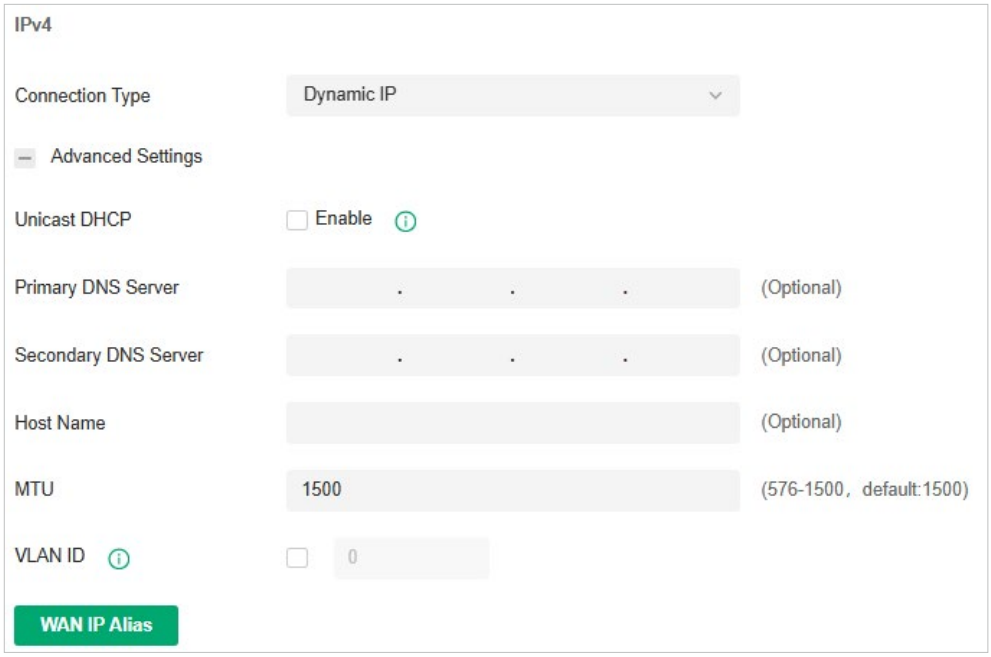
- Set Up IPv4 Connection

Go to Network Config > Network Settings > WAN. In the WAN Config section, click the edit icon of a WAN port and configure the 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. MAP-E: If your ISP provides you with a MAP-E account, select MAP-E. DS-Lite: If your ISP provides you with a DS-Lite account, select DS-Lite.

■ Dynamic IP

Choose Connection Type as Dynamic IP and configure the parameters.

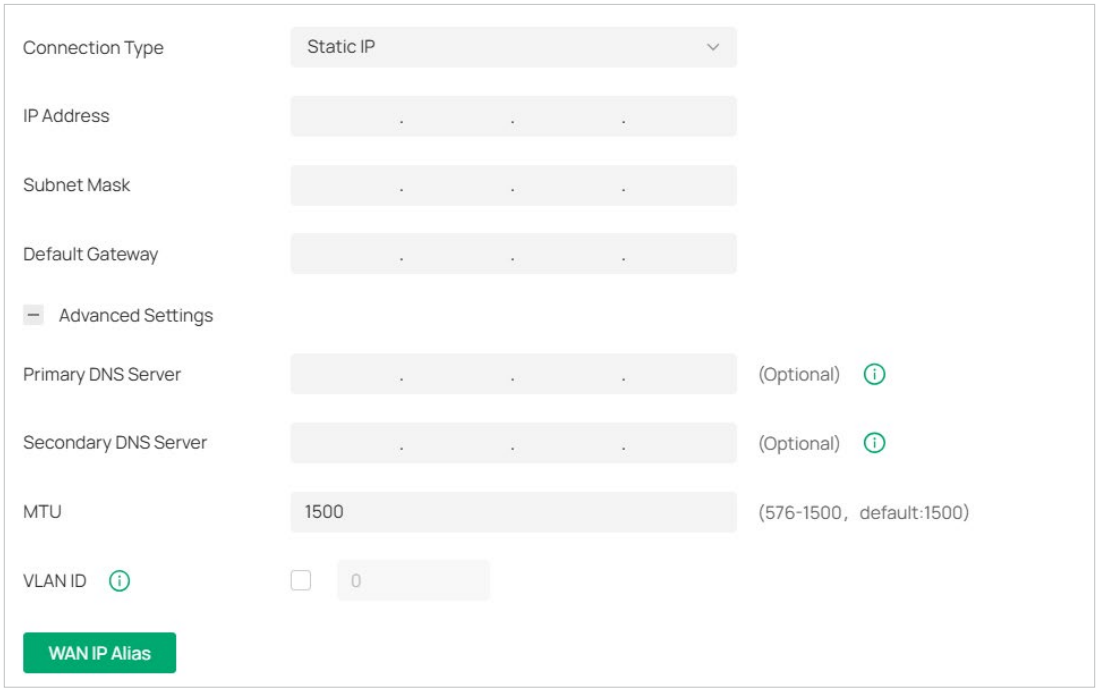


Unicast DHCP	With this option enabled, the gateway will require the DHCP server to assign the IP address by sending unicast DHCP packets. Usually you need not to enable the option.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
Host 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 ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority 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 0 to 7. None means the packet will be forwarded without any operation.
WAN IP Alias	WAN IP Alias supports configuring multiple IP addresses on one WAN port, and these IP addresses can be used to configure virtual server and other functions.

- **Static IP**

  Choose Connection Type as Static IP and configure the parameters.

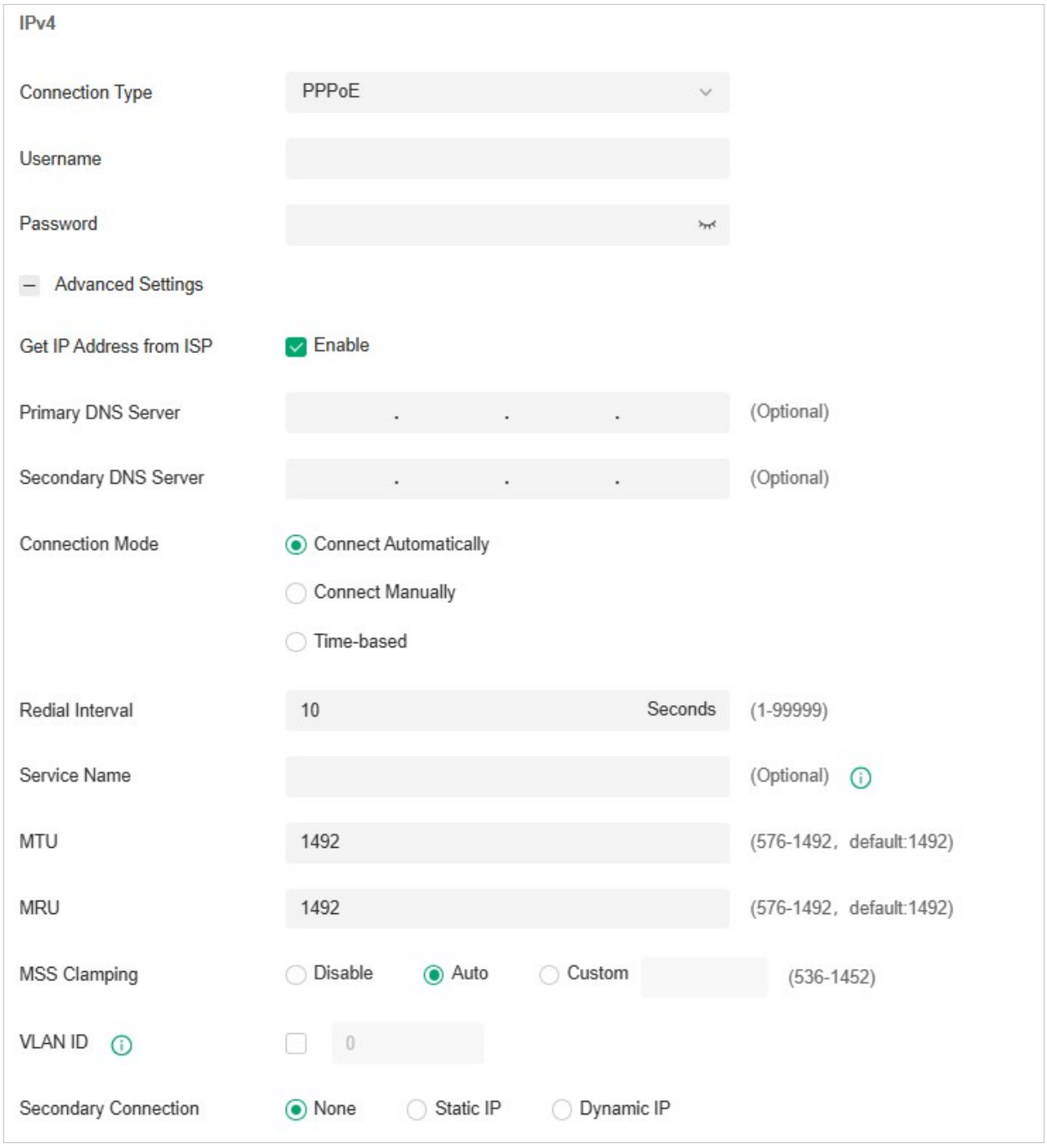


IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Default Gateway	Enter the default gateway provided by your ISP.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
MTU	Specify 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 ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.

VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority 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 0 to 7. None means the packet will be forwarded without any operation.
WAN IP Alias	WAN IP Alias supports configuring multiple IP addresses on one WAN port, and these IP addresses can be used to configure virtual server and other functions.

- **PPPoE**

  Choose Connection Type as PPPoE and configure the parameters.



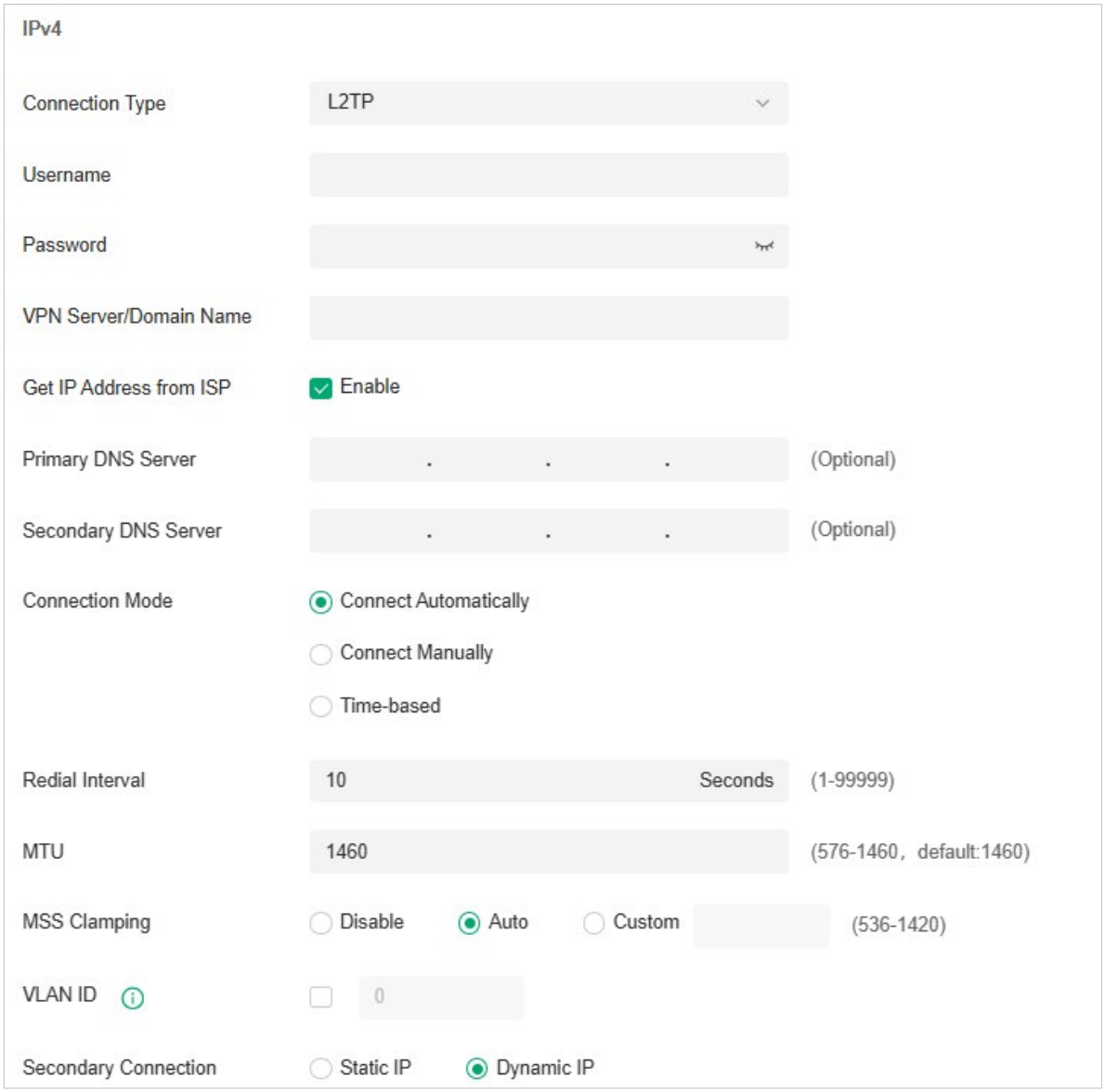
Username	Enter the PPPoE username provided by your ISP.
Password	Enter the PPPoE password provided by your ISP.
Get IP address from ISP	With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection. With this option disabled, you need to specify the IP Address provided 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.
Redial Interval	Specify how often the gateway tries to redial after the connection is down.
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.
MRU	Specify the MRU (Maximum Receive Unit) of the WAN port. MRU is the maximum data unit transmitted in the Data link layer.
MSS Clamping	Specify the upper limit of the value of the MSS (Maximum Segment Size) field negotiated by the sending and receiving parties when establishing TCP connection to avoid IP fragmentation. If the value of the MSS field negotiated by the communication parties exceeds the specified value, the gateway will change the negotiated MSS field to the specified value Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties. Auto: Automatically calculate MSS value based on path MTU. Custom: Select this option to specify the MSS value. It should not exceed the MTU value.
VLAN ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority 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 0 to 7. None means the packet will be forwarded without any operation.

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 parameters.



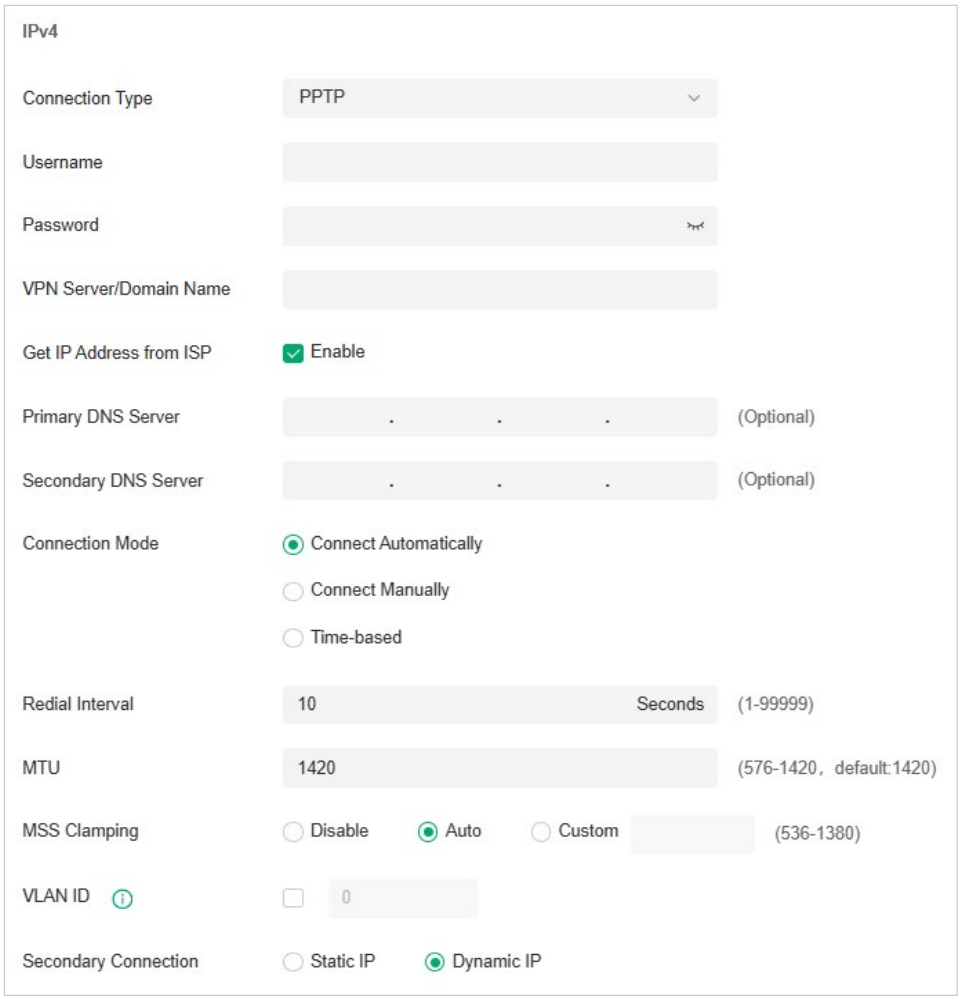
Username	Enter the L2TP username provided by your ISP.
Password	Enter the L2TP password provided by your ISP.

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.
Redial Interval	Specify how often the gateway tries to redial after the connection is down.
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.
MSS Clamping	Specify the upper limit of the value of the MSS (Maximum Segment Size) field negotiated by the sending and receiving parties when establishing TCP connection to avoid IP fragmentation. If the value of the MSS field negotiated by the communication parties exceeds the specified value, the gateway will change the negotiated MSS field to the specified value Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties. Auto: Automatically calculate MSS value based on path MTU. Custom: Select this option to specify the MSS value. It should not exceed the MTU value.
VLAN ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority 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 0 to 7. None means the packet will be forwarded without any operation.

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.

■ PPTP

Choose Connection Type as PPTP and configure the parameters.

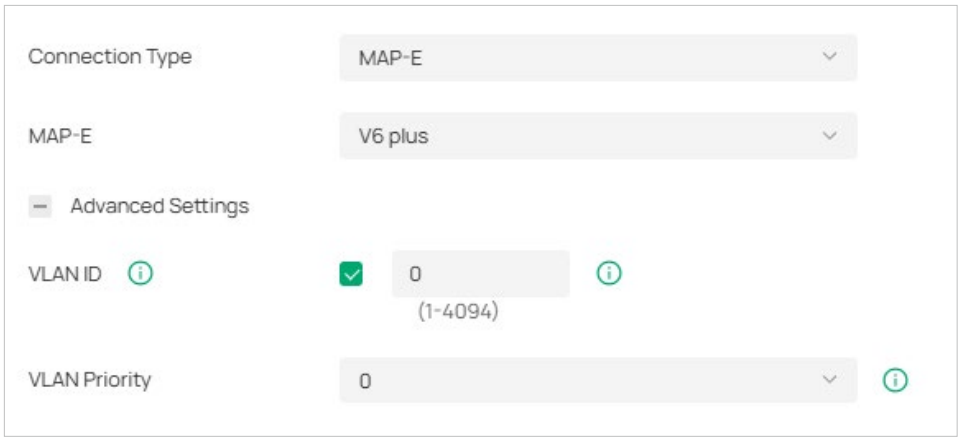


Username	Enter the PPTP username provided by your ISP.
Password	Enter the PPTP password provided by your ISP.
VPN Server / Domain Name	Enter the VPN Server/Domain Name provided by your ISP.

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.
Redial Interval	Specify how often the gateway tries to redial after the connection is down.
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.
MSS Clamping	Specify the upper limit of the value of the MSS (Maximum Segment Size) field negotiated by the sending and receiving parties when establishing TCP connection to avoid IP fragmentation. If the value of the MSS field negotiated by the communication parties exceeds the specified value, the gateway will change the negotiated MSS field to the specified value Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties. Auto: Automatically calculate MSS value based on path MTU. Custom: Select this option to specify the MSS value. It should not exceed the MTU value.
VLAN ID	Add the WAN port to a VLAN and you need to specify the VLAN ID. Generally, you don't need to manually configure it unless required by your ISP.
VLAN Priority	Priority is only available when Internet VLAN is enabled. The VLAN Priority 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 0 to 7. None means the packet will be forwarded without any operation.
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.

- **MAP-E**

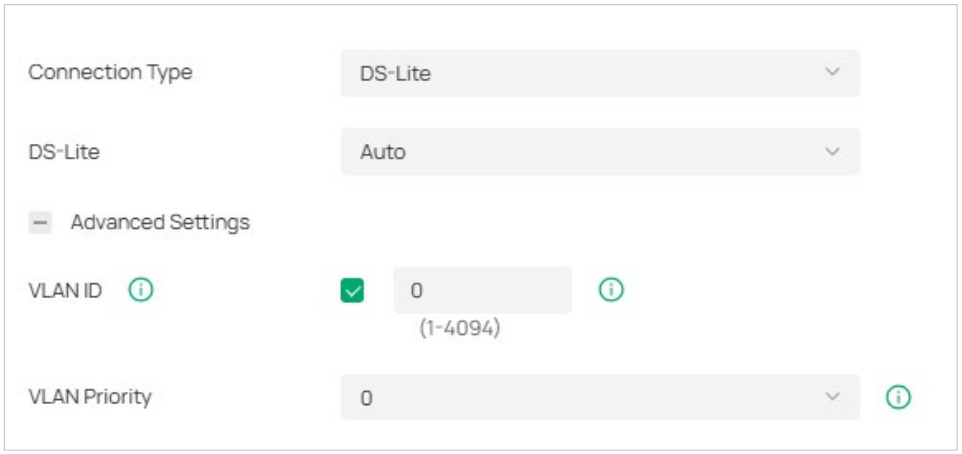
  Choose Connection Type as MAP-E according to your ISP information, click Advanced to configure the parameters as needed. With this connection type configured, some features on this WAN port (such as VPN, SD-WAN, IGMP, DDNS, UPnP, Disable NAT, Port Forwarding, NAT ALG) will not be available.



MAP-E	V6 plus, IPv6 Option, and OCN virtual connect are supported.
VLAN ID	If the WAN port has VLAN enabled, enter the VLAN ID, and the WAN port will automatically join the VLAN. By default, the egress rule of VLAN is UNTAG, so the packets sent by the WAN port do not carry VLAN tags. If you want the packets sent by the WAN port to carry VLAN tags, configure its egress rule as TAG.
VLAN Priority	Priority is available only when VLAN is enabled. The VLAN Priority feature can prioritize the internet traffic as needed. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 0 to 7.

- **DS-Lite**

  Choose Connection Type as DS-Lite according to your ISP information, click Advanced to configure the parameters as needed. With this connection type configured, some features on this WAN port (such as VPN, SD-WAN, IGMP, DDNS, UPnP, Disable NAT, Port Forwarding, NAT ALG) will not be available.



DS-Lite	Select the connection type according to your ISP information. Auto: AFTR name will be automatically identified based on your ISP information. Manual: Manually enter the information provided by your ISP, which could be a URL or an IPv6 address. Transix(gw.transix.jp): Provided by Multifeed. IPv4 traffic is tunneled and encapsulated to the carrier's AFTR for centralized NAT translation. Xpass(dgw.xpass.jp): Provided by ARTERIA. Its underlying mechanism aligns with transix, enabling IPv4 access through carrier-grade NAT. V6 connect(dslite.v6connect.net): Provided by Asahi Net. It employs DS-Lite protocol encapsulation for IPv4 traffic, with all NAT state managed by the carrier side.
VLAN ID	If the WAN port has VLAN enabled, enter the VLAN ID, and the WAN port will automatically join the VLAN. By default, the egress rule of VLAN is UNTAG, so the packets sent by the WAN port do not carry VLAN tags. If you want the packets sent by the WAN port to carry VLAN tags, configure its egress rule as TAG.
VLAN Priority	Priority is available only when VLAN is enabled. The VLAN Priority feature can prioritize the internet traffic as needed. You can determine the priority level for the traffic by specifying the tag. The tag ranges from 0 to 7.

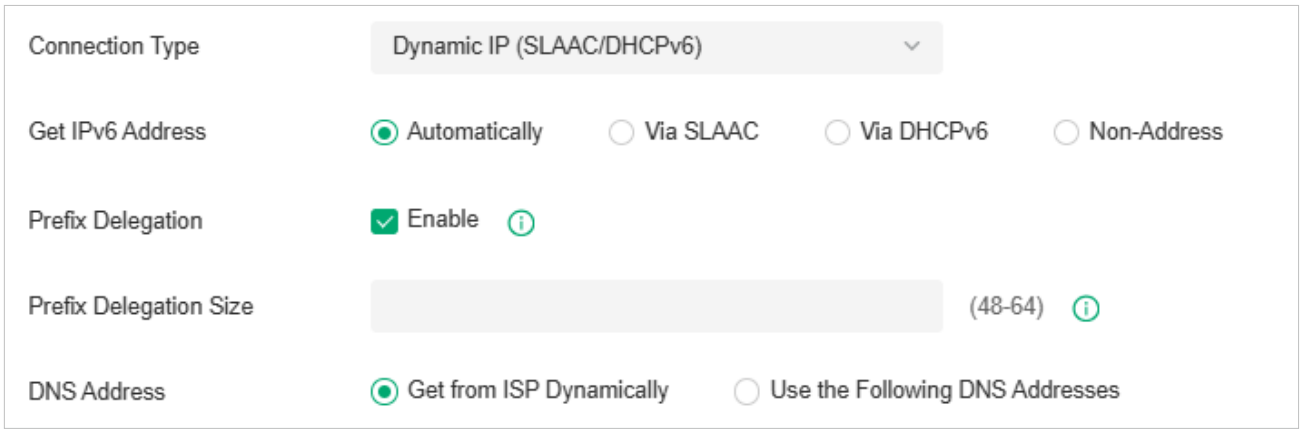
- Set Up IPv6 Connection

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 parameters.



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.

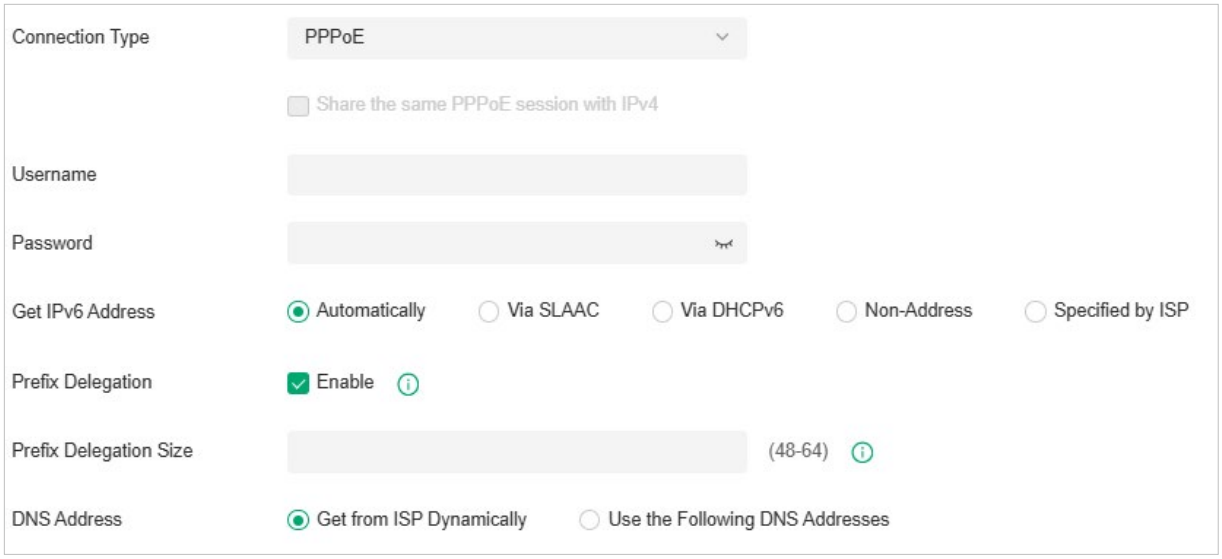
- **Static IP**

  Choose Connection Type as Static IP and configure the parameters.

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**

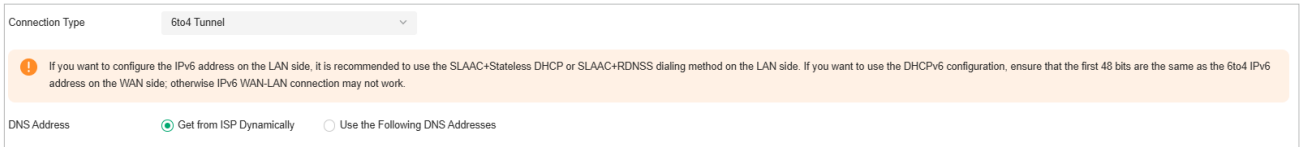
Choose Connection Type as PPPoE and configure the following parameters. Then click Apply.



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 parameters.



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.

- Set Up MAC Address

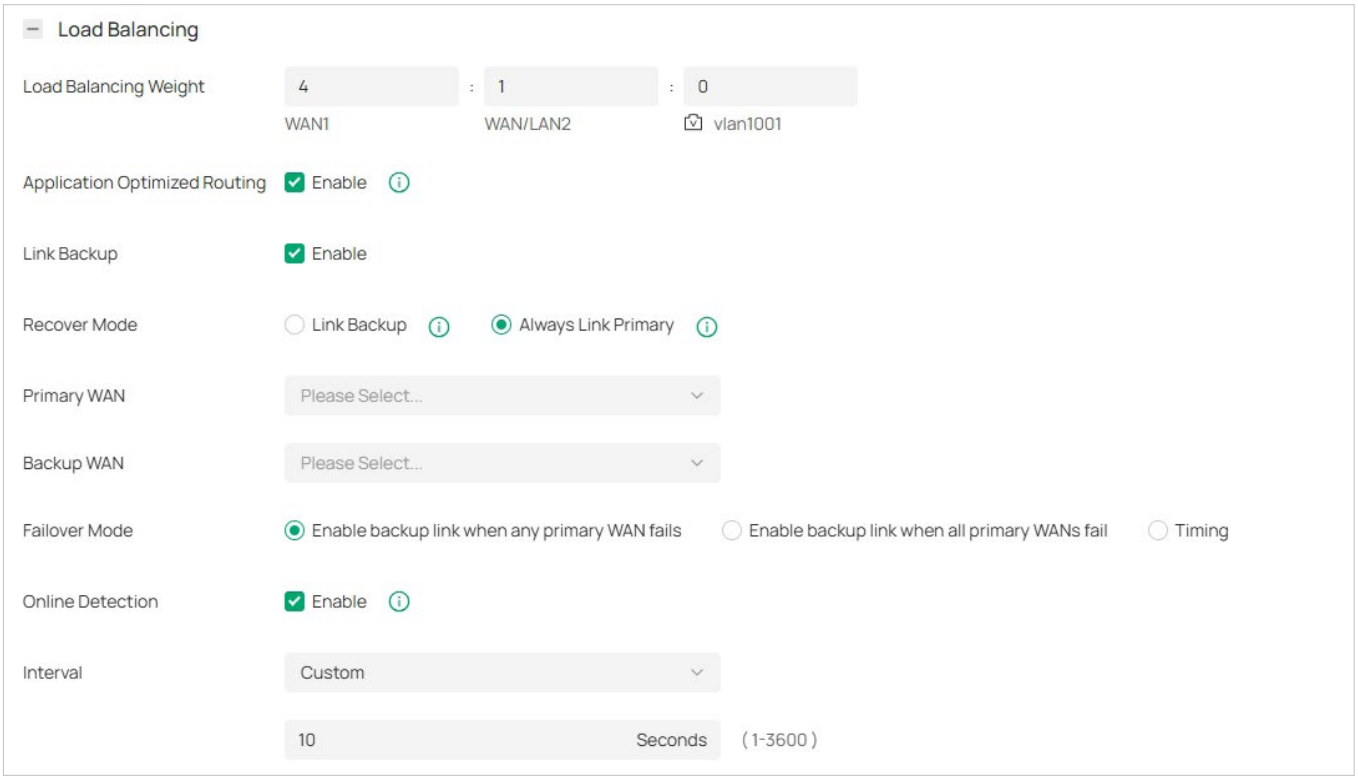
Go to Network Config > Network Settings > WAN. In the WAN Config section, click the edit icon of a WAN port and configure the MAC address according to actual needs.

MAC Clone	Enable this option and specify the MAC address of the WAN interface if needed. Typically, this is required when your ISP has bound the MAC address with your account or IP address. If you are not sure, contact the ISP.

12. 2 Configure Load Balancing

When more than one WAN port (including Virutal WAN) is configured, you can configure Load Balancing to optimize the resource utilization if needed.

Go to Network Config > Network Settings > WAN. In Load Balancing, configure the following parameters and click Apply.



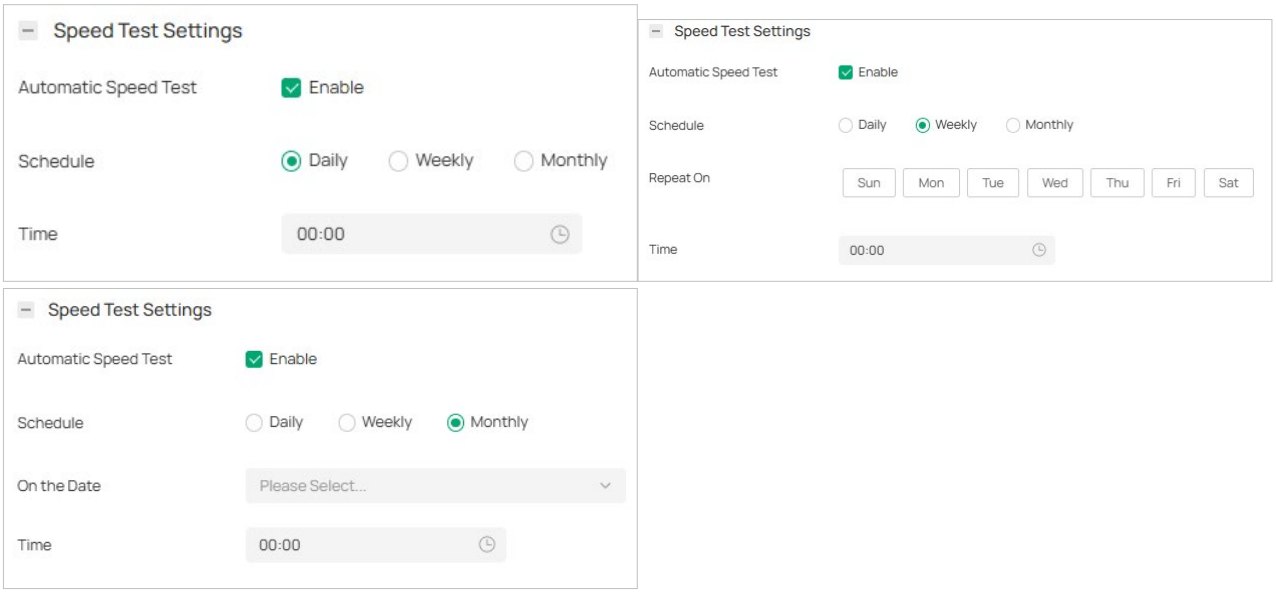
Load Balancing Weight	Specify the ratio of network traffic that each WAN port carries.
Application Optimized Routing	With Application Optimized Routing enabled, the gateway will consider the source IP address and destination IP address (or destination port) of the packets as a whole and record the WAN 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 gateway will switch all the new sessions from dropped lines automatically to another to keep an always on-line network.
Recover 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.
Primary WAN	Specify the primary WAN port. You can choose one or more primary WAN ports to perform load balance.

Backup WAN	Specify a backup WAN which will take over to forward the traffic when the primary WAN fails.
Failover Mode	Select when to enable the backup link. Enable backup link when any primary WAN fails: Link Backup will be enabled when any one of the primary WANs fails. Enable backup link when all primary WANs fail: Link Backup will be enabled only when all primary WANs fail. Timing: Link Backup will be enabled after the specified effective time is reached. When the effective time starts, traffic on the primary WAN will be switched to the backup WAN; when the effective time ends, traffic on the backup WAN will be switched to the primary WAN.
Online Detection Interval	Select how often the WAN ports detect WAN connection status. If you don't want to enable online detection, select Disable. 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.

12. 3 Configure Speed Test Settings

Configure the speed test setting, and the system will automatically test the speed of all WAN ports according to predefined time.

Go to Network Config > Network Settings > WAN. In Speed Test Settings, check the box to enable Automatic Speed Test, specify the test schedule and click Apply.



Schedule	Specify the schedule mode to automatically test the speed.
Daily	When this option is selected, specify the specific time, and the system will automatically test the speed at this specific time every day.
Weekly	With this option is selected, select the day and specify time to repeat, and the system will automatically test the speed at the specific time on the selected day.
Monthly	With this option is selected, select the date of every month and specify time to repeat, and the system will automatically test the speed at the specific time on the selected date each month.

12. 4 Configure Dynamic DNS

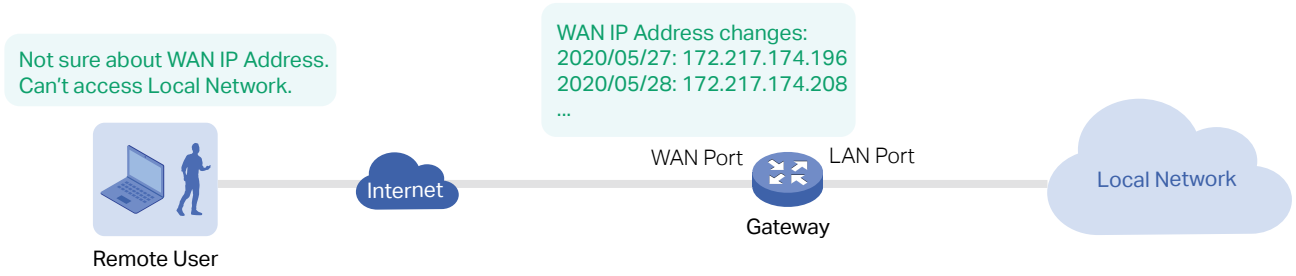
Overview

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.

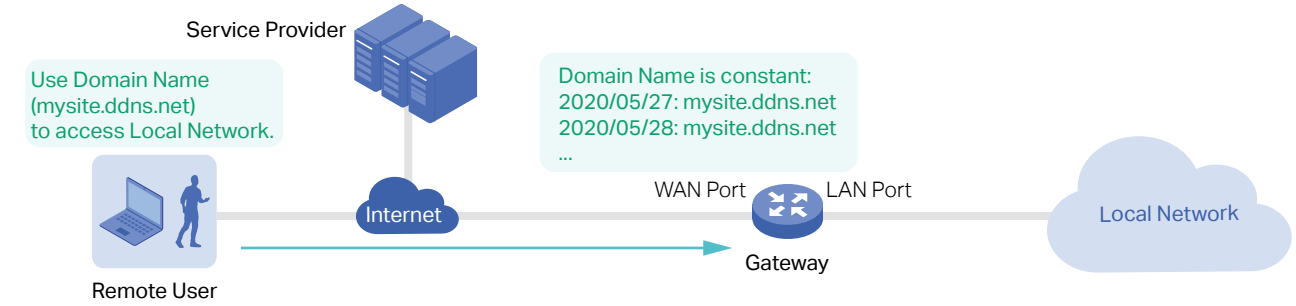
Before:

- 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.



After:

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

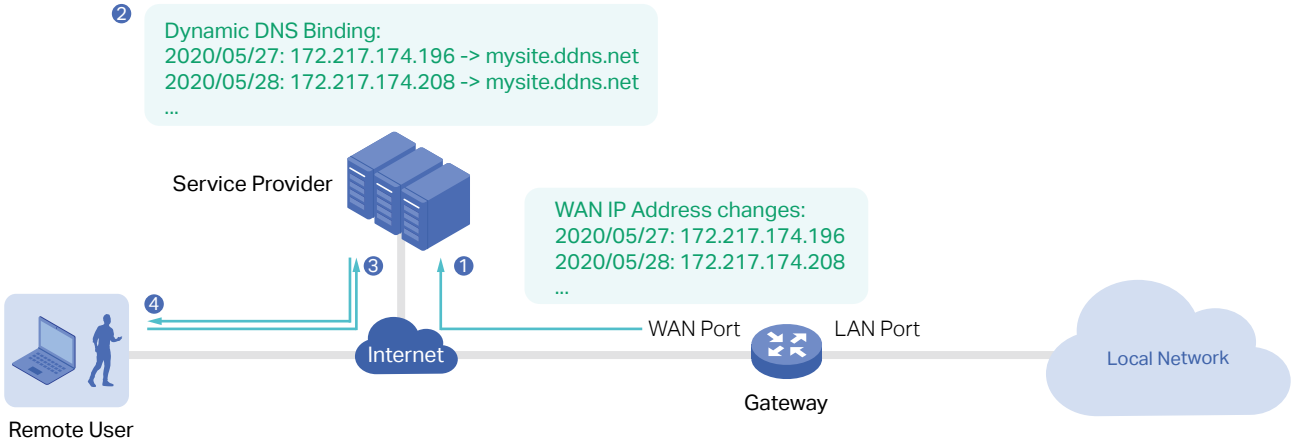


Prerequisite:

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

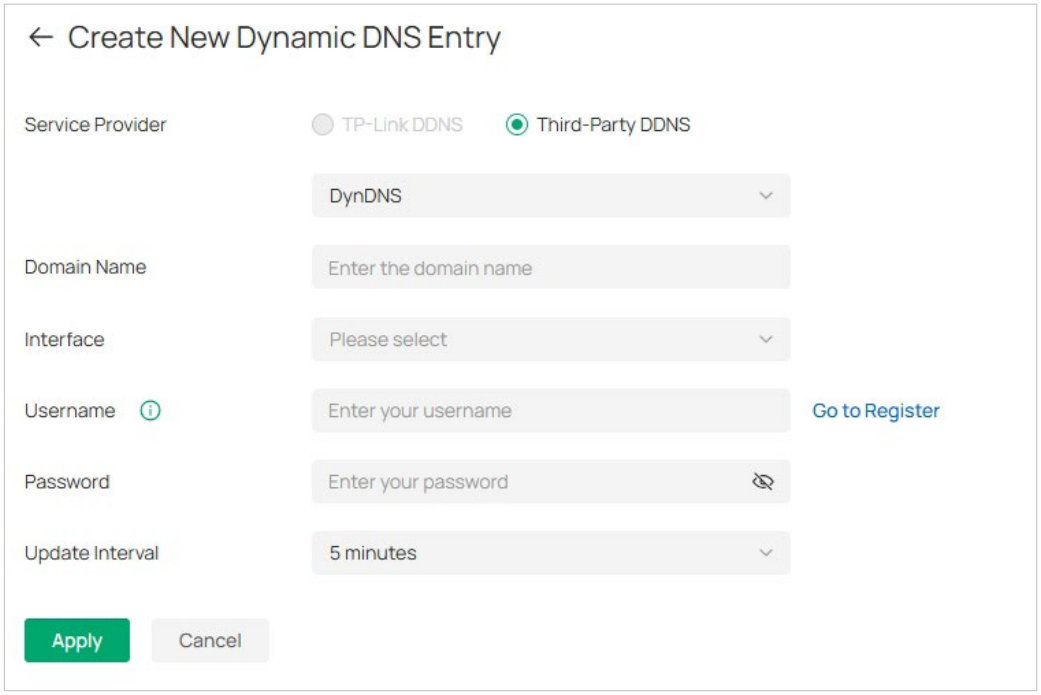
How Dynamic DNS works:

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



Configuration

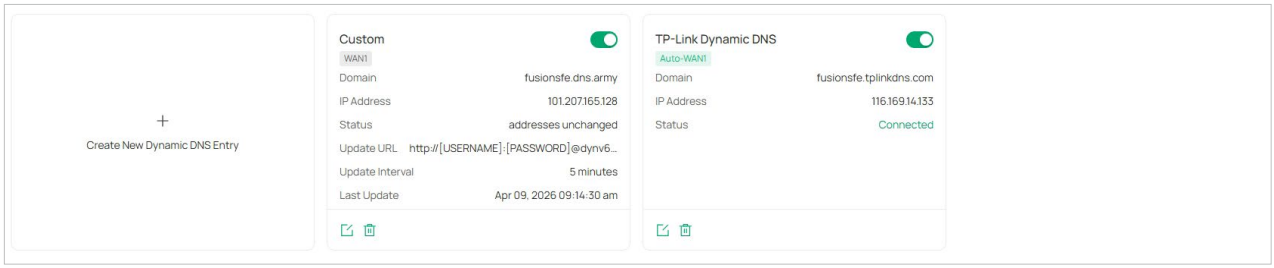
1. Go to Network Config > Network Settings > WAN > Dynamic DNS.
2. Click Create New Dynamic DNS Entry, to load the following page. Configure the parameters.



Service Provider	Select the Dynamic DNS service provider. TP-Link DDNS: Uses TP-Link's built-in DDNS service. The domain is registered and managed directly through the controller. Third-Party DDNS: Uses an external DDNS provider. You must register an account and domain name on the provider's website in advance.
Binding Mode	(For TP-Link DDNS only) Select how the domain is bound to WAN interfaces. Auto: Automatically binds the domain to an active WAN interface. When WAN failover occurs, the domain is updated to another active WAN interface. Note: If services such as Port Forwarding or VPN servers are bound to a specific WAN interface, they may become unreachable via the domain after a failover. Use Manual mode if a fixed WAN binding is required. Manual: Manually bind the domain to a specific WAN interface. Multiple domain–WAN mappings are supported, allowing different domains to be assigned to different WAN interfaces.
Interface	Select the WAN interface used for the DDNS update. In Auto mode, the active WAN interface is selected automatically. In Manual mode, select the specific WAN interface for the domain.
Domain Name	Enter the domain name used for Dynamic DNS. For TP-Link DDNS, enter a custom domain name. The domain will be registered and managed by TP-Link automatically through the controller. For Third-Party DDNS, enter the domain name registered with the service provider.
Username	(For Third-Party DDNS only) Enter your username for the DDNS service provider. If you haven't registered at the service provider, click Go To Register.
Password / Token	(For Third-Party DDNS only) Enter the password or token/API key provided by the DDNS service provider.
Update Interval	Specify how often the gateway reports its WAN IP address to the DDNS service. The gateway performs updates periodically based on the configured interval. An immediate update may also be triggered when a WAN IP change is detected. **Note:** The update interval behavior may vary across DDNS providers. In such cases, the gateway follows the update policy defined by the provider.

Update URL	(For Custom Third-Party DDNS only) Enter the update URL provided by the DDNS service provider. Example format: http://[USERNAME]:[PASSWORD]@api.cp.easydns.com/dyn/tomato.php?hostname=[DOMAIN]&myip=[IP] The gateway uses this URL to update the WAN IP address to the DDNS service.

3. Click Create. The new entry will be listed. You can toggle on/off the switch to enable/disable the entry.



Chapter 13

Configure LAN Networks

This chapter guides you on how to configure LAN networks with the Fusion gateway. The chapter includes the following sections:

13. 1 Configure LAN Networks

Overview

The LAN page 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.

Guidelines

To create a LAN, follow the guidelines:

1) Create a new Network with specific purpose. Select the device to serve as the DHCP Server based on the purpose of the VLAN, configure the VLAN on the selected device, specify the VLAN ID, and set related network parameters.

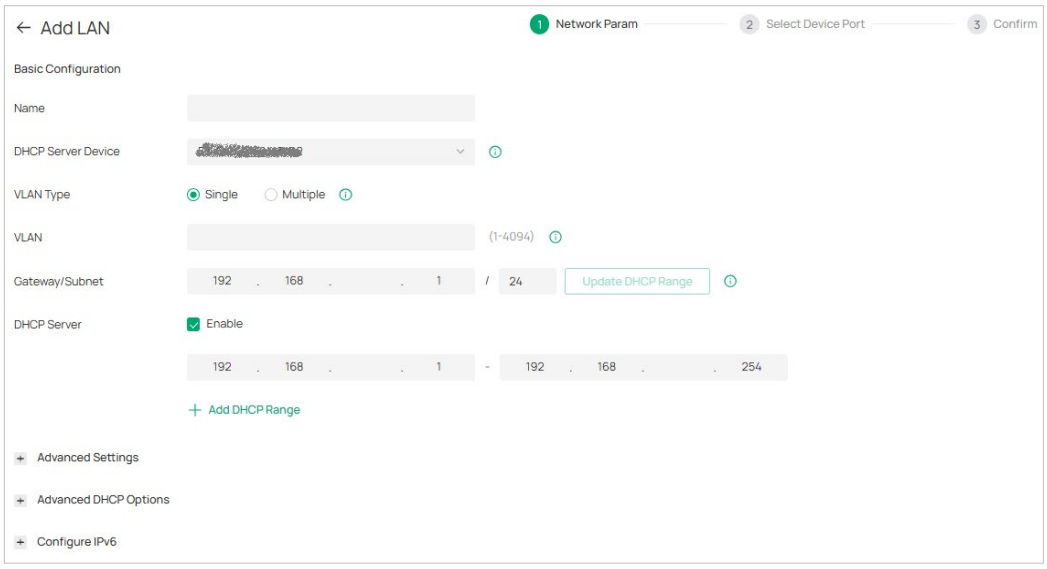
2) Bind the VLAN to the destination device port according to the actual use scenario. It can flexibly divide the network logic boundary to meet different business requirements.

3) Confirm the configuration and apply to activate the VLAN.

4) View the devices that are currently functioning in this VLAN through the topology view or check the configuration of this VLAN on the device ports through the port view.

Configuration

1. Go to Network Config > Network Settings > LAN. Click Add to create a network.



2. Set the network name and VLAN type.

Name	Enter a name to identify the network.

DHCP Server Device	Select a device with Layer 3 DHCP server capability to provide IP address assignment for this VLAN. This can be a gateway, L3 switch that support DHCP services. For the Default VLAN, only gateway can be selected as the DHCP server.
VLAN Type	Specify whether to use a single VLAN or multiple VLANs. If the VLAN Type is "Multiple" and the DHCP Server Device Type is "Gateway", a single network containing multiple VLAN IDs will be created. If the VLAN Type is "Multiple" and the DHCP Server Device Type is "External Device" or "None", multiple networks will be created, each corresponding to one VLAN.

- **If you select a gateway, configure the following parameters:**

VLAN	Enter a VLAN ID with the value between 1 and 4094. Each VLAN can be uniquely identified by its VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.
Gateway/Subnet	Enter the IP address and subnet mask in the CIDR format. The CIDR Notation here includes the IP address and subnet mask of the default gateway.The summary of the information that you entered will show up below in realtime.
DHCP Server	Click the checkbox to allow the device 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. If selected, set the starting and ending IP addresses of the DHCP address pool in the fields provided.
DHCP Range	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. You can also click Add DHCP Range to manually add multiple DHCP ranges as needed.

You can expand and configure Advanced Settings if needed.

Enable Internet Access	Whether to enable internet access for devices on this network.
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.

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.
Lease Time	Specify how long a client can use the IP address assigned from this address pool.
ARP Detection	When enabled, the gateway will broadcast ARP requests to obtain the status of the dumb terminal. It is recommended that the subnet mask be no less than 24 bits.
Domain Name	Enter the domain name.
Isolate Network	Enable this option if you want to isolate the network.
Snooping	Select the Snooping function to be enabled. IGMP Snooping: Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic. MLD Snooping: Click the checkbox to monitor MLD (Multicast Listener Discovery) traffic and thereby manage IPv6 multicast traffic.
DHCP Next Server	Specify the server IP address that the DHCP client will use in the next step.
Legal DHCP Servers	With Legal DHCP Server enabled, Omada switches ensure that users get IP addresses only from the DHCP servers whose IP addresses are specified here.
Legal DHCPv6 Servers	With Legal DHCPv6 Server enabled, Omada switches ensure that users get IPv6 addresses only from the DHCPv6 servers whose IPv6 addresses are specified here.
DHCP L2 Relay	With DHCP L2 relay enabled, Omada switches configure the Option 82 field of the DHCP packets and transmit the packets in the LAN.

You can expand and configure Advanced DHCP Options or configure Custom Options if needed.

Option 2	DHCP clients use DHCP option 2 to configure the time offset. The time offset field specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Option 42	DHCP clients use DHCP option 42 to configure the NTP server address.
Option 44	DHCP clients use DHCP option 44 to configure the NetBIOS over TCP/IP name server.

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 67	Option 67 tells the client a path to a file from a TFTP server (option 66) that will be retrieved and used to boot. That file needs to be a basic boot loader that will do any other required work.
Option 138	Enter the value for DHCP Option 138. It is used in discovering the devices by the controller.
Option 252	Option 252 provides a DHCP client a URL to use to configure its proxy settings. It's defined in draft-ietf-wrec-wpad-01. If it was a statement like 'wpad-proxy-url' then only systems that understood it could use it (they'd have to recognize that string and know how to handle it)

You can expand and configure IPv6 connections for the LAN clients if needed. 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.

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 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.
DNS Server	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.
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.
RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.
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.
Address Prefix	With Get from Prefix Delegation selected, enter the Address Prefix, 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. Go to Network Config > Network Settings > WAN 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.
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.

RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.
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.
Address Prefix	With Get from Prefix Delegation selected, enter the Address Prefix, 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.
RA Priority	Specify the router priority to help a host choose its default gateway. If a host receives RA messages from multiple routers, it will select the router with the highest RA priority as the default gateway. In the case of routers with the same priority, it will select the router whose RA message is received first as the default gateway.
RA Valid Lifetime	Specify the validity lifetime of the prefix. The addresses automatically generated with the prefix can be used normally during the valid lifetime, and they will become invalid and be deleted after the valid lifetime expires.
RA Preferred Lifetime	Specify the preferred lifetime for stateless auto-configuration of addresses with the prefix. After the preferred lifetime expires, the addresses automatically configured by the hosts with this prefix will be abolished. A host cannot use an abolished address to establish a new connection, but it can still receive packets whose destination address is an abolished address. The RA Preferred Lifetime must be less than or equal to the RA Valid Lifetime.
With Pass-Through selected, configure the following parameters.	
IPv6 Prefix Delegation Interface	Select the WAN port using Pass-Through (Bridge) for the IPv6 connection.

- **If you select a switch, configure the following parameters:**

VLAN	Enter a VLAN ID with the value between 1 and 4094. Each VLAN can be uniquely identified by its VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.
IP Address Mode	Select a method to configure the IP for the DHCP Server Static: Specify the IP of DHCP servers manually. Enter the IP address of server in IP Address/Subnet field. DHCP: The DHCP server is automatically assigned an IP address in the network.
IP Address/Subnet	Enter the IP address and subnet mask in the CIDR format.
DHCP Mode	Select a mode for the clients in the VLAN to obtain their IP address. None: Do not use DHCP to assign IP addresses. DHCP Server: Assign an IP address to the clients through a DHCP server. When DHCP Server is selected, you can specify the DHCP Range, and the IP addresses in the range can be assigned to the clients in the VLAN. Also, it is optional for you to specify the DHCP Option 138, Primary/Seconday DNS, Default Gateway, and Lease Time. DHCP Option 138 informs the DHCP client of the controller's IP address when the client sends a request to the DHCP server, and specify Option 138 as the controller's IP address here. Lease Time decides how long the client can use the assigned IP address. DHCP Relay: It allows clients in the VLAN to obtain IP addresses from a DHCP server ion different subnet. When DHCP Relay is selected, specify the IP address of the DHCP server in Server Address.
DHCP Range	Enter the starting and ending IP addresses of the DHCP address pool in the fields provided.
DNS Server	Specify DNS servers manually. Enter the IP address of a server in each DNS server field.
Default Gateway	Specify default gateway manually. Enter the IP address of the default gateway in the field.
Lease Time	Specify how long a client can use the IP address assigned from this address pool.

You can expand and configure Advanced Settings if needed.

Snooping	Select the Snooping function to be enabled. IGMP Snooping: Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic. MLD Snooping: Click the checkbox to monitor MLD (Multicast Listener Discovery) traffic and thereby manage IPv6 multicast traffic.
Legal DHCP Servers	With Legal DHCP Server enabled, Omada switches ensure that users get IP addresses only from the DHCP servers whose IP addresses are specified here.

Legal DHCPv6 Servers	With Legal DHCPv6 Server enabled, Omada switches ensure that users get IPv6 addresses only from the DHCPv6 servers whose IPv6 addresses are specified here.
DHCP L2 Relay	With DHCP L2 relay enabled, Omada switches configure the Option 82 field of the DHCP packets and transmit the packets in the LAN.

You can expand and configure Advanced DHCP Options or configure Custom Options if needed.

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

- **If you select External Device, configure the following parameters:**

Note: This VLAN will be managed by an external device for network services. Please ensure that the external device has correctly configured the interface gateway and DHCP settings for this VLAN.

VLAN Type	Specify whether to use a single VLAN or multiple VLANs. If the VLAN Type is "Multiple" and the DHCP Server Device Type is "Gateway", a single network containing multiple VLAN IDs will be created. If the VLAN Type is "Multiple" and the DHCP Server Device Type is "External Device" or "None", multiple networks will be created, each corresponding to one VLAN.
VLAN	Enter a VLAN ID with the value between 1 and 4094. Each VLAN can be uniquely identified by its VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.

You can expand and configure Advanced Settings if needed.

Snooping	Select the Snooping function to be enabled. IGMP Snooping: Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic. MLD Snooping: Click the checkbox to monitor MLD (Multicast Listener Discovery) traffic and thereby manage IPv6 multicast traffic.
Legal DHCP Servers	With Legal DHCP Server enabled, Omada switches ensure that users get IP addresses only from the DHCP servers whose IP addresses are specified here.
Legal DHCPv6 Servers	With Legal DHCPv6 Server enabled, Omada switches ensure that users get IPv6 addresses only from the DHCPv6 servers whose IPv6 addresses are specified here.
DHCP L2 Relay	With DHCP L2 relay enabled, Omada switches configure the Option 82 field of the DHCP packets and transmit the packets in the LAN.

- **If you select None, configure the following parameters:**

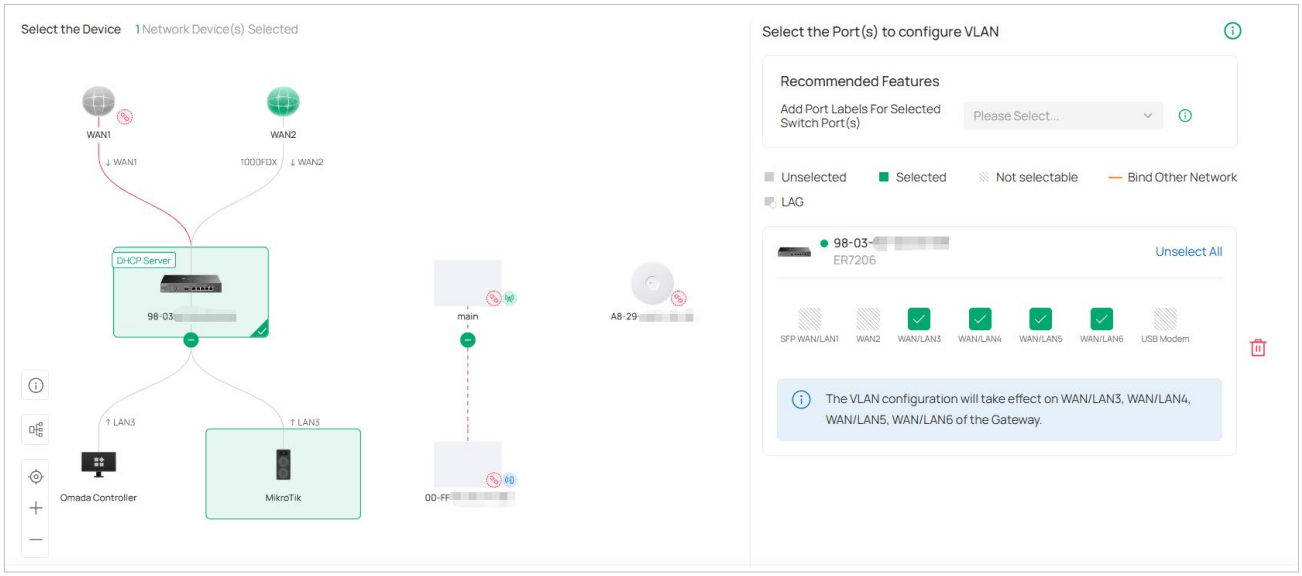
Note: This VLAN has no gateway and no DHCP service, and will operate as a pure Layer 2 switching network. Devices within the VLAN need to be manually configured with static IP addresses and can only communicate with other devices in the same VLAN.

VLAN Type	Specify whether to use a single VLAN or multiple VLANs. If the VLAN Type is “Multiple” and the DHCP Server Device Type is “Gateway”, a single network containing multiple VLAN IDs will be created. If the VLAN Type is “Multiple” and the DHCP Server Device Type is “External Device” or “None”, multiple networks will be created, each corresponding to one VLAN.
VLAN	Enter a VLAN ID with the value between 1 and 4094. Each VLAN can be uniquely identified by its VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.

You can expand and configure Advanced Settings if needed.

Snooping	Select the Snooping function to be enabled. IGMP Snooping: Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic. MLD Snooping: Click the checkbox to monitor MLD (Multicast Listener Discovery) traffic and thereby manage IPv6 multicast traffic.
Legal DHCP Servers	With Legal DHCP Server enabled, Omada switches ensure that users get IP addresses only from the DHCP servers whose IP addresses are specified here.
Legal DHCPv6 Servers	With Legal DHCPv6 Server enabled, Omada switches ensure that users get IPv6 addresses only from the DHCPv6 servers whose IPv6 addresses are specified here.
DHCP L2 Relay	With DHCP L2 relay enabled, Omada switches configure the Option 82 field of the DHCP packets and transmit the packets in the LAN.

3. Click Next. Select the port(s) to configure VLAN. The VLAN determines the Port VLAN Identifier (PVID) for switch ports. If you set the VLAN Type to Multiple in the previous step, select the port(s) to add it to the tagged network.



4. Configure recommended features if needed.

Port Isolation	When enabled, Port Isolation will be applied to the selected ports to enhance security.
Flow Control	When enabled, 802.3 pause frames notify IPCs to temporarily buffer video data during network congestion, preventing frame loss that would occur when packets are dropped. This requires IPC support for the protocol.
Add Port Labels For Selected Switch Port(s)	This option is used to add labels to the selected switch ports, facilitating centralized port management on the Device Config > Switch Ports page.

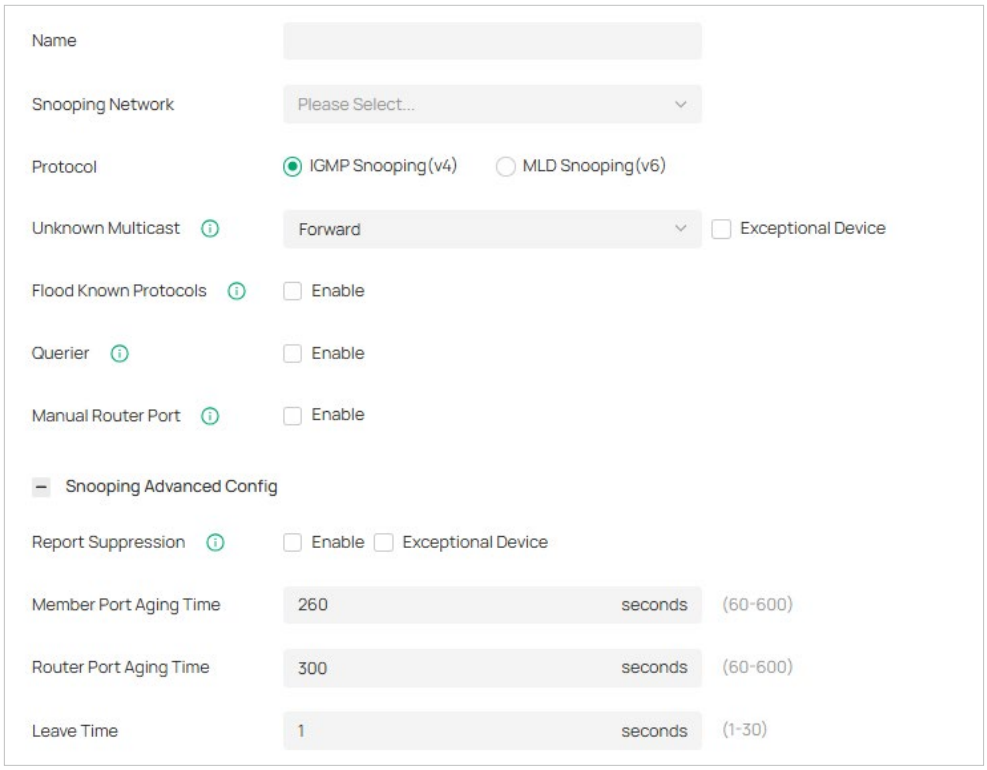
5. Click Next. Confirm your settings and click Apply. The VLAN network will be added to the list.

   Now you can view the devices that are currently functioning in this VLAN through the topology view or check the configuration of this VLAN on the device ports through the port view.

13. 2 Configure Multicast Snooping

You can configure Multicast Snooping to optimize multicast traffic management.

1. Go to Network Config > Network Settings > LAN > Multicast Snooping. Click +Add.



2. Configure the parameters and apply the settings.

Name	Enter a name to identify the Multicast network.
Snooping Network	Select the target network for multicast configuration, which will automatically enable its multicast snooping.
Protocol	Choose between IGMP (IPv4) or MLD (IPv6) based on network protocol requirements.
Unknown Multicast	Specify handling method for unidentified multicast packets. Forward: Flood unknown multicast traffic within VLAN. Discard: Drop unknown multicast packets. Router Port First: Forward to router ports (static/dynamic) if available; otherwise flood within VLAN. Exceptional Device: When enabled, you can click +Add to add exceptional devices and specify how unknown multicast packets from the selected devices are processed.
Flood Known Protocols	When enabled, IGMP Snooping will be activated, Unknown Multicast will be discarded, and the Switch can transparently transmit SSDP messages.
Querier	Set a switch as the querier for a specific network, and configure more parameters in Advanced Settings.

Manual Router Port	Manually set Static Router Port and Forbidden Router Port. Static Router Port: Select one or more ports to be the Static Router Ports in the network. All multicast data in this network will be forwarded through the static router ports. Forbidden Router Port: Select one or more ports to forbid them from being router ports in the network.
Report Suppression	When enabled, the switch will only forward the first IGMP report message for each multicast group to L3 devices during one query interval. This feature prevents duplicate report messages from being sent to the L3 devices. Exceptional Device: When enabled, you can click +Add to add exceptional devices and these exceptional devices will not apply report suppression.
Member Port Aging Time	Specify the aging time of the member ports in the Network. If the switch does not receive any IGMP membership report messages for a specific multicast group from a dynamic member port, it will no longer consider this port as a member port of this multicast group and delete it from the multicast forwarding table.
Router Port Aging Time	Specify the aging time of the router ports in the Network. If the switch does not receive any IGMP general query message from a dynamic router port within the router port aging time, the switch will no longer consider this port as a router port and delete it from the router port list.
Leave Time	Specify the leave time for the Network. When the switch receives a leave message from a port to leave a multicast group, it will wait for a leave time before removing the port from the multicast group. During the period, if the switch receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows: If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends. The Leave Time mechanism will not take effect when Fast Leave takes effect.

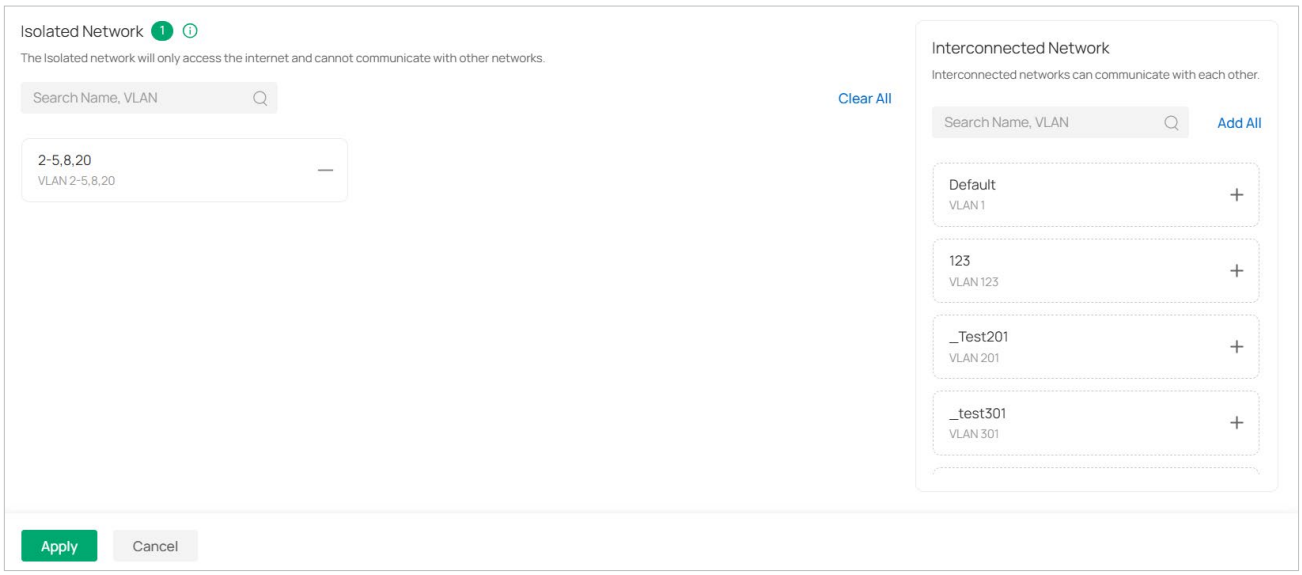
13. 3 Configure Network Isolation

When creating a VLAN, you can configure whether to isolate network segments in the advanced settings.

You can also configure network isolation on the Isolation Settings page to manage communication between VLANs.

Note: Network Isolation is only supported for networks with the Omada Gateway configured as the DHCP Server Device.

1. Go to Network Config > Network Settings > LAN > Isolation Settings.



2. Select the network to be isolated. Click the Add button on the right or drag to move the Network to the Isolated Network area to isolate it.
3. Click the Apply button to apply the settings.

13. 4 Configure DHCP Reservation

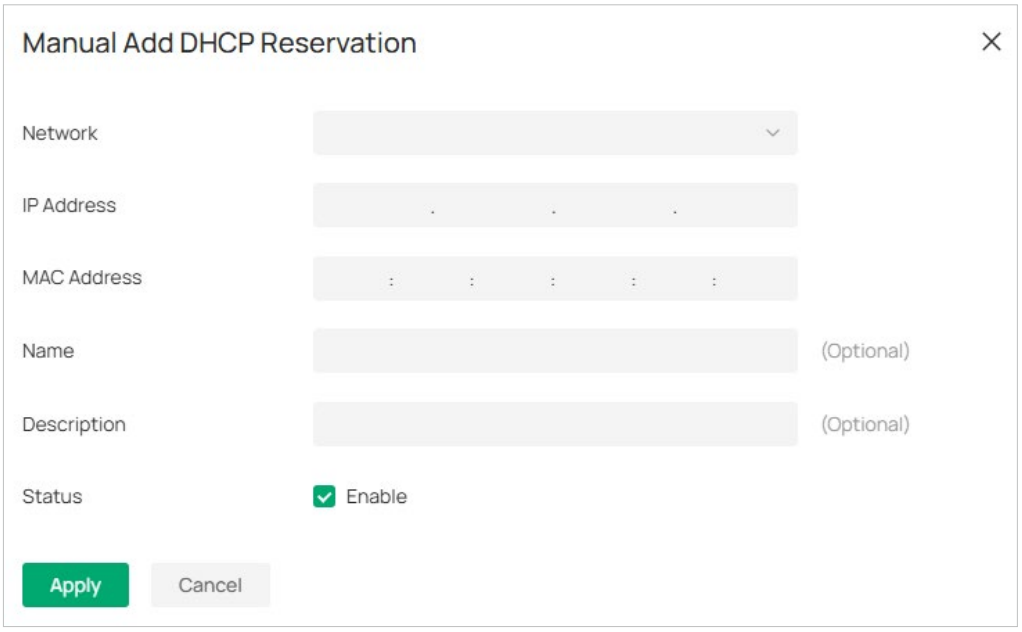
Overview

DHCP Reservation allows you to reserve specific IP addresses for devices/clients in your network, and centrally manage the IP addresses. Besides the gateway, the switch now also supports the DHCP reservation function; meanwhile, for gateways with this function, the DHCP Options field content can be reserved for clients/devices.

Configuration

- **To manually add DHCP Reservation entries:**

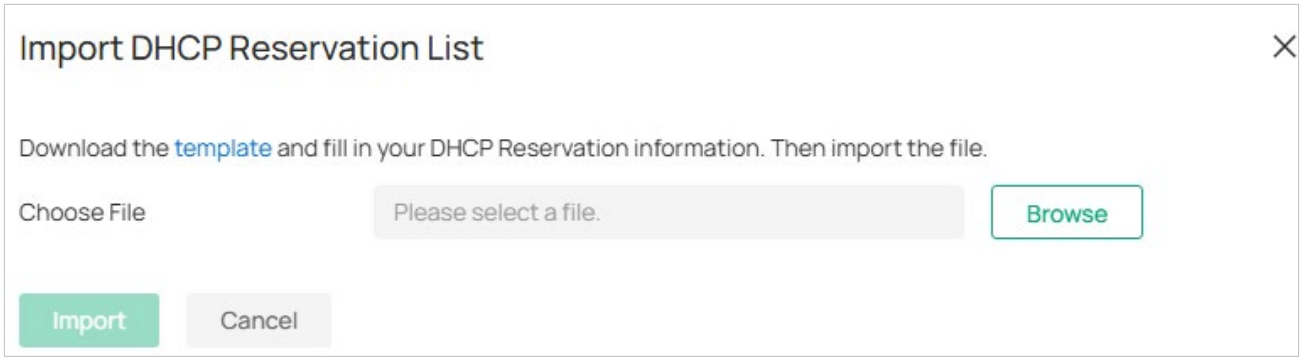
1. Go to Network Config > LAN > DHCP Reservation.
2. Click Manual Add and configure the parameters. Then click Apply.



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

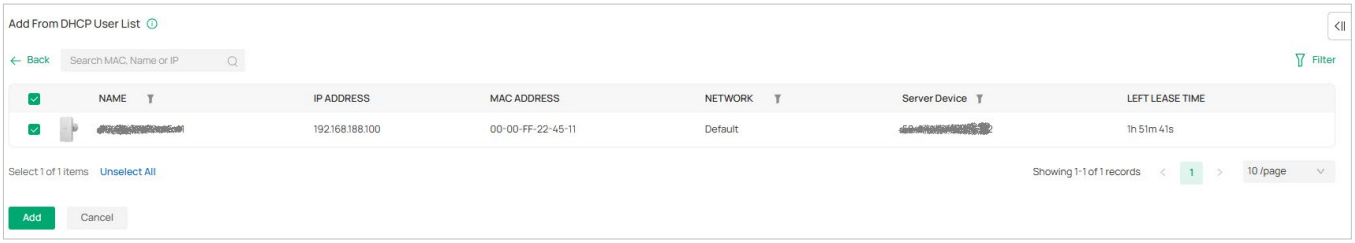
- **To import DHCP Reservation List:**

1. Go to Network Config > LAN > DHCP Reservation.
2. Click Import and import the customized template. You can download the template, then edit and upload it for batch import.



- **To add from DHCP user list:**

1. Go to Network Config > LAN > DHCP Reservation.
2. Click Add From DHCP User List and select from the list. Then click Add.

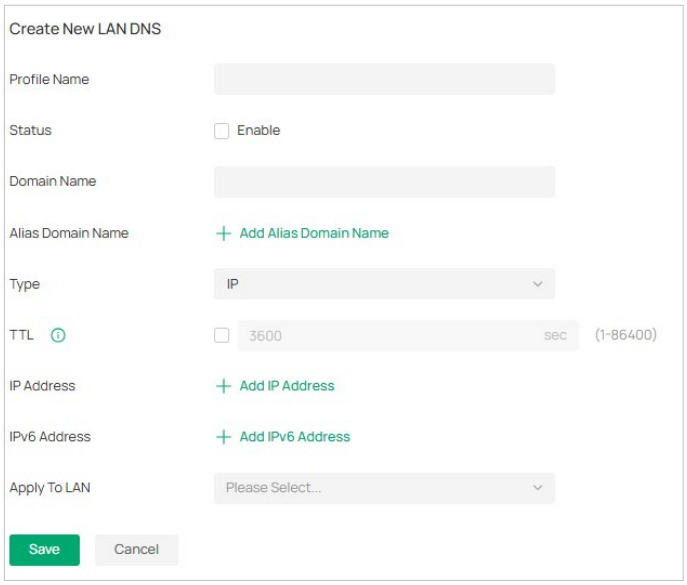


- **To filter DHCP Reservation List:**

1. Go to Network Config > LAN > DHCP Reservation.
2. Click Filter and filter the list by type or network.

13. 5 Configure Local DNS

1. Go to Network Config > Network Settings > LAN > Local DNS.
2. Click Create New LAN DNS to load the following page, set the parameters, and save the settings.



Profile Name	Specify the name of the profile.
Status	Whether to enable this entry.
Domain Name	Enter the domain name.
Alias Domain Name	If a server provides different services and has multiple domain names, you can enter them here.
Type	There are three options, IP, CNAME, and FORWARD. IP: When selected, the gateway will respond to the DNS query of the specified domain name, and use the configured IP address as the DNS response to directly reply to the LAN host. Select this type when there is a web server in the intranet and you want hosts in the LAN to access the web server through private IP addresses instead of public IP addresses. CNAME: When selected, the gateway will map the domain name to the configured CNAME domain name, send it to the DNS server for query, and then reply to the LAN host with the IP corresponding to the CNAME domain name. FORWARD: When selected, the gateway will forward the DNS query of the LAN host to the specified DNS server, and reply the DNS response to the LAN host. The forwarding priority is higher than other public configurations, such as the DNS Server configured on the WAN port.
TTL	When the Type is IP, set TTL to specify the amount of time DNS information that is allowed to be cached before it expires and needs to be refreshed. It is recommended to use the default TTL for each record.
IP Address	When the Type is IP, it is the IPv4 address of the returned DNS response.

IPv6 Address	When the Type is IP, it is the IPv6 address of the returned DNS response.
Apply To LAN	When the Type is IP or CNAME, it is the LAN network to which the rule applies. You can choose to apply all LANs or apply to a single LAN or multiple LANs.
CNAME	When Type is CNAME, set the domain name to which Domain Name and Alias Domain Name need to be mapped.
DNS Server	When the Type is FORWARD, set the Domain Name and Alias Domain Name to be forwarded to a specific DNS Server, up to two DNS Servers can be configured.

3. Configure DNS Cache if needed. DNS caching further speeds up domain name translation/resolution by handling it for recently visited addresses before the request is sent to the internet. Even if your network can use a large number of public DNS servers for translation/resolution, it's still faster to have a local copy. Check the box to enable it and specify the time to live (TTL) value in seconds. When the life cycle of the DNS entry exceeds the TTL value, the DNS cache will be automatically cleared. The range is 1-86400. If it's not specified, the system will use the default TTL value of each DNS message.

Chapter 14

Configure Wireless Networks

Wireless networks enable your wireless clients to access the internet. Once you set up a wireless network, your APs 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 APs 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.

This chapter guides you on how to configure wireless networks with the Fusion gateway. The chapter includes the following sections:

14. 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

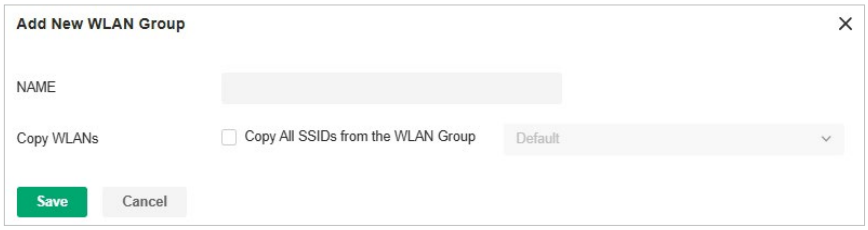
3) Apply the WLAN group to your APs

Step 1: Create a WLAN Group

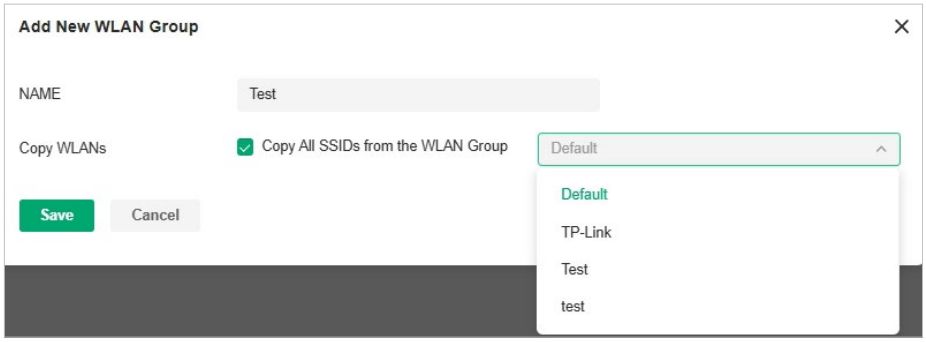
Note: The Fusion gateway provides a default WLAN group. If you simply want to configure wireless networks for the default WLAN group and apply it to all your APs, skip this step.

1. Go to Network Config > Network Settings > WLAN to load the following page.

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.



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.



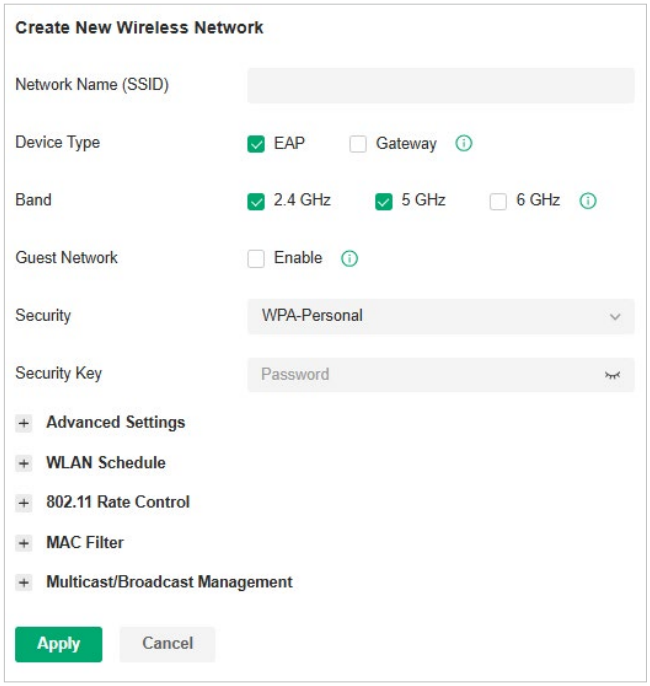
4. Click Save. The new WLAN Group is added to the WLAN Group list. You can select a WLAN Group from the list to further create and configure its wireless networks. You can click the Edit icon to edit the name of the WLAN Group. You can click the Delete icon to delete the WLAN Group.

Step 2: Create Wireless Network

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

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

Note: The 6 GHz band is only available for certain devices.



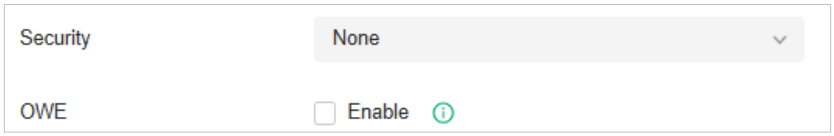
Network Name (SSID)	Enter the network name (SSID) to identify the wireless network. The users of wireless clients choose to connect to the wireless network according to the SSID, which appears on the WLAN settings page of wireless clients.

Device Type	Select the type of devices that the wireless network can apply to.
Band	Enable the radio band(s) for the wireless network. When 6GHz is turned on, Security cannot be PPSK with/without RADIUS since 6GHz does not support them.
Guest Network	With Guest Network enabled, all the clients connecting to the SSID are blocked from reaching any private IP subnet.
Security	Select the encryption method for the wireless network based on needs.

3. Select the security strategy for the wireless network.

- **None**

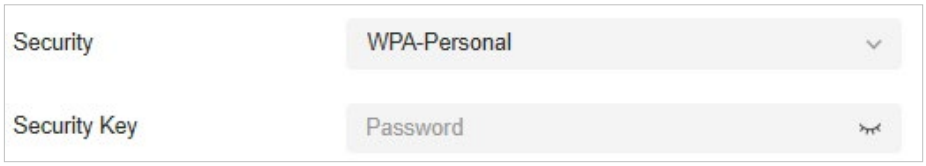
With None selected, the hosts can access the wireless network without authentication, which is applicable to lower security requirements.



OWE	Opportunistic Wireless Encryption, also known as Enhanced Open, is a certification provided by the Wi-Fi Alliance as part of the WPA3 wireless security standard. OWE will enable two wireless APs per radio, one for access of OWE-supported stations, and one for access of other stations. An SSID with OWE enabled will be counted as two SSID entries.

- **WPA-Personal**

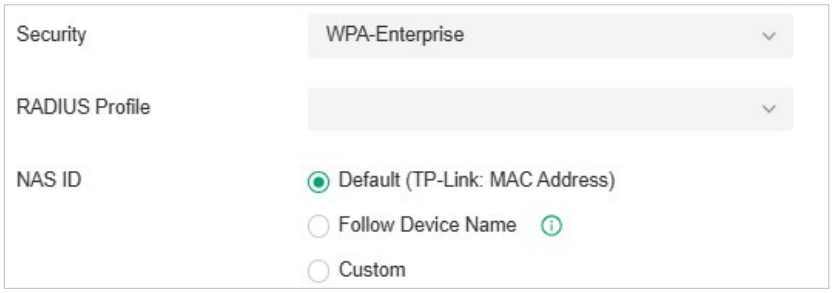
With WPA-Personal selected, traffic is encrypted with a Security Key you set,



Security Key	Specify a security key to encrypt the traffic.

- **WPA-Enterprise**

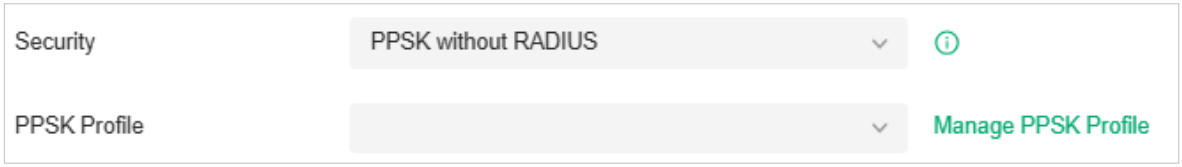
WPA-Enterprise requires an authentication server to authenticate wireless clients, and probably an accounting server to record the traffic statistics.



RADIUS Profile	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 the network profile configuration section in this guide.
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. The NAS ID can be a default one (TP-Link: MAC Address), follow the device name, or a customized one.

- **PPSK without RADIUS**

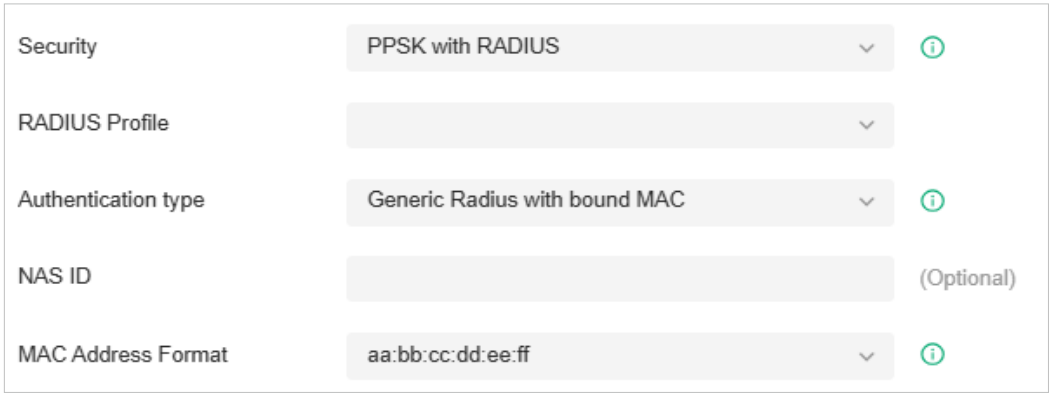
PPSK (private pre-shared key) can provide a unique PSK for each wireless user. Compared with the traditional SSID solution with one password for all users, it is more secure.



PPSK Profile	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 the network profile configuration section in this guide.

- **PPSK with RADIUS**

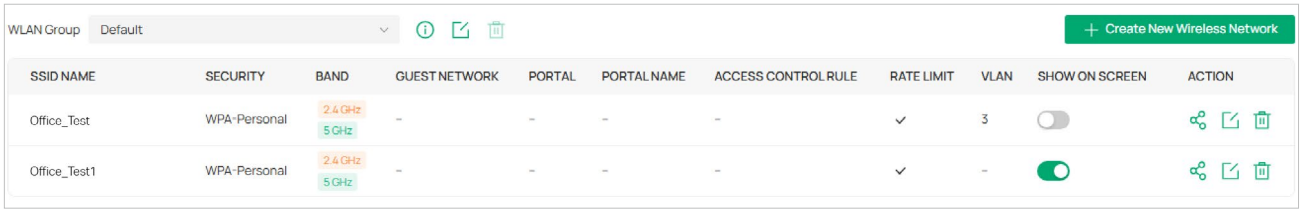
PPSK (private pre-shared key) can provide a unique PSK for each wireless use. PPSK with RADIUS requires an authentication server to authenticate wireless clients and probably an accounting server to record the traffic statistics. The SSID will not be applied to the device firmware not supporting PPSK.



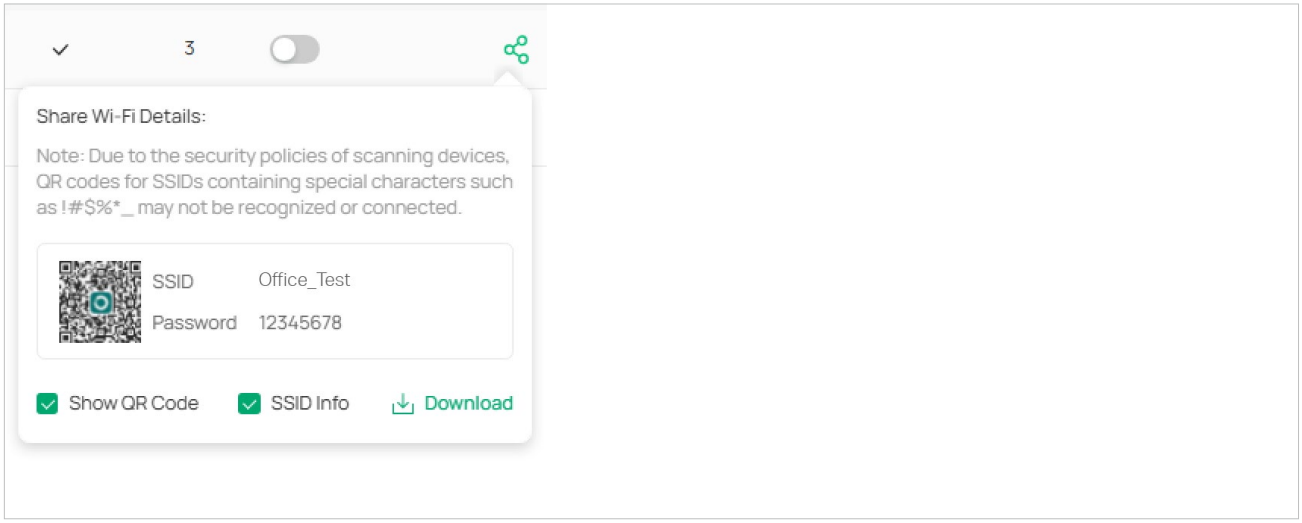
RADIUS Profile	Select a RADIUS Profile, which records the settings of the authentication server and accounting server. You can create a RADIUS Profile by clicking + Create New Radius Profile from the drop-down list of RADIUS Profile. For details, refer to the network profile configuration section in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

Authentication type	Choose the authentication type. Generic Radius with bound MAC: This method uses a device's unique MAC address as the username and password for a RADIUS server to grant or deny network access. This type needs to specify device MAC addresses. EKMS: The EKMS (Eleven Key Matching Service) authentication type is used to connect to the ElevenOS server. Only the EKMS authentication method in PPSK with RADIUS supports domain name. Generic Radius with unbound MAC: This method uses a client's MAC address as the username and password for a RADIUS server to grant or deny network access. This type does not need to specify device MAC addresses.
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 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.

4. (Optional) You can also configure Advanced Settings, WLAN Schedule, 802.11 Rate Control, and MAC Filter, and more 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 the Edit icon in the ACTION column to edit the wireless network. You can click the Delete icon in the ACTION column to delete the wireless network.



You can hover over the icon in the ACTION column to find the Wi-Fi Details to share.



Step 3: Apply the WLAN Group

Note: The Fusion gateway provides a default WLAN group. If you simply want to configure wireless networks for the default WLAN group and apply it to all your APs, skip this step.

- **Apply to a Single AP**

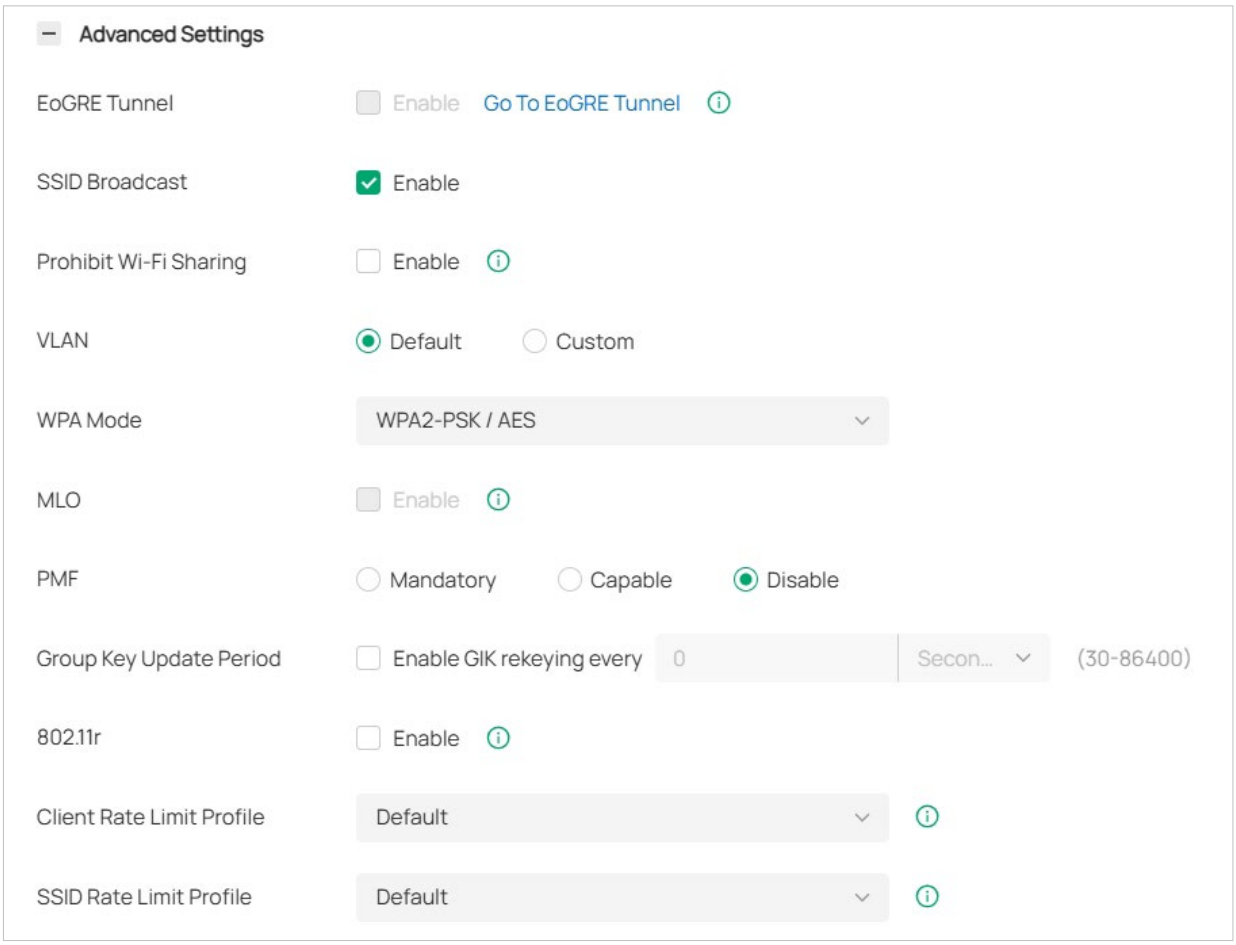
  Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Wireless > WLANs. Select the WLAN group and apply the settings.

- **Apply to APs in batch**

1. Go to Devices > Device List. Click Batch Action, select Batch Config, check the boxes of your desired APs, and click Config.
2. In the Properties window, go to Wireless > WLANs. Select the WLAN group and apply the settings.

14. 2 Configure Advanced Settings

Go to Network Config > Network Settings > WLAN, click the Edit icon 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.



EoGRE Tunnel	Toggle on to enable the EoGRE (Ethernet over GRE) Tunnel for the wireless network. **Note:** If the function is unavailable, go to Device Config > AP > EoGRE Tunnel to enable the feature globally.
SSID Broadcast	With SSID Broadcast enabled, APs 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.
Prohibit Wi-Fi Sharing	When enabled, the connected clients will be prohibited to share the Wi-Fi with other clients.

VLAN	Configure the uplink port VLAN(s) corresponding to the SSID. Default: Using untagged transmission. Custom: Configure an SSID-based VLAN pool by binding one or multiple networks (by network) or manually entering one or multiple VLAN IDs (by VLAN). When a client connects to the SSID, it will be assigned to a VLAN in the VLAN pool you configured. If a device does not support multiple VLANs, the smallest VLAN you configured will be applied to the SSID.
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: APs automatically decide the encryption type in the authentication process.
MLO	MLO (Multi-Link Operation) enables Wi-Fi 7 devices to simultaneously send and receive data across different frequency bands and channels. This ensures fast and reliable connections even in dense network environments.
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 (Group Integrity Key) rekeying and specify the time period.
802.11r	802.11r allows faster roaming when both the AP and client have 802.11r capabilities. However, older devices may be incompatible with the feature.
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.

14. 3 Configure Hotspot 2.0

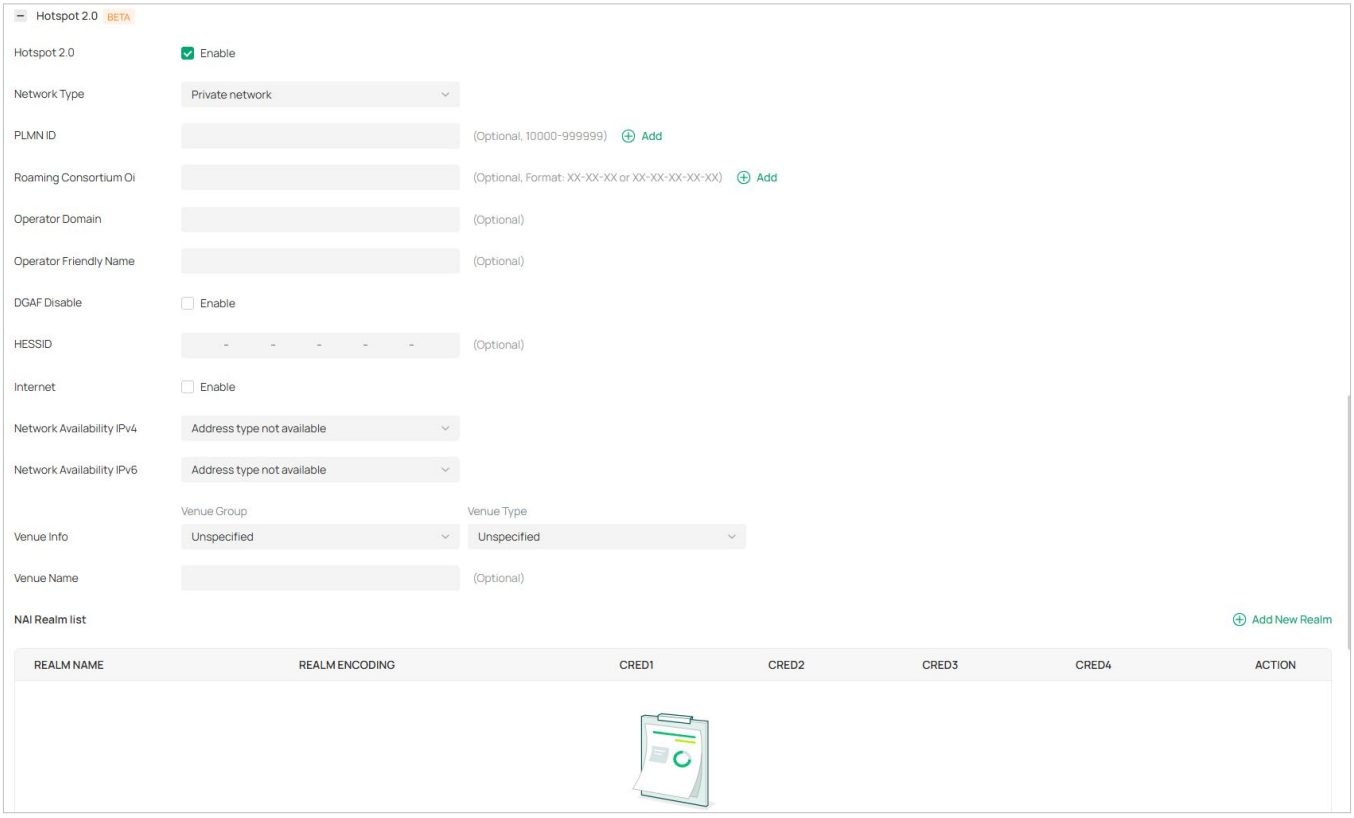
Overview

Hotspot 2.0 is a wireless network technology based on the IEEE 802.11u standard. It provides a simplified network selection mechanism for wireless clients, enabling them to automatically discover and securely access Hotspot 2.0-certified Wi-Fi networks.

Hotspot 2.0 is only available for a wireless network using WPA3-Enterprise encryption.

Configuration

Go to Network Config > Network Settings > WLAN, click the Edit icon in the ACTION column of a wireless network that is using WPA3-Enterprise encryption, and click Hotspot 2.0 to load the following page. Enable Hotspot 2.0 and configure the parameters. Then click Apply.



Network Type	Specify the 802.11u network type: private network, private network with guest access, chargeable public network, free public network, personal device network, emergency services only network, test or experimental, or wildcard.
PLMN ID	Enter the PLMN (Public Land Mobile Network) ID of the 802.11u 3GPP cellular network, which consists of the MCC (Mobile Country Code) and MNC (Mobile Network Code). Wireless clients can obtain this information through ANQP queries to determine whether to access the network. This is applicable to networks that have roaming relationships with mobile operators.

Roaming Consortium Oi	Enter the 802.11u roaming organization identifiers. For a network that has roaming relationships with other network operators, you can configure a roaming organization list for wireless clients to automatically identify trusted roaming network partners.
Operator Domain	Enter the domain name of the access network operator. Wireless clients can obtain this information through ANQP queries as the basis for network selection.
Operator Friendly Name	Network operator friendly name. This parameter can be used to define the names of different language environments, so that users of different languages can easily select the network. Currently, only English format input is provided.
DGAF Disable	In DGAF (downstream group-addressed forwarding) disable mode, the AP will not forward downstream multicast and broadcast packets. Downstream multicast and broadcast packets use the same GTK (Group Temporal Key) key, which poses a security risk. The AP will discard these ARP and multicast packets to prevent attackers from exploiting the vulnerability that all clients in the same BSS use the same GTK key to forge group address frames and attack clients. This function is disabled by default. When it is enabled, some multicast services will be unavailable. To ensure normal internet access, the AP will enable the ARP proxy and disable ARP-to-unicast conversion.
HESSID	Homogenous Extended Service Set Identifier. It is used to identify the same type of ESS network set. An area may have multiple Hotspot 2.0 networks. Based on the unique HESSID, wireless clients can identify which networks provide the same service without having to re-acquire network parameters. HESSID should be consistent with one of the BSSIDs of the APs in the zone.
Internet	Internet access support status (network reachability).
Network Availability IPv4	Available type information of IPv4 addresses. When a wireless client accesses a Hotspot 2.0 network, the AP can pass the available types of IPv4 addresses in the network to the client as ANQP parameters, so that the client can understand the types of IP addresses that can be obtained after accessing the network.
Network Availability IPv6	Available type information of IPv6 addresses. When a wireless client accesses a Hotspot 2.0 network, the AP can pass the available types of IPv6 addresses in the network to the client as ANQP parameters, so that the client can understand the types of IP addresses that can be obtained after accessing the network.
Venue Info	Indicates the venue information using the combination of the network's venue group and venue type (using the international building code). When a wireless client attempts to access a Hotspot 2.0 network, it can obtain the location type information of the current network from the AP for network selection.
Venue Name	Network's venue name, identifying the physical location of the network.

NAI Realm list	Add a profile to identify and describe a NAI (Network Access Identifier) realm accessible using the AP, and the method that this NAI realm uses for authentication. Realm name: The name of the NAI realm. Usually the domain name of the service provider. Realm Encoding: NAI realm name format. Two formats are supported: • RFC4282: Realm formatted according to RFC 4282. • UTF-8: UTF-8 formatted string not formatted according to IETF RFC 4282. EAP Method: EAP authentication method supported by the NAI realm. Authentication param: Configure the EAP authentication parameter identifier and authentication parameters.

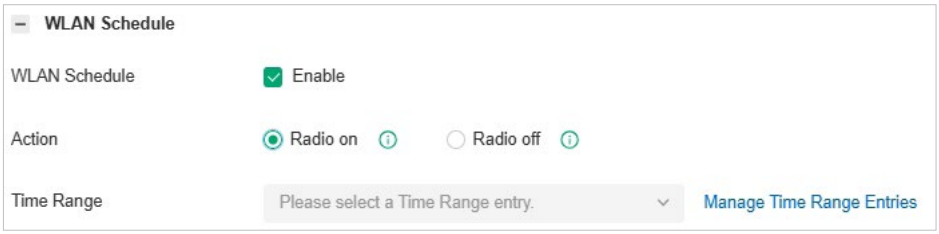
14. 4 Configure WLAN Schedules

Overview

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

Configuration

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



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

14. 5 Configure 802.11 Rate Control

Overview

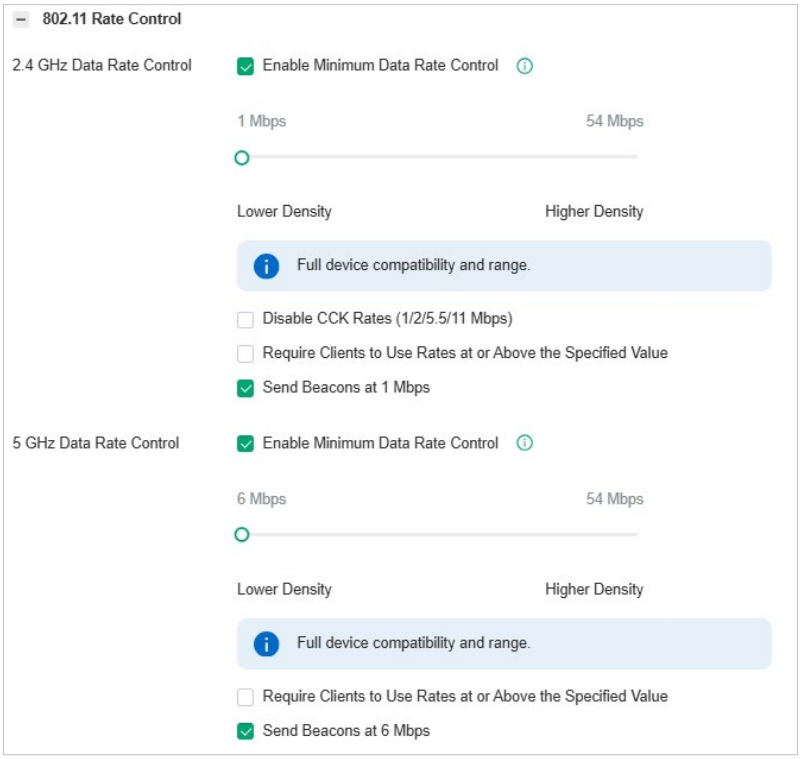
Note: 802.11 Rate Control is only available for certain devices.

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

Configuration

Go to Network Config > Network Settings > WLAN, click the Edit icon 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.



Enable Minimum Rate Control	When enabled, you can use the slider to set allowed bit rates on your 2.4 / 5 GHz network. This controls both data and management frames. Disabling lower rates improves high-density network performance but may make older devices incompatible and reduce wireless range. To control management frames separately, enable Management Rate Control.

Enable Management Rate Control	When enabled, you can independently set bit rates for management frames to optimize airtime usage. Higher minimum rates of management frames reduce overhead in dense environments but may affect network discovery range. Adjust based on your network requirements and client capabilities. Note: This feature is not supported on devices running older firmware versions.
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.

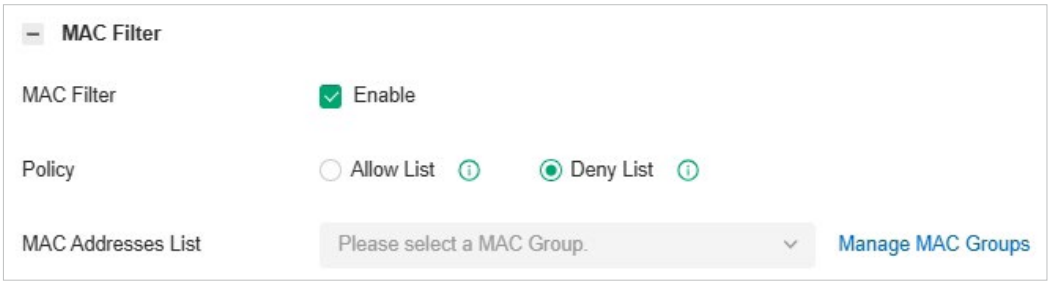
14. 6 Configure MAC Filtering

Overview

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

Configuration

Go to Network Config > Network Settings > WLAN, click the Edit icon in the ACTION column of the wireless network which you want to configure, and click MAC Filter to load the following page. Enable MAC Filter and configure the parameters .Then click Apply.



Policy	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 the network profile configuration section in this guide.

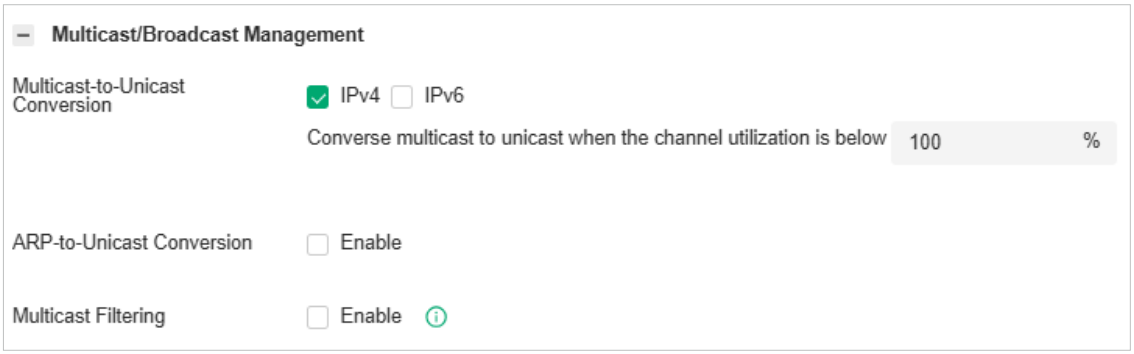
14. 7 Configure Multicast/Broadcast Management

Overview

Multicast/Broadcast Management allows packet conversion and multicast filtering.

Configuration

Go to Network Config > Network Settings > WLAN, click the Edit icon in the ACTION column of the wireless network which you want to configure, and click Multicast/Broadcast Management to load the following page. Configure the parameters .Then click Apply.



Multicast-to-Unicast Conversion	When the channel utilization is below the set value, the Wireless Device will convert the IPv4/IPv6 multicast packets into unicast packets and send them to the corresponding clients based on the learned multicast relationships. This improves the transmission efficiency of IPv4/IPv6 multicast.
ARP-to-Unicast Conversion	When enabled, the controller will convert ARP packets into unicast packets.
Multicast Filtering	When enabled, the device will filter the multicast packets of the specified protocols. Improper settings may cause network issues
Filtering Protocols	Choose IGMP/mDNS/ND/Others according to your need. Choose Others for MAC-based filtering, which will filter IP multicast packets that are not using IGMP, MLD, mDNS, or ND protocols.
MAC Group	If you want to allow packets from specific addresses to pass through, you can choose MAC Group and Create New MAC Group. Here you can set MAC Group Name and choose different methods to add the MAC Address.

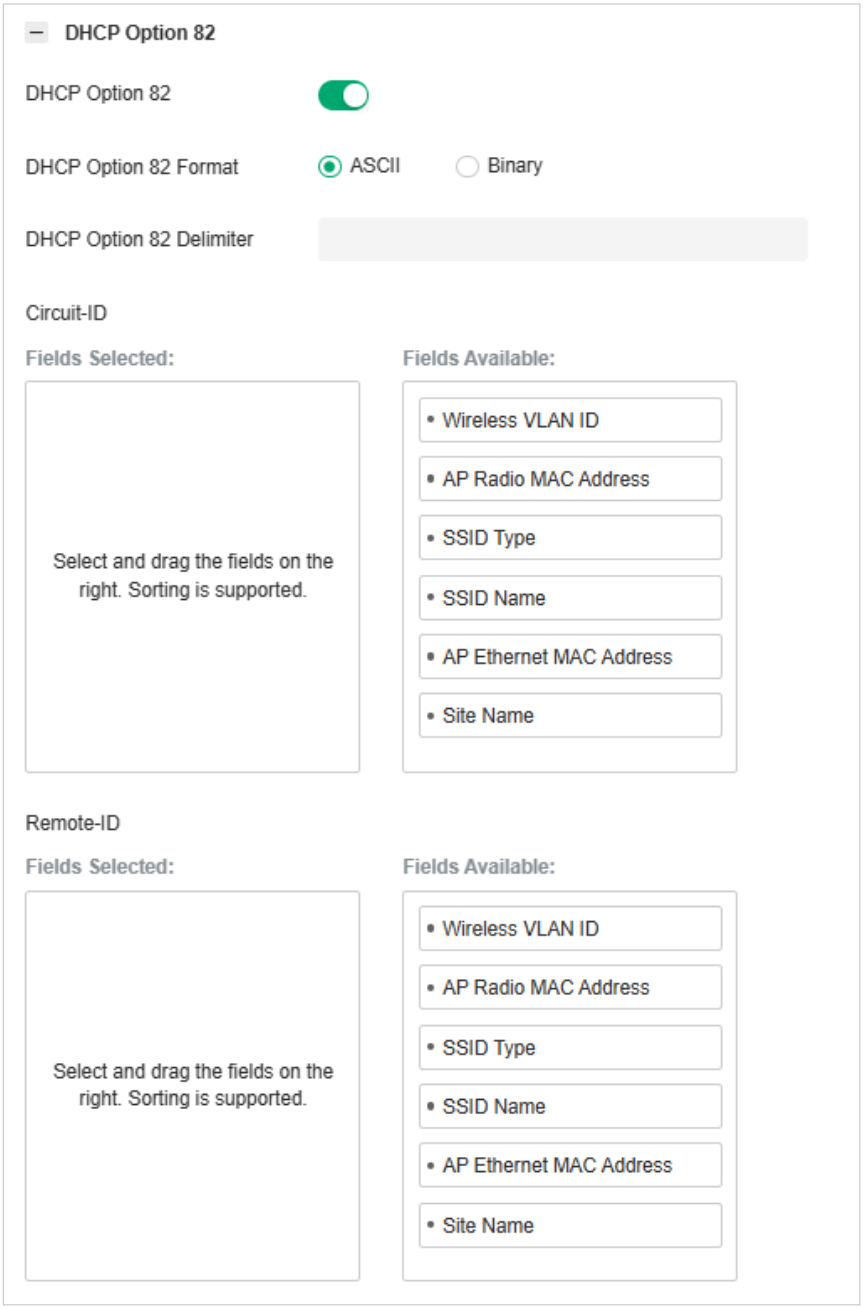
14. 8 DHCP Option 82

Overview

DHCP option 82, also known as the DHCP relay agent information option, provides additional security when using DHCP to assign network addresses. It enables the Fusion gateway to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.

Configuration

Go to Network Config > Network Settings > WLAN, click the Edit icon in the ACTION column of the wireless network which you want to configure, and click DHCP Option 82 to load the following page. Configure the parameters. Then click Apply.



DHCP Option 82	Toggle on to enable DHCP Option 82.
DHCP Option 82 Format	Select the format of DHCP Option 82: ASCII or Binary.
DHCP Option 82 Delimiter	Enter the delimiter of DHCP Option 82 (single punctuation mark).
Circuit-ID	Identifies the circuit (interface or VLAN) on the switching device on which the request was received.
Remote-ID	Identifies the remote host.

14. 9 Configure WLAN Optimization

Overview

WLAN Optimization helps improve the wireless network performance. With the WLAN Optimization feature, the Fusion gateway will detect WiFi interference and monitor the wireless environment. Based on the environmental factors including network topology, deployment size, traffic, and client factors, the Fusion gateway can determine the optimum wireless configurations (such as channel, bandwidth, power, etc.) for the access points (APs), and thus ensures that wireless clients of each AP can enjoy better WiFi experience.

In WLAN Optimization, the results of the last 10 scans are displayed. You can manually run a WLAN optimization immediately or set up auto WLAN optimization.

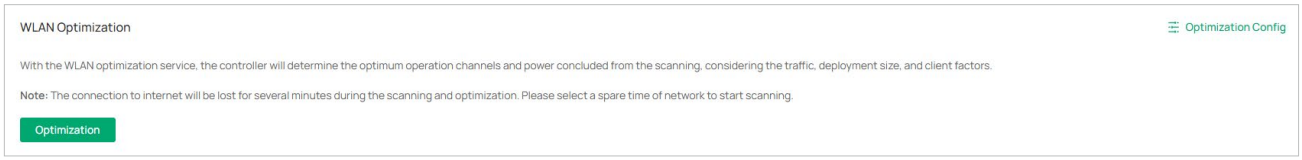
In Optimization History, the past optimization records are displayed, and you can also restore the previous optimization results if needed.

Manually Run a WLAN Optimization

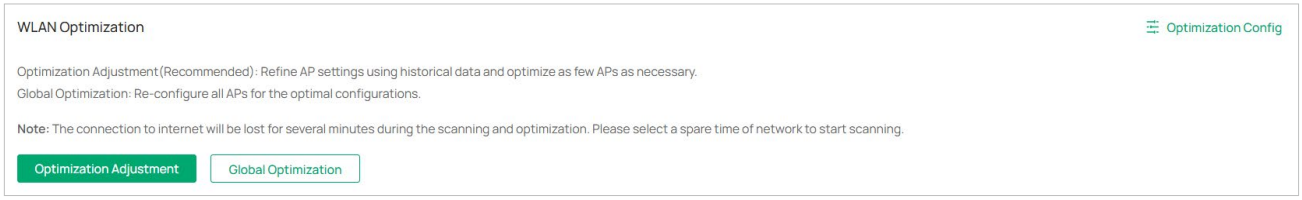
Note: The connection to internet will be lost for several minutes during the scanning and optimization. Please select a spare time of network to start scanning.

1. Go to Network Config > Network Settings > WLAN > WLAN Optimization.
2. In the WLAN Optimization section, run a WLAN Optimization.

   • In the initial optimization, click Optimization to run a global optimization to reconfigure wireless settings across all APs.



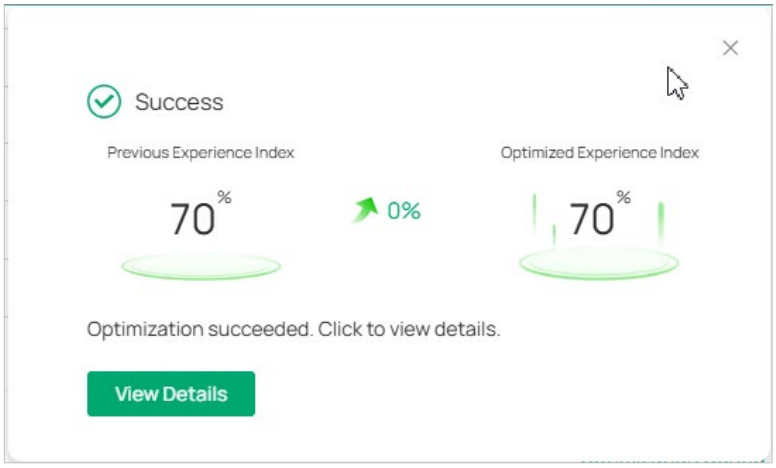
   • In later optimizations, you can click Optimization Adjustment (recommended) or Global Optimization to run an optimization.



Optimization Adjustment	The controller refines the wireless settings of APs based on historical optimization results, historical client behavior, and the current wireless environment, optimizing as few APs as necessary. Wireless connections may be interrupted during optimization. This optimization option is recommended, but it is only available for non-initial optimizations since it requires historical optimization data.

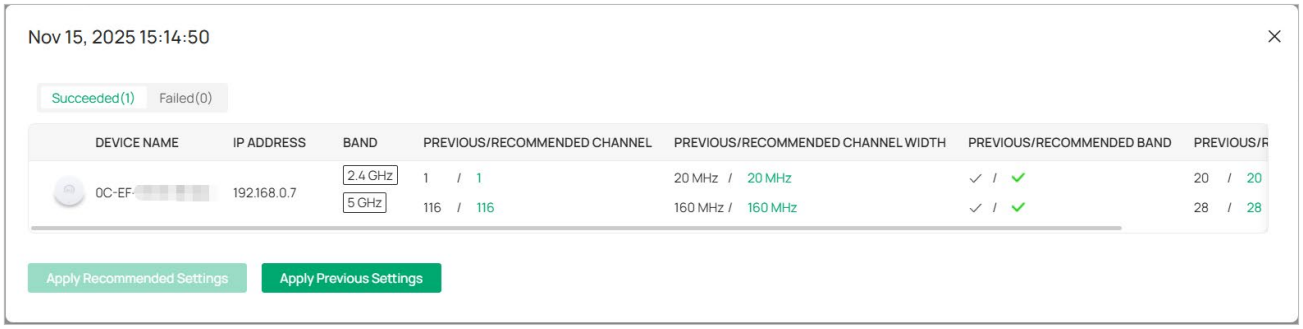
Global Optimization	The controller reconfigures the wireless settings of all APs for optimal overall network performance. Wireless connections may be interrupted during optimization.

3. The Fusion gateway will scan the wireless environment to conclude the optimum WLAN network configurations and display the result after completing the optimization.



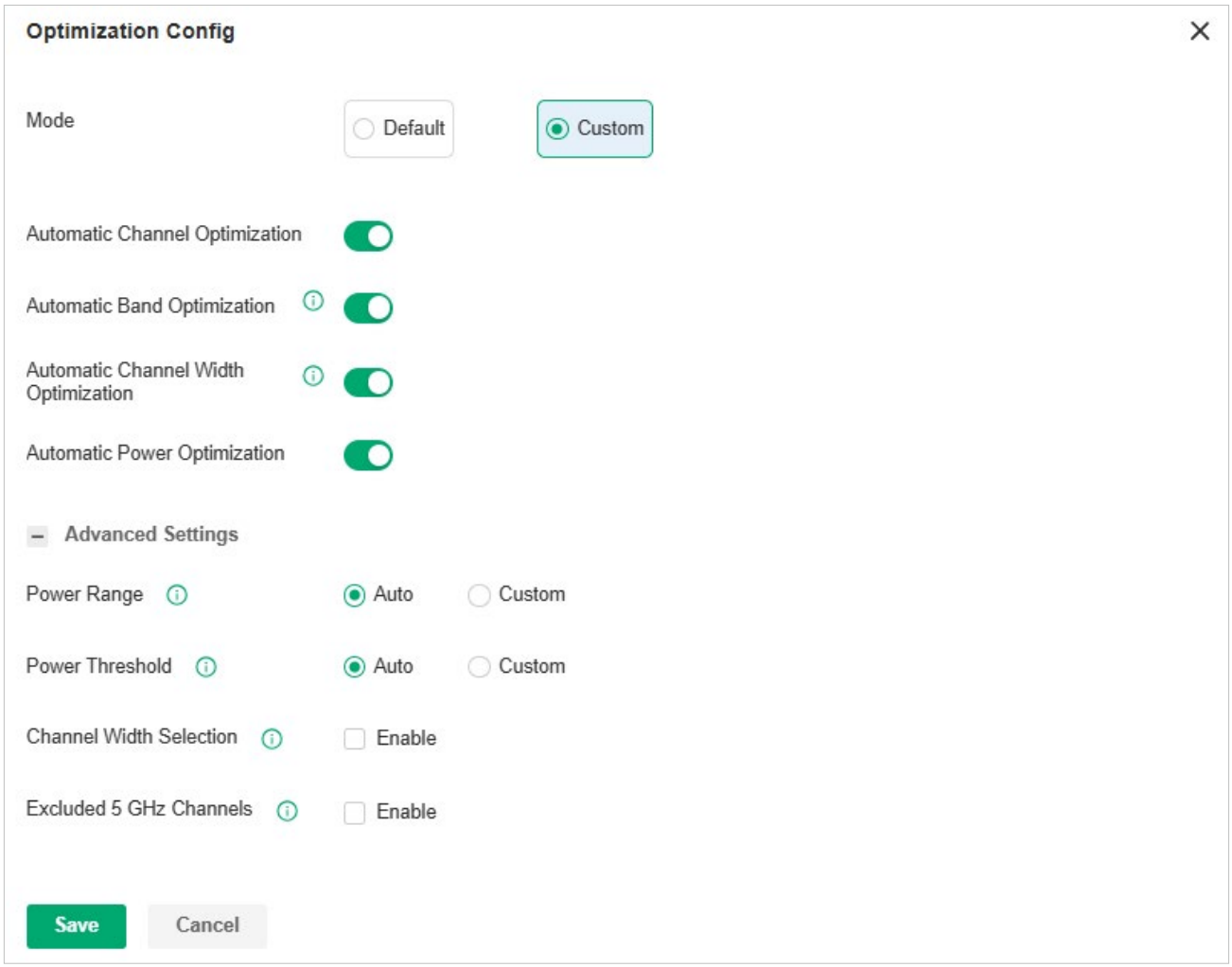
4. Click View Details to display more info. You can click Apply Previous Settings if you want to restore the previous optimization results.

Tip: You can also view the optimization results in the Optimization History.



Customize Optimization Config

If you want to custom optimization configurations, click Optimization Config on the WLAN Optimization page, then set the parameters according to actual needs.

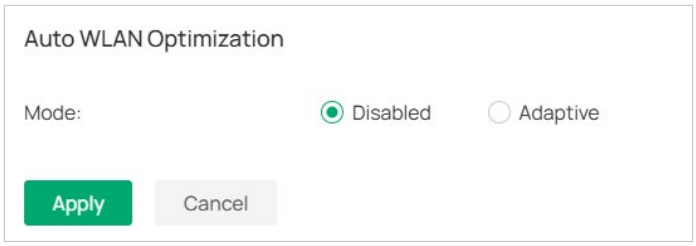


Mode	Specify the optimization mode. Default: The controller will conduct the optimization with the default configurations. Custom: The controller will conduct the optimization with the configurations you set.
Automatic Channel Optimization	Enable this function, and the controller will scan the wireless environment to conclude the optimum operation channels for the APs.
Automatic Band Optimization	Enable this function in a high-density deployment scenario, and the controller will scan the wireless environment and determine whether to turn off some radio bands to reduce network interference, hence improving the performance of the entire network.
Automatic Channel Width Optimization	Enable this function in a high-density deployment scenario, and the controller will scan the wireless environment and determine whether to reduce some radio bandwidth to reduce network interference, hence improving the performance of the entire network.
Automatic Power Optimization	Enable this function, and the controller will scan the wireless environment to conclude the optimum transmission power for the APs.

Power Range	Select Custom if you want to optimize the power within the specified range. You can limit the transmit power range of each wireless device after the power deployment is completed. For high-density deployment, you can try to set a smaller power range. An over-low value may lead to limited coverage, while an over-high value may lead to strong interference. (Note: The deployment may fail if the minimum power you select exceeds the maximum power of the AP to be deployed.)
Power Threshold	Select Custom if you want to optimize the power within the specified threshold. You can adjust the power deployment override threshold according to the actual deployment height and spacing of wireless devices, achieving optimal wireless coverage after RF optimization. The larger the threshold, the larger the adjusted overall power value.
Channel Width Selection	Select the channel width for each band, and the optimization will maintain the selected channel width.
Excluded 5 GHz Channels	When enabled, you can specify the channels so they will not execute the automatic optimization.

Set Up Auto WLAN Optimization

1. Go to Network Config > Network Settings > WLAN > WLAN Optimization.
2. In the Auto WLAN Optimization section, specify the auto optimization mode.



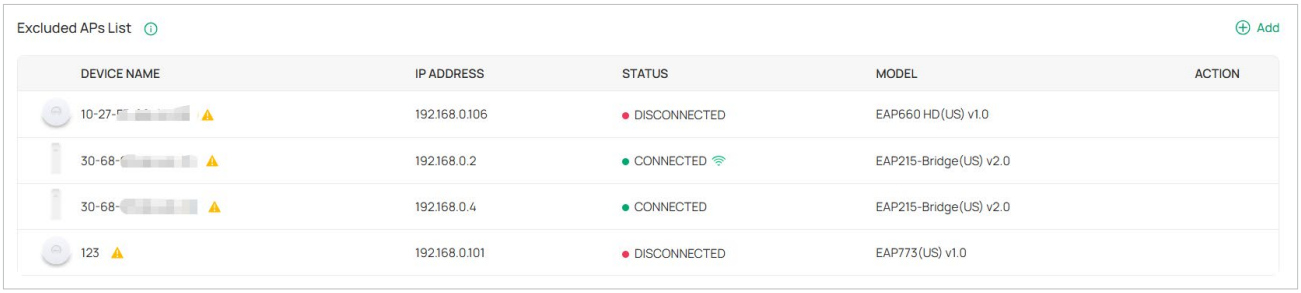
Mode	Specify the auto optimization mode. Disabled: Do not optimize WLAN performance automatically. Adaptive: The controller intelligently optimizes the wireless network based on the global network monitoring data from the controller and the network conditions reported by the devices.

3. Apply the settings. Adaptive optimizations will be automatically triggered once the topology or Wi-Fi environment changes.

Exclude APs from WLAN Optimization

If you want to exclude cetain APs from WLAN optimization, locate the Excluded APs List on the WLAN Optimization page, click Add to add the APs.

Some APs will be added to the list automatically, including APs in the mesh network and APs with unsupported firmware.


Excluded APs List
Add
DEVICE NAME
IP ADDRESS
STATUS
MODEL
ACTION
10-27-
192.168.0.106
DISCONNECTED
EAP660 HD(US) v1.0
30-68-
192.168.0.2
CONNECTED
EAP215-Bridge(US) v2.0
30-68-
192.168.0.4
CONNECTED
EAP215-Bridge(US) v2.0
123
192.168.0.101
DISCONNECTED
EAP773(US) v1.0

Chapter 15

Configure VPN Networks

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

This chapter guides you on how to configure VPN networks with the Fusion gateway. The chapter includes the following sections:

15. 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:

- **Lightlink VPN**

Lightlink VPN is designed for zero-configuration remote access, allowing users to securely connect to your network from anywhere.

- **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. The 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.

- **WireGuard VPN**

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.

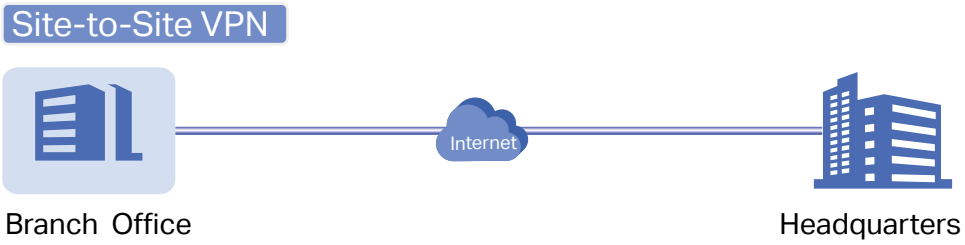
- **SSL VPN**

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.

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.



  The gateway supports the following types of Site-to-Site VPNs:

  - WireGuard

    Create a WireGuard VPN tunnel between two peer gateways over internet, from a local gateway to a remote gateway that supports WireGuard. Omada managed gateway on this site is the local peer gateway.

  - IPsec

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

- **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:

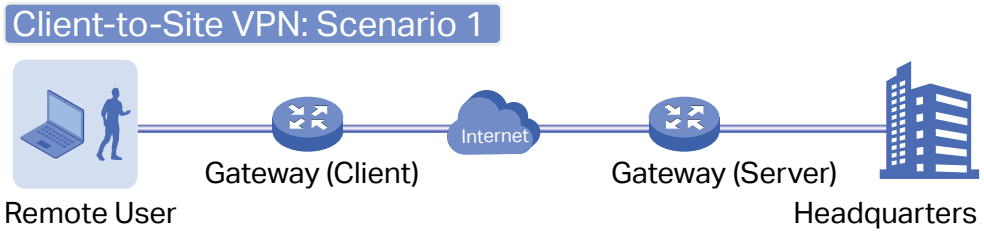
  - VPN Server

    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 WireGuard, OpenVPN, IPSec, SSL VPN, L2TP, or PPTP as the tunneling protocol.

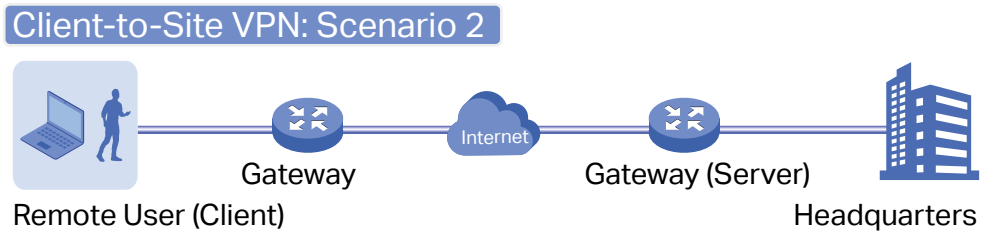
  - VPN Client

    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 WireGuard, OpenVPN, L2TP, or PPTP 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 WireGuard, 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.

15. 2 Configure Lightlink VPN

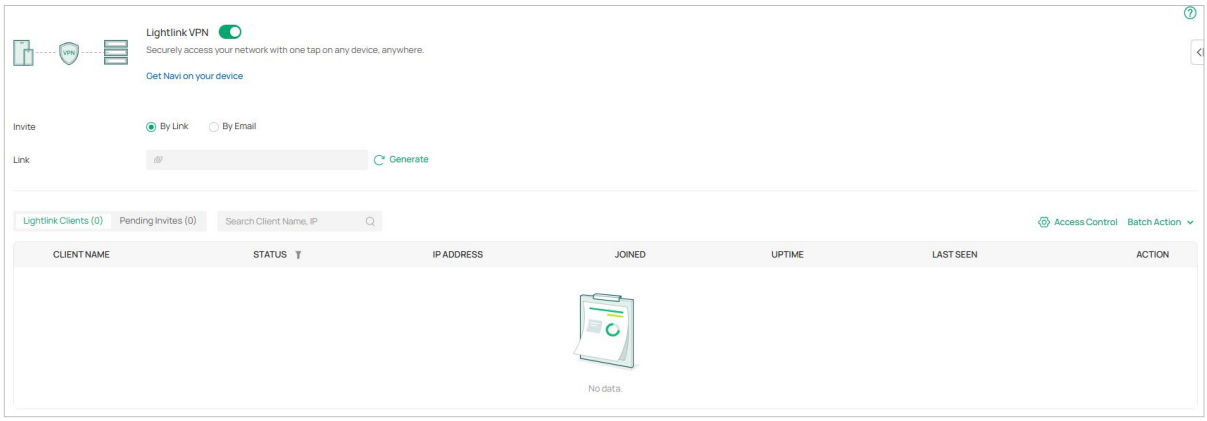
Lightlink VPN is designed for zero-configuration remote access, allowing users to securely connect to your network from anywhere.

Lightlink VPN uses an invite-based setup. The administrator generates an invite (link or email), and the invited user opens it in the Navi App and taps Connect to start the VPN.

■ Create Lightlink VPN

To configure Lightlink VPN, follow the steps below:

1. Go to Network Config > VPN > Lightlink VPN and toggle on the switch to enable Lightlink VPN.



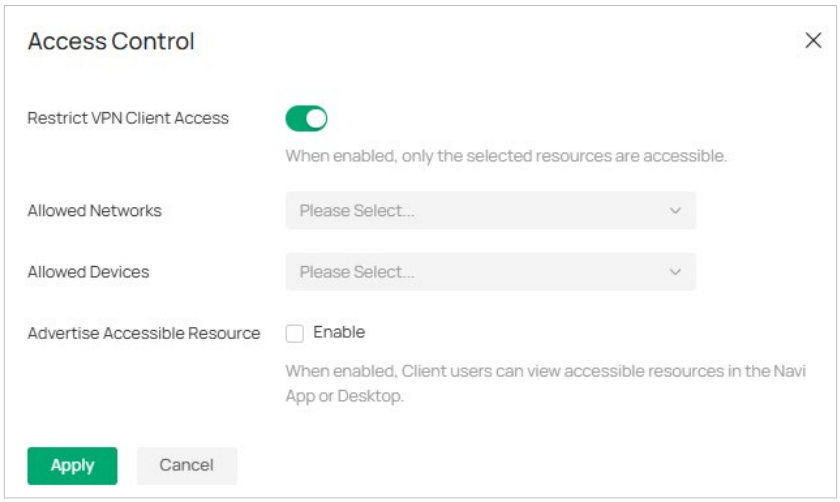
2. Select the Invite method, By Link or By Email. Each invite link expires after 24 hours and can be used once per client.
   - If you select By Link, click Generate to generate a shareable invite link for remote users to join the VPN.
   - If you select By Email, enter the recipient email addresses and click Send Invites to send invitations (up to 5 per invite).
3. Open the invite in the Lightlink Client (Navi App / Desktop). The VPN configuration is applied automatically. Tap Connect to start the VPN.
4. After the VPN connection is established. You can manage the clients and pending invites. The Lightlink Clients list displays VPN clients that have joined the controller and their connection status. The Pending Invites list displays unused invite links that have been generated.

■ (Optional) Configure Access Control

You can control what local networks and devices VPN clients can access. By default, access control is disabled, and all local resources are accessible.

To configure access control, follow the steps below:

1. Go to Network Config > VPN > Lightlink VPN, click Access Control, and toggle on the switch to Restrict VPN Client Access.



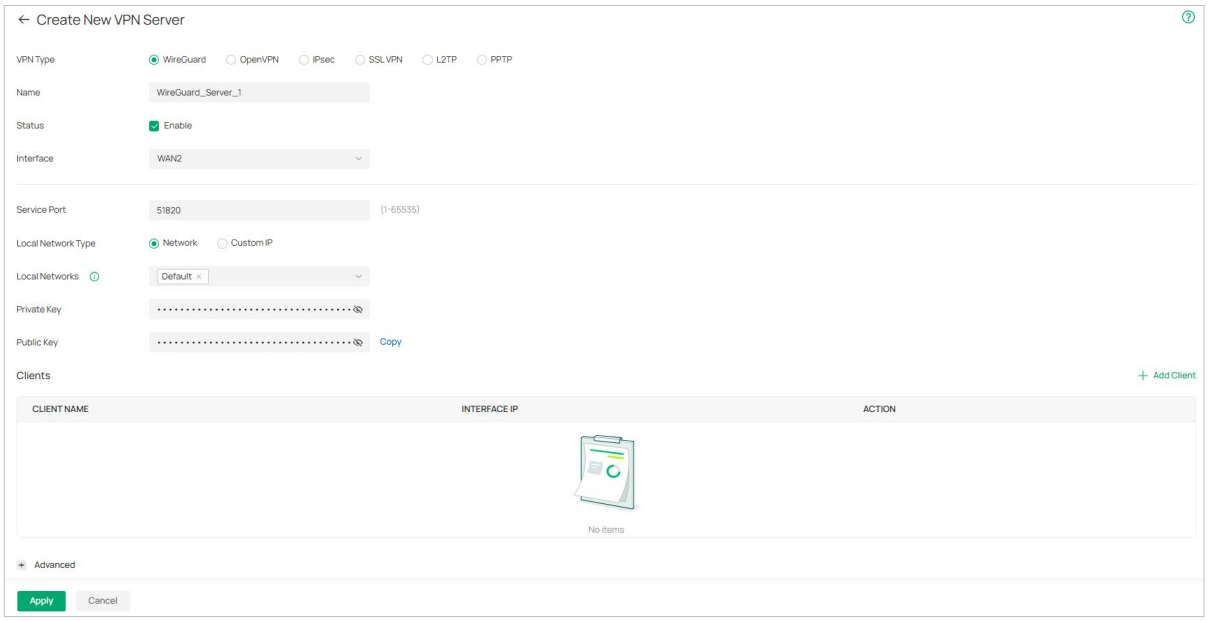
2. Specify Allowed Networks. Select the local LAN networks that VPN clients can access.
3. Specify Allowed Devices. Select specific local devices that VPN clients can access.
4. Enable Advertise Accessible Resources to display allowed networks and devices in the VPN client (Navi app) for easier access.
5. Click Apply to save the settings.

15. 3 Configure VPN Server

A VPN server provides secure network access for VPN clients. The gateway works as a VPN server to provide a remote host with access to the local network via tunneling protocols, including WireGuard, OpenVPN, IPsec, SSL VPN, L2TP and PPTP.

15. 3. 1 Configuring the gateway as a WireGuard VPN server

1. Go to Network Config > VPN > VPN Sever. Click Create New VPN Server to load the following page.

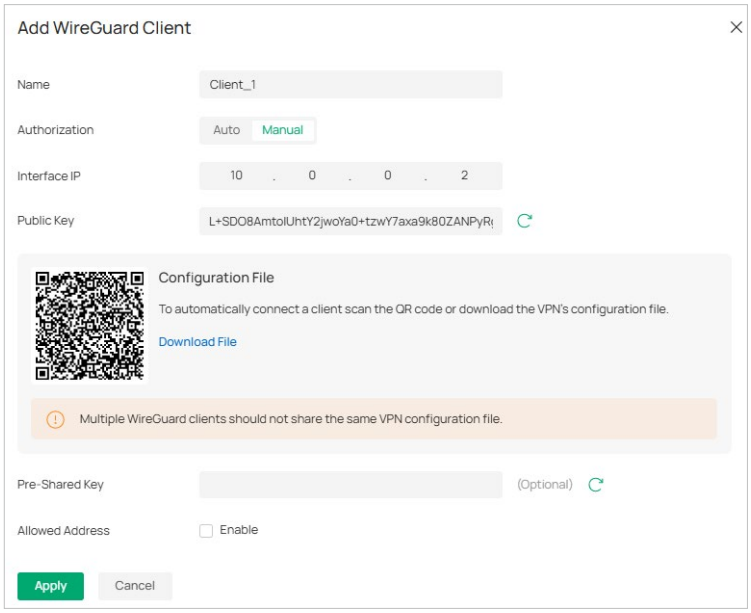


2. Select the VPN type as WireGuard. Refer to the following table to configure the required parameters.

Name	Enter a name to identify the VPN server.
Status	Click the checkbox to enable the VPN server.
Interface	Select a WAN interface whose IP will serve as the client's endpoint and be written into the client's configuration file. The client will access the WireGuard Server through this WAN interface and establish a connection.
Service Port	Specify the port number that the WireGuard interface listens to.

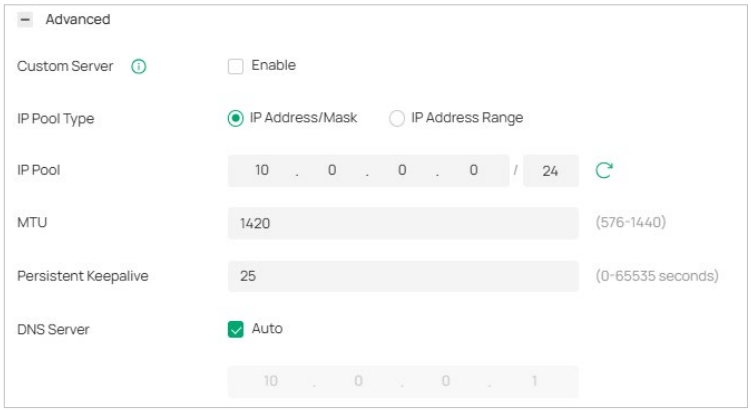
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
Private Key	Specify the private key of the WireGuard interface. The value will be automatically generated on the device.
Public Key	Specify the public key of the WireGuard interface. This field will be automatically generated based on the private key.

3. In the Clients section, click Add Client, configure the following parameters, and click Apply.



Name	Specify the name that identifies the WireGuard client.
Authorization	Choose to automatically generate a WireGuard client configuration, or manually customize the client entries. If you choose to manually customize the client entries, you need to configure the Interface IP, Public Key, Pre-Shared Key and Allowed Address.
Interface IP	Specify the IP address of the WireGuard client. The IP address is automatically assigned in sequence by the IP Pool.
Public Key	Specify the public key of the client.
Preshared Key	Check the box to specify an optional shared key.
Allowed Address	Check the box to specify the address segment that allows traffic to pass through. Generally, you can fill in the subnet address of the peer. If this option is not enabled, the system will use the client's Interface IP.

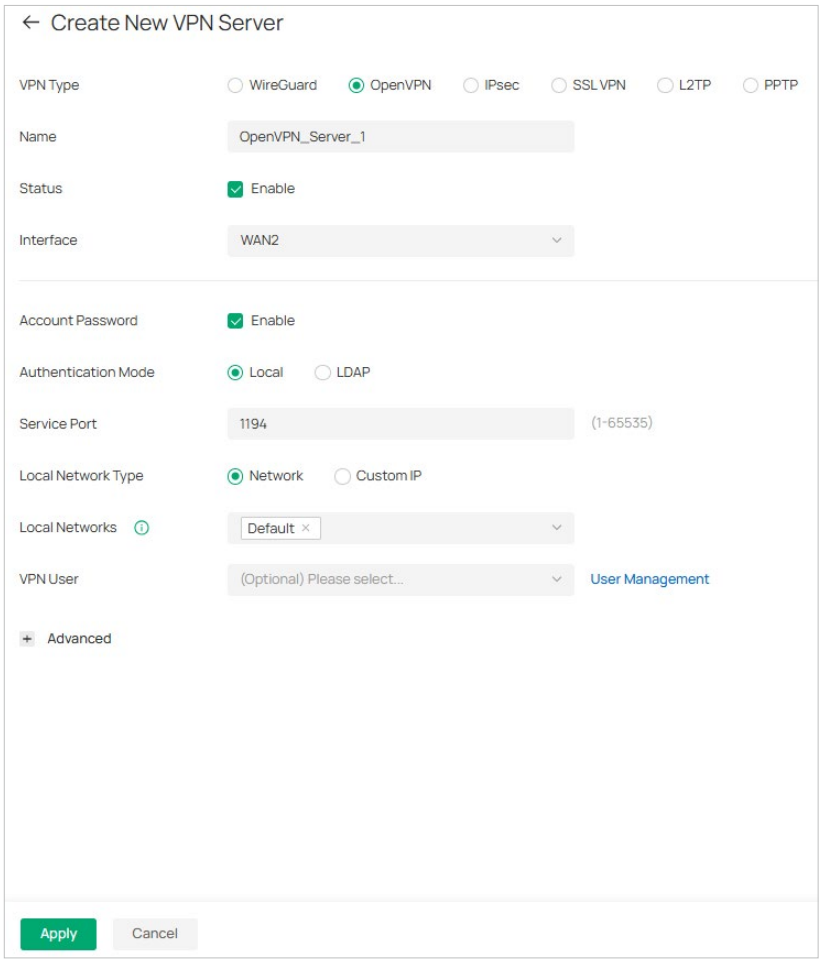
4. Click Advanced to configure the following parameters as needed, and click Apply.



Custom Server	When enabled, the customized server address (IP address or domain name) can be written into the certificate for the client to identify and connect to the WireGuard server.
IP Pool Type	Specify the format of the IP pool.
IP Pool	If you select IP Address/Mask type, enter the IP Address and subnet Mask to decide the range of VPN IP pool. If you select IP Address Range type, enter the start and end IP addresses of the VPN IP pool.
MTU	Specify the MTU value of the WireGuard interface. The recommended value is as follows: For static/dynamic dialing: 1420 For PPPoE/L2TP/PPTP dialing: WAN port MTU - 80
Persistent Keepalive	Specify the tunnel keepalive packet interval.
DNS Server	When enabled, the system will automatically generate the DNS server information and send it to the client. By default, the device's default LAN gateway (IPsec, L2TP, PPTP) or the virtual IP assigned to the current server by IP Pool (OpenVPN, SSL VPN, WireGuard) will be used as the DNS address.
Primary/Secondary DNS Server	If you need to manually configure the DNS server, deselect the Auto box, then specify the DNS address to be assigned to the VPN client (eg 8.8.8.8). You can enter the gateway's LAN IP.

15. 3. 2 Configuring the gateway as an OpenVPN server

1. Go to Network Config > VPN > VPN Server. Click Create New VPN Server to load the following page.

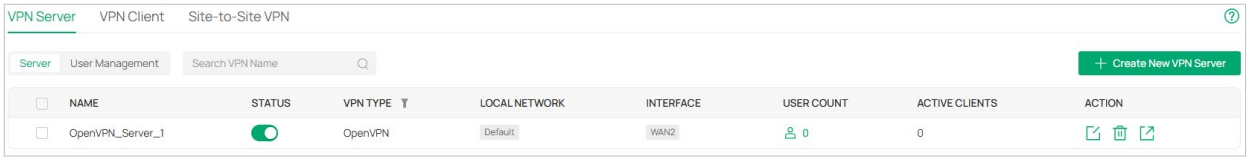


2. Select the VPN type as OpenVPN. Refer to the following table to configure the required parameters.

Name	Enter a name to identify the VPN server.
Status	Click the checkbox to enable the VPN server.
Interface	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.
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 User Management page.
Authentication Mode	Specify the authentication method used by the OpenVPN server. Local: Use a built-in authentication server to authenticate when the tunnel is created. If you don't have an additional external server, you can choose local authentication. LDAP: Use an external LDAP server to authenticate when the tunnel is created. When this option is specified, select an LDAP entry that you have configured in Profiles > LDAP Profile.
Service Port	Enter a VPN service port to which a VPN device connects.

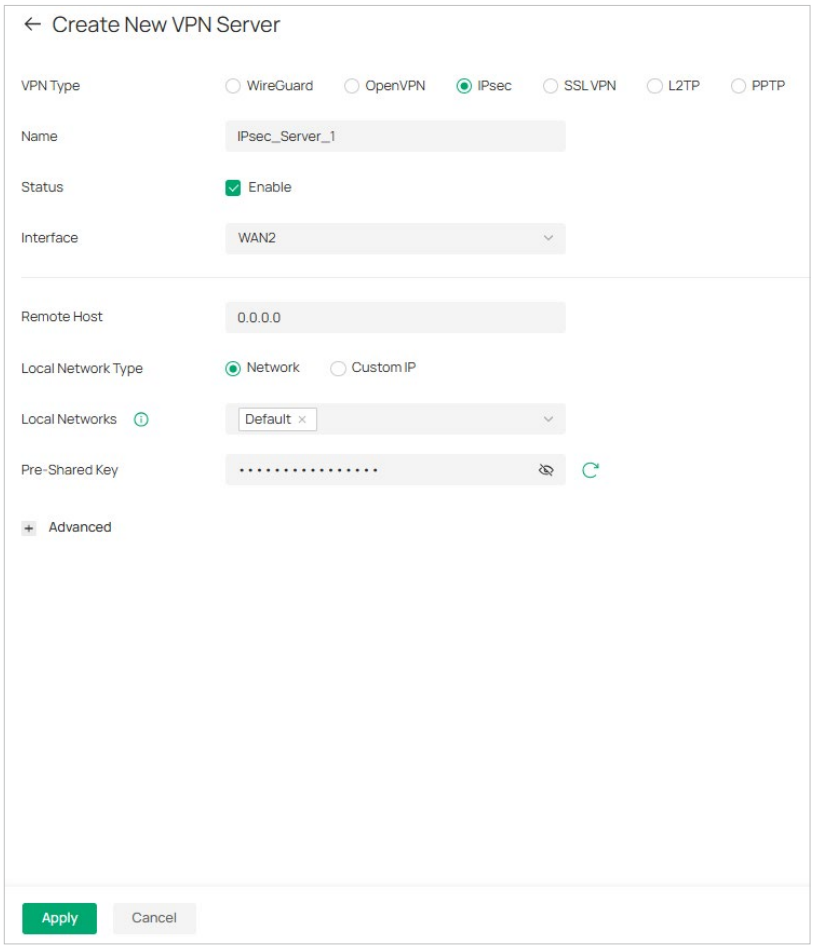
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
VPN User	Select a user associated to the VPN server. Click Add User to add a new user. You can manage the users on the User Management page.
Click Advanced to configure the following parameters as needed.	
Tunnel Mode	Select the tunnel mode: Split or Full. Split: Only the traffic of the specified local network can pass through the tunnel. Full: Allow all client traffic to pass through the tunnel..
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 gateway.
DNS Server	When enabled, the system will automatically generate the DNS server information and send it to the client. By default, the device's default LAN gateway (IPsec, L2TP, PPTP) or the virtual IP assigned to the current server by IP Pool (OpenVPN, SSL VPN, WireGuard) will be used as the DNS address.
Primary/Secondary DNS Server	If you need to manually configure the DNS server, deselect the Auto box, then specify the DNS address to be assigned to the VPN client (eg 8.8.8.8). You can enter the gateway's LAN IP.
Change UDP Protocol to TCP	Enable this option so the OpenVPN protocol will switch from the default UDP protocol to the TCP protocol.

3. Click Apply to save the settings. After clicking Apply to save the VPN server configuration, you will see the server entry and click the export icon 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.



15. 3. 3 Configuring the gateway as an IPsec VPN server

1. Go to Network Config > VPN > VPN Server. Click Create New VPN Sever to load the following page.



2. Select the VPN type as IPsecVPN. Refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the VPN server.
Status	Click the checkbox to enable the VPN server.
Interface	Specify the WAN port on which the IPsec tunnel is established.
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.

3. Click Advanced to configure the following parameters as needed.

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 gateway.
DNS Server	When enabled, the system will automatically generate the DNS server information and send it to the client. By default, the device's default LAN gateway (IPsec, L2TP, PPTP) or the virtual IP assigned to the current server by IP Pool (OpenVPN, SSL VPN, WireGuard) will be used as the DNS address.
Primary/Secondary DNS Server	If you need to manually configure the DNS server, deselect the Auto box, then specify the DNS address to be assigned to the VPN client (eg 8.8.8.8). You can enter the gateway's LAN IP.

Besides, 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 Apply.

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.
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 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.

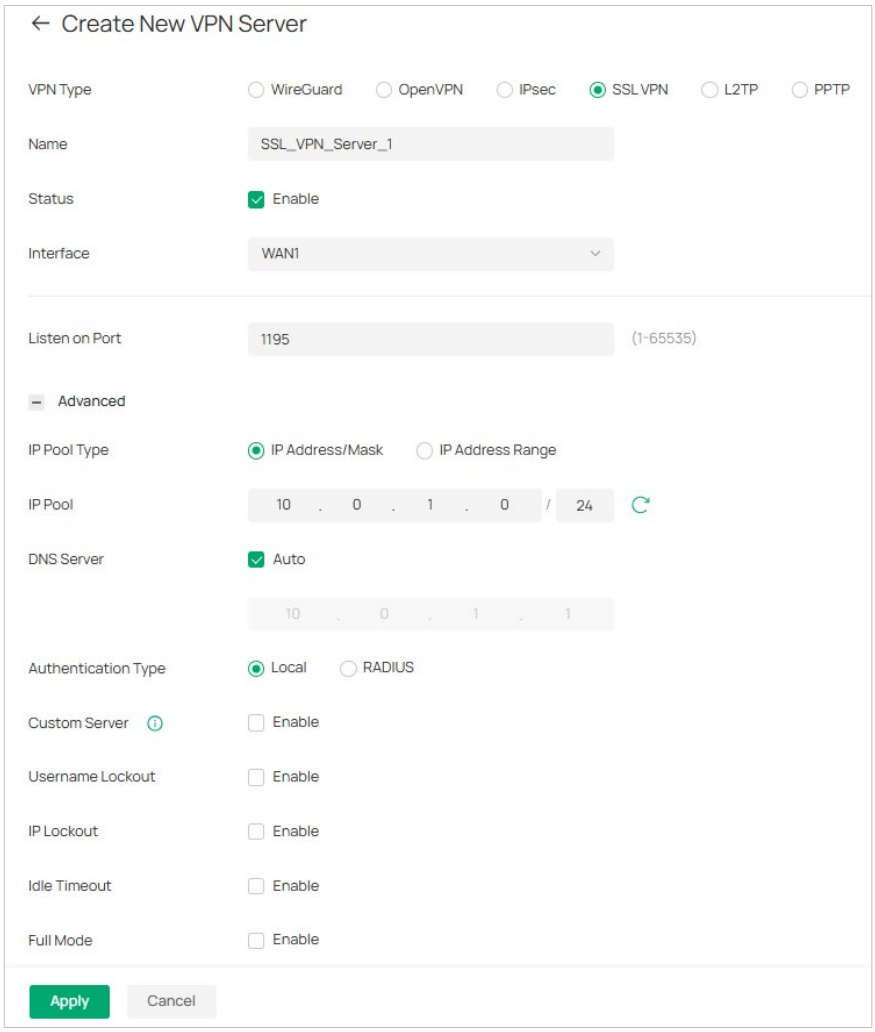
Remote ID	When the Remote ID Type is configured as Name, enter a name of the remote peer as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
SA Lifetime	Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, 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 gateway 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.

15. 3. 4 Configuring the gateway as an SSL VPN server

1. Go to Network Config > VPN > VPN Server. Click Create New VPN Sever to load the following page.



2. Configure the VPN Server.

   a. Select the VPN type as SSL VPN. Refer to the following table to configure the required parameters.

Name	Enter a name to identify the VPN server.
Status	Click the checkbox to enable the VPN server.
Interface	Select the port for the SSL VPN server to listen on, and the VPN tunnel will take effect on the port.
Listen on Port	Specify the port for the SSL VPN server to listen on.

   b. Click Advanced to configure the following parameters as needed.

IP Pool Type	Specify the format of the IP pool, and then specify the IP pool address. If you select IP Address/Mask, enter the IP Address and subnet Mask to decide the range of VPN IP pool. If you select IP Address Range, enter the start and end IP addresses of the VPN IP pool.

DNS Server	When enabled, the system will automatically generate the DNS server information and send it to the client. By default, the device's default LAN gateway (IPsec, L2TP, PPTP) or the virtual IP assigned to the current server by IP Pool (OpenVPN, SSL VPN, WireGuard) will be used as the DNS address.
Primary/Secondary DNS Server	If you need to manually configure the DNS server, deselect the Auto box, then specify the DNS address to be assigned to the VPN client (eg 8.8.8.8). You can enter the gateway's LAN IP.
Authentication Type	Select the authentication for the clients: Local or RADIUS. If you selected RADIUS, configure the following parameters: User Group: Specify the default user group in radius authentication mode. When the VPN server cannot find the value of the CLASS attribute in the authentication success message, it will assign the default resource permissions according to the user group. You can manage the VPN user group on the User Management > User Group page. 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 gateway 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.

c. Click Apply to save the settings.

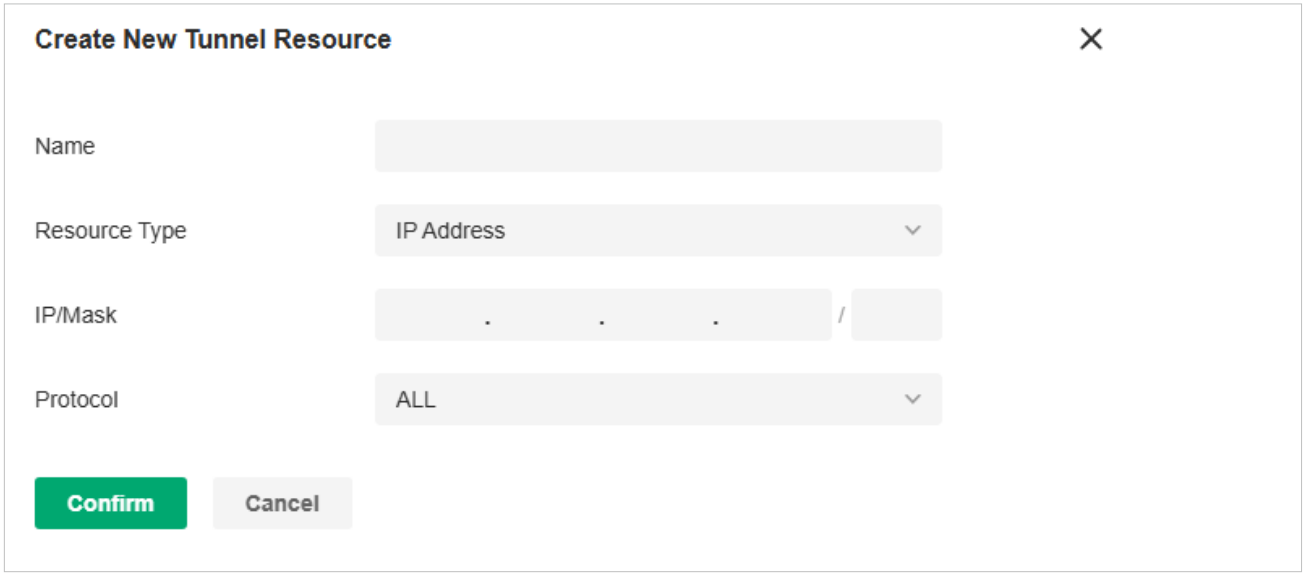
3. Configure the Resource Management

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).

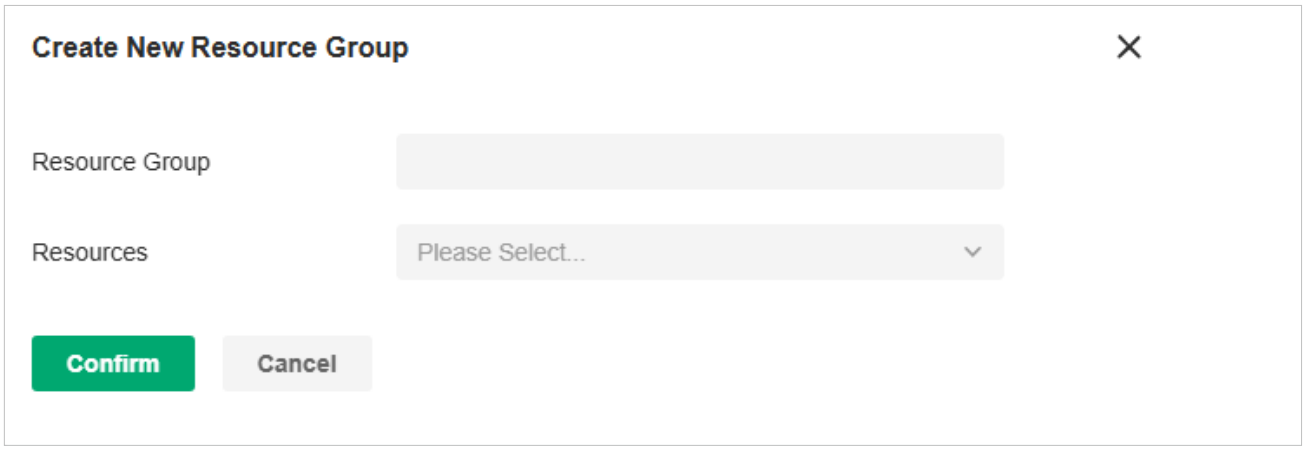
a. Go to Network Config > VPN > VPN Server > User Management > User Group, and click Resource Management.

b. In Tunnel Resources, click Create New Tunnel Resource to load the following page. Configure the parameters and click Confirm.



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 gateway 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.

c. In Resource Group, click Create New Resource Group to load the following page. Configure the parameters and click Confirm.



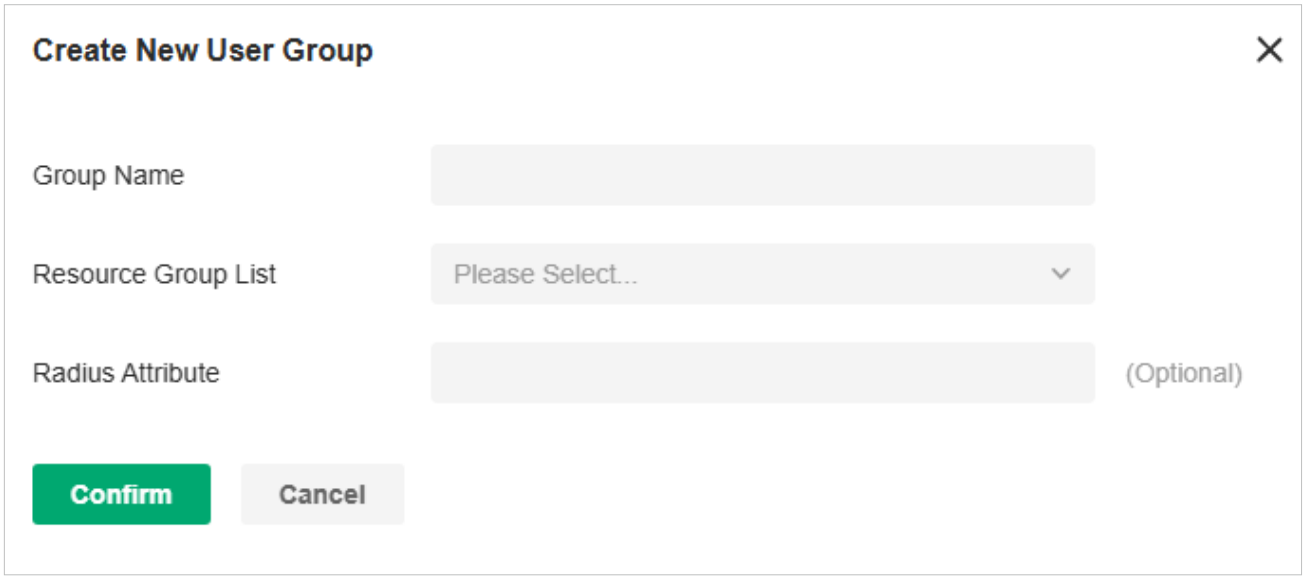
Resource Group	Specify a name for the resource group.
Resources	Select the resources for the group.

4. Configure the User Group

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

a. Go to Network Config > VPN > VPN Server > User Management > User Group.

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



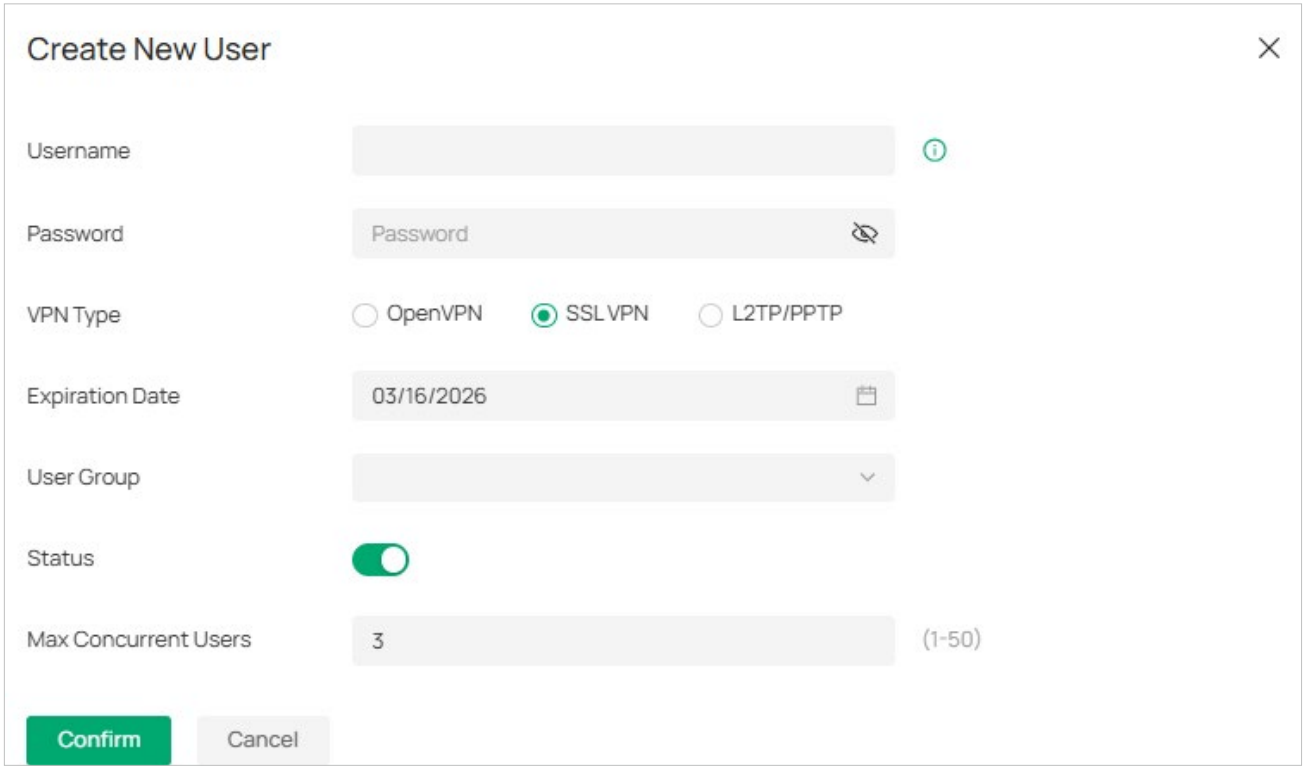
Group Name	Specify a name for the user group.
Resource Group List	Select the resource group for the user group.
Radius Attribute	Only valid in radius authentication mode. It maps the user group with radius grouping information (which is carried by the CLASS attribute 25).

5. Configure the User List

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

a. Go to Go to Network Config > VPN > VPN Server > User Management > User List.

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



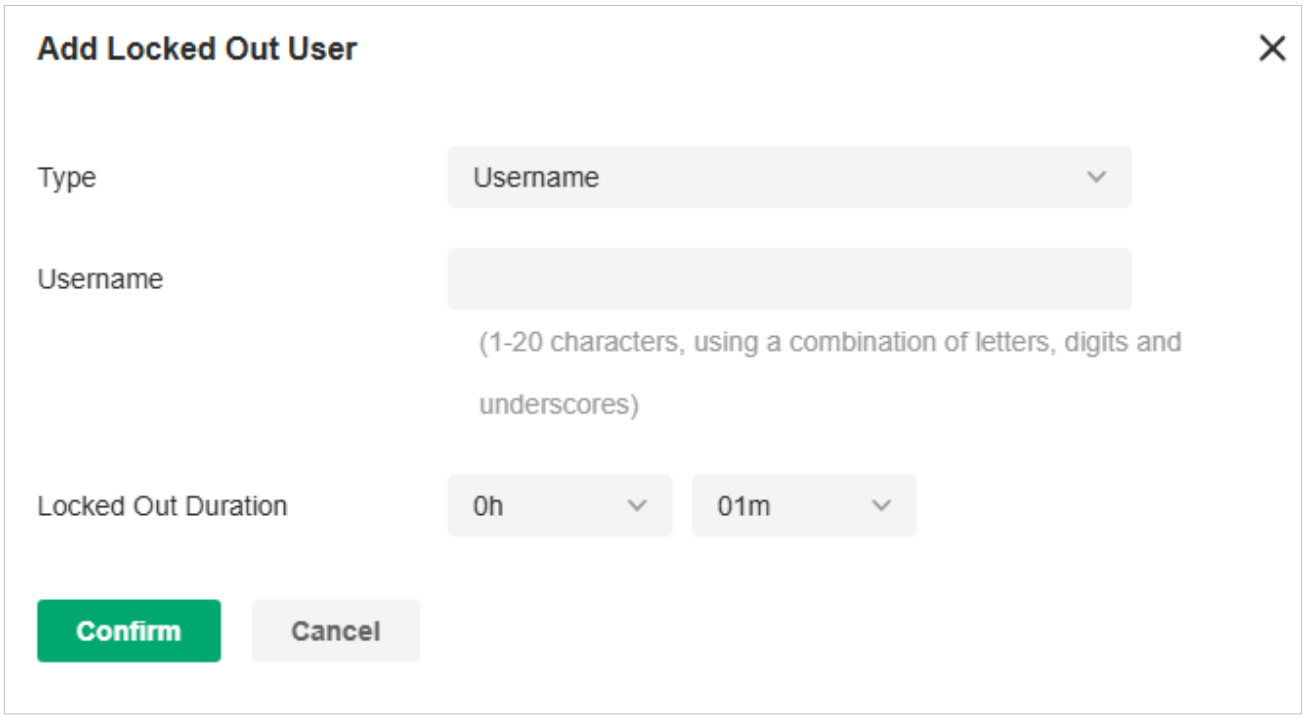
Username	Specify the username a client used for login.
Password	Specify the password a client used for login.
VPN Type	Choose the VPN Type as SSL VPN.
Expiration Date	Specify when the user account will expire.
User Group	Select which group the user belongs to. A user can only be added to one user group.
Status	Click the checkbox to enable this entry.
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.

6. Configure the Locked Out User.

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

a. Go to Network Config > VPN > VPN Server > User Management > Locked Out User.

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

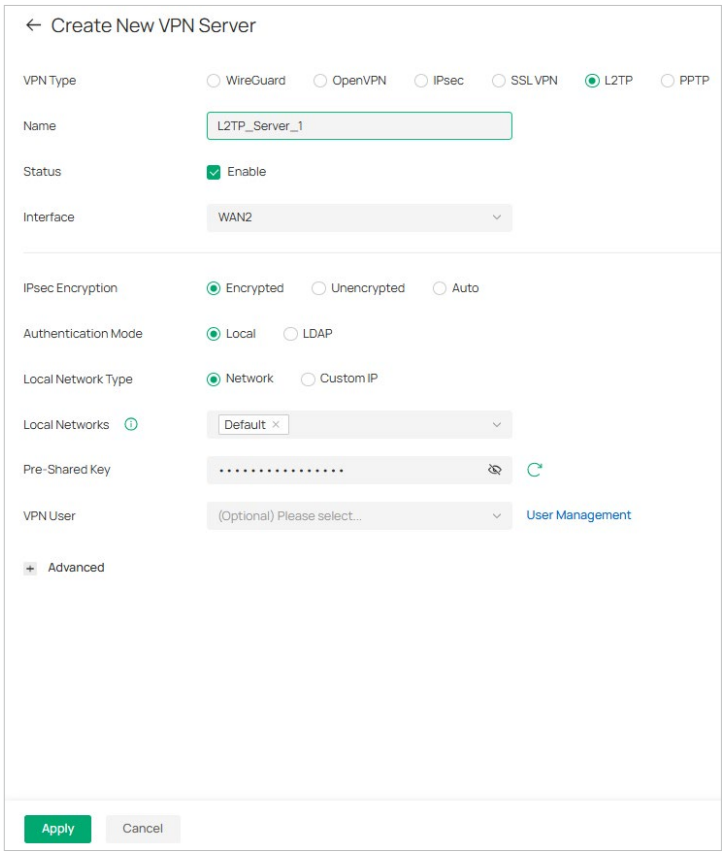


Type	Specify the locked out type. If you selected Username, specify the username of a locked out user. If you selected IP Address, specify the IP address of a locked out user.
Lockout Duration	Specify how long the entry will be locked out.

7. Go to Network Config > VPN > VPN Server, and click the Export icon to export the VPN configuration file. The VPN configuration file will be exported for clients to access the VPN.

15. 3. 5 Configuring the gateway as an L2TP VPN server

1. Go to Network Config > VPN > Server. Click Create New VPN Sever to load the following page.



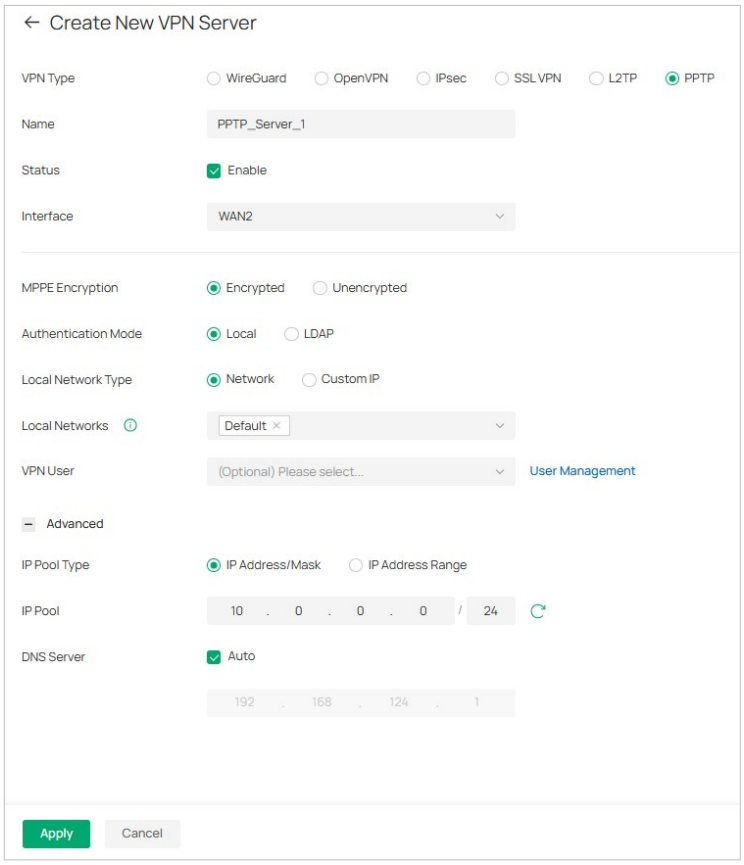
2. Select the VPN type as L2TP. Refer to the following table to configure the required parameter, and click Apply to save the settings..

Name	Enter a name to identify the VPN server.
Status	Click the checkbox to enable the VPN server.
Interface	Specify the WAN port used for L2TP tunnel.
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: Use a built-in authentication server to authenticate when the tunnel is created. If you don't have an additional external server, you can choose local authentication. LDAP: Use an external LDAP server to authenticate when the tunnel is created.
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 gateways must use the same pre-shared secret key for authentication.
VPN User	Select a user associated to the VPN server. Click Add User to add a new user. You can manage the users on the User Management page.
Click Advanced to configure the following parameters as needed.	
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.
DNS Server	When enabled, the system will automatically generate the DNS server information and send it to the client. By default, the device's default LAN gateway (IPsec, L2TP, PPTP) or the virtual IP assigned to the current server by IP Pool (OpenVPN, SSL VPN, WireGuard) will be used as the DNS address.
Primary/Secondary DNS Server	If you need to manually configure the DNS server, deselect the Auto box, then specify the DNS address to be assigned to the VPN client (eg 8.8.8.8). You can enter the gateway's LAN IP.

15. 3. 6 Configuring the gateway as a PPTP VPN server

1. Go to Network Config > VPN > VPN Server. Click Create New VPN Sever to load the following page.



2. Select the VPN type as PPTP. Refer to the following table to configure the required parameter, and click Apply to save the settings..

Name	Enter a name to identify the VPN policy.
Status	Click the checkbox to enable the VPN policy.
Interface	Specify the WAN port used for L2TP tunnel.
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: Use a built-in authentication server to authenticate when the tunnel is created. If you don't have an additional external server, you can choose local authentication. LDAP: Use an external LDAP server to authenticate when the tunnel is created.

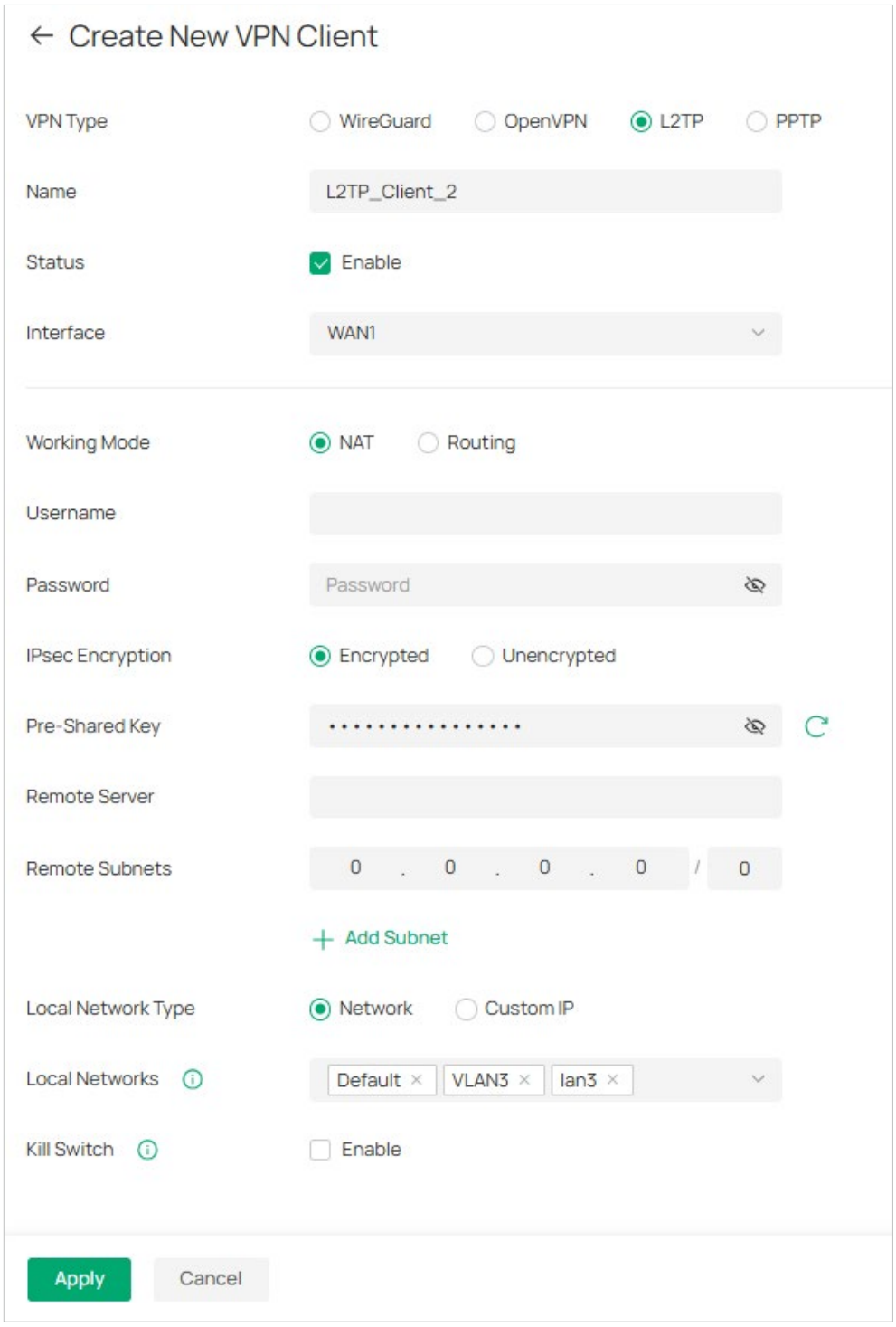
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.
VPN User	Select a user associated to the VPN server. Click Add User to add a new user. You can manage the users on the User Management page.
Click Advanced to configure the following parameters as needed.	
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.
DNS Server	When enabled, the system will automatically generate the DNS server information and send it to the client. By default, the device's default LAN gateway (IPsec, L2TP, PPTP) or the virtual IP assigned to the current server by IP Pool (OpenVPN, SSL VPN, WireGuard) will be used as the DNS address.
Primary/Secondary DNS Server	If you need to manually configure the DNS server, deselect the Auto box, then specify the DNS address to be assigned to the VPN client (eg 8.8.8.8). You can enter the gateway's LAN IP.

15. 4 Configure VPN Client

A VPN client securely connects to the VPN server. The gateway works as a VPN client to help create VPN tunnels between its connected hosts and the VPN server via tunneling protocols, including WireGuard, OpenVPN, L2TP and PPTP. Remote hosts connected to the gateway can access the local networks without running VPN client software.

15. 4. 1 Configuring the gateway as an L2TP VPN client

1. Go to Network Config > VPN > VPN Client. Click Create New VPN Client to load the following page.



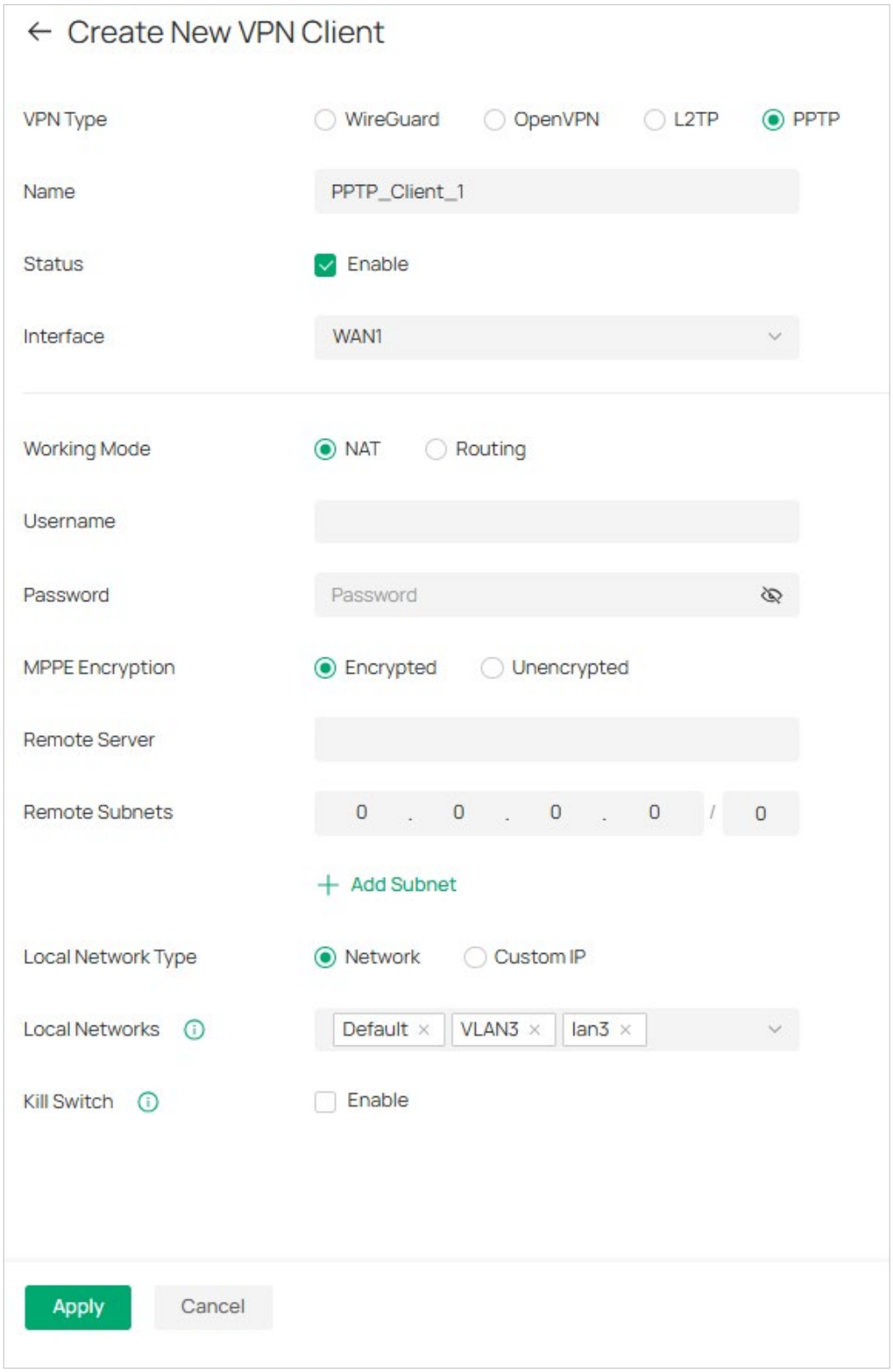
2. Select the VPN type as L2TP. Refer to the following table to configure the required parameter, and click Apply to save the settings.

Name	Enter a name to identify the VPN client.
Status	Click the checkbox to enable the VPN client.
Interface	Specify the WAN port used for L2TP tunnel..

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.
Pre-shared Key	When the IPsec Encryption is configured as Encrypted, specify the Pre-shared Key for IKE authentication.
Remote Server	Enter the IP address or domain name of the L2TP server.
Remote Subnets	Enter the LAN Subnets of VPN Server which you can access via VPN connection. You can click Add Subnet to add multiple subnets.
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.
Kill Switch	When enabled, the system prevents the client device from connecting to the internet if the VPN connection drops. However, if static routes or policy routes are configured for this client device, this device can still connect to the internet according to the routing policy.

15. 4. 2 Configuring the gateway as a PPTP VPN client

1. Go to Network Config > VPN > VPN Client. Click Create New VPN Client to load the following page.



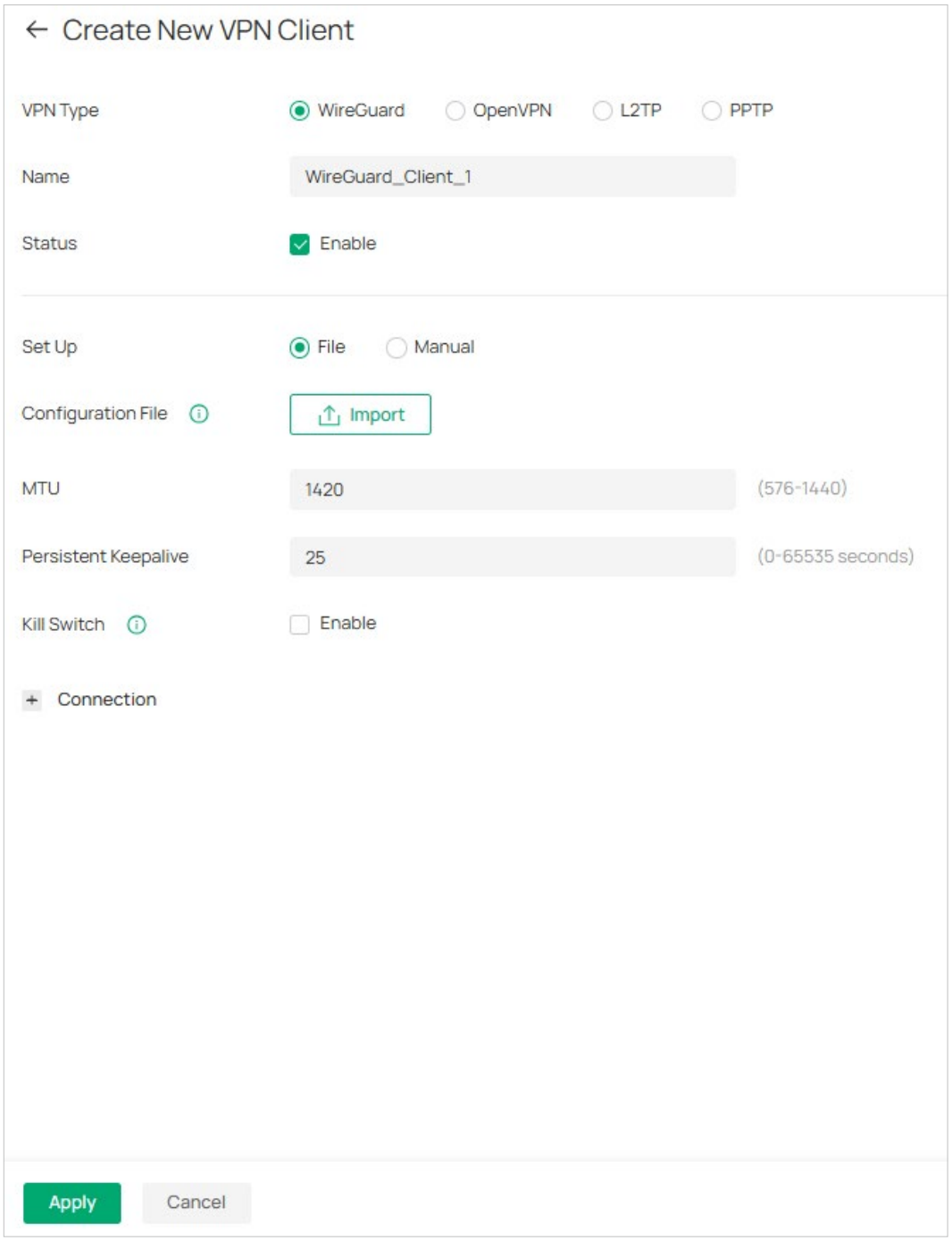
2. Select the VPN type as PPTP. Refer to the following table to configure the required parameter, and click Apply to save the settings.

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

Interface	Specify the WAN port used for PPTP tunnel..
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 LAN Subnets of VPN Server which you can access via VPN connection. You can click Add Subnet to add multiple subnets.
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.
Kill Switch	When enabled, the system prevents the client device from connecting to the internet if the VPN connection drops. However, if static routes or policy routes are configured for this client device, this device can still connect to the internet according to the routing policy.

15. 4. 3 Configuring the gateway as a WireGuard client

1. Go to Network Config > VPN > VPN Client. Click Create New VPN Client to load the following page.



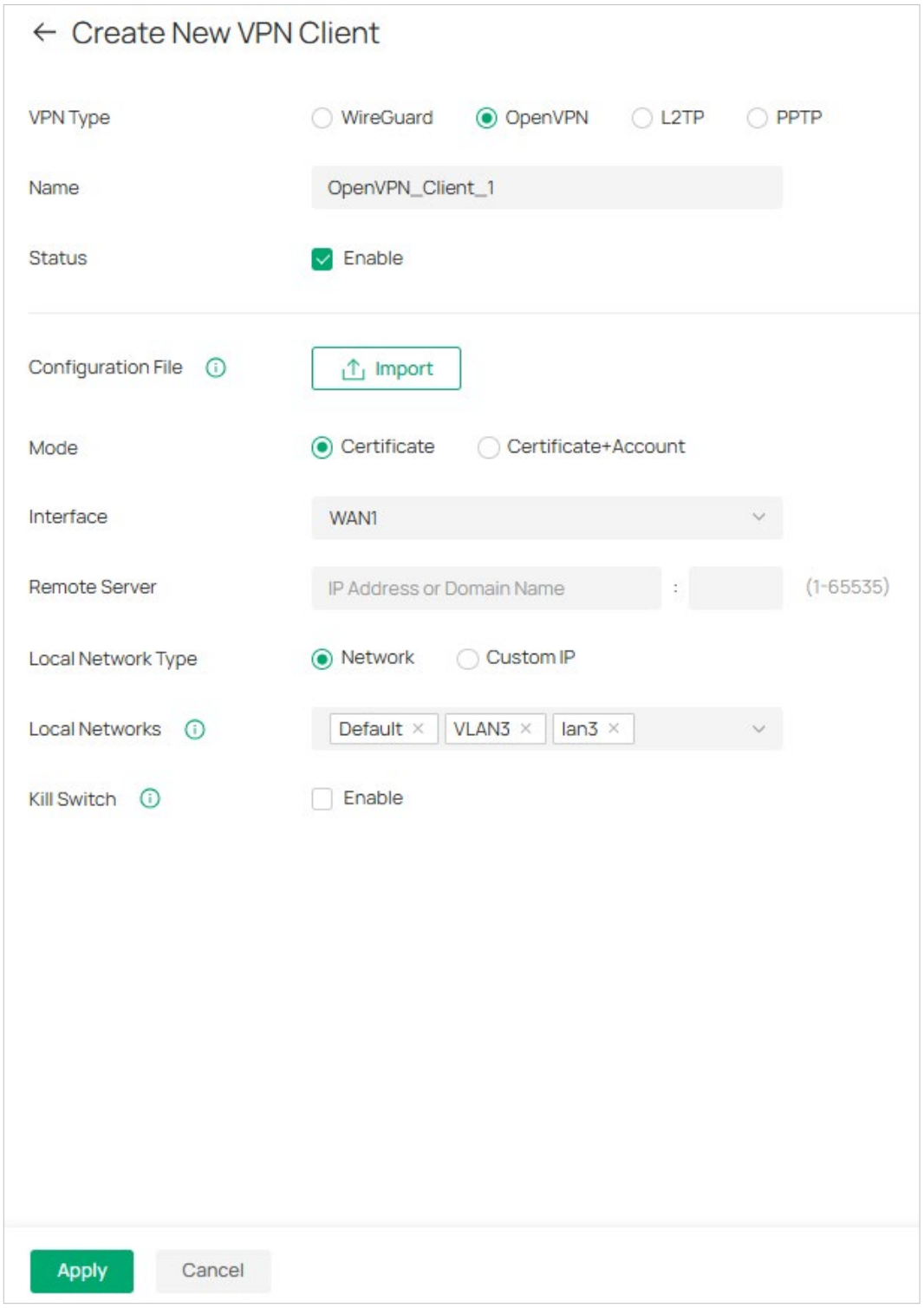
2. Select the VPN type as WireGuard. Refer to the following table to configure the required parameter, and click Apply to save the settings.

Name	Enter a name to identify the VPN client.
Status	Click the checkbox to enable the VPN client.
Set Up	Choose to set up the client via a configuration file or manually. If you choose to set up the client manually, you need to manually configure the Connection parameters.

Configuration File	If you choose to set up the client via a configuration file, click the Import button to import the WireGuard file that ends in .conf generated by the WireGuard server. Only one file can be imported.
MTU	Specify the MTU value of the WireGuard interface. The recommended value is as follows: For static/dynamic dialing: 1420 For PPPoE/L2TP/PPTP dialing: WAN port MTU - 80
Persistent Keepalive	Specify the tunnel keepalive packet interval
Kill Switch	When enabled, the system prevents the client device from connecting to the internet if the VPN connection drops. However, if static routes or policy routes are configured for this client device, this device can still connect to the internet according to the routing policy.
Click Connection to expand the parameters.	
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.
Public Key	Specify the public key of the WireGuard interface. This field will be automatically generated based on the private key.
Tunnel IP	Specify the IP address of the WireGuard interface.
Remote Server	Specify the IP address or domain name of the server.
Public Server Key	Specify the public key of the server.
Pre-Shared Key	Specify an optional shared key.
Primary/Secondary DNS Server	Specify the DNS dns server.
Allowed Server Address	Specify the address segment that allows traffic to pass through. Generally, you can fill in the subnet address of the peer.
Local Network Type	LSelect the type to set the local network for VPN Policy, there are two types: Network and Custom IP.
Local Networks	Select the local networks to apply the VPN Policy. The VPN Policy will only apply to the selected or filled local network.
Client Port	Specify the port number that the WireGuard interface listens to.

15. 4. 4 Configuring the gateway as an OpenVPN client

1. Go to Network Config > VPN > VPN Client. Click Create New VPN Client to load the following page.



2. Select the VPN type as OpenVPN. Refer to the following table to configure the required parameter, and click Apply to save the settings.

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

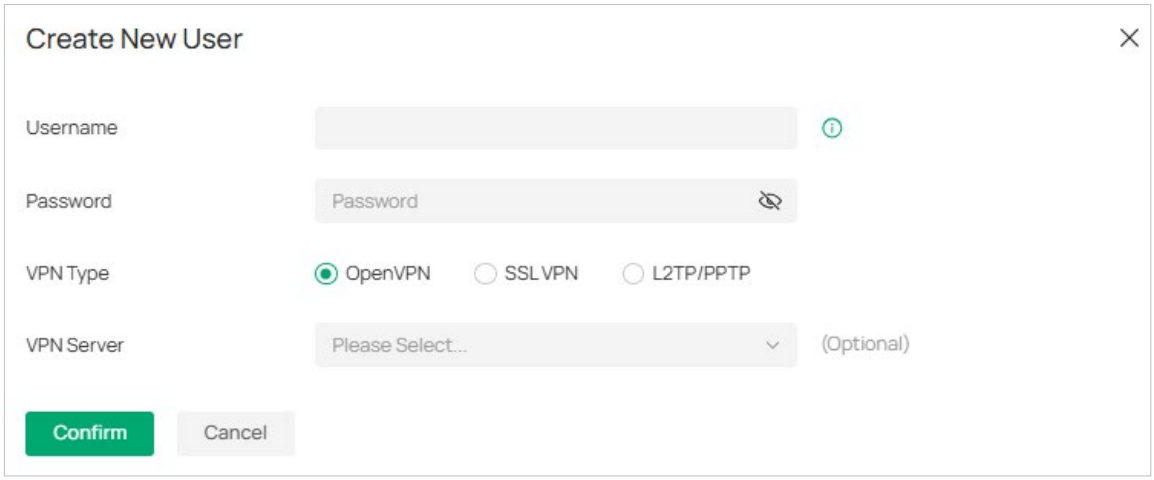
Configuration File	Click the Import button to import the OpenVPN file that ends in .ovpn generated by the OpenVPN server. Only one file can be imported. If the certificate file and configuration file are generated singly by the OpenVPN server, combine two files and import the whole file.
Mode	Select 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.
Kill Switch	When enabled, the system prevents the client device from connecting to the internet if the VPN connection drops. However, if static routes or policy routes are configured for this client device, this device can still connect to the internet according to the routing policy.

15. 5 User Management

After configuring the gateway as an OpenVPN, SSL VPN, L2TP or PPTP server, you can create VPN connection accounts for remote devices to connect to the VPN server.

To configure the users, follow these steps:

1. Go to Network Config > VPN > VPN Server > User Management. Click Create New User to add a new entry of VPN User.



2. Specify the parameters and click Confirm.

Username	Specify the account name used for the VPN tunnel.
Password	Specify the account password used for the VPN tunnel. Your VPN clients will use the account name and password for authentication.
VPN Type	Choose the VPN user you want to add.
For OpenVPN type	
VPN Server	Select the OpenVPN server to which the user belongs. Only the server with the username and password authentication option enabled can be selected.
For SSLVPN type	
Expiration Date	Specify when the user will expire.
User Group	Select which group the user belongs to. A user can only be added to one user group.
Status	Toggle on to enable the user entry.
Max Concurrent Users	Specify the maximum number of clients using the username for login concurrently. After the maximum number is reached, new login attempts will be rejected.
For L2TP/PPTP type	
VPN Server	Select the L2TP/PPTP server to which the user belongs. Only the server with the username and password authentication option enabled can be selected.

Local IP Address	Specify the local virtual IP address for the VPN server. Please avoid using the IP address in the DHCP range, which may cause IP confliction, you can enter the LAN IP of the gateway. To find out the DHCP Range, go to Network Settings > MENU.LAN > VLAN and view the information of the desired network.
Mode	Specify the network mode. There are two modes: Client: Select this option when the L2TP/PPTP client is a single host. It's commonly used to access the internal service from outside. Network Extension Mode: Select this option when the L2TP/PPTP client is a VPN gateway. The tunneling request is always initiated by a device. It's commonly used for access between two offices.
Max Concurrent Users	Specify the maximum number of connections that the tunnel can support. Wihen Client Mode is enabled, it can be used to limit the number of devices connected at the same time.
Remote Subnets	Specify a remote network. (This is the IP address range of the LAN on the remote peer of the L2TP/PPTP tunnel.) It's the combination of IP address and subnet mask. It takes effect when Network Extension Mode is enabled.

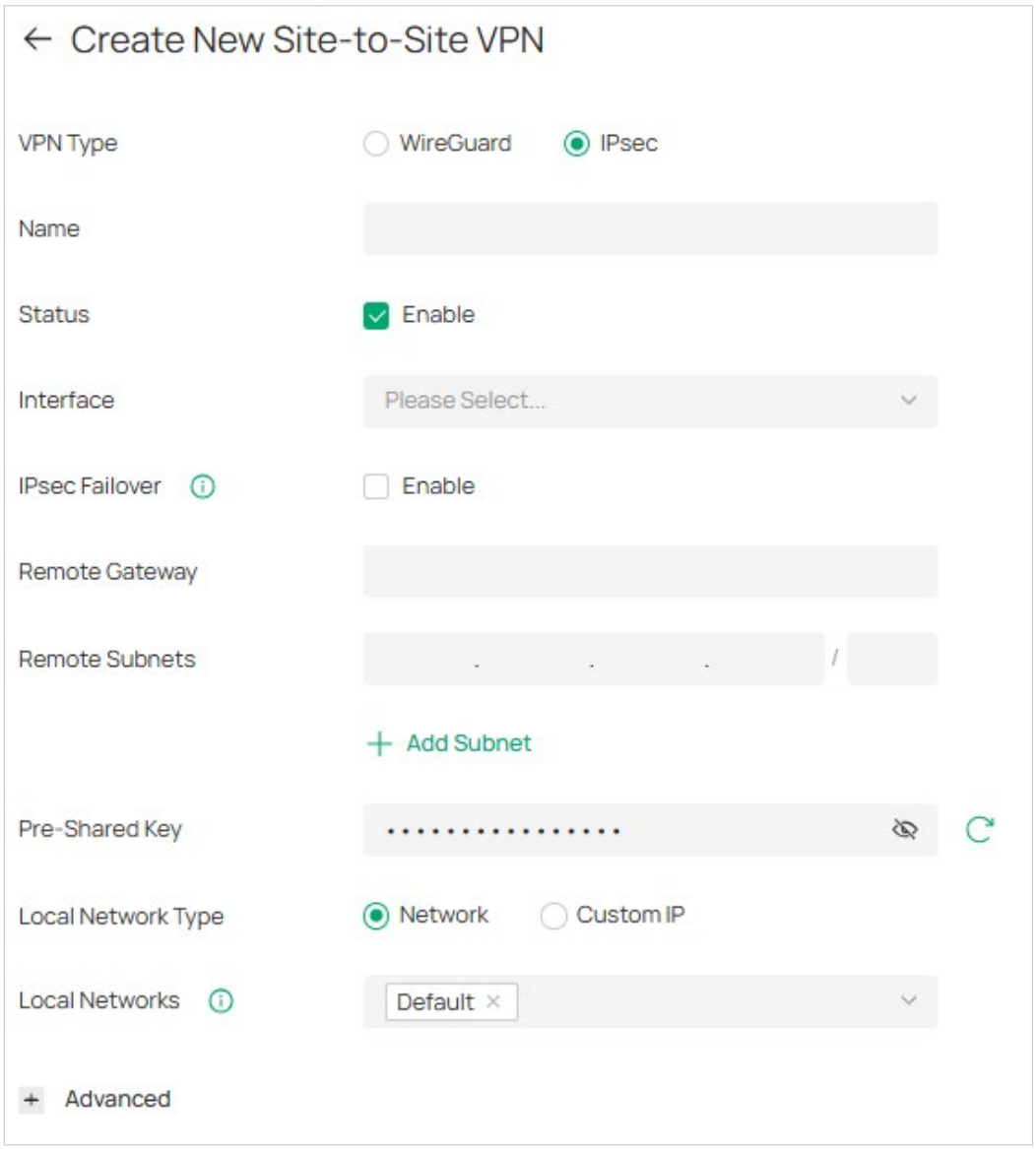
To edit or delete the VPN users, click the icon in the Action column. You can further filter the entries based on the VPN Server.

15. 6 Configure the Site-to-Site VPN

You can establish a secure connection between two locations to enable communication between networks. The gateway supports the following types of Site-to-Site VPNs.

15. 6. 1 Configuring IPsec VPN

1. Go to Network Config > VPN > Site-to-Site VPN. Click Create New Site-to-Site VPN to load the following page.

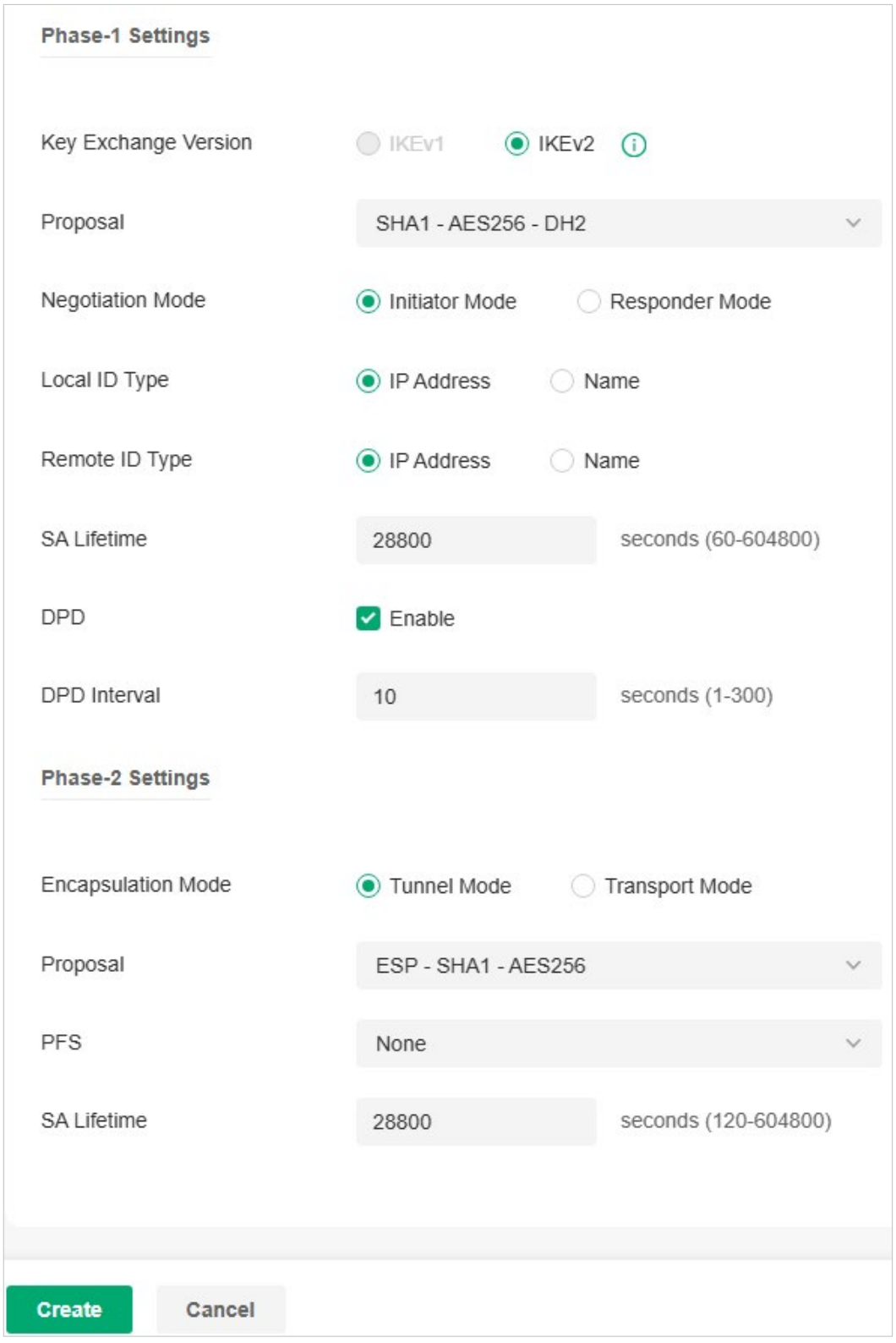


2. Select the VPN type as IPsec and refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the VPN tunnel.

Status	Click the checkbox to enable the VPN tunnel.
Interface	Specify the WAN port on which the IPsec tunnel is established.
IPsec Failover	Check the box to enable the IPsec Failover as needed. Backup WAN: Specify the IPsec secondary interface. Automatic Failback: Select this function to automatically switch back to the primary connection when it is reachable. Gateway Failover TimeoutWhen selected, the system will query whether the primary connection is reachable within the configured time, and if yes, it will switch back to the primary connection.
Remote Gateway	Enter an IP address or a domain name (1 to 253 characters) as the remote gateway. 0.0.0.0 represents any IP address. Only when the negotiation mode is set to Responder Mode in Phase-1 Settings can you enter 0.0.0.0.
Remote Subnets	Specify the remote network. It's always the IP address range of LAN on the remote peer of the VPN tunnel. It's the combination of IP Address and subnet mask. Traffic to the remote network will be forwarded via IPsec tunnel.
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.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Select the local networks to apply the VPN Policy. The VPN Policy will only apply to the selected or filled local network. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.

3. Click Advanced Settings to load the following page.



Advanced settings include Phase-1 settings and Phase-2 settings. Phase-1 is used to set up a secure encrypted channel which the two peers can negotiate Phase-2, and then establish the IKE Security Associations (IKE SA). Phase-2 is used to negotiate about a set of parameters that define what traffic can go through the VPN, and how to encrypt and authenticate the traffic, then establish the IPsec Security Associations (IPsec SA).

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

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.
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 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.

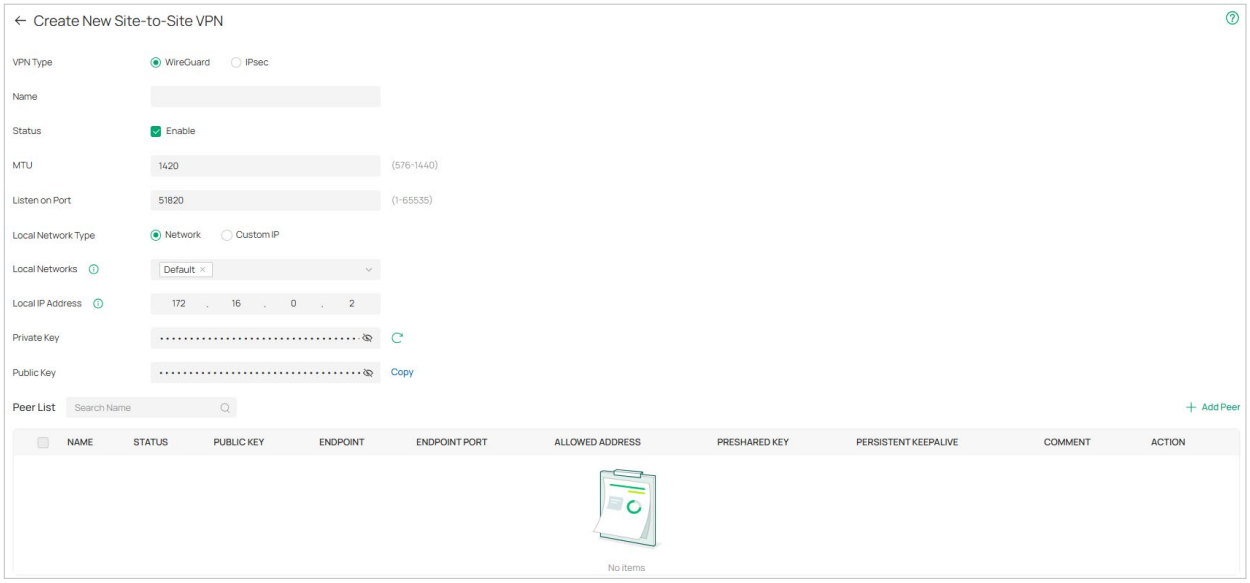
Local ID	When the Local ID Type is configured as Name, enter a name for the local device as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).
Remote ID Type	Specify the type of Remote ID which indicates the authentication identifier received from the peer 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 gateway 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.

15. 6. 2 Configuring WireGuard VPN

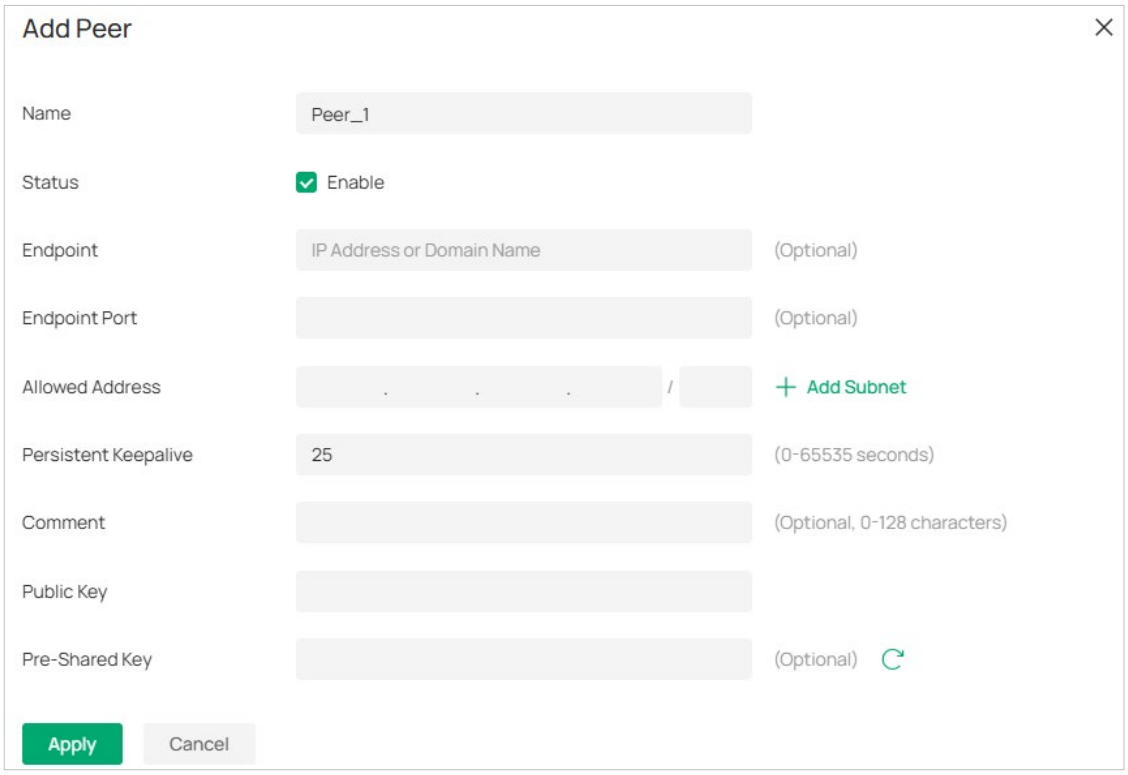
1. Go to Network Config > VPN > Site-to-Site VPN. Click Create New Site-to-Site VPN to load the following page.



2. Select the VPN type as WireGuard and refer to the following table to configure the required parameters and click Apply.

Name	Enter a name to identify the VPN tunnel.
Status	Click the checkbox to enable the VPN tunnel.
MTU	Specify the MTU value of the WireGuard interface. The recommended value is as follows: For static/dynamic dialing: 1420 For PPPoE/L2TP/PPTP dialing: WAN port MTU - 80
Listen on Port	Specify the port number that the WireGuard interface listens to.
Local Network Type	Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Select the local networks to apply the VPN Policy. The VPN Policy will only apply to the selected or filled local network. Custom IP: Specify the IP address of the WireGuard interface. Select a reserved address to avoid IP conflicts.
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.
Public Key	Specify the public key of the WireGuard interface. This field will be automatically generated based on the private key.

3. In the Peer List, click Add Peer and configure the following parameters, and then click Apply.



Name	Enter a name to identify the WireGuard peer.
Status	Specify whether to enable the peer.
Endpoint	Specify the IP address or domain name of the peer..
Endpoint Port	Specify the port number of the peer.
Allowed Address	Specify the address segment that allows traffic to pass through. Generally, you can fill in the subnet address of the peer.
Persistent Keepalive	Specify the tunnel keepalive packet interval.
Comment	Enter the description of the peer.
Public Key	Specify the public key of the peer.
Pre-Shared Key	Specify an optional shared key.

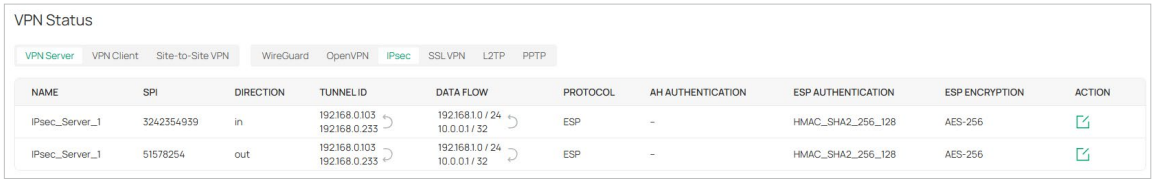
4. Click Apply to save the settings.

15. 7 View VPN Status

Once the VPN tunnel is established, you can check the VPN status.

To view the VPN status, follow these steps:

1. Go to Network Config > VPN > VPN Status.



2. Click the desired tab to display the connection status and information of the VPN tunnel.

VPN Server-WireGuard	
NAME	Displays the name of the VPN policy.
IP POOL	The IP Pool of each VPN policy.
SERVER ADDRESS	Displays the address of the VPN server. By default, it is bound to the selected WAN IP.
PORT	Displays the service port currently monitored by the VPN server.
ACTIVE CLIENTS	Displays the number of active clients currently connected to the VPN server.
CLIENTS	Click to display the details client information.
VPN Server-OpenVPN	
USER	Displays the account name of OpenVPN client.
INTERFACE	INTERFACE: The WAN port used by the VPN tunnel.
LOCAL IP	Displays the assigned virtual local IP address of the tunnel.
REMOTE LOCAL IP	Displays the assigned virtual remote local IP address of the tunnel.
DNS	Displays the DNS address of the tunnel.
DOWNLOAD PKTS	Displays the number of packets received by the VPN server.
DOWNLOAD BYTES	Displays the downstream throughput.
UPLOAD PKTS	Displays the number of packets sent by the VPN server.
UPLOAD BYTES	Displays the upstream throughput.
UPTIME	Displays how long the tunnel has been up.

ACTION	TERMINATE: Disconnects a client.
VPN Server-IPsec	
NAME	Displays the name of the VPN policy.
SPI	Displays the SPI (Security Parameter Index) of the SA, including outgoing SPI and incoming SPI. The SPI of each SA is unique.
DIRECTION	Displays the direction (in: incoming/out: outgoing) of the SA.
TUNNEL ID	Displays the IP addresses of the local and remote peers.
DATA FLOW	Displays the Local Subnet and Remote Subnet/host covered by the SA.
PROTOCOL	Displays the authentication protocol and encryption protocol used by the SA.
AH AUTHENTICATION	Displays the AH authentication algorithm used by the SA.
ESP AUTHENTICATION	Displays the ESP authentication algorithm used by the SA.
ESP ENCRYPTION	Displays the ESP encryption algorithm used by the SA.
VPN Server-SSL VPN	
USERNAME	Displays the username a client used for login.
LOGIN IP	Displays the IP address of a client.
VIRTUAL IP	Displays the virtual IP address assigned to a client by the SSL VPN server.
LOGIN TIME	Displays the time when a client logged in.
STATISTICS	Displays the total upload and download traffic of a client.
ACTION	Lock or disconnect a client. LOCK: Disconnects the client and adds them to Locked Out Users. Locked-out users cannot log in again. To enable Username Lockout or IP Lockout, go to the VPN > VPN Server Page. DISCONNECT: Disconnects a client.
VPN Server-L2TP/PPTP	
USER	Displays the account name of the VPN tunnel.
INTERFACE	The WAN port used by the VPN tunnel.
LOCAL IP	Displays the assigned virtual local IP address of the tunnel.
REMOTE LOCAL IP	Displays the assigned virtual remote local IP address of the tunnel.
DNS	Displays the DNS address of the tunnel.

DOWNLOAD PKTS	Displays the number of packets received by the VPN server.
DOWNLOAD BYTES	Displays the downstream throughput.
UPLOAD PKTS	Displays the number of packets sent by the VPN server.
UPLOAD BYTES	Displays the upstream throughput.
UPTIME	Displays how long the tunnel has been up.
ACTION	TERMINATE: Disconnects a client.
VPN Client-WireGuard	
NAME	Displays the name of the VPN policy.
REMOTE SERVER	The IP address or domain name of VPN server.
LISTEN PORT	The port number that the WireGuard interface listens to.
SERVER	Click to check the detailed information of the connected VPN server.
VPN Client-OpenVPN/L2TP/PPTP	
INTERFACE	The WAN port used by the VPN tunnel.
TUNNE	Displays the name of the VPN policy.
REMOTE LOCAL IP	Displays the remote local IP address of the tunnel.
DNS	Displays the DNS address of the tunnel.
DOWNLOAD PKTS	Displays the number of packets received by the peer.
DOWNLOAD BYTES	Displays the amount of data received by the peer.
UPLOAD PKTS	Displays the number of packets sent by the peer.
UPLOAD BYTES	Displays the amount of data sent by the peer.
UPTIME	Displays how long the tunnel has been up.
Site-to-Site VPN-WireGuard	
NAME	Displays the name of the VPN policy.
LISTEN PORT	The port number that the WireGuard interface listens to.
PEER CONNECTED/ DISCONNECTED	The number of connected/disconnected peers.
PEERS	Click to display the detailed information of the peers.

Site-to-Site VPN-IPsec	
NAME	Displays the name of the VPN policy.
SPI	Displays the SPI (Security Parameter Index) of the SA, including outgoing SPI and incoming SPI. The SPI of each SA is unique.
DIRECTION	Displays the direction (in: incoming/out: outgoing) of the SA.
TUNNEL ID	Displays the IP addresses of the local and remote peers.
DATA FLOW	Displays the Local Subnet and Remote Subnet/host covered by the SA.
PROTOCOL	Displays the authentication protocol and encryption protocol used by the SA.
AH AUTHENTICATION	Displays the AH authentication algorithm used by the SA.
ESP AUTHENTICATION	Displays the ESP authentication algorithm used by the SA.
ESP ENCRYPTION	Displays the ESP encryption algorithm used by the SA.

Chapter 16

Configure Network Security

Network Security is a portfolio of features designed to improve the usability and ensure the safety of your network and data. It implements policies and controls on multiple layers of defenses in the network.

This chapter guides you on how to configure network security with the Omada Fusion gateway. The chapter includes the following sections:

16. 1 Configure Content Filtering

Overview

Content Filtering allows you to control access to websites and online content based on security and usage policies. It protects your network from web-based threats, restricts inappropriate content, and can also block online ads for a better browsing experience.

In Content Filtering, the system inspects the domains and URLs in HTTP, HTTPS, and DNS requests and compares them with:

- The content categories you select in each rule
- The DNS-based ad blocker database (when Ad Blocker is enabled)
- Your custom Allow List and Block List entries

Requests that match a blocked item are intercepted according to the rule. Rules can be applied to specific networks, IP groups, or individual client devices whose traffic passes through the gateway and EAPs.

Note that the sequence of the Content Filtering rules is critical. 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.

To reorder the list, click and drag an entry up or down.

Configuration

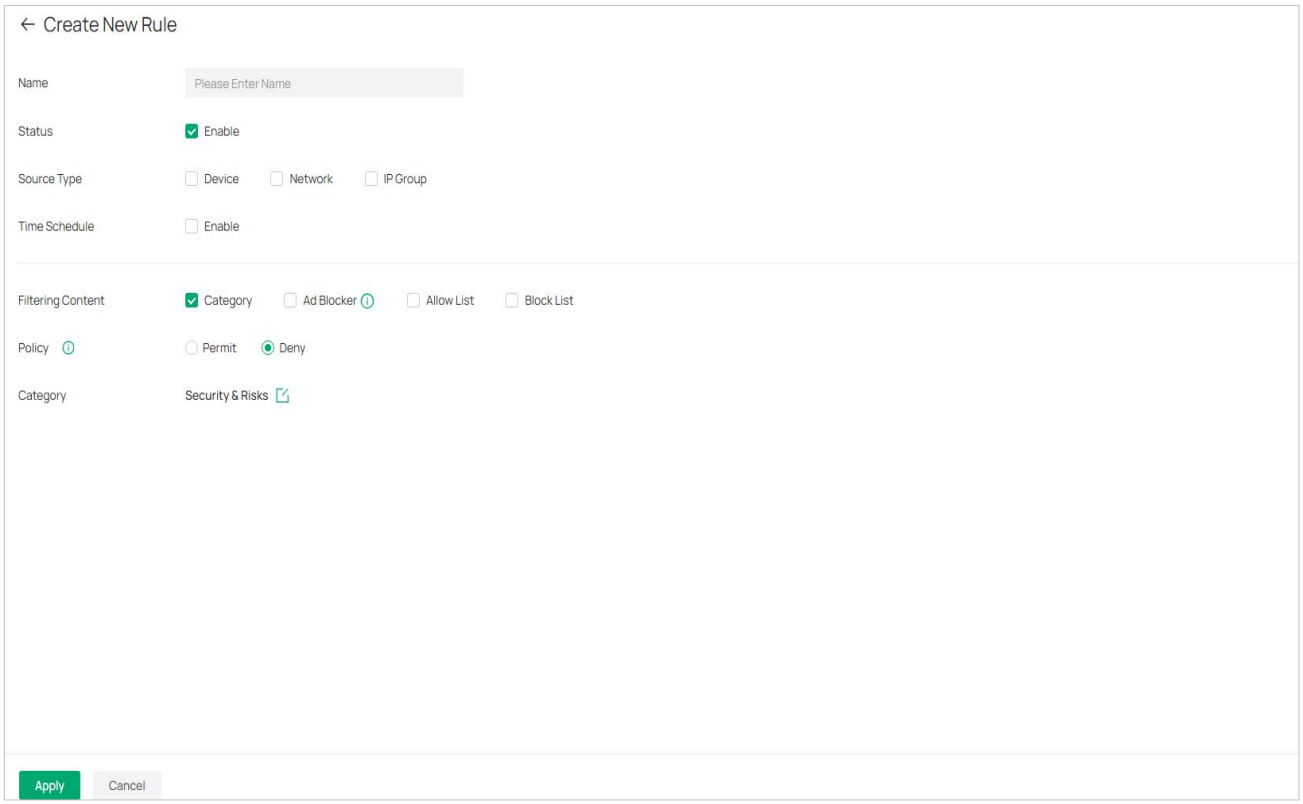
To complete the Content Filtering configuration, follow these steps:

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

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

■ **Configuring Gateway Rules**

1. Go to Network Config > Security > Content Filtering.
2. Click Create New Rule to add a content filtering rule.



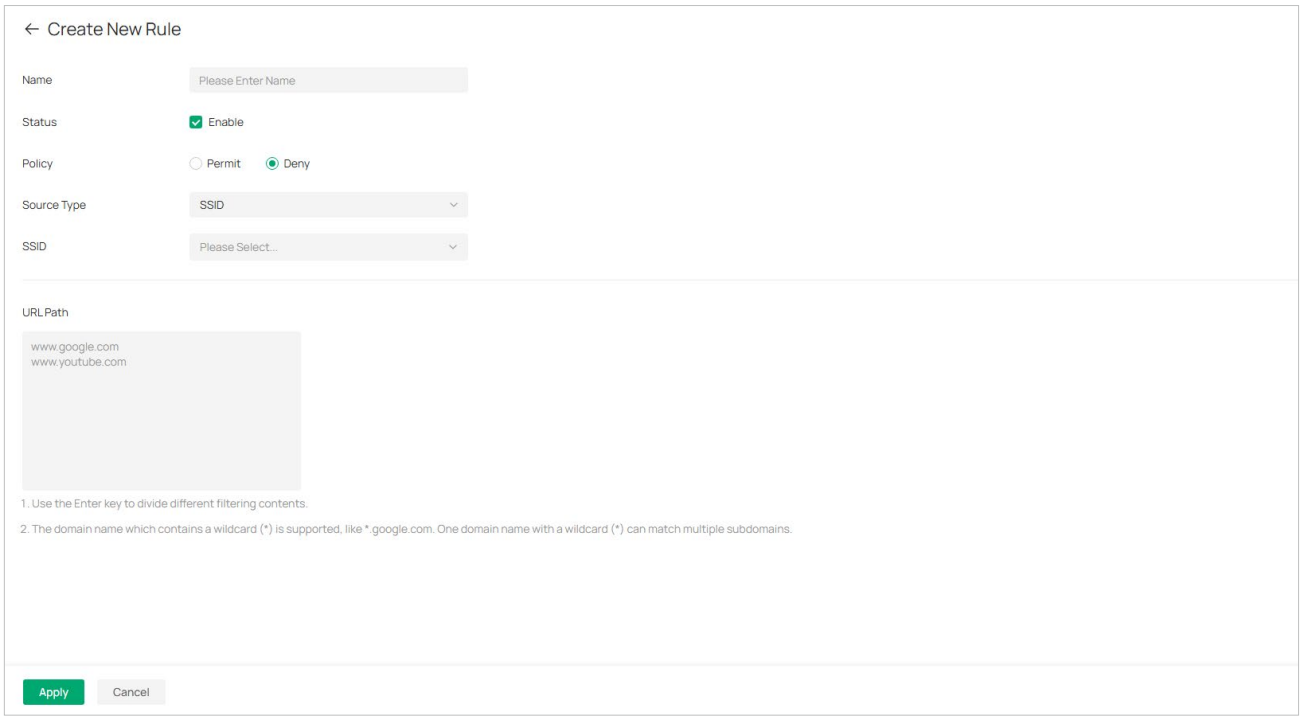
3. In the rule, specify the basic settings, including Name, Status, Source Type, Time Schedule, optional Category , Ad Blocker,and Allow List / Block List entries and click Apply.
4. (Optional) Click General Config to configure global settings, including Block Page, Safe Search and Ad Blocker Auto Update.
5. Back on the rule list page, drag and drop the rows to adjust the rule order as needed.

Name	Enter a name to identify the Content Filtering rule.
Status	Click the checkbox to enable or disable the rule.
Source Type	Select the source of the packets to which this rule applies. You can select one or more source types. Device :With Device selected, choose one or more devices from the list. The rule will apply only to traffic coming from these devices. Network: With Network selected, choose the network you have created from the drop-down list. The gateway filters the packets sourced from the selected network. If no networks have been created, you can select the default network (LAN), or go to Network Config > Network Settings > LAN to create one. IP Group: With IP Group selected, choose the IP Group you have created from the drop-down list. The gateway examines whether the source IP address of the packet belongs to this IP Group. If no IP Groups have been created, click + Create New IP Group on this page or go to Network Config > Profile > Groups to create one.
Time Schedule	Specify when the rule will take effect. You can configure a custom time schedule.

Filtering Content	Select one or more filtering mechanisms for this rule. At least one option must be enabled.
Category	Category defines which types of web content are evaluated by this rule. The selected categories work together with the Policy setting to determine whether matching traffic is allowed or blocked.
Ad Blocker	Enable Ad Blocker to block online ads using a DNS-based database of known advertising and tracking domains. When enabled, the gateway checks DNS requests against this database and blocks domains associated with ads or tracking content.
Allow List and Block List	Use the Allow List and Block List to define custom exceptions in addition to the selected categories and ad blocker database. Smart Match: If a URL contains a key word specified in the list, the rule will be applied to this URL. Exact Match: If a URL exactly matches a URL path specified in the list, the rule will be applied to this URL. You can add entries individually or import them from a file, depending on the Fusion gateway version.
Policy	Select the action to be taken when traffic matches the selected content categories in this rule. Deny: Discard the matched packets and prevent clients from accessing the corresponding URLs or domains. Permit: Forward the matched packets and allow clients to access the corresponding URLs or domains.
Category	Security & Risks (Default): Blocks categories under Security & Risks to provide basic network protection. Custom: Allows you to manually select the content categories to apply in this rule.
Ad Blocker Auto Update	Enable Ad Blocker Auto Update to automatically keep the ad blocker database up to date. The database is updated regularly. The latest update time is shown at the bottom of the Ad Blocker Auto Update as “Ad Blocker Database updated: YYYY-MM-DD HH:MM:SS”.
Block Page	Enable this option to display a block page to users when their request is denied by Content Filtering rules.
Block Page Message (Optional)	Customize the message shown on the block page. This can be used to explain the reason or provide contact information.
Safe Search	Enable Safe Search to enforce the safe search mode of supported search engines. When enabled, the gateway rewrites search requests so that inappropriate search results are filtered out.

Configuring EAP Rules

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



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

Name	Enter a name to identify the Content Filtering rule.
Status	Click the checkbox to enable the Content 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. The EAP will filter the packets sourced from the wireless devices connected to the selected SSID
URL Path	If a URL is the same as any of the entire URL rules specified in the filtering content, the filtering rule will be applied to this URL.

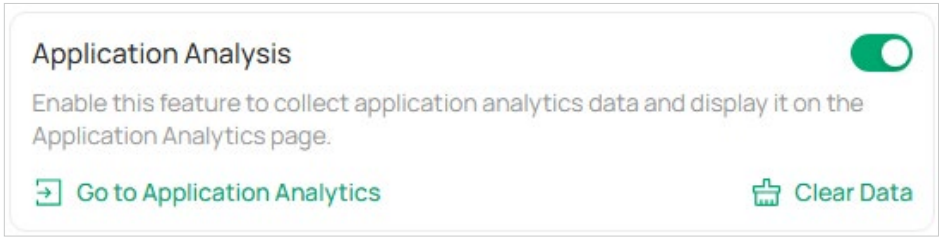
16. 2 Configure Application Control

Overview

Deep Packet Inspection (DPI) enables identification, analysis, and control of application-layer traffic. It uses up-to-date signatures to detect which apps consume the most bandwidth. When enabled, the device collects and saves traffic insights.

Configuration

1. Go to Network Config > Security > Application Control.
2. Toggle to enable Application Analysis, and the application analytics will be collected and saved. The results can be viewed on the Insights > Application Analytics page.



Application Analytics	Toggle to enable DPI analysis statistics.
Clear Data	Click and select a time range to clear DPI data for that period.
Name	Displays the application name.
Category	Displays the application category.

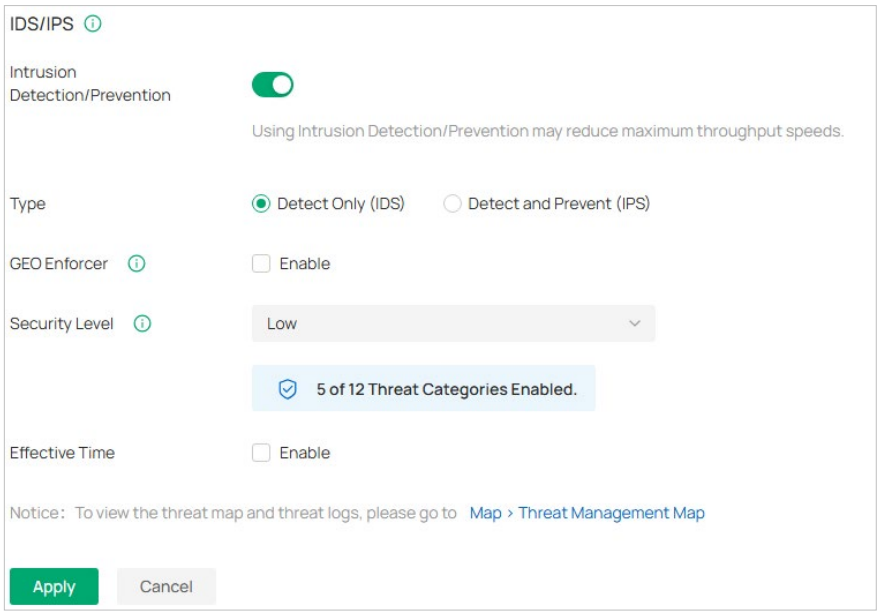
16. 3 Configure IDS/IPS for Threat Management

IDS/IPS is a security mechanism that detects intrusions based on attack characteristics. It can detect buffer overflows, Trojan horses, worms, SQL injections and other attacks to protect the network security of users.

Note: Using Intrusion Detection/Prevention may reduce maximum throughput speeds.

16. 3. 1 Configure IDS/IPS

1. Go to Network Config > Security > IDS/IPS.
2. Enable Intrusion Detection/Prevention and configure the parameters.

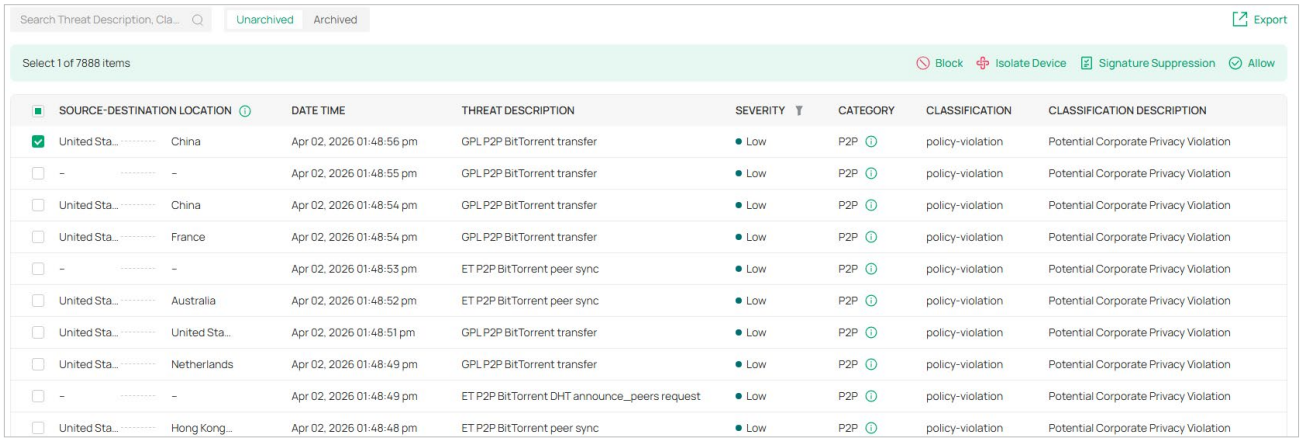


Type	Specify the working mode. In IDS mode, the system will only report the threat log. In IPS mode, the system will block the corresponding connection for 300s after a threat is detected.
GEO Enforcer	Enable geographic location identification of threat logs.
Security Level	Choose the protection level. A higher protection level means more threat types are detected, while a lower protection level only detects some important threats. You can also customize the protection level.
Effective Time	Specify the effective time period of the IDS/IPS module.

Click Apply. When the device discovers a threat, the corresponding threat log will be displayed on the Threat Management page. For a specific threat log, you can choose a specified response strategy.

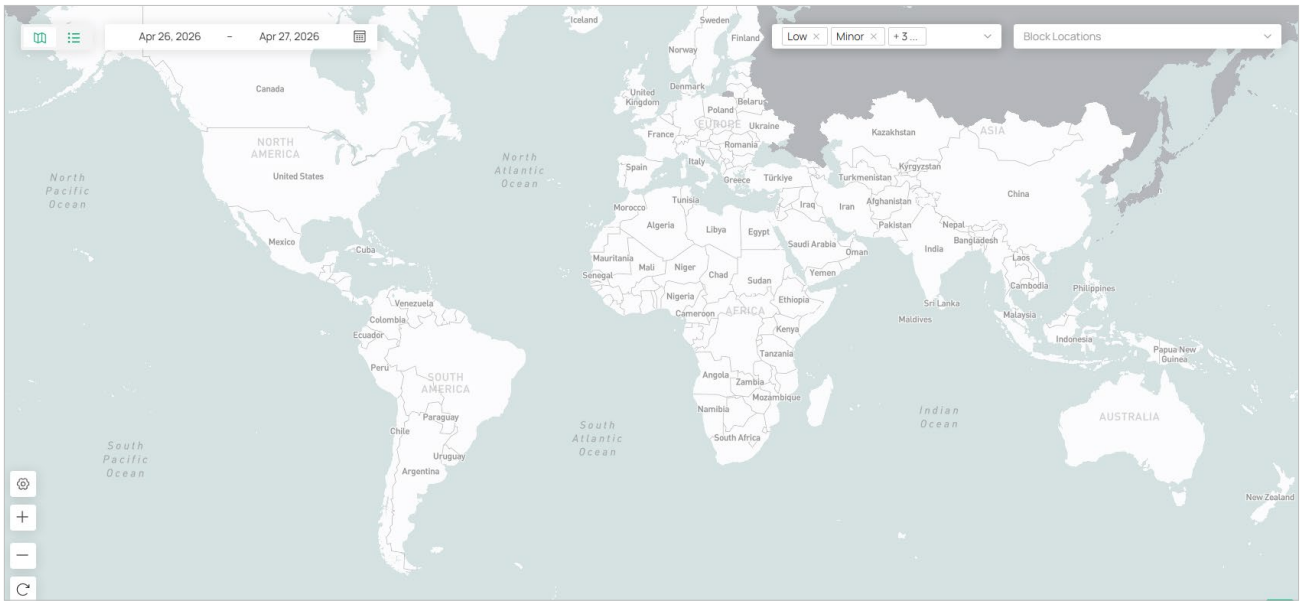
16. 3. 2 Manage Threats

1. Go to Map > Threat Management Map, You can manage threats in a list or map.
2. In the Threat Management List, click a threat that the system discovered, then you can choose a specified response strategy for the corresponding attack IP: Block, Isolate Device, Signature Suppression, or Allow.



Block	Drop traffic to/from the external IP address and the specific internal IP address. If you block an entry, it will be added to the Block List at Network Config > Security > IDS/IPS.
Isolate Device	Drop traffic to/from the external IP address and any internal IP address.
Signature Suppression	Mute the alerting on certain signatures. This will also disable blocking on traffic matching the designated suppression rule. If you suppress the signature of an entry, it will be added to the Signature Suppression list at Network Config > Security > IDS/IPS.
Allow	Trust the IP address so that the traffic, depending on the direction selected, will not get blocked to or from the identified IP address. If you allow an entry, it will be added to the Allow List at Network Config > Security > IDS/IPS.

3. In the Threat Management Map, you can view the threat sources and numbers of attacks that the system has discovered. You can click a number in the map to view attack details. You can right-click a location to block its attack events and manage the Block Locations list. If excessive attacks have been detected, you can choose specific severity levels to display.



4. You can further check and edit processed entries at Network Config > Security > IDS/IPS.

- **Block List**

  The Block List page displays all block entries added through the Threat Management page. You can choose to block all traffic of the source IP in the threat log, or block all traffic between the source IP and the destination IP in the threat log.

- **Allow List**

  On the Allow List page, users can view/edit the exemption entries of IDS/IPS detection, so that the specified objects will no longer trigger threat logs.

  Click Create New Allow List and configure the parameters.

Direction	Specify the location of the object (target) exempt from triggering the threat: source, destination, or both directions.
Track By	Specify the type of object (target) exempt from triggering the threat: IP address, Network, or Subnet.
IP Address/Network/ Subnet	Specify the value of the object.

- **Signature Suppression**

  The Signature Suppression page displays all the signature suppression entries added through the Threat Management page, and the objects with signature suppressed will no longer trigger specific threat logs.

Category	Specify the classification of the attack characteristics to exempt.
Signature	Specify the attack signature to exempt.
Type	Specify the type of traffic that suppresses the signature: based on all traffic or data packets.
Direction	Specify the location of the signature suppression object: source, destination, or both directions.
Track By	Specify the type of object (target) exempt from triggering the threat: IP address or Subnet.
IP Address/Network/ Subnet	Specify the value of the object.

16. 4 Configure Secure DNS

Overview

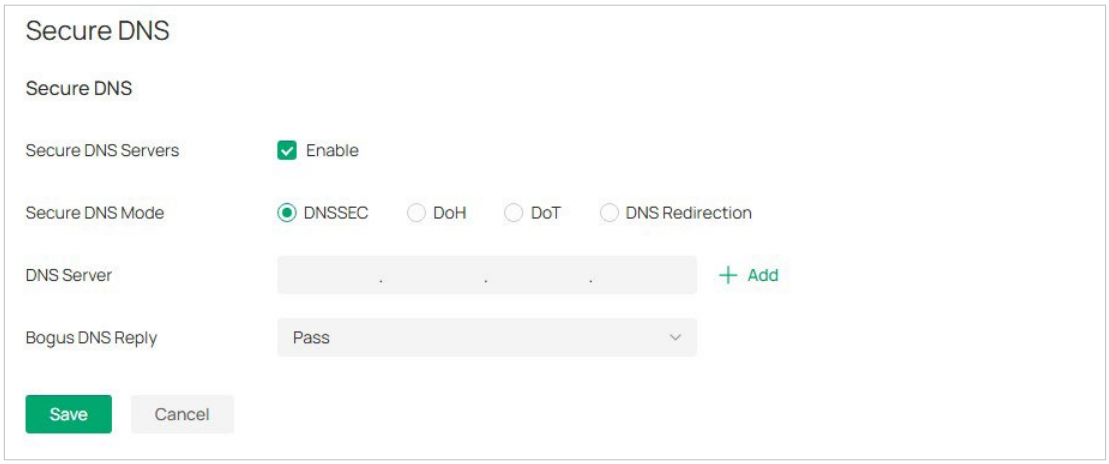
Secure DNS provides the LAN side clients with the DNS query service. It forwards the DNS request from the LAN side clients to the selected upstream DNS server and forwards the DNS reply accordingly.

DNSSEC (DNS Security Extensions), DoT (DNS over TLS), DoH (DNS over Https) and DNS Redirection are four security options for Secure DNS. DNSSEC will verify the integrity of DNS records, and DoT / DoH will encrypt the query. When DNS Redirection enabled, DNS requests from the selected LAN network will be intercepted and forwarded to a specific DNS server, even if the DNS server set on the client device is not the router's LAN IP.

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

Configuration

1. Go to Network Config > Security > Secure DNS.
2. Enable this feature, configure the parameters, and click Save.



Secure DNS Mode	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). Primary DNS Server:Specify the primary upstream DNS server. Secondary DNS Server:Specify the secondary upstream DNS server.
Apply Network	Specify the effective LAN network to apply DNS Redirection.

16. 5 Configure the Firewall

Overview

Firewall is used to enhance the network security.

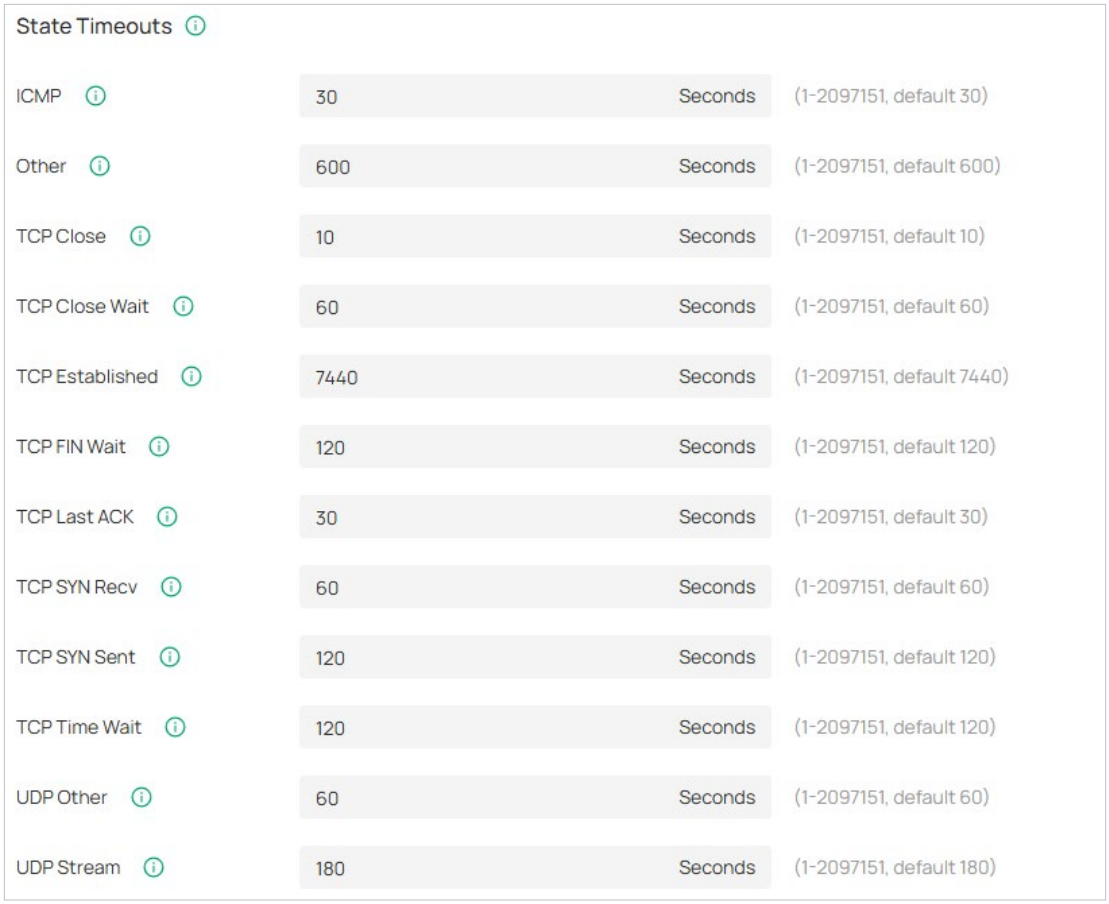
In State Timeouts, you can specify a number of timeouts for sessions including TCP, UDP, and ICMP connection. The packets will be forwarded within the specified timeout. When there is no response after the specified time, the session or status will be closed. State timeout will help close inactive sessions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

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

16. 5. 1 Configuring Stateful Firewall

Configuring State Timeouts

1. Go to Network Config > Security > Firewall > Stateful Firewall.
2. In the Sate Timeouts, set the time limit for the different sessions. Click Save.

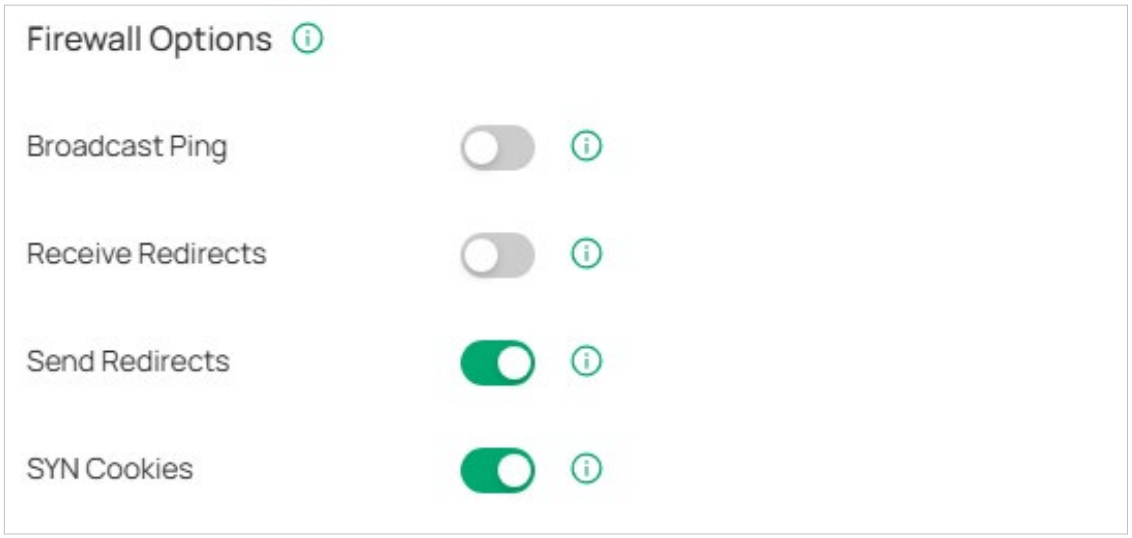


ICMP	The ICMP session will be closed if there is no response after the set time.

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

1. Go to Network Config > Security > Firewall > Stateful Firewall.
2. In the Firewall Options, enable the firewall options based on needs. Click Save.



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.

16. 5. 2 Configure 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.

Fusion gateway provides two kinds of attack defense: flood defense and packet anomaly defense.

- **Flood Defense**

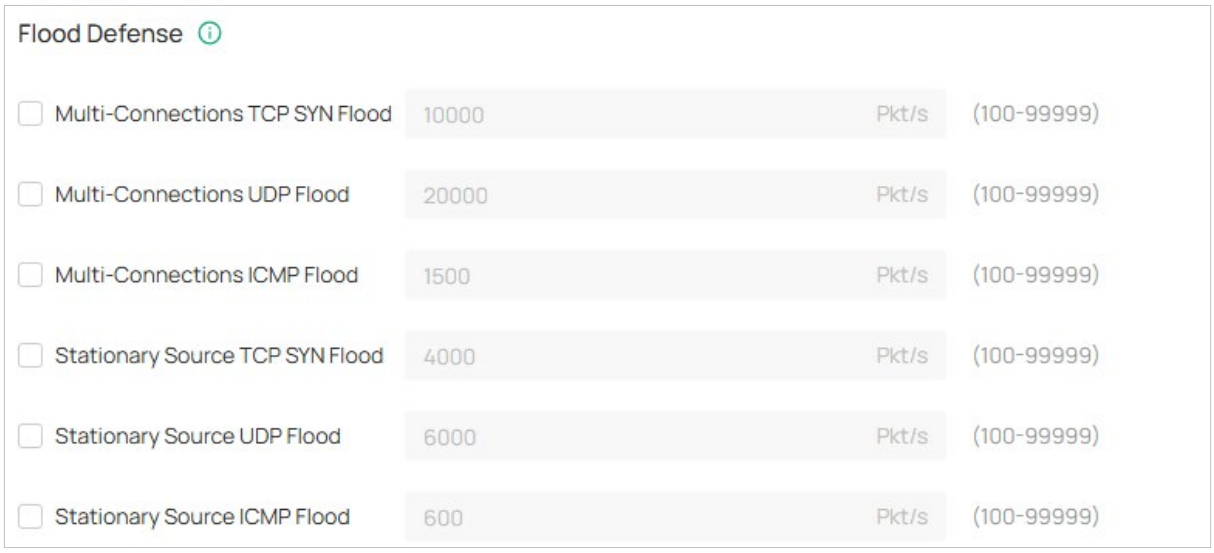
Flood defense detects flood attacks including TCP SYN flood attacks, UDP flood attacks, and ICMP flood attacks in real time, and limits the receiving rate of the packets to protect the device. The flood attacks occur when a large number of fake packets are sent to a target device, and the target device is busy with these fake packets and cannot process normal services.

- **Packet Anomaly Defense**

Packet anomaly defense discards the anomalous packets directly. Anomalous packets are packets that do not conform to standards or contain errors that make them unsuitable for processing.

Configuring Flood Defense

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

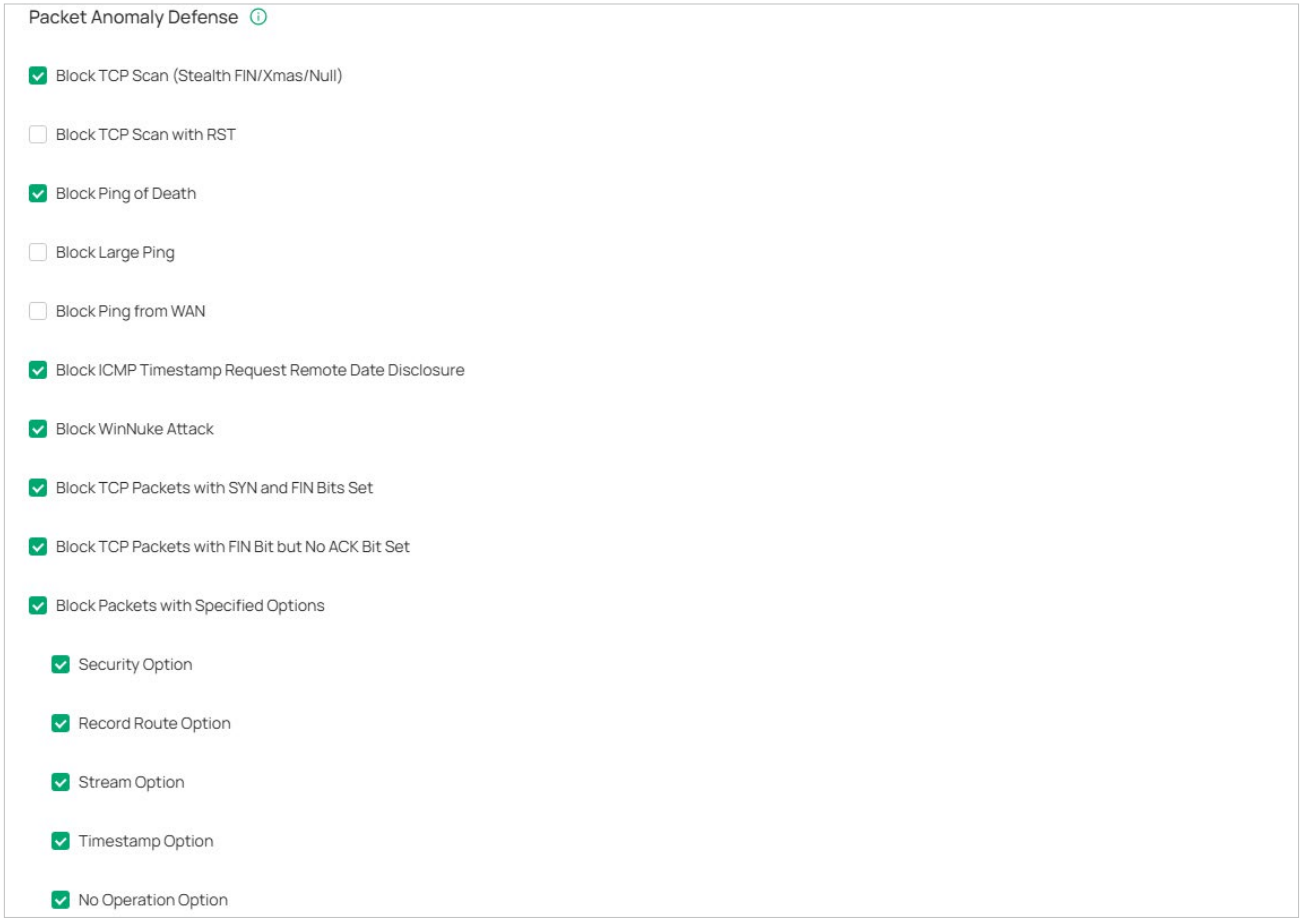


Multi-Connections TCP SYN Flood	With this feature enabled, the gateway limits the rate of receiving TCP SYN packets from all the clients to the specified rate. A TCP SYN flood attack occurs when the attacker sends the target system with a succession of SYN (synchronize) requests. When the system responds, 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.
Multi-Connections UDP Flood	With this feature enabled, the gateway limits the rate of receiving UDP packets from all the clients to the specified rate. 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.
Multi-Connections ICMP Flood	With this feature enabled, the gateway limits the rate of receiving ICMP packets from all the clients to the specified rate. An ICMP flood occurs when an attacker sends many ICMP Echo messages to the target device, and the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected.
Stationary Source TCP SYN Flood	With this feature enabled, the gateway limits the rate of receiving TCP SYN packets from a single client to the specified rate 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.
Stationary Source UDP Flood	With this feature enabled, the gateway limits the rate of receiving UDP packets from a single client to the specified rate. 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.

Stationary Source ICMP Flood	With this feature enabled, the gateway limits the rate of receiving ICMP packets from a single client to the specified rate. An ICMP flood occurs when an attacker sends many ICMP Echo messages to the target device, and the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected.

Configuring Packet Anomaly Defense

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



Block TCP Scan (Stealth FIN/Xmas/Null)	With this option enabled, the router will filter the TCP scan packets of Stealth FIN, Xmas and Null: Stealth FIN Scan: The attacker sends the illegal packet with its FIN field set to 1. The FIN field is used to request disconnection. 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 the option enabled, the router will automatically reply a RST packet when it receives TCP SYN packets; with the option disabled, the router will automatically drop the packets and not respond.
Block Ping of Death	With this option enabled, the router will block Ping of Death attack. Ping of Death attack means that the attacker sends abnormal ping packets 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 the customized value or 4028 bytes (default value) to protect the system from Large Ping attack.
Block Ping from WAN	With this option enabled, the gateway will block the ICMP request from WAN.
Block ICMP Timestamp Request Remote Date Disclosure	With this option enabled, the device will block all ICMP Timestamp (Type 13) packets.
Block WinNuke Attack	With this option enabled, the router will block WinNuke attacks. WinNuke attack refers to a remote denial-of-service attack(DoS) that affects some Windows operating system, such as the Windows 95 and Windows NT. 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, you can choose the following options based on needs: Security Option, Loose Source Route Option, Strict Source Route Option, Record Route Option, Stream Option, Timestamp Option, and No Operation Option.

16. 6 Configure IMPB

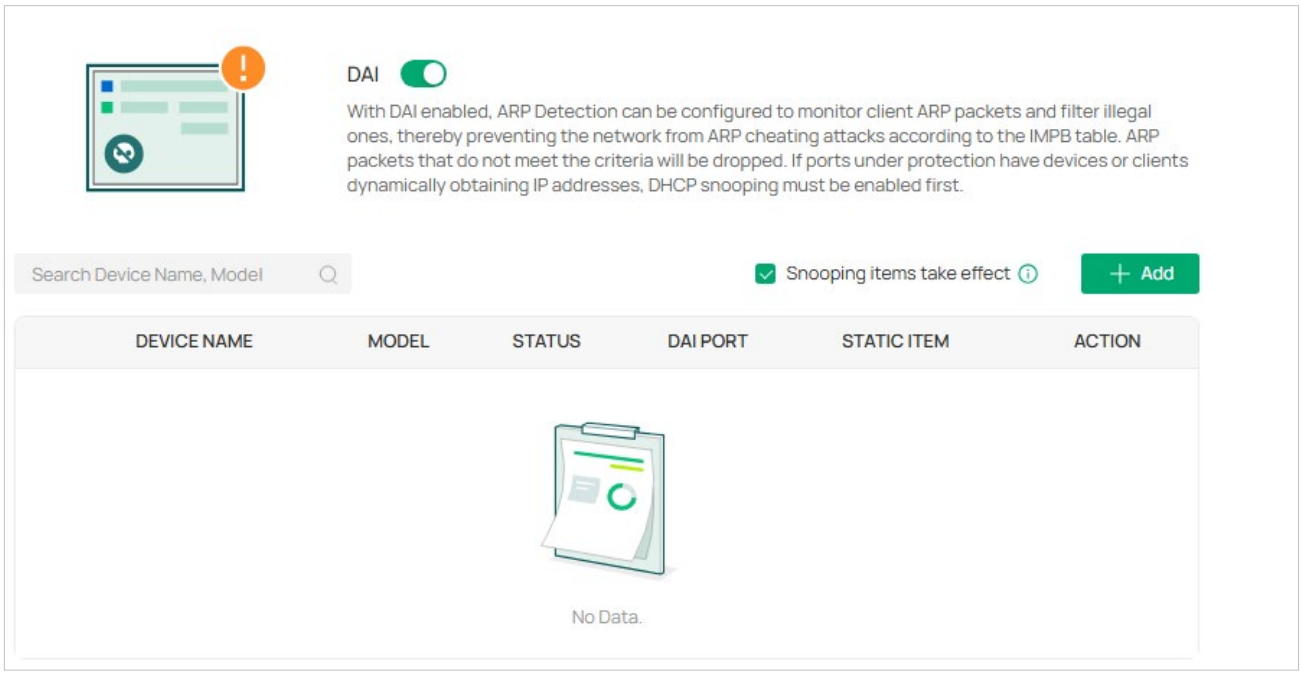
Overview

With DAI (Dynamic ARP Inspection) enabled, ARP Detection can be configured to monitor client ARP packets and filter illegal ones, thereby preventing the network from ARP cheating attacks according to the IMPB table. ARP packets that do not meet the criteria will be dropped. If ports under protection have devices or clients dynamically obtaining IP addresses, DHCP snooping must be enabled first.

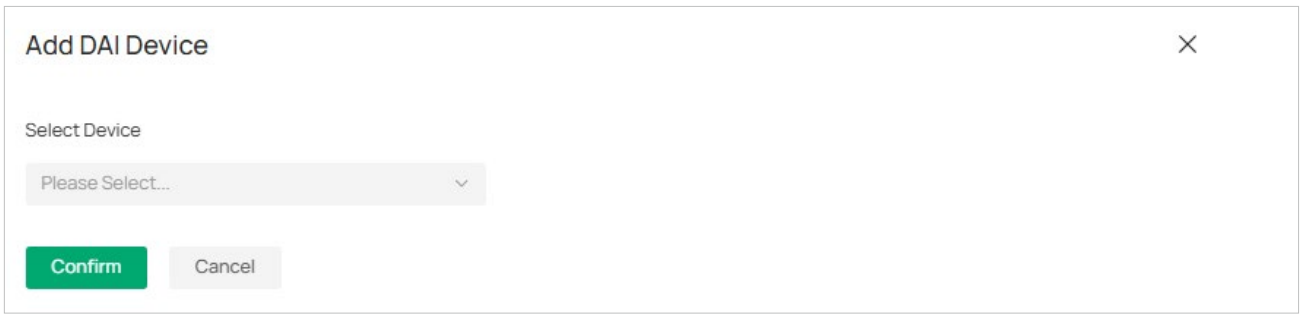
With DHCP snooping enabled, the switch can monitor the IP address obtaining process of the DHCP client, and record the IP address, MAC address, VLAN ID and the connected port number of the DHCP client for DAI.

Configuring DAI

1. Go to Network Config > Security > IMPB > DAI.
2. Enable DAI. Click Add to add devices that need to enable the DAI functionality.



3. Select the desired device from the drop-down list.

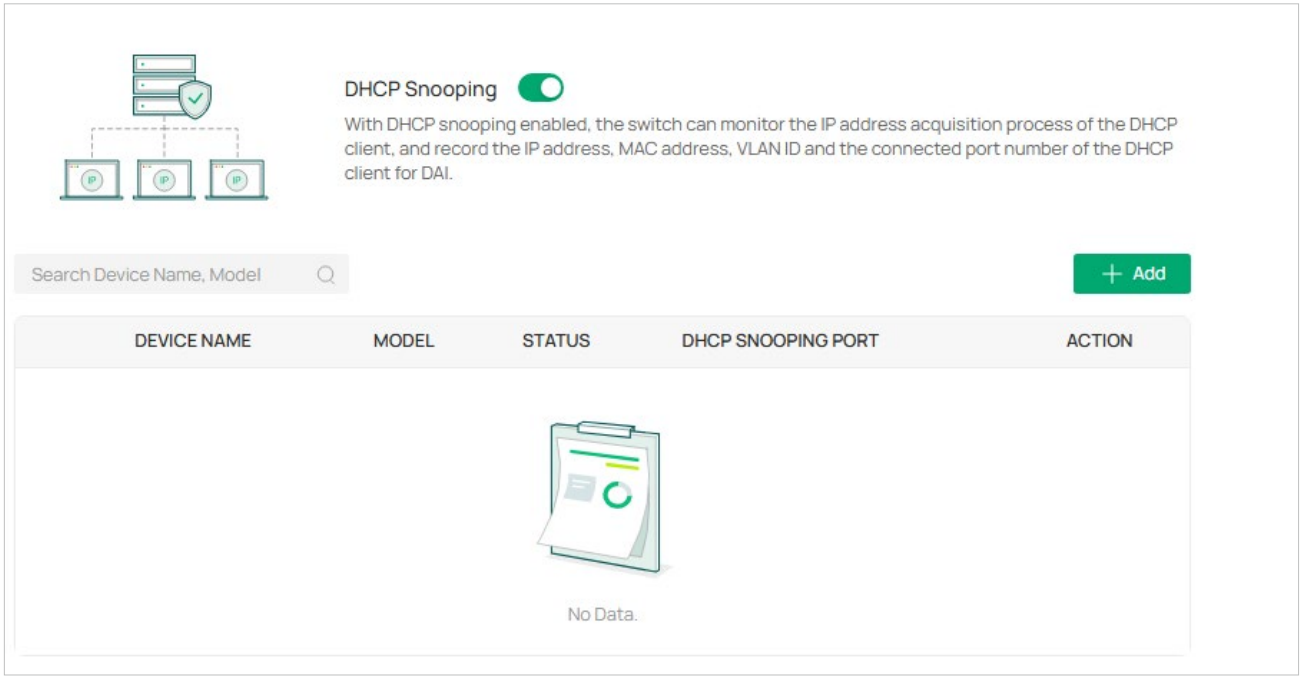


4. Set the ports on the selected device that require DAI enabled. If you have already enabled DHCP snooping, you can click to choose all ports with DHCP snooping enabled. Click Confirm

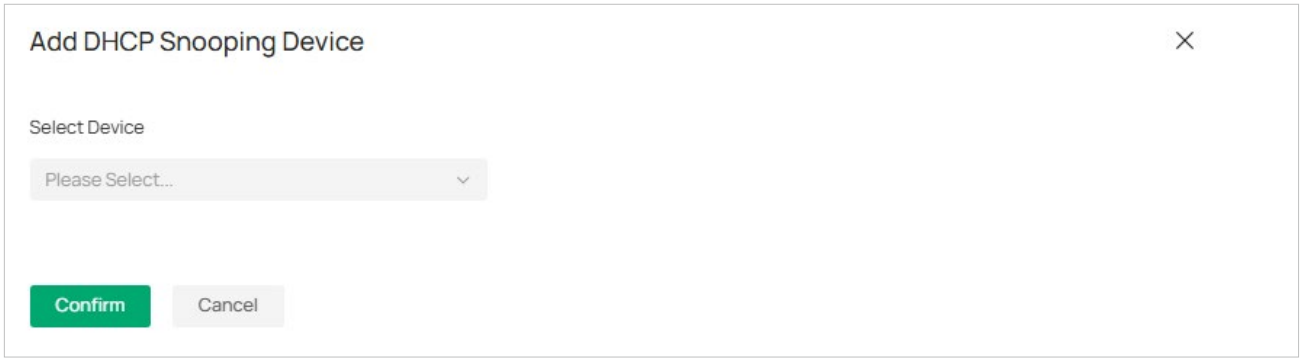
5. Click the Edit icon to modify the protection ports. If a static IP client is connected to a port with protection enabled, you must add its Port, IP Address, MAC Address, Client Name, and VLAN ID to the static entries; otherwise, this client will be unable to access the network normally. This supports manual addition and batch import.
6. Click Add Item to add entries one by one by manually entering entry details.
7. Click Import to import multiple entries via a spreadsheet template.
8. If you need to apply DAI to dynamic entries monitored by DHCP snooping, check the Snooping items take effect.

Configuring DHCP Snooping

1. Go to Network Config > Security > IMPB > DHCP Snooping.
2. Enable DHCP Snooping. Click Add to add devices that need to enable the DHCP snooping functionality.



3. Select the desired device from the dropdown list.



4. Set the ports on the selected device that need to enable snooping. Click Confirm

Chapter 17

Configure Traffic Management Settings

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

This chapter guides you on how to configure network traffic management settings with the Fusion gateway. The chapter includes the following sections:

17. 1 Configure 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.

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 Fusion gateway, 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 Fusion gateway, 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 Fusion gateway, they can be applied to the APs 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

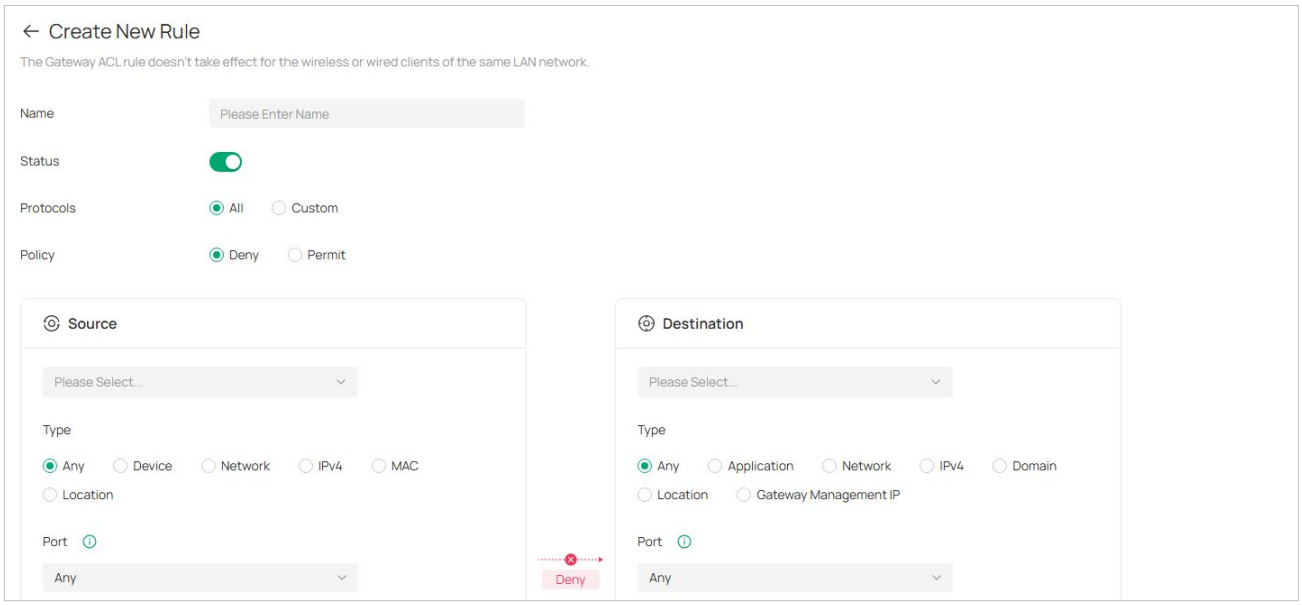
To complete the ACL configuration, follow these steps:

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. Go to Network Config > Traffic Management > ACL. On Gateway ACL tab, click Create New Rule to load the following page.



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

Name	Enter a name to identify the ACL.
Status	Toggle on to enable the ACL.
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.You can click +Custom to customize protocols. When you select TCP/UDP,All, you can set the port number of a packet as packet-filtering criteria in the rule. When you select ICMP/ICMPv6, you can set the ICMP Type and ICMP Code of a packet as packet-filtering criteria in the rule. ICMP Type: Match the traffic with the specific ICMP Type. 255 means all types are included. ICMP packets with both the type and code fields matched are considered as the target packets. ICMP Code: Match the traffic with the specific ICMP Code. 255 means all codes are included. ICMP packets with both the type and code fields matched are considered as the target packets.
Policy	Select the action to be taken when a packet matches the rule. Permit: Forward the matched packet. Deny: Discard the matched packet.
Direction	Specify the source/destination interface for the rule. You can select LAN, WAN and VPN. LAN: Match the traffic from/to LAN. WAN: Match the traffic from/to the specific WAN. VPN: Match the traffic from/to the specific VPN.

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

Source/Destination Type	Select the source/destination type of the created rule. Any: Match all traffic. Device: Match the traffic from the specific Device. Application: Match the traffic to the specific App/App Category. Network: Match the traffic from/to the specific network. If no networks have been created, you can select the default network (LAN), or go to Network Config > Network Settings > LAN to create one. IP: Match the traffic from/to the specific IP/IP Group. If no IP Groups have been created, click + Add IP Group on this page or go to Network Config > Profile > Groups to create one. MAC: Match the traffic from the specific MAC/OUI/MAC Group. If no MAC Groups have been created, click + Add MAC Group on this page or go to Network Config > Profile > Groups to create one. Domain: Match the traffic from the specific Domain/Domain Group. If no Domain Groups have been created, click + Add Domain Group on this page or go to Network Config > Profile > Groups to create one. Location: Match the traffic from/to Location/Location Group. If no Location Groups have been created, click + Add Location Group on this page or go to Network Config > Profile > Groups to create one. Gateway Management IP: Match the traffic to Gateway Management IP.
Source/Destination Port:	Match the traffic from/to the source/destination port. Select a TCP or UDP port, or choose Any. Only TCP or UDP traffic will be matched. Traffic using other protocols will be excluded. If Match Opposite Port is selected, the rule applies to TCP and UDP traffic outside the specified ports, as well as all other protocols. Traffic on the selected TCP or UDP ports will not be matched.

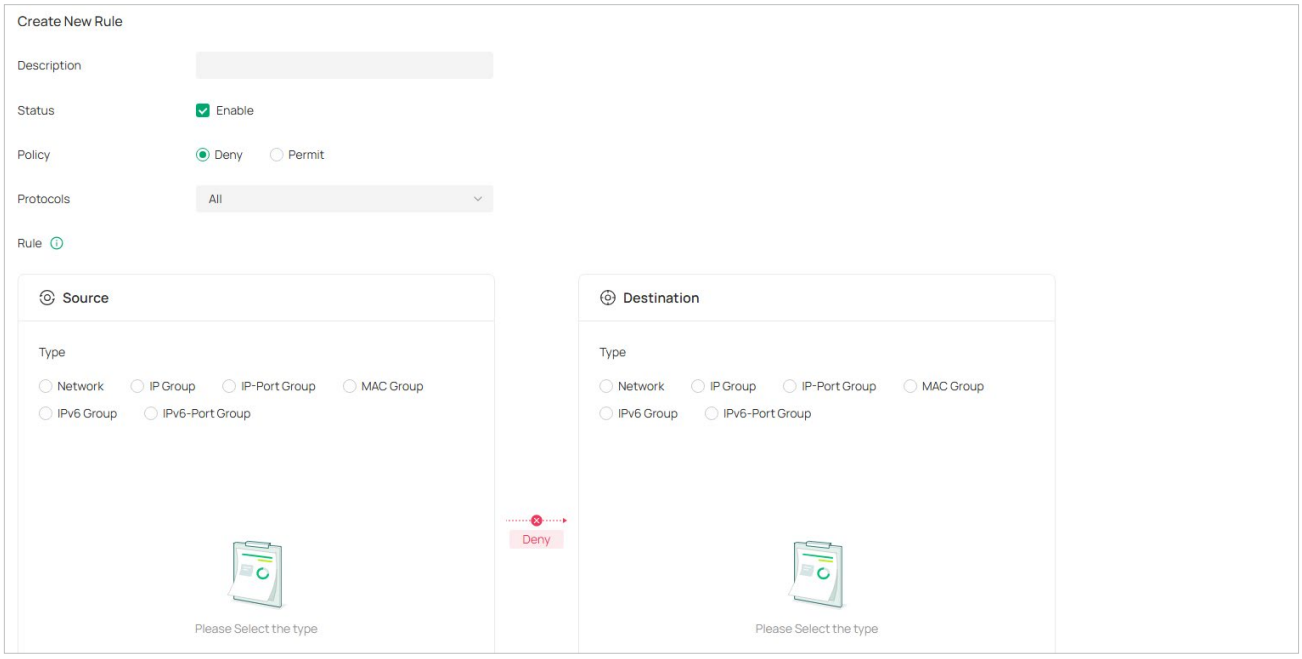
Set the advanced settings according to your needs:

IP Version	Specify the IP version to apply the rule: IPv4 or IPv6.
Log	When enabled, the system can collect ACL entry effective log. To use this function, please configure the remote logging function first.
Time Range	Create the time range or select an existing time range for the acl rule to take effect.
Bi-Directional	In the LAN-LAN direction, click the checkbox to enable the gateway 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.

States Type	Determine the type of stateful ACL rule. It is recommended to use the default Auto type. Auto: 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 gateway 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. Match State Invalid: Match the connections that do not behave as expected.

■ Configuring Switch ACL

1. Go to Network Config > Traffic Management > ACL. Under the Switch ACL tab, click Create New Rule to load the following page.



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

Description	Enter a description 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. With one of TCP, UDP or both are selected, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.
Rule	Source/Destination: Select the source/destination criteria from the drop-down list to compare against a packet. Network: Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Network Config > Network Settings > LAN to create one. IP Group: Select the IP Group you have created. If no IP Groups have been created, click + Create on this page or go to Network Config > Profile > Groups to create one. The system 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 Network Config > Profile > Groups to create one. The system 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, go to Network Config > Profile > Groups to create one. The system 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 Network Config > Profile > Groups to create one. The system will examine whether the destination IPv6 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 Network Config > Profile > Groups to create one. The system will examine whether the destination IPv6 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 Create. Note that a switch ACL takes effect only after it is bound to a port or VLAN.

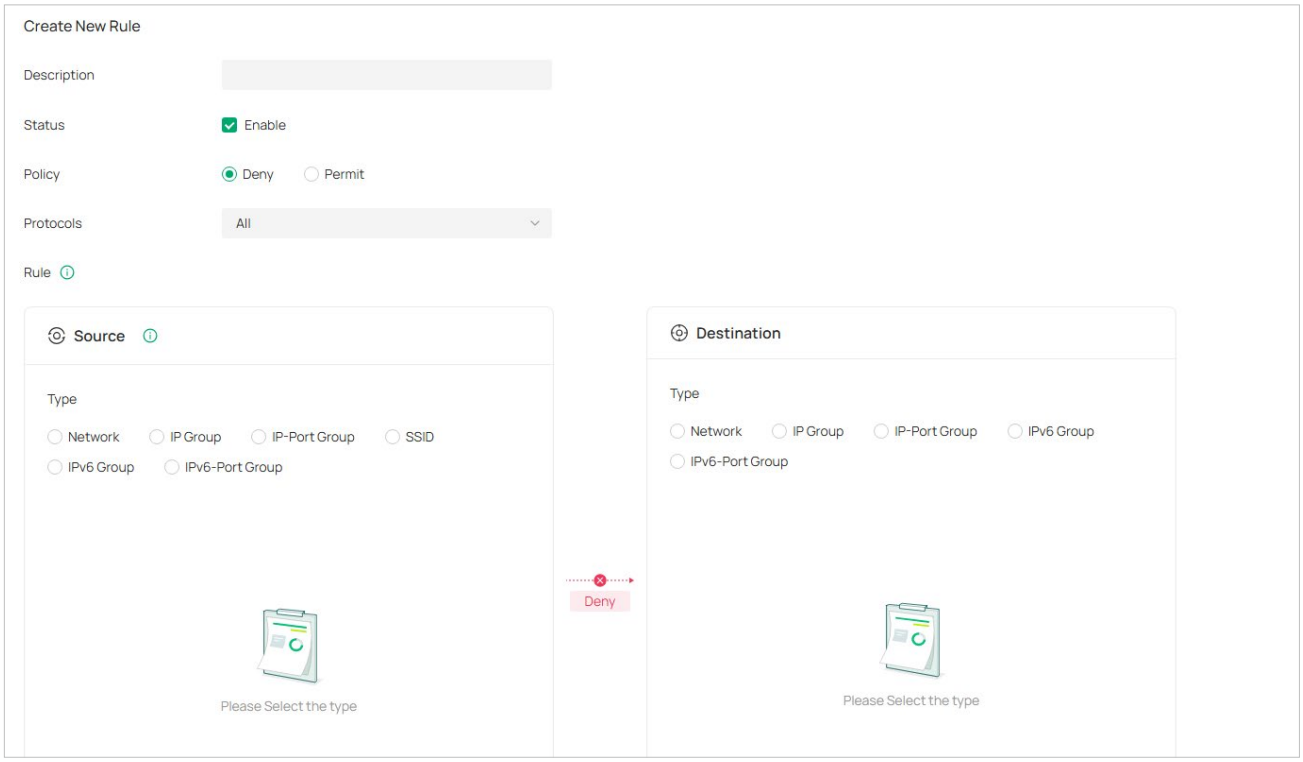
Binding Type	Specify whether to bind the ACL to ports or a VLAN. Select a VLAN from the drop-down list as the interface to be bound with the ACL. If no VLANs have been created, you can select the default VLAN ,or go to Network Config > Network Settings > LAN to create one.
Ports	Select All Ports or Custom 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.
VRF	Select the VRF where the ACL takes effect.
Switches	Select or as the interfaces to be bound with the ACL. With selected, the rule is applied to all switches. With selected, the rule is applied to the selected switches. Click the switches from the to select the binding switches.

Set the advanced settings according to your needs:

Time Range	Create the 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.

■ Configuring EAP ACL

1. Go to Network Config > Traffic Management > ACL. Under the EAP ACL tab, click Create New Rule to load the following page.



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

Description	Enter a description 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. With one of TCP, UDP or both are selected, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.
Rule	Source/Destination: Select the source/destination criteria from the drop-down list to compare against a packet. Network: Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Network Config > Network Settings > LAN to create one. IP Group: Select the IP Group you have created. If no IP Groups have been created, click + Create on this page or go to Network Config > Profile > Groups to create one. The system 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 Network Config > Profile > Groups to create one. The system 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 Network Config > Network Settings > WLAN to create one.The system 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 Network Config > Profile > Groups to create one. The system will examine whether the destination IPv6 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 Network Config > Profile > Groups to create one. The system will examine whether the destination IPv6 address and port number of the packet are in the IPv6-Port Group.

17. 2 Configure Routing Settings

Overview

- **Static Route**

  Static route designates the next hop or interface to which the network traffic is forwarded. In most cases, static routes are applied when dynamic routing is unavailable or when dynamically learned routes are not preferred.

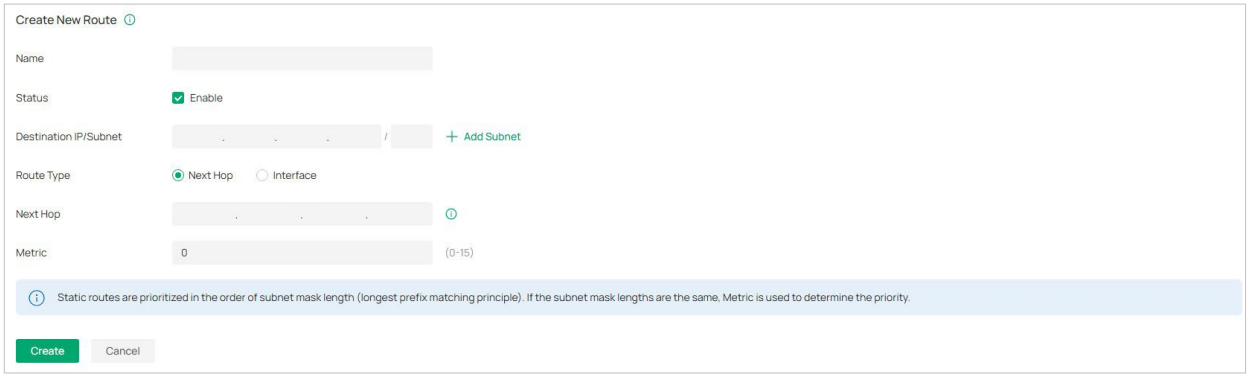
- **Policy Routing**

  Policy routing allows users to customize rules for the gateway to forward the packets. Once policy routing is configured and enabled, the gateway will check the source, destination, and the protocol of the network traffic first. When the traffic matches the user-defined policies, it will be forwarded according to the specific polices. In this way, policy routing provides great flexibility for networking.

Configuration

- **Static Route**

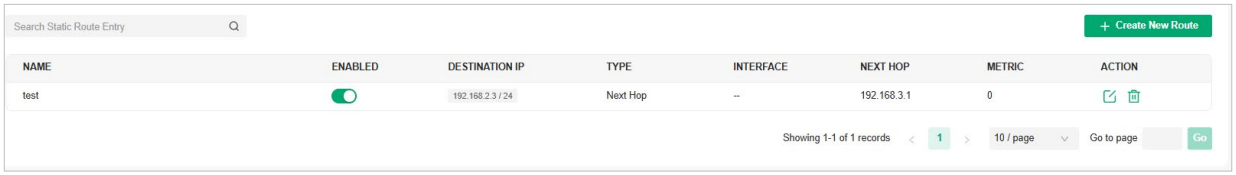
  1. Go to Network Config > Traffic Management > Routing > Static Route.
  2. Click Create New Route to load the following page and configure the parameters.



Name	Enter a name to identify the static route entry.
Status	Click the checkbox to enable the static route entry.
Destination IP/Subnet	Specify the destination IP or subnet of the network traffic. The traffic will be forwarded to the specified destination

Route Type	Select the route type of the created entry. 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 network interface. You need to specify the network interface based on needs.
Metric	Specify a Metric value. Static routes are prioritized in the order of subnet mask length (longest prefix matching principle). If the subnet mask lengths are the same, Metric is used to determine the priority.

3. Click Create. The new Static Route entry is added to the table. You can click the Edit icon to edit the entry. You can click the Delete icon to delete the entry.

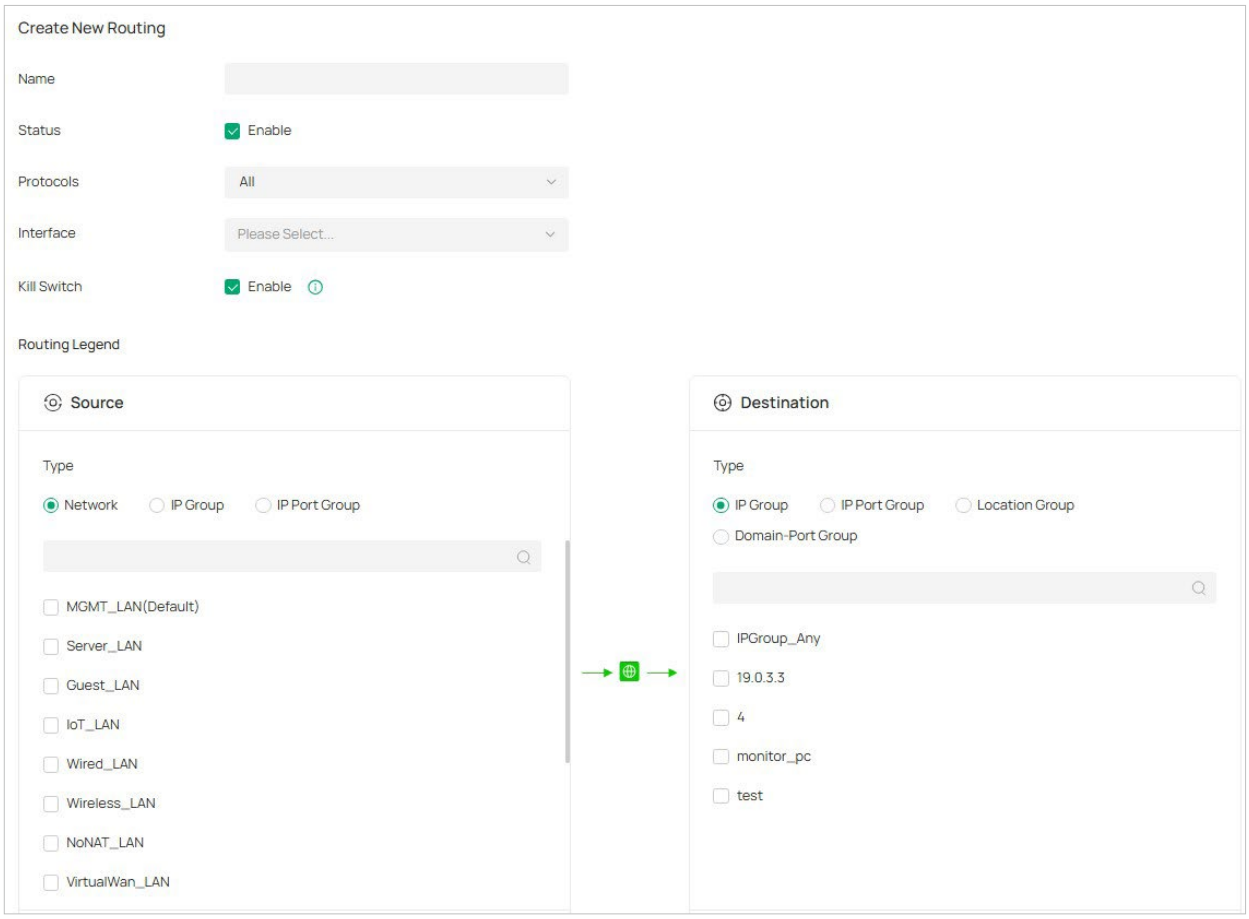


Note:

- Static route take effects with a higher priority over policy routing.
- Static routes are prioritized in the order of subnet mask length (longest prefix matching principle). If the subnet mask lengths are the same, Metric is used to determine the priority.

■ Policy Routing

1. Go to Network Config > Traffic Management > Routing > Policy Routing.
2. Click Create New Routing to load the following page and configure the parameters.



Name	Enter a name to identify the policy routing entry.
Status	Click the checkbox to enable the policy routing entry.
Protocols	Select the protocols, and the policy routing entry will apply to the traffic when it conforms to the selected protocols. The policy routing entry takes effect only when the traffic matches the criteria of the entry including the protocols.
Interface	Select the WAN port, and the traffic will be forwarded through the selected port. Select multiple WAN ports for load balancing as needed. The available VPN client options are PPTP and L2TP.
Kill Switch	When enabled, if the WAN port goes down, all traffic received on this WAN port will not be forwarded.

Routing Legend	Specify the source and destination of the traffic which the policy routing entry applies to. The policy routing entry takes effect only when the traffic matches the criteria of the entry including the source and destination. Network: Select the network interfaces for the traffic source. IP Group: Select the IP Group for the traffic source or destination. You can create a new IP Group in this page, or go to Network Config > Profile > Groups to create one. IP Port Group: Select the IP Port Group for the traffic source or destination. You can create a new IP Port Group in this page, or go to Network Config > Profile > Groups to create one. Location Group: Select the Location Group for the traffic destination. You can create a new Location Group in this page, or go to Network Config > Profile > Groups to create one. Domain-Port Group: Select the Domain-Port Group for the traffic destination. You can create a new Domain-Port Group in this page, or go to Network Config > Profile > Groups to create one.

3. Click Create. The new Policy Routing entry is added to the table. You can click the Edit icon to edit the entry. You can click the Delete to delete the entry.

Note:

Static route take effects with a higher priority over policy routing.

17. 3 Configure Gateway QoS

Overview

Gateway QoS prioritizes important application traffic when the network becomes congested.

QoS rules take effect after the bandwidth thresholds configured in Bandwidth Control are reached.

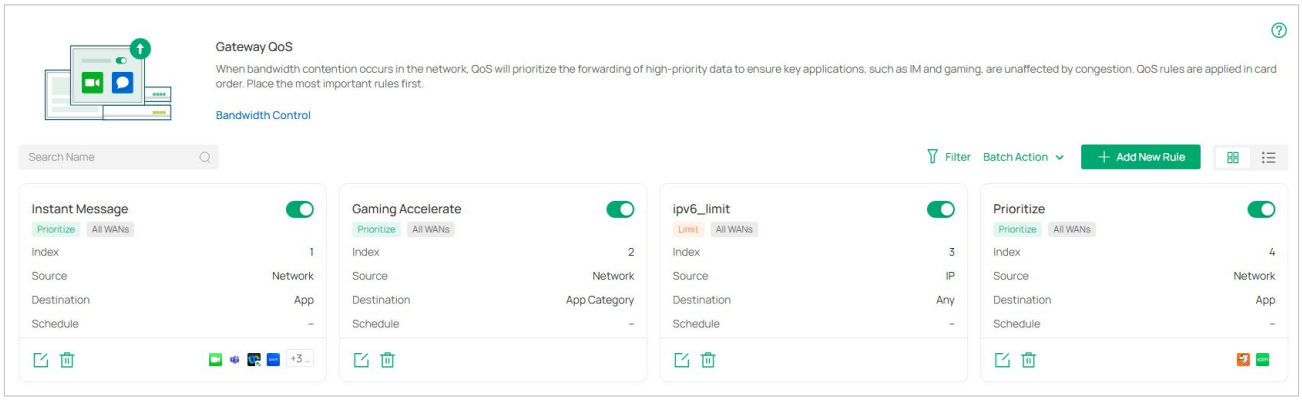
If bandwidth is sufficient, QoS effects may be less noticeable.

For accurate QoS behavior, configure Upstream and Downstream bandwidth in Bandwidth Control based on your actual WAN speed.

Configuration

- **Configure Gateway QoS (Rule List / Card)**

1. Go to Network Config > Traffic Management > Gateway QoS.
2. Toggle the rule switch on/off to enable or disable the rule.

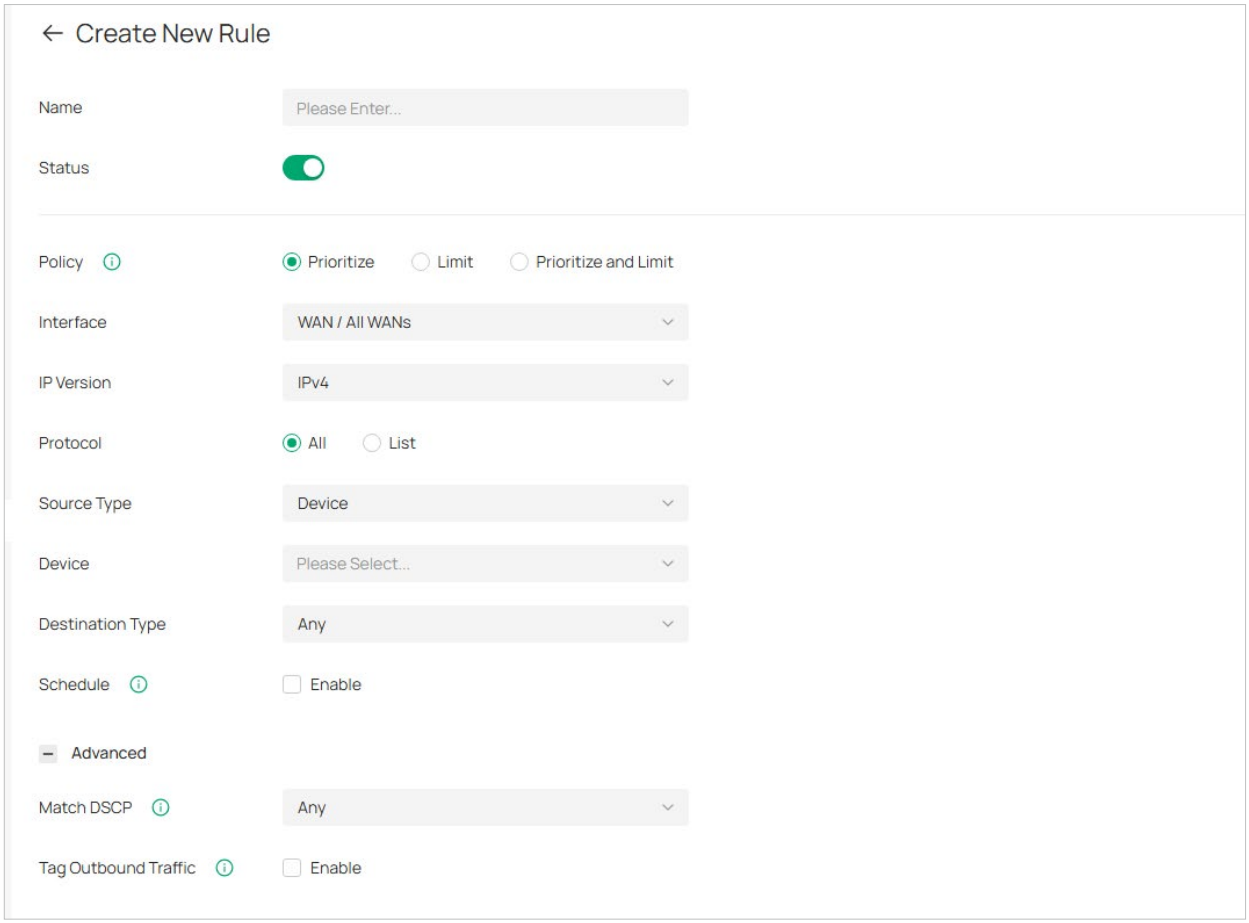


Rule Name	Displays the rule name.
Status	Toggle to enable/disable the rule.
Policy	Displays the traffic handling policy (Prioritize/Limit/Prioritize and Limit).
Interface	Displays the WAN interface range to which the rule applies (e.g., All WANs).
Source	Displays the traffic source match condition.
Destination	Displays the traffic destination match condition.
Schedule	Displays the time range when the rule takes effect.

Note:

When bandwidth contention occurs in the network, QoS will prioritize the forwarding of high-priority data to ensure key applications, such as IM and gaming, are unaffected by congestion. QoS rules are applied in card order. Place the most important rules first.

3. You can click + Add New Rule, configure the rule parameters, then click Apply.



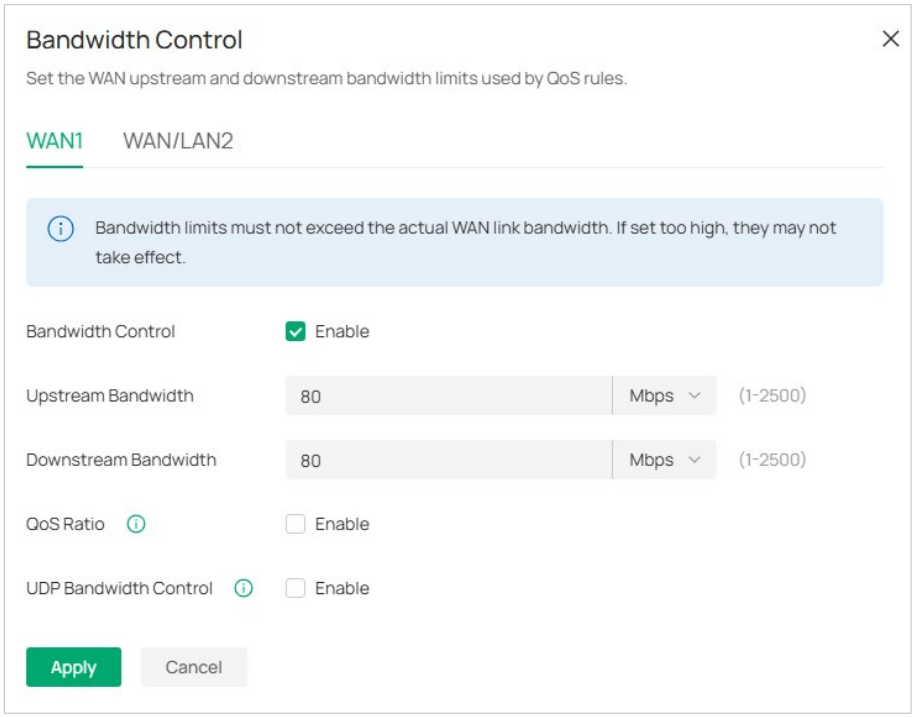
4. Click the Edit or Delete button to edit or delete the rule. Click Filter and select conditions (Policy/Source/Destination) to quickly locate rules. You can also click Batch Action on the upper right to Batch Disable / Batch Enable / Batch Delete rules.

Name	Enter a name for the rule.
Status	Toggle to enable/disable the rule.
Policy	Prioritize: Prioritize the matched traffic. Limit: Limit the matched traffic to a specified upload/download bandwidth. Prioritize and Limit: Prioritize matched traffic and enforce upload/download bandwidth limits.
Interface	Select the interface range (e.g., All WANs).

Upload Bandwidth Limit (Enable)	Enable the upload bandwidth limit and set the value/unit.
Upload Bandwidth Speedburst	Set the burst mode for uploads (Off / Short / Long).
Download Bandwidth Limit (Enable)	Enable the download bandwidth limit and set the value/unit.
Download Bandwidth Speedburst	Set the burst mode for downloads (Off / Short / Long).
IP Version	Select the IP version: IPv4 or IPv6.
Protocol	Select the traffic protocol (default: All).
Source	Select the source match condition (default: Any).
Destination	Select the destination match condition (default: Any).
Schedule	Select a time range for the rule to take effect. Click Time Range to manage time range profiles.
Advanced	Click to display and configure additional advanced options if available.

■ Bandwidth Control

1. Go to Network Config > Traffic Management > Gateway QoS.
2. Click Bandwidth Control to load the following page. This page allows you to set the WAN upstream and downstream bandwidth limits used by QoS rules.



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.
QoS Ratio	If enabled, the QoS rules will only take effect when the throughput of this WAN reaches the the specified bandwidth ratio.
UDP Bandwidth Control	UDP traffic will be limited to the specified bandwidth ratio when the network is congested.

17. 4 Configure Switch QoS

Overview

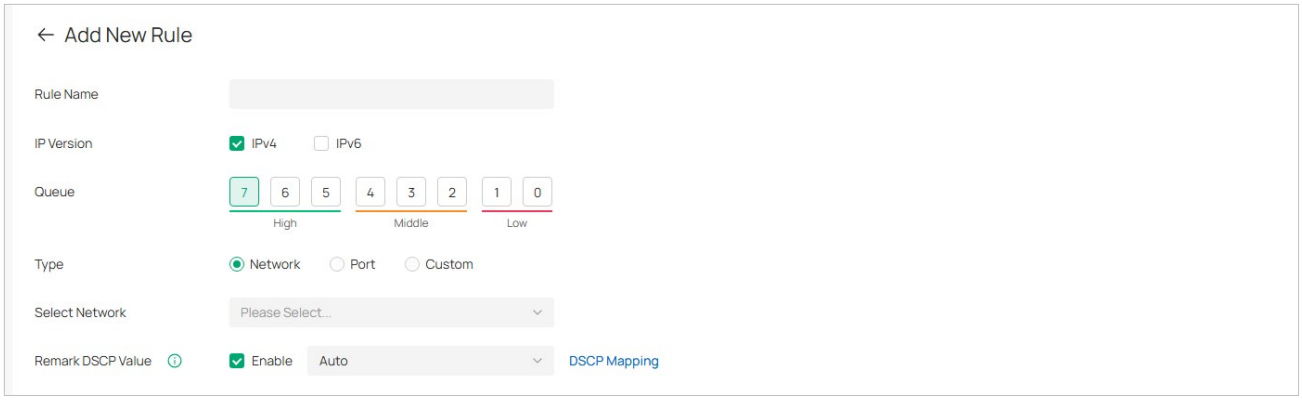
Switch QoS intelligently schedule network resources by configuring traffic categories (queues). When network bandwidth contention occurs, the system will prioritize forwarding high-priority data to prevent key applications such as voice and video from being affected by congestion. Based on DSCP-based scheduling, it enables customized priority adjustments for specific networks, ports, or traffic through rule creation, while allowing DSCP tag modification to achieve network-wide prioritized traffic scheduling.

When the switch QoS is activated, it prioritizes matching the configured rules in sequence. If no rules are matched, the system will determine the forwarding queue for packets based on DSCP mapping.

Configuration

■ Configure Switch QoS

1. Go to Network Config > Traffic Management > Switch QoS.
2. Click + Add New Rule to load the following page, configure rules based on your needs for network, port, or custom types, then click Apply.



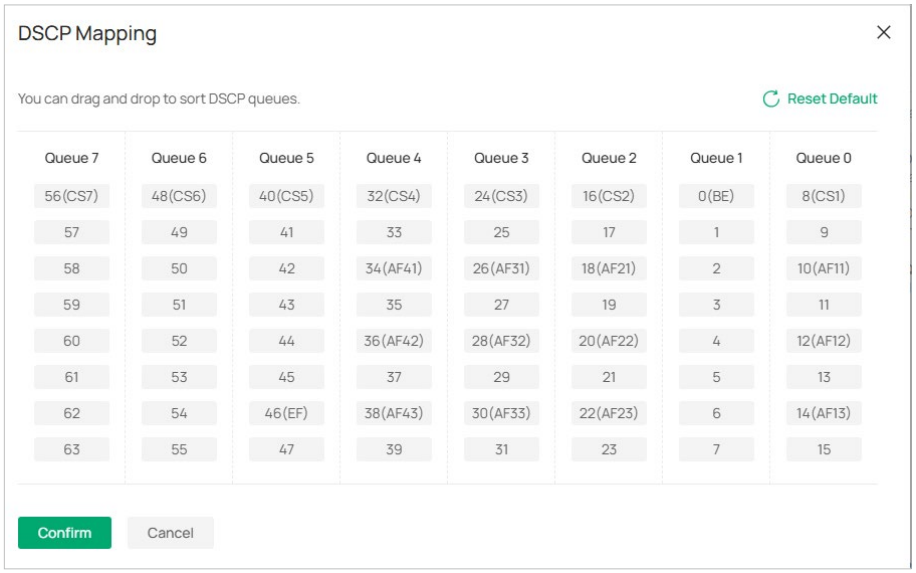
Rule Name	Specify the name of the rule.
IP Version	Select whether the rule applies to IPv4 or IPv6 packets.
Queue	Select the queue to which the rule is mapped.
Type	Select the type of rule. When Network is selected, you can choose the corresponding network. When Port is selected, you can choose the corresponding port. When Custom is selected, you can configure matching conditions such as Network, Protocol, Source Port, Destination Port, and DSCP to identify traffic. You can also specify the switch ports where the rule applies.

Remark DSCP Value	It is recommended to enable this feature. Modifying the DSCP value of traffic ensures that its forwarding priority across the entire network aligns with the configured Queue value. When set to Auto, the appropriate DSCP value is automatically adjusted based on the Queue value configured in the Rule.

3. You can click the Edit or Delete button to edit or delete the rule.

■ DSCP Mapping

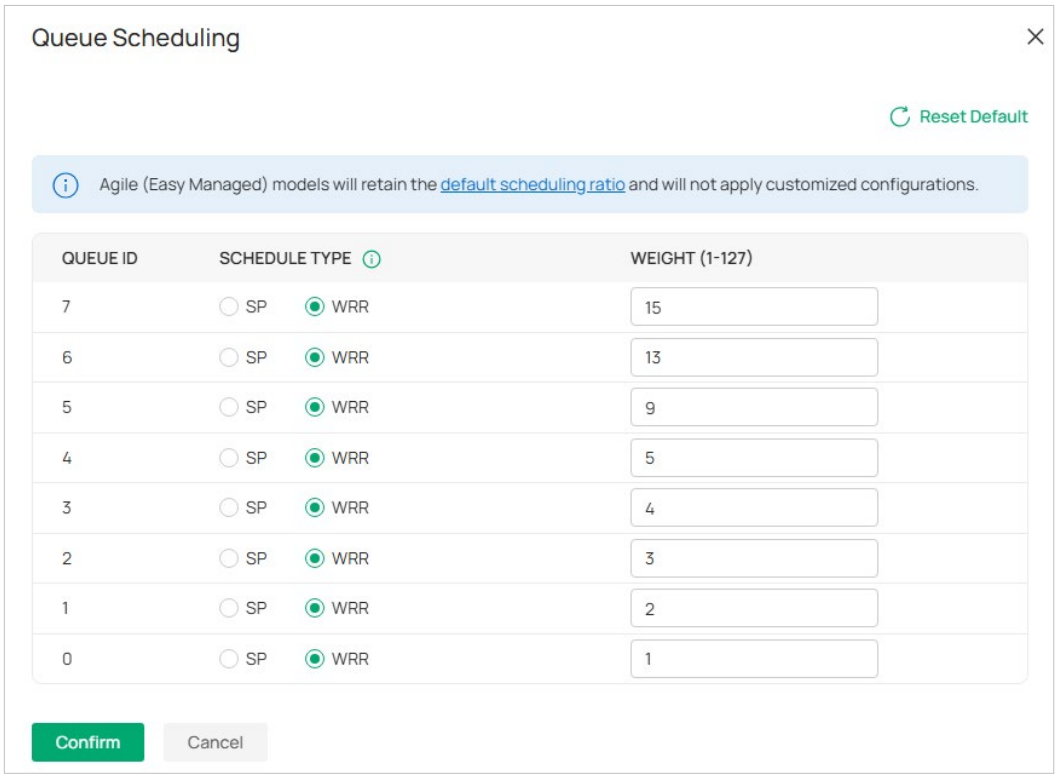
1. Go to Network Config > Traffic Management > Switch QoS.
2. Click DSCP Mapping to load the following page. You can drag and drop to sort DSCP queues.



DSCP Mapping	DSCP is a 6-bit field in the IP header, with a value range of 0 to 63. It labels packets with a “service class” marker, allowing network devices to implement QoS policies. By default, Omada maps DSCP values to different Queues according to industry standards to enforce QoS policies.

■ Queue Scheduling

1. Go to Network Config > Traffic Management > Switch QoS.
2. Click Queue Scheduling to load the following page. You can configure the scheduling method for different queues when congestion occurs.



Queue Scheduling	Used to configure the scheduling method for different queues when congestion occurs. SP(Strict Priority): When congestion occurs, packets in the queue with higher priority occupies the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. WRR(Weighted Round Robin): When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight.

Note:

When a queue is configured as SP, the queues above it must also be SP mode.

17. 5 Configure NAT Settings

Overview

- **Port Forwarding**

  Port forwarding is an application of NAT (Network Address Translation) that redirects a communication request from one combination of IP address and port number to another combination, and it takes effect when the traffic is being processed by a gateway. Port forwarding allows a host on the Internet to connect to a specific computer or service within a local-area network.

- **ALG**

  ALG (Application Layer Gateway Service) manages specific application protocols and serves as an intermediary between the internet and an application server. ALG ensures that certain application-level protocols function appropriately through your gateway.

- **UPnP**

  UPnP (Universal Plug and Play) is the networking protocol that allows devices to discover each other and then establish connections for communication. It is convenient to realize seamless connections between the devices with the help of UPnP.

- **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.

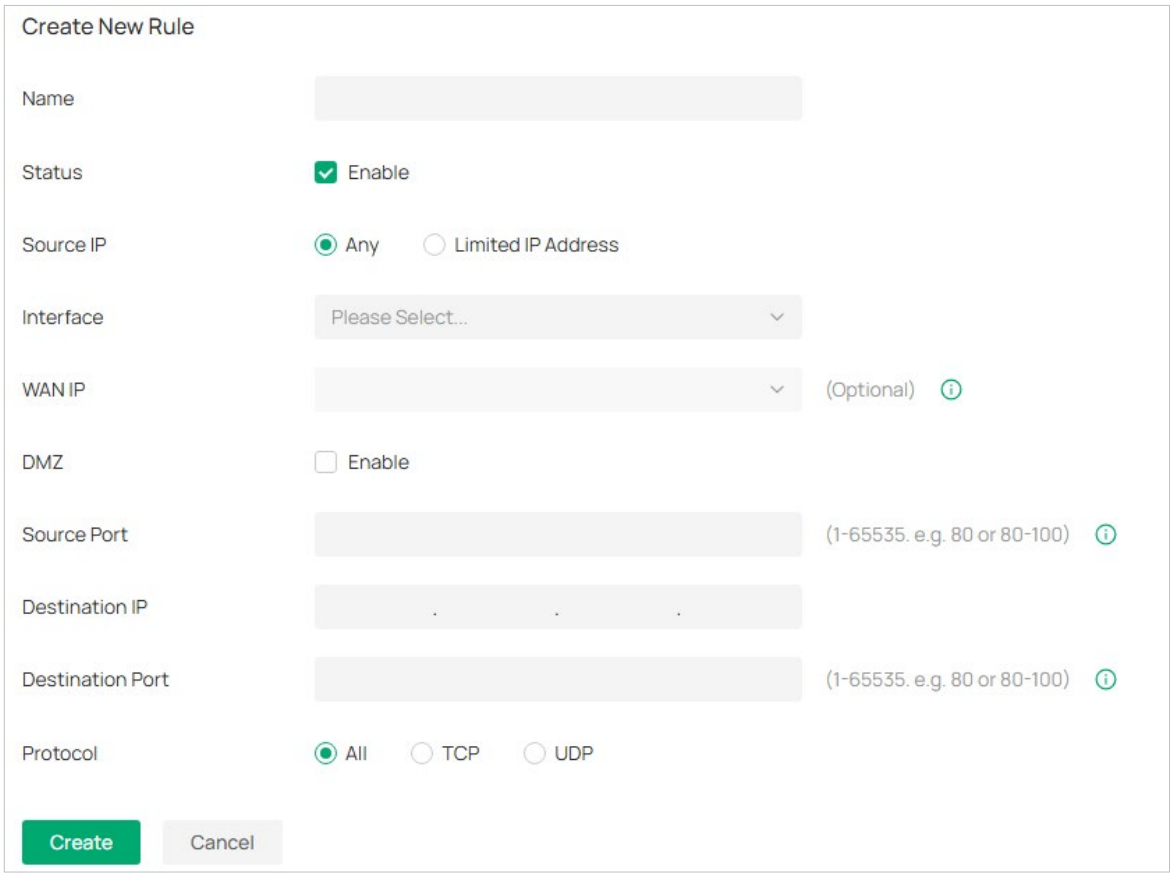
- **Disable NAT**

  With a Disable NAT rule, LAN-side devices can directly access the WAN side through their own IP addresses, or WAN-side devices can directly access the LAN side. Select one or more LAN networks and a WAN port, then packets of the devices connected to the selected LAN networks will be sent out directly from the corresponding WAN port without NAT translation.

Configuration

- **Port Forwarding**

  1. Go to Network Config > Traffic Management > NAT > Port Forwarding.
  2. Click Create New Rule to load the following page and configure the parameters.



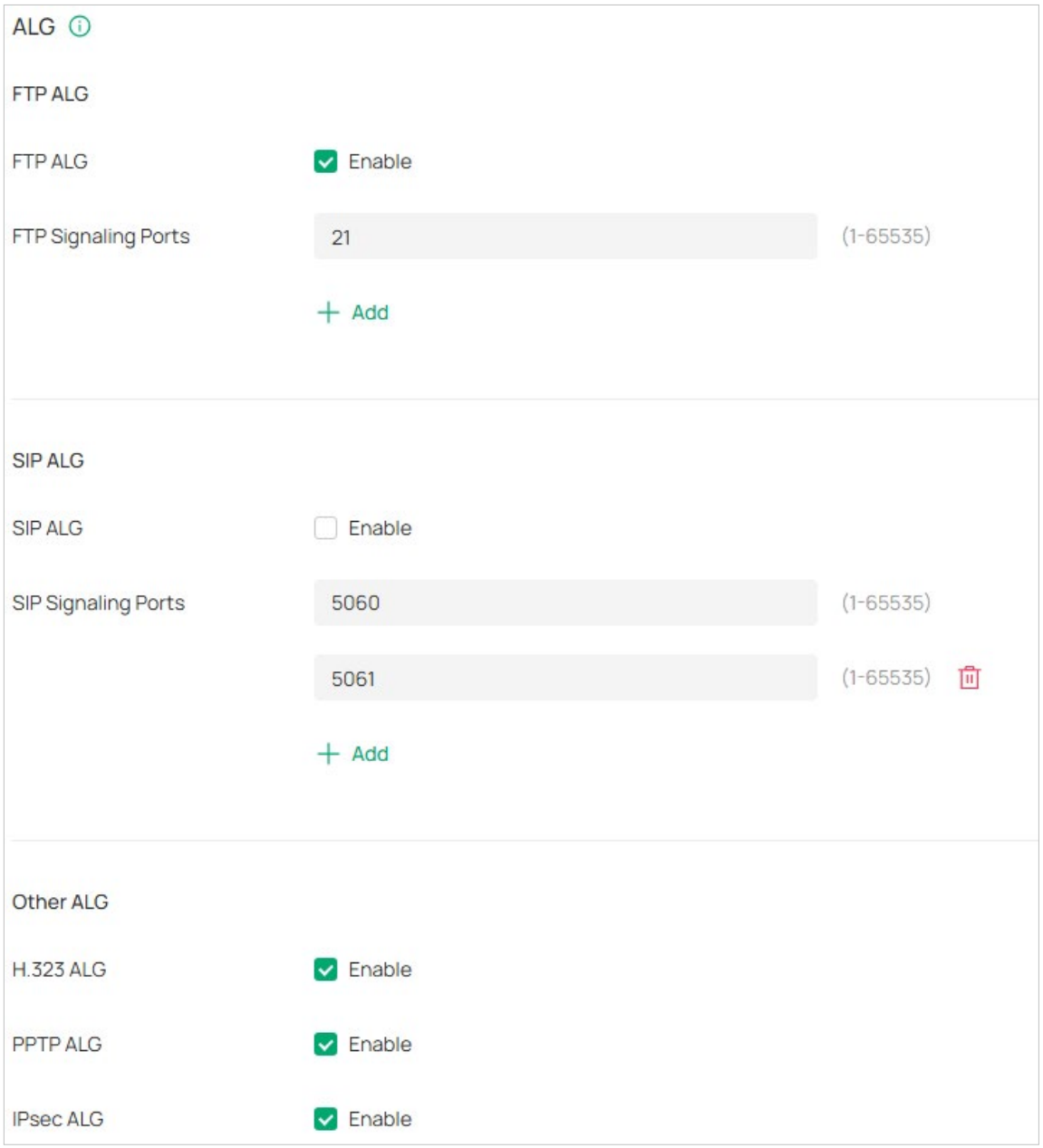
Name	Enter a name to identify the port forwarding rule.
Status	Click the checkbox to enable the port forwarding rule.
Source IP	Select the source IP of the created rule. Any: The rule applies to traffic from any source IP address. Limited IP Address: The rule only applies to traffic from specific IP addresses. With this option selected, specify the IP addresses and subnets based on needs.
Interface	Select the interface to which the rule applies. When the traffic is received through the selected WAN port, it will be forwarded according to the rule.
WAN IP	Select the WAN IP which is used to configure virtual server and other functions.
DMZ	With DMZ (Demilitarized Zone) enabled, all ports are open and the traffic from the external network is forwarded to the specified destination IP in the LAN. Use DMZ when you are not sure which ports to open for specific applications. With DMZ disabled, the traffic will be forwarded to the destination port of the destination IP in the LAN only when it matches the source port and the protocol. You need to specify the source port, destination IP, destination port, and protocol.
Source Port	Specify the source port that the gateway uses to receive the traffic from the internet. Only the traffic which matches the source port and the protocol is forwarded.

Destination IP	Specify the destination IP of the host in the LAN to which the traffic is forwarded.
Destination Port	Specify the destination port of the host in the LAN to which the traffic is forwarded.
Protocol	Select the protocol with which the network traffic is transmitted. If you want both TCP traffic and UDP traffic to be forwarded, select All. Only the traffic which matches the source port and the protocol is forwarded.

3. Click Create. The new Port Forwarding entry is added to the table. You can click the Edit icon to edit the entry. You can click the Delete icon to delete the entry.

■ ALG

1. Go to Network Config > Traffic Management > NAT > ALG.
2. Enable or disable certain types of ALG based on needs and click Apply.



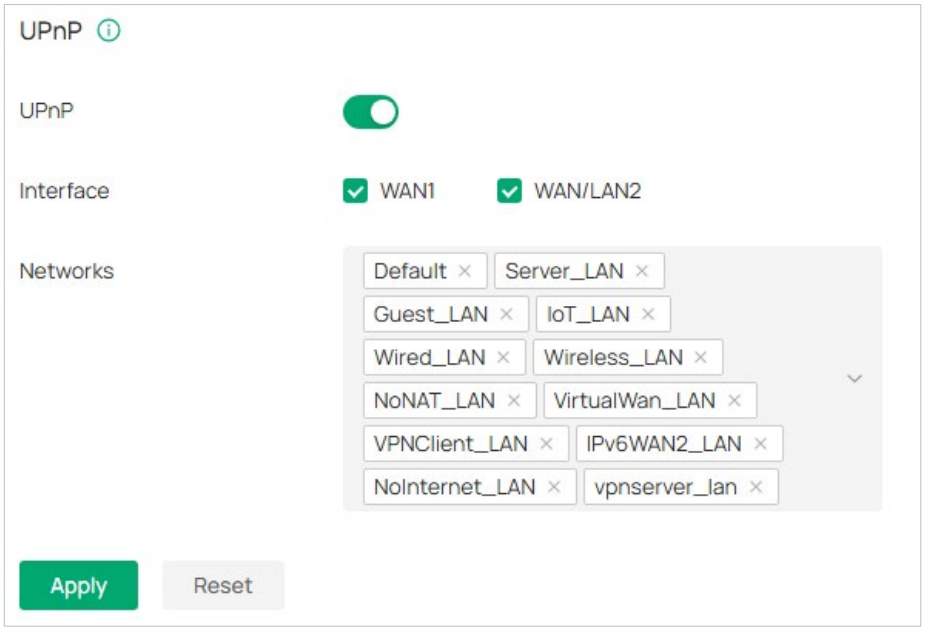
FTP ALG	FTP (File Transfer Protocol) ALG allows the FTP server and client to transfer data using the FTP protocol in the following scenarios: • The FTP server is in the LAN, while the FTP client is on the internet. • The FTP server is on the internet, while the FTP client is in the LAN.
FTP Signaling Ports	If you want to change the listening port for FTP signaling messages, configure this item. You can add new listening ports by clicking the + button (up to 8 ports are supported).
SIP	If the SIP client or server modifies the IP and port of SIP signaling messages, disable this feature.

SIP ALG	SIP (Session Initiation Protocol) ALG allows the IP phones and multimedia devices to set up connections using the SIP protocol in the following scenarios: • One of the endpoints is in the LAN, while the other is on the internet. • The endpoints are in different LANs.
SIP Signaling Ports	If you want to modify the listening ports for SIP signaling messages, configure this item. You can add new listening ports by clicking the + button (up to 8 ports supported).
TCP	Enable this option if your SIP signaling uses the TCP protocol and the device needs to modify the IP address and port in SIP messages. This helps subsequent media data traverse the device's NAT and establish a session.
UDP	Enable this option if your SIP signaling uses the UDP protocol and the device needs to modify the IP address and port in SIP signaling messages. This helps subsequent media data traverse the device's NAT and establish a session.
Restrict Peer to Peer Signaling Connection	Enable this option if you want SIP signaling connections to only arrive from registered IP addresses. SIP signaling connections from unregistered IP addresses will be discarded.
Restrict Peer to Peer Media Connection	Enable this option if you want SIP media connections to only arrive from registered IP addresses. SIP media connections from unregistered IP addresses will be discarded. The restriction may become invalid if you actively send media streams to unregistered IP addresses.
Enable Configure SIP Inactivity Timeout	Enable this option if you want to apply timeout limits to SIP signaling and media connections on the device. These timeout settings will override the SIP session timeout specified in SIP registration response packets.
SIP Signaling Inactivity Timeout	Modify this item if you want to adjust the timeout duration for SIP signaling sessions (1 – 86,400 seconds). Most SIP clients periodically send registration packets to the SIP server to keep sessions active. If your SIP client lacks this mechanism and no calls are made during the timeout period, the device will delete the signaling session after the timeout expires. This item only takes effect for remote clients and UDP protocol.
SIP Media Inactivity Timeout	Modify this item if you want to adjust the timeout duration for SIP media sessions (1 – 86,400 seconds). If no media packets are transmitted during the timeout period, the device will terminate the media session. Afterward, you will lose audio and must initiate a new call to resume communication. This item only takes effect for remote clients.
H.323 ALG	H.323 ALG allows the IP phones and multimedia devices to set up connections using the H.323 protocol in 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 (Point-to-point Tunneling Protocol) ALG allows the PPTP server and client to set up a PPTP VPN in 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.

IPsec ALG	IPsec (IP Security Protocol) ALG allows the IPsec endpoints to set up an IPsec VPN in the following scenarios: • One of the endpoints is in the LAN, while the other is on the internet. • The endpoints are in different LANs.

UPnP

1. Go to Network Config > Traffic Management > NAT > UPnP.
2. Enable the UPnP, and configure the parameters. Click Apply.



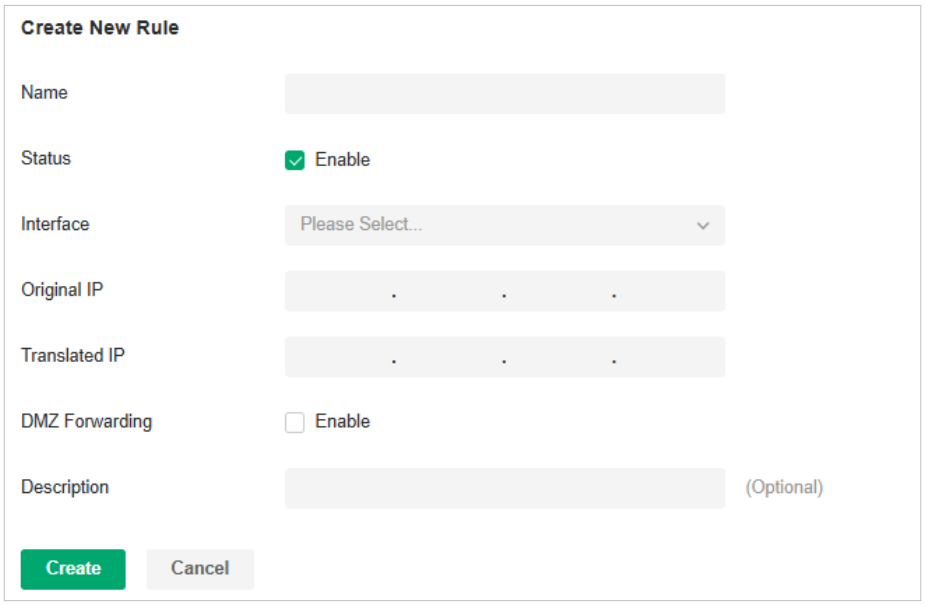
Interface	Select the WAN port which UPnP takes effect.
Networks	Select the LAN interface which UPnP takes effect.

Note:

When setting open ports for UPnP, do not select the reserved ports (500/4500 is reserved for IPsec, 1723/1701 is reserved for PPTP/L2TP, 1194 is reserved for OpenVPN, 51820 is reserved for WireGuard, and the specific ports you reserved).

One-to-One NAT

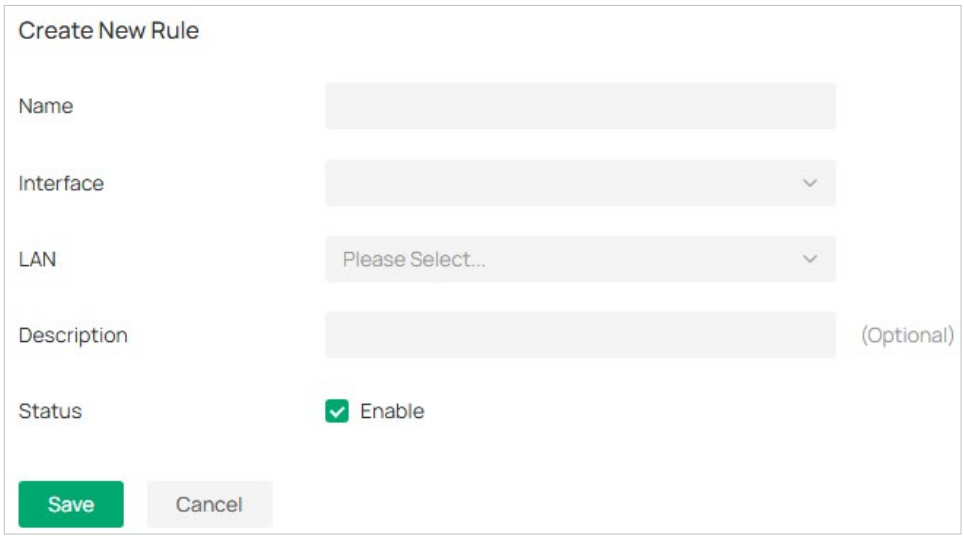
1. Go to Network Config > Traffic Management > NAT > One-to-One NAT.
2. Click Create New Rule to load the following page and configure the parameters.



Name	Enter a name to identify the one-to-one NAT rule.
Status	Click the checkbox to enable the one-to-one NAT rule.
Interface	Specify the effective WAN interface for the rule. Currently, only WAN interfaces using the Dynamic IP, Static IP, PPPoE, L2TP, or PPTP connection types are supported.
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	Enter a brief description for the rule entry to facilitate your management.

■ Disable NAT

1. Go to Network Config > Traffic Management > NAT > Disable NAT.
2. Click Create New Rule to load the following page and configure the parameters.



Name	Enter a name to identify the rule.
Interface	Select the WAN port to send out packets. A WAN port can be used in one Disable NAT rule only.
LAN	Select one or more LAN networks. A LAN network can be used in one Disable NAT rule only.
Description	Enter a description for identification.
Status	Check the box to enable the rule.

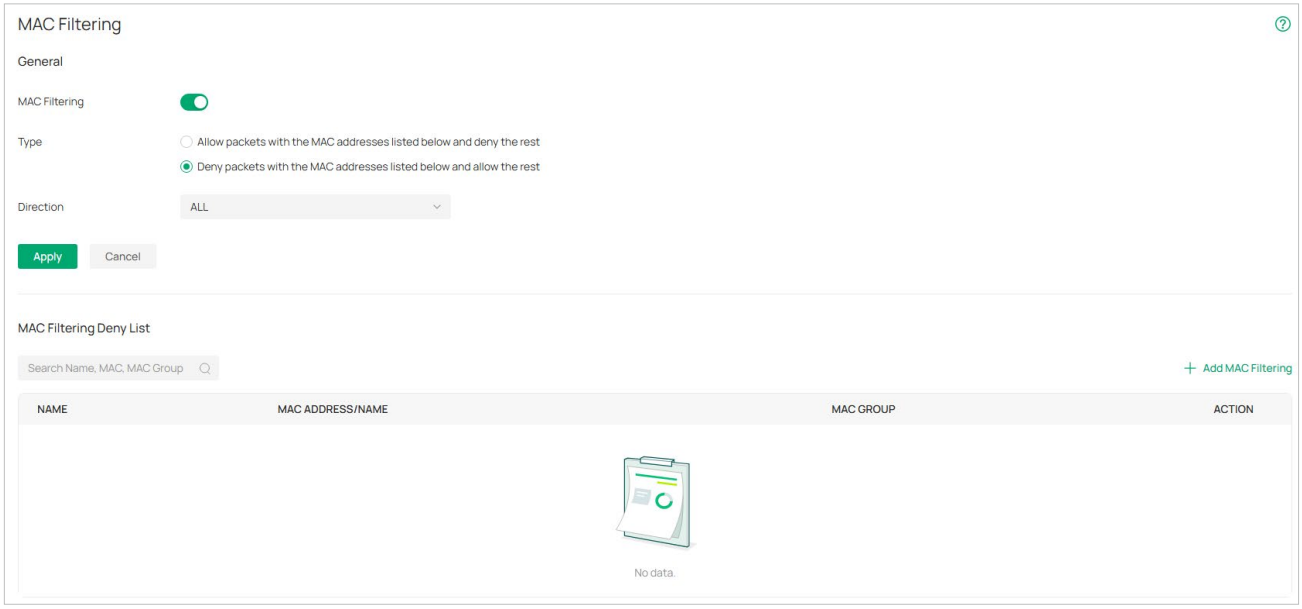
17. 6 Configure MAC Filtering

Overview

MAC Filtering can drop or allow packets from certain devices passing through the router based on the MAC address of the devices. After the MAC filtering policy and MAC filtering list are configured, the router will apply the filter policy to the packets matching the MAC address, and thus limit network traffic and manage network access behaviors.

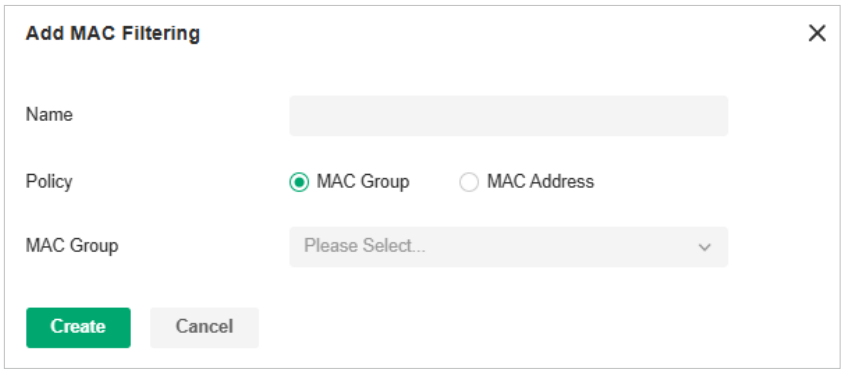
Configuration

1. Go to Network Config > Traffic Management > MAC Filtering.
2. Enable MAC Filtering and and configure the general parameters.



Enable MAC Filtering	Enable the MAC Filtering feature.
Type	Select the mode of MAC Filtering. Allow packets with the MAC addresses listed below and deny the rest: Select to allow packets with the listed MAC address to pass through the gateway, and packets with other MAC addresses will be dropped. Deny packets with the MAC addresses listed below and allow the rest: Select to drop packets with the listed MAC address, and packets with other MAC addresses will be allowed to pass through the gateway.
Direction	Select All when you want to apply the policy to traffic both from LAN to LAN and from LAN to WAN. Select LAN -> WAN when you want to apply the policy only to traffic from LAN to WAN.

3. Click Add MAC Filtering to add MAC addresses or groups to the list.



Name	Specify the name for the entry.
MAC Address	Specify the MAC address of the device, and the MAC filtering policy will be applied to traffic with the MAC address.
MAC Group	Specify the MAC Group of the device,and the MAC filtering policy will be applied to traffic with the MAC Group.

17. 7 Configure IP-MAC Binding

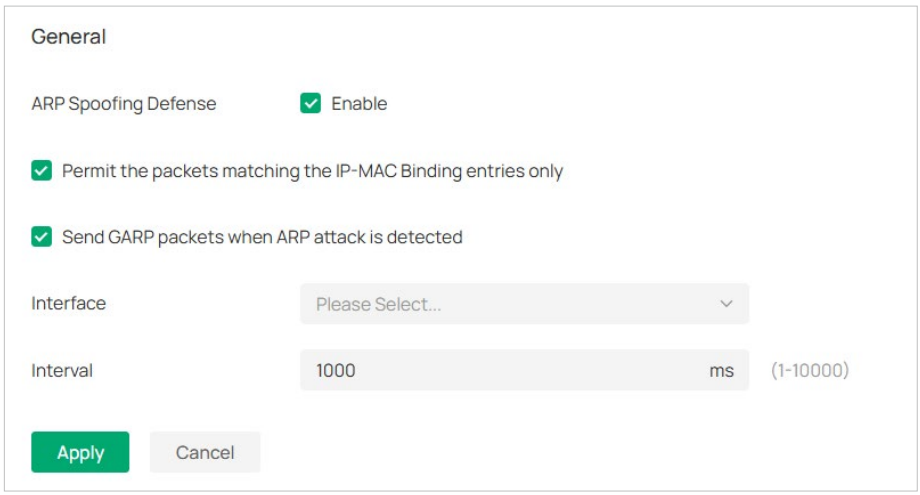
Overview

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

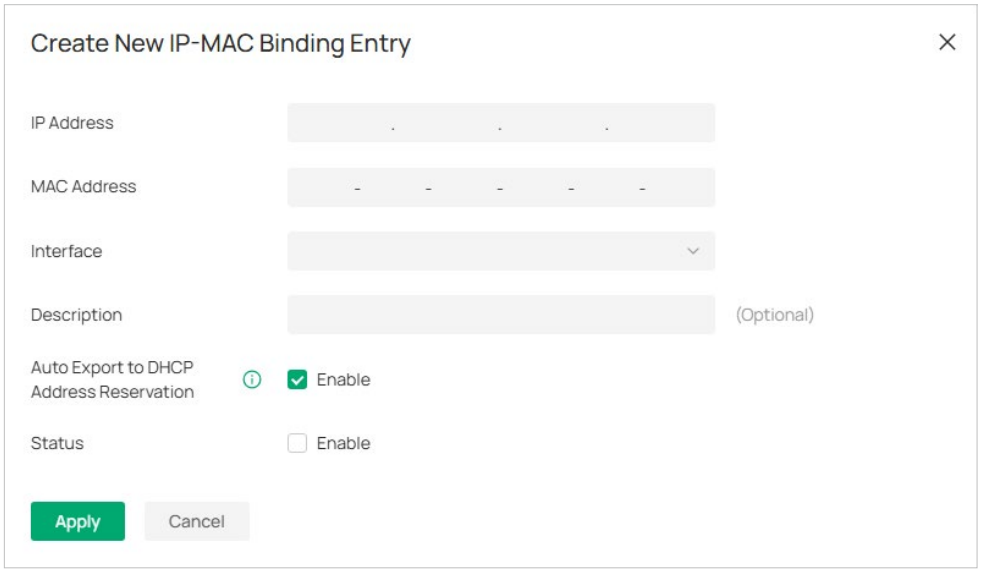
1. Go to Network Config > Traffic Management > IP-MAC Binding.
2. Enable ARP Spoofing Defense and configure general settings. Click Apply.



ARP Spoofing Defense	Check the box to globally enable ARP Spoofing Defense.
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 gateway 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.
Interface	Select the interface to send GARP packets when an ARP attack is detected.

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.



IP Address	Specify the IP address to be bound.
MAC Address	Specify the MAC address to be bound.
Interface	Select the interface to send GARP packets when an ARP attack is detected.
Description	Enter a description for identification.
Auto Export to DHCP Address Reservation	When the interface is set to LAN, enabling this option will synchronize the newly created IP-MAC Binding entry to DHCP Reservation list
Status	Enable the entry. Only when the status is enabled will the entry take effect.

4. Click Export to export the template in csv format. Based on this template, add IP-MAC Binding entries that need to be imported.
5. Click Import and import the customized template. You can download the template, then edit and upload it for batch import.

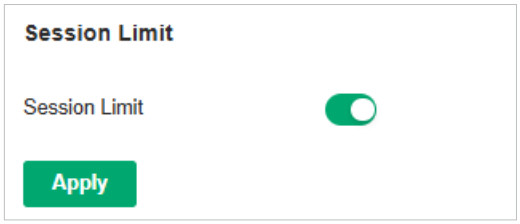
17. 8 Configure Session Limit

Overview

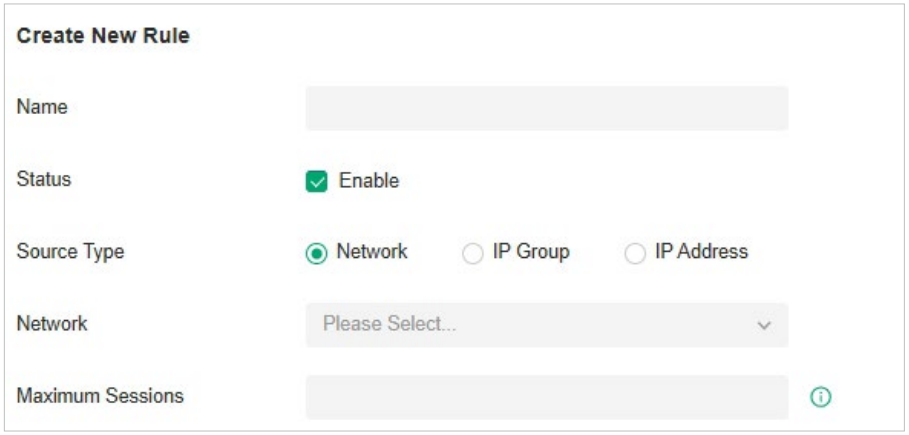
Session limit feature limits the number of sessions that specific sources can use. This feature can prevent the network resources and bandwidth from being exhausted by some hosts which use too many sessions at one time, and therefore optimizes network performance.

Configuration

1. Go to Network Config > Traffic Management > Session Limit.
2. In Session Limit, enable session limit and click Apply.



3. In Session Limit Rule List, click + Create New Rule to load the following page and specify the parameters for the new session rule of limit.



Name	Enter a name to identify the session limit rule.
Status	Click the checkbox to enable the session limit rule.

Source Type	Select the source of the created rule. Network: The rule applies to specific LAN networks. With this option selected, choose the network. If you want to create or customize networks, go to Network Config > Network Settings > LAN. IP Group: The rule applies to specific IP groups. With this option selected, choose the IP group. If you want to create or customize IP groups, go to Network Config > Profile > Groups. IP Address: The rule applies to specific IP addresses. With this option selected, specify one or multiple IP addresses. The rules with IP address source type have higher priority than the rules with other source types.
Maximum Sessions	Enter the maximum number of sessions of the specific sources. The gateway will limit the sessions of the source when its number exceeds the maximum value.

4. Click Save. The new Session Limit rule is added to the list. You can click the Edit icon to edit the rule. You can click the Delete icon to delete the rule.

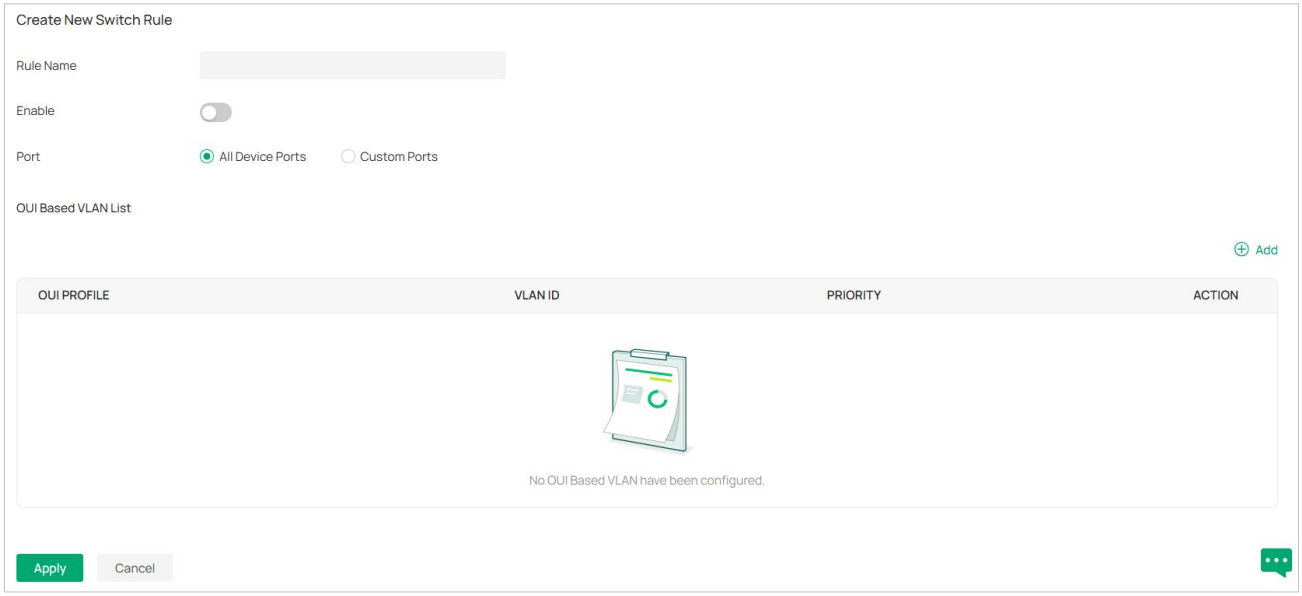
17. 9 Configure OUI-Based VLAN

Overview

The OUI-Based VLAN function can perform VLAN and priority division and processing on device data packets starting with specific MAC addresses based on OUIs.

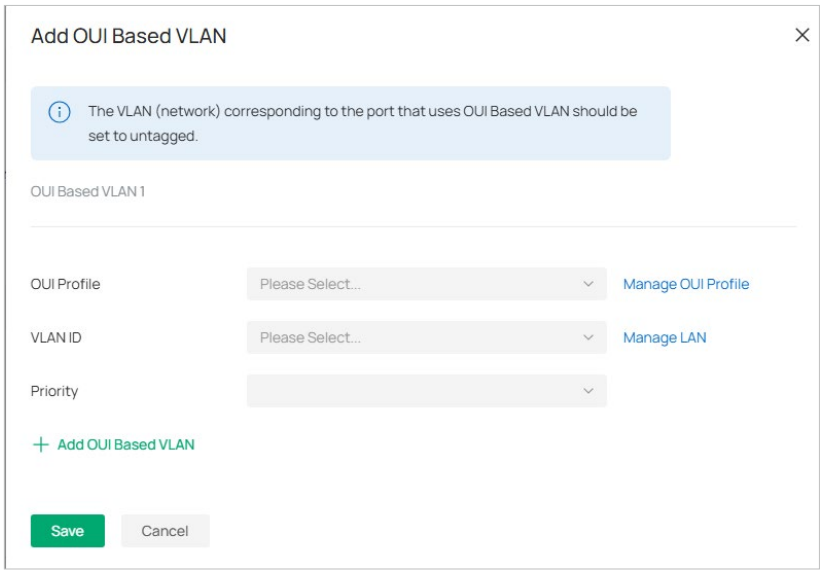
Configuration

1. Go to Network Config > Traffic Management > OUI-Based VLAN.
2. Click Create New Switch Rule.



3. Specify the rule name and enable the function.
4. Specify the effective ports. You can choose all device ports or specify some ports of some switches for the rule to take effect.
5. In the OUI Based VLAN List, Click Add to add an OUI-Based VLAN.

Note: The VLAN (network) corresponding to the port that uses OUI Based VLAN should be set to untagged.



Rule Name	Specify the rule name.
Enable	Enable this function.
Port	Specify the effective ports. You can choose All Device Ports or some ports of some switches for the rule to take effect.
Excluded Switches List	List of devices for which this function cannot be applied because the firmware version does not support it.
OUI Profile	Specify the corresponding OUI Profile.
VLAN ID	Specify the corresponding OUI Based VLAN ID.
Priority	Specify the priority, and the corresponding data packet will be marked with this priority for transmission.

Chapter 18

Configure Network Authentication

Authentication is a portfolio of features designed to authorize network access to clients, which enhances the network security. Omada provides authentication services covering all the needs to authenticate both wired and wireless clients.

This chapter guides you on how to configure network authentication with the Fusion gateway. The chapter includes the following sections:

18. 1 Configure Portal Authentication

Overview

Portal authentication provides authentication service 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. APs 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 APs are connected and working properly.

The Fusion gateway provides several 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 Fusion gateway.

- **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 Fusion gateway within a predefined time usage. Voucher codes can be printed out from the Fusion gateway, 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.

- **RADIUS Server**

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

- **External LDAP Server**

  Clients are required to enter the correct username and password created on the external LDAP 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 the Fusion gateway.

- **Google**

  Clients will be redirected to the Google login page and are required to complete the Google account login to pass the authentication.

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**

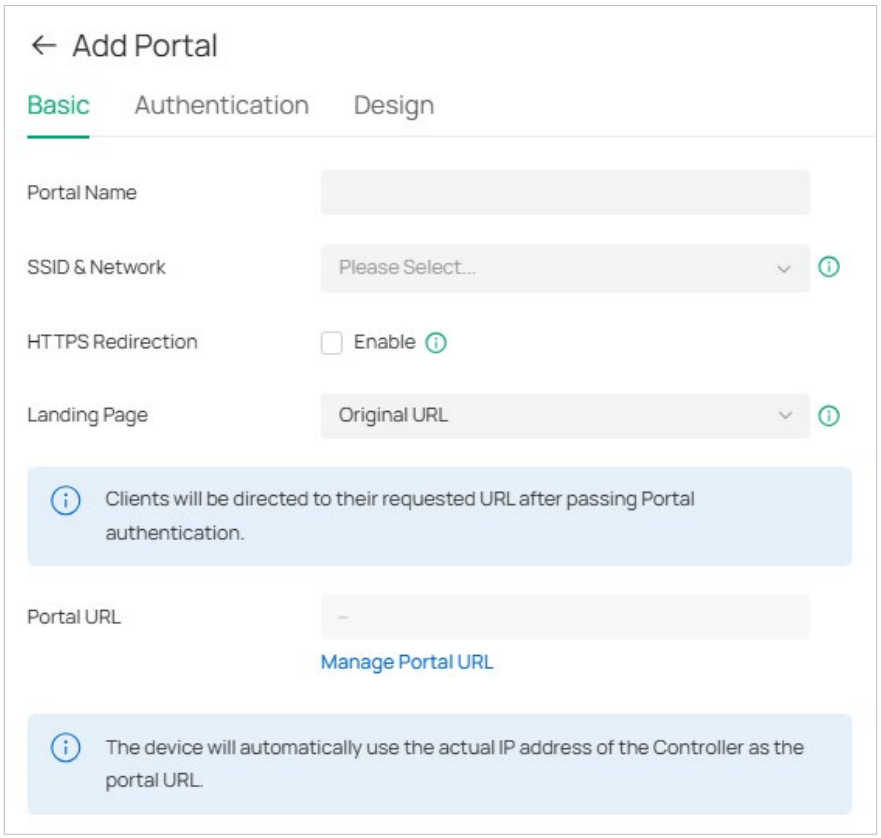
  Pre-Authentication Access allows unauthenticated clients to access the specific network resources.

- **Authentication-Free Client**

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

Create New Portal

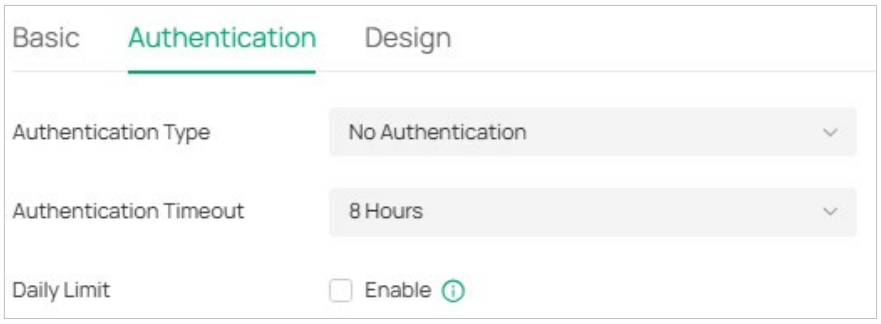
1. Go to Network Config > Authentication > Portal.
2. On Portal tab, click Create New Portal.



3. Specify the portal name. Select the SSIDs and LAN networks for the portal to take effect. The clients connected to the selected SSIDs or LAN networks will have to log into a web page to establish verification before accessing the network.
4. Configure redirection and landing settings.

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. Success Page: Clients will see the Portal success page after passing Portal authentication.
Portal URL	Displays the URL address that will be used for this Portal authentication page.

5. Go to Authentication section. Select the Authentication Type and configure authentication settings.



■ 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.

■ Simple Password

Password	Specify the password for the portal.
Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.

■ Hotspot

Type	Select one or more authentication types according to your needs. Clients can access the network after passing any type of the authentication.

With different types of Hotspot selected, configure the related parameters.

- **Voucher Portal**

Voucher	Select Voucher and click Voucher Manager to manage the voucher codes. Refer to the voucher configuration chapter in this guide for detailed information about how to create vouchers.

- **Local User Portal**

Local User	Select Local User and click User Management to manage the information of the login accounts. Refer to the account configuration chapter in this guide for detailed information about how to create Local Users.

- **SMS Portal**

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

SMS	Clients can get verification codes using their mobile phones and enter the received codes to pass the authentication.
Twilio SID	Enter the Account SID for Twilio API Credentials.
Auth Token	Enter the Authentication Token for Twilio API Credentials.
Operating Phone Number	Enter the phone number that is used to send verification messages to the clients.
Allow Maximum Verification Code Times	Click the checkbox and enter the maximum number of users allowed to be authenticated using the same telephone 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.

- **RADIUS Portal**

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

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 the information of the RADIUS server which provides a method for storing the authentication information centrally.
Portal Logout	Check the box to allow clients to log out of the portal by accessing a URL (portal.tplink.net/portal/logout by default). You can change the default URL by editing Portal Logout Domain in the Settings > System Settings. Some devices may require firmware update to support Portal Logout. Please refer to Configuration Result for details.
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.

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.

■ 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 click 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.
Portal Logout	Check the box to allow clients to log out of the portal by accessing a URL (portal.tplink.net/portal/logout by default). You can change the default URL by editing Portal Logout Domain in the undefined. Some devices may require firmware update to support Portal Logout. Please refer to Configuration Result for details.
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.

■ External LDAP Server

Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.
LDAP Profile	Select the LDAP profile you have created. If no LDAP profiles have been created, click Create New LDAP Profile from the drop-down list or click Manage LDAP Profile to create one. The LDAP profile records information of the LDAP server including the server address, port and so on.
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.

■ External Portal Server

Custom Portal Server	Specify the IP address or URL that redirect to an external portal server.

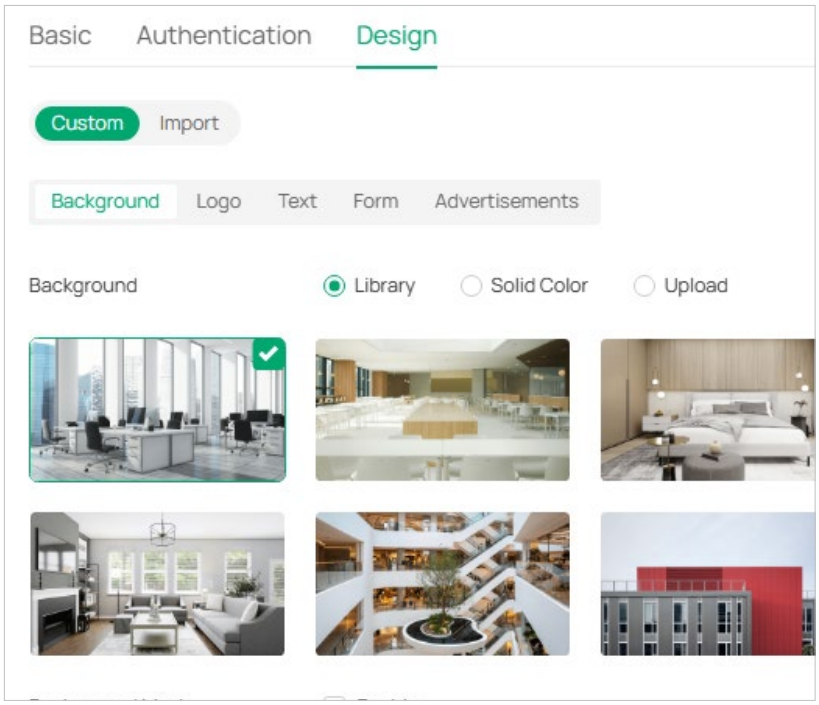
■ Google

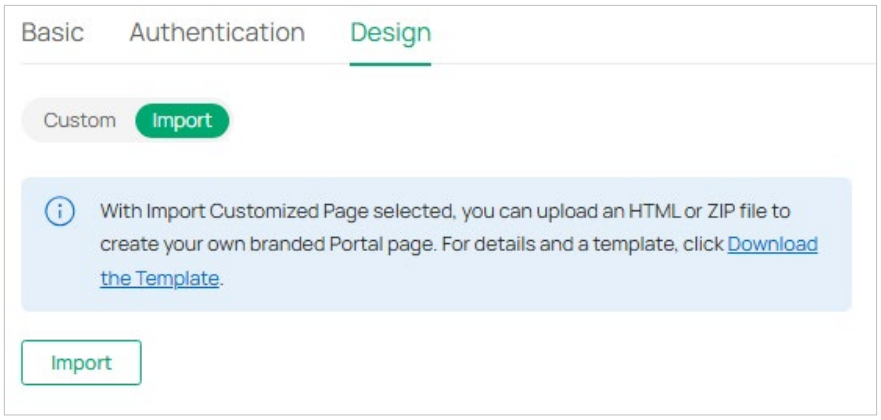
Authentication Timeout	Select the login duration. Clients will be off-line after the authentication timeout.
Client ID	Enter the Client ID provided by Google to integrate with Google OAuth 2.0.
Client Secret	Enter the Client Secret provided by Google to integrate with Google OAuth 2.0.

(Optional) Portal Customization

When creating or editing a portal entry, you can customize the Portal page in the Design section.

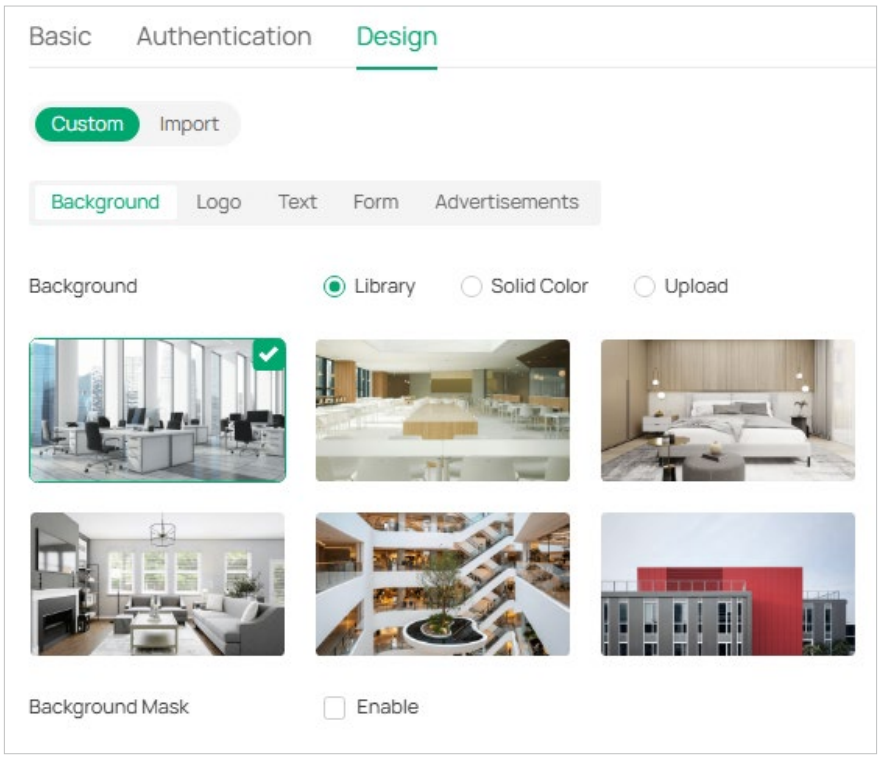
Note: Portal Customization is not available when you configure external authentication types.





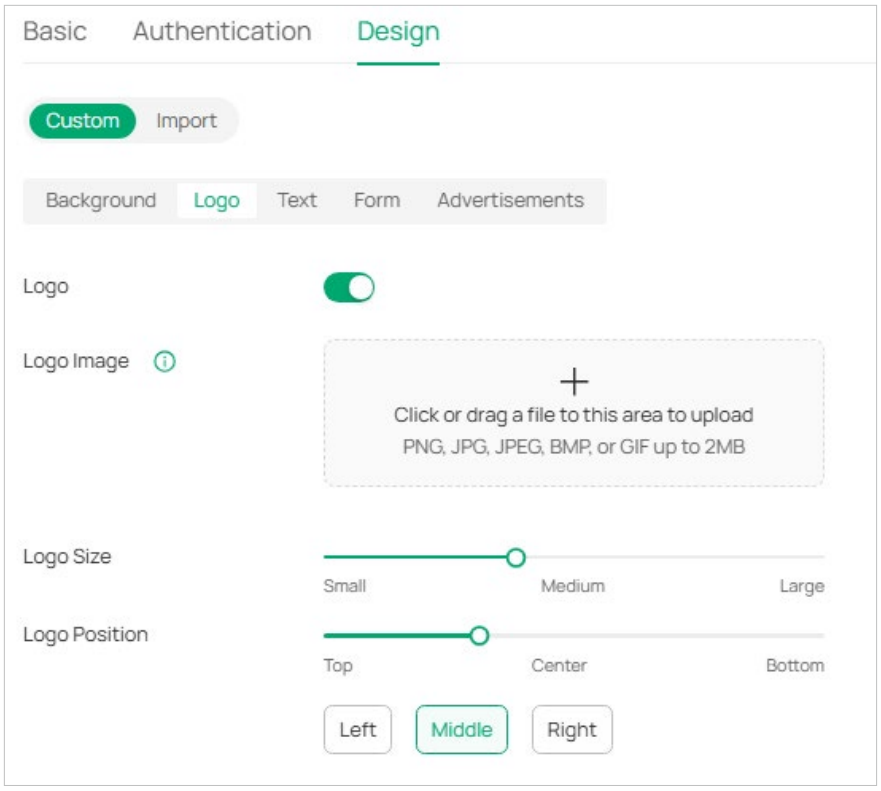
Custom	Edit the related parameters to customize the portal page based on the provided page.
Import	Click Import to import your unique Portal page for branding it as per your business.

Background



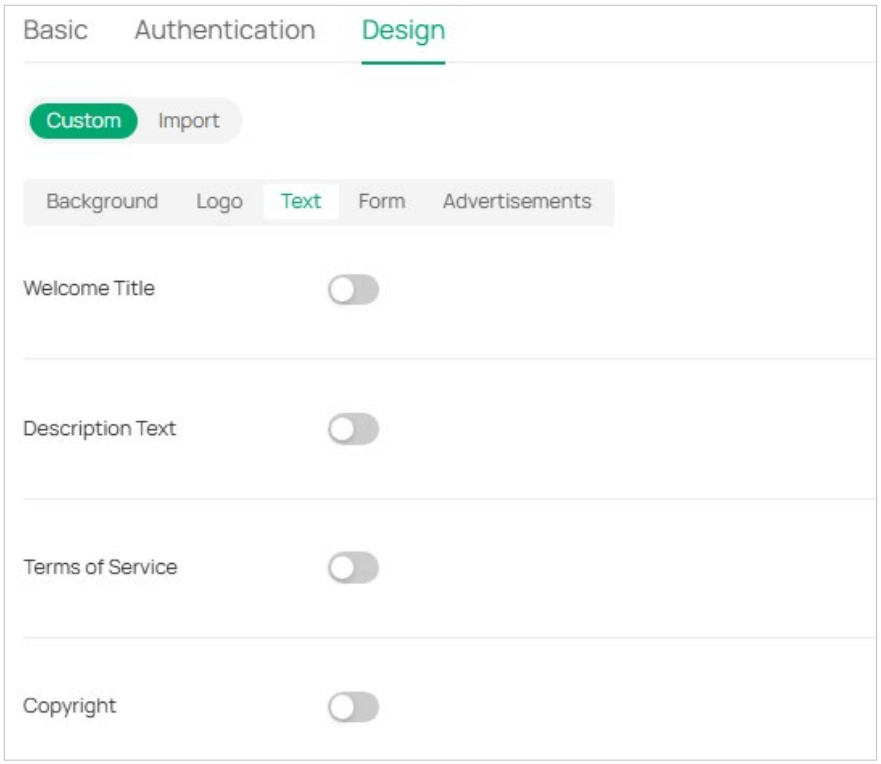
Background	Select the background type. Library: Select a background picture from the image library. Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker. Upload: Click Choose and select a picture from your PC as the background. Unified Image: With this feature enabled, the background picture will be the same for both the web and mobile portal pages. With this feature disabled, you can upload separate background pictures for the web and mobile portal pages respectively.
Background Mask	Enable the background mask to add a overlay on the background.

Logo



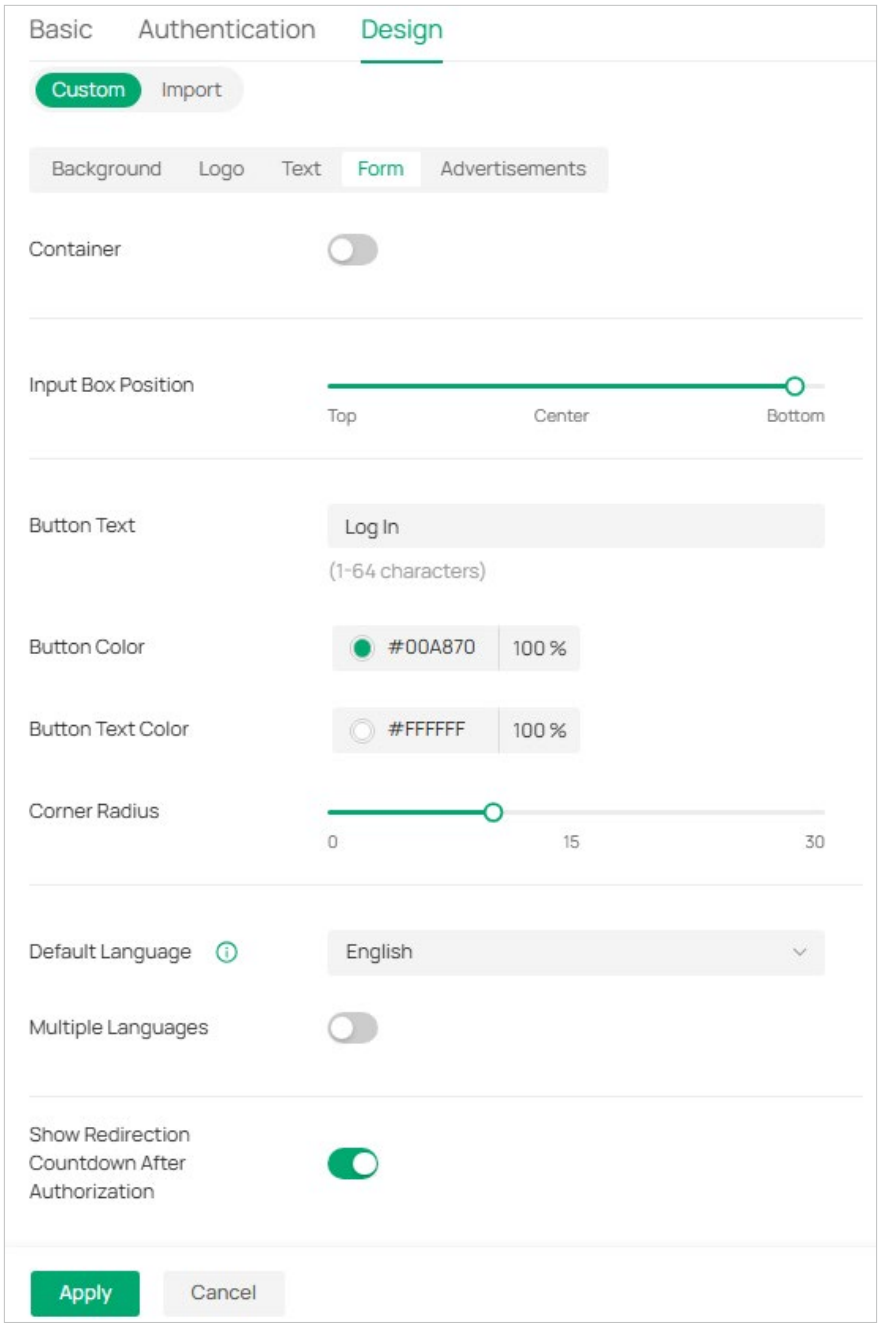
Logo	Click the checkbox to enable the log to display on the Portal page.
Logo Image	Select a picture from your PC as the logo.
Logo Size	Adjust the logo size on the Portal page.
Logo Position	Adjust the logo position on the Portal page.

Text



Welcome Title	Enable the toggle and enter content 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.
Description Text	Enable the toggle and enter content as the description 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	Enable the toggle 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.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.
Copyright	Enable the toggle and enter content as the copyright 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.

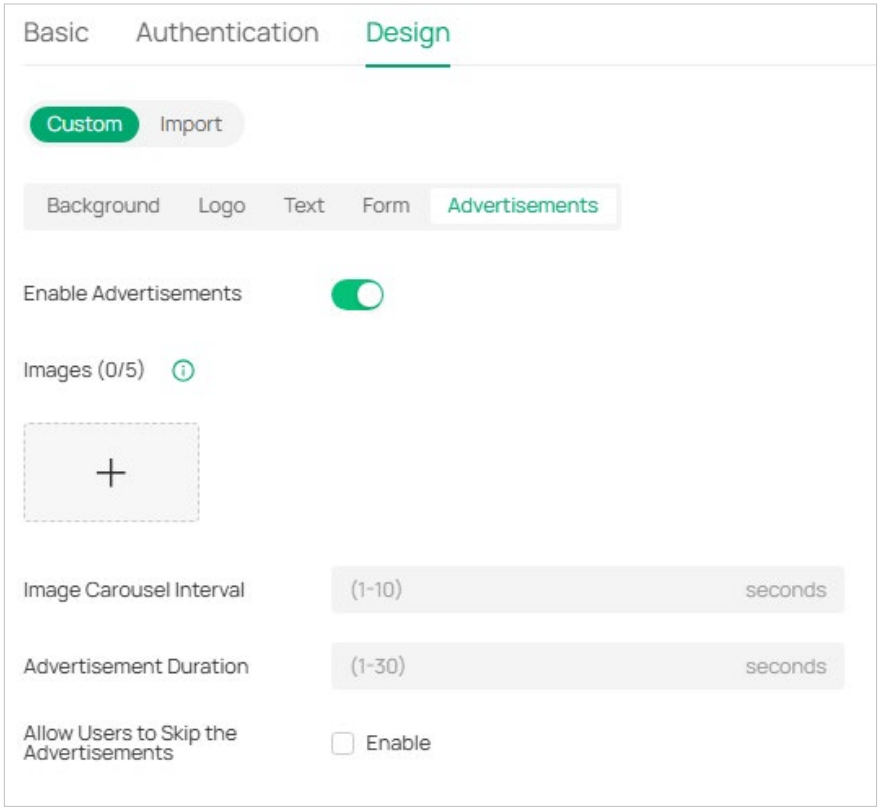
Form



Container	Enable the toggle to add a container to the page. You can select All or Half as the container type. Configure the container color by entering the hexadecimal HTML color code manually or through the color picker, adjust the corner radius, and enable background blur for the container.
Input Box Color	Configure your desired background color for the input box by entering the hexadecimal HTML color code manually or through the color picker.
Input Text Color	Configure your desired text color for the input box by entering the hexadecimal HTML color code manually or through the color picker.
Stroke Color	Configure your desired color for the input box stroke by entering the hexadecimal HTML color code manually or through the color picker.

Corner Radius	Adjust the input box corner radius.
Input Box Position	Adjust the input box position on the Portal page.
Button Text	Enter content as the button text.
Form Auth Button Text	Enter content as the form auth button text.
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.
Corner Radius	Adjust the input box corner radius.
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.
Multiple Languages	With this feature enabled, the portal page will support multiple languages. The default language follows the browser setting, and users can manually switch languages on the page.
Show Redirection Countdown After Authorization	With this feature enabled, a countdown for the redirection will be displayed after successful authentication.

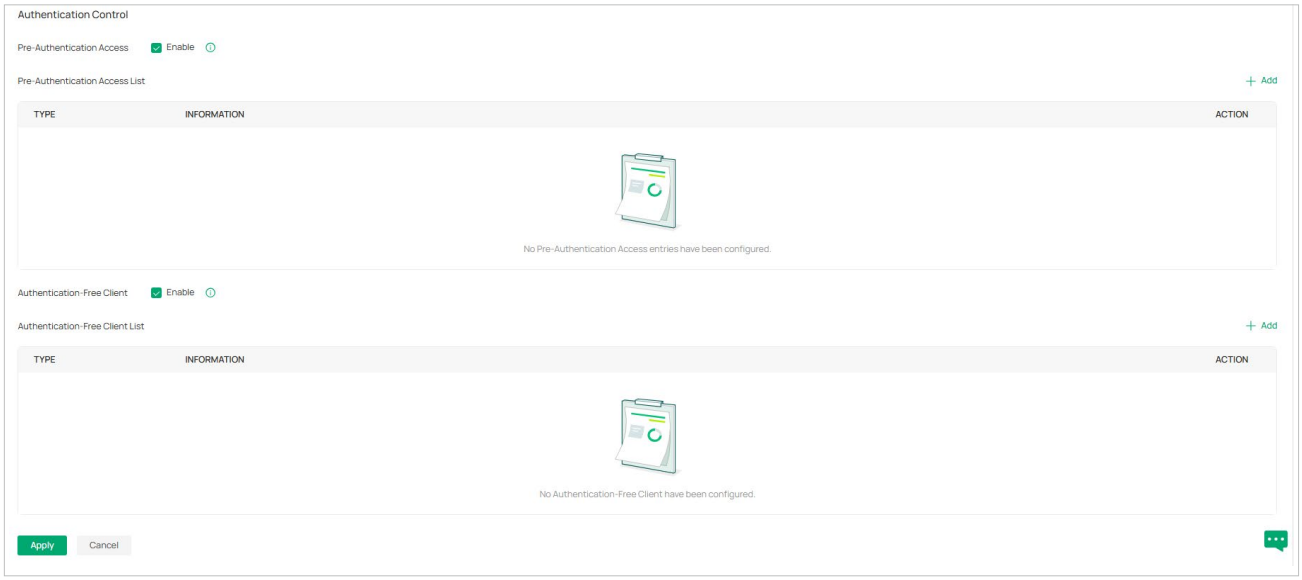
■ Advertisements



Enable Advertisements	Enable the toggle 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.
Images	Select pictures from your PC as the advertisement pictures. When several pictures are added, they will be played in a loop.
Image 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.
Advertisement Duration	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.
Allow Users to Skip the Advertisements	Click the checkbox to allow users to skip the advertisement.

(Optional) Authentication Control

On Authentication Control tab, you can configure access control rules if needed.



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

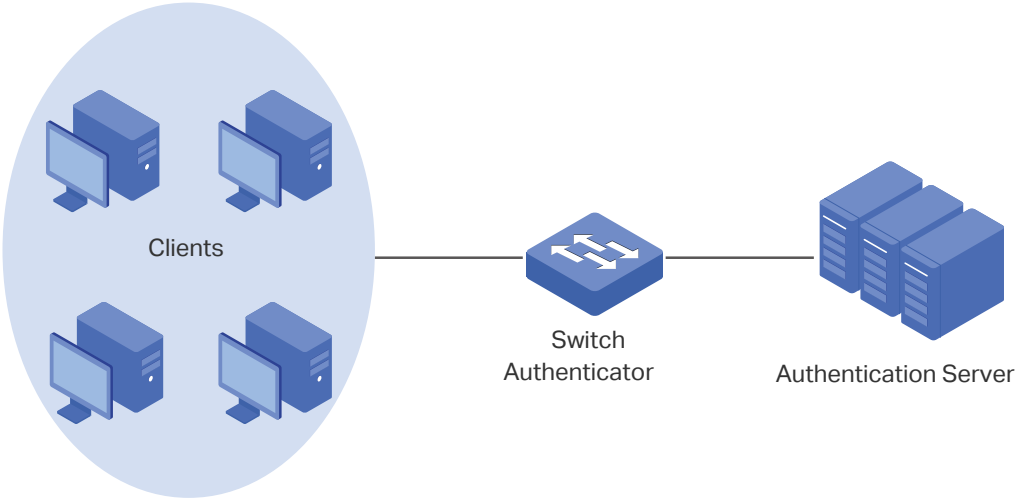
18. 2 Configure 802.1X Authentication

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.

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.

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.

Configuring Switch 802.1X

To complete the 802.1X configuration for a switch, follow these steps:

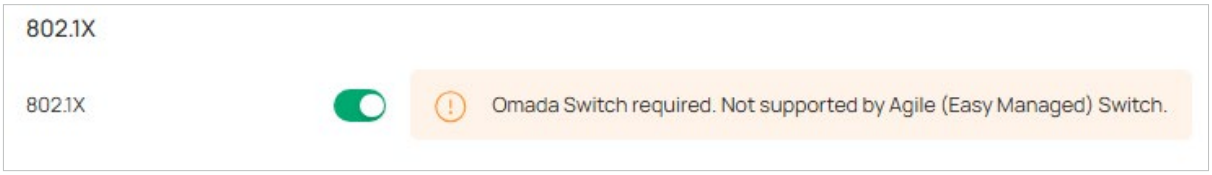
1) Enable 802.1X.

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

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

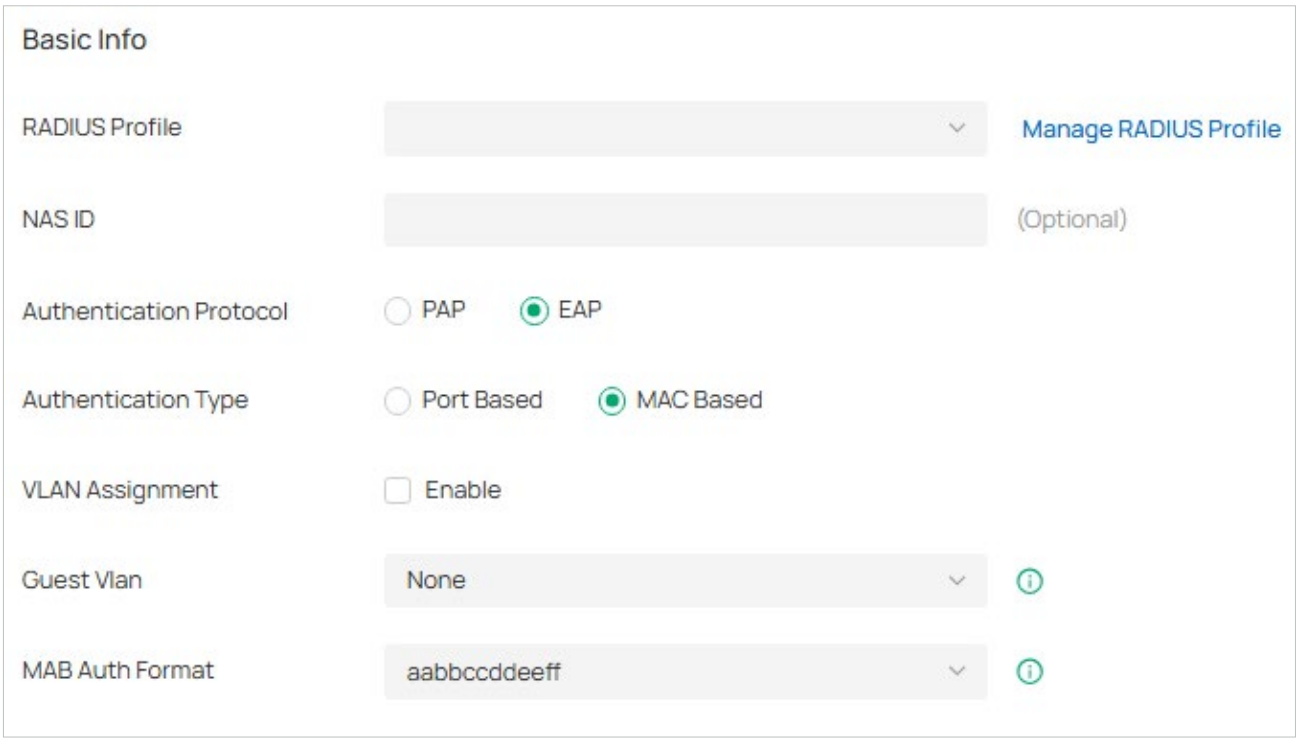
Step 1: Enable 802.1X

Go to Network Config > Authentication > Switch 802.1X. Click to enable 802.1X.



Step 2: Configure RADIUS Profile and Parameters

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.



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

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 AP 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 AP packets are converted to other protocol (such as RADIUS) packets, and transmitted to the RADIUS server. EAP: The AP 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 AP 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.
Guest Vlan	Assign a VLAN for guest clients whose authentication fails or times out.
MAB Auth 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.

Step 3: Select the Ports

1. Click + Add to select the switch.

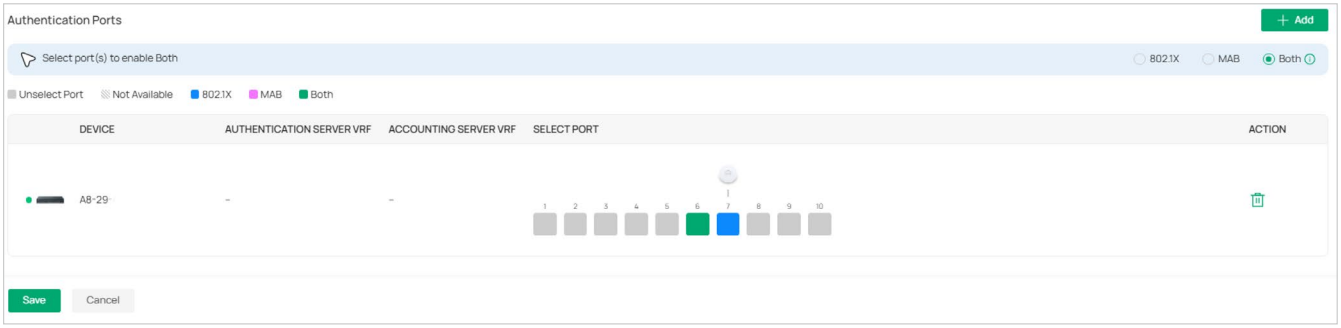
2. Select the ports to enable 802.1X authentication or MAB for them.

To enable 802.1X authentication for switch ports, click 802.1X and select the corresponding ports. The ports will be marked as ■.

To enable MAB for switch ports, click MAB and select the corresponding ports. The ports will be marked as ■.

To enable both 802.1X and MAB for switch ports, click Both and select the corresponding ports. The ports will be marked as ■.

Note: You can enable MAB only on 802.1X-enabled ports.



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 gateway.
- 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.

Configuring EAP 802.1X

To complete the 802.1X configuration for an AP, follow these steps:

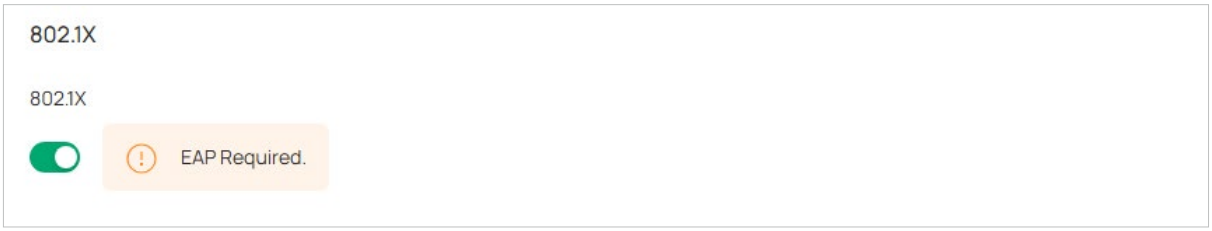
1) Enable 802.1X.

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

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

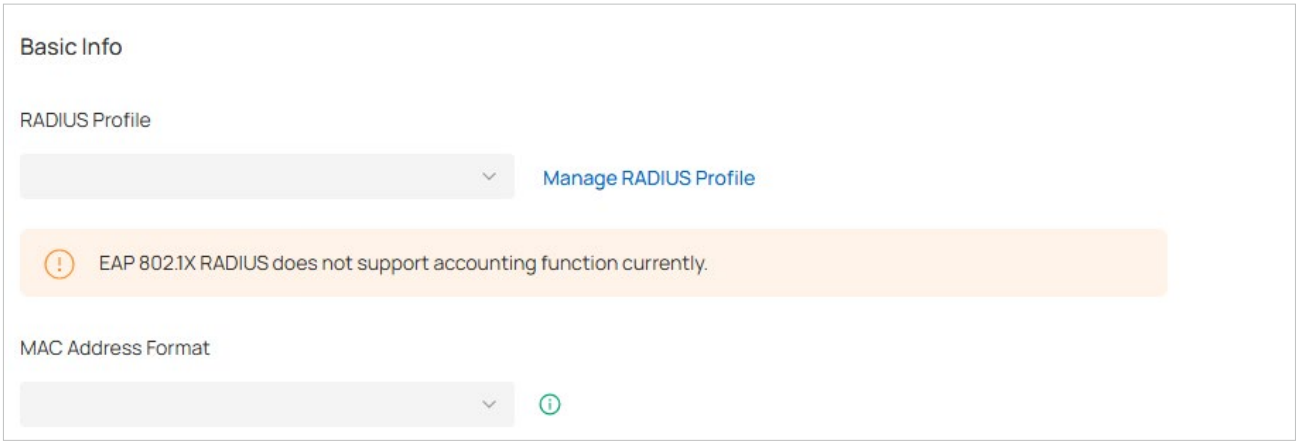
Step 1: Enable 802.1X

Go to Network Config > Authentication > EAP 802.1X. Click to enable 802.1X.



Step 2: Configure RADIUS Profile and Parameters

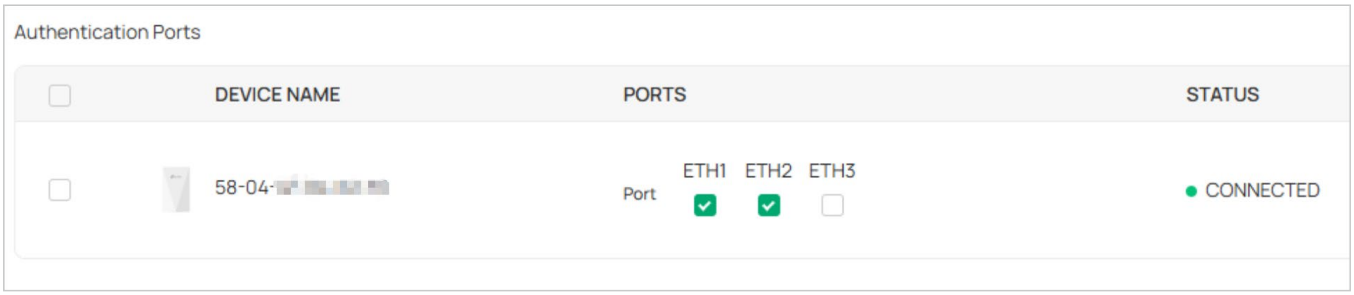
Select the RADIUS profile you have created. If no RADIUS profiles have been created, click Create New RADIUS Profile from the drop-down list or Manage RADIUS Profile to create one. The RADIUS profile records the information of the RADIUS server which acts as the authentication server during 802.1X authentication.



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.

Step 3: Select the Ports

Select the ports to enable 802.1X authentication for them.



18. 3 Configure MAC-Based Authentication

Overview

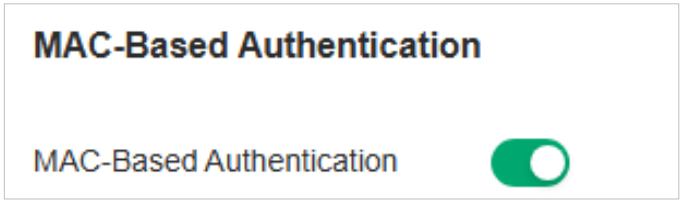
MAC-Based Authentication allows or disallows clients access to wireless networks based on the MAC addresses of the clients. In this authentication method, the Fusion gateway takes wireless clients' MAC addresses as their usernames and passwords for authentication. The RADIUS server authenticates the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

Note:

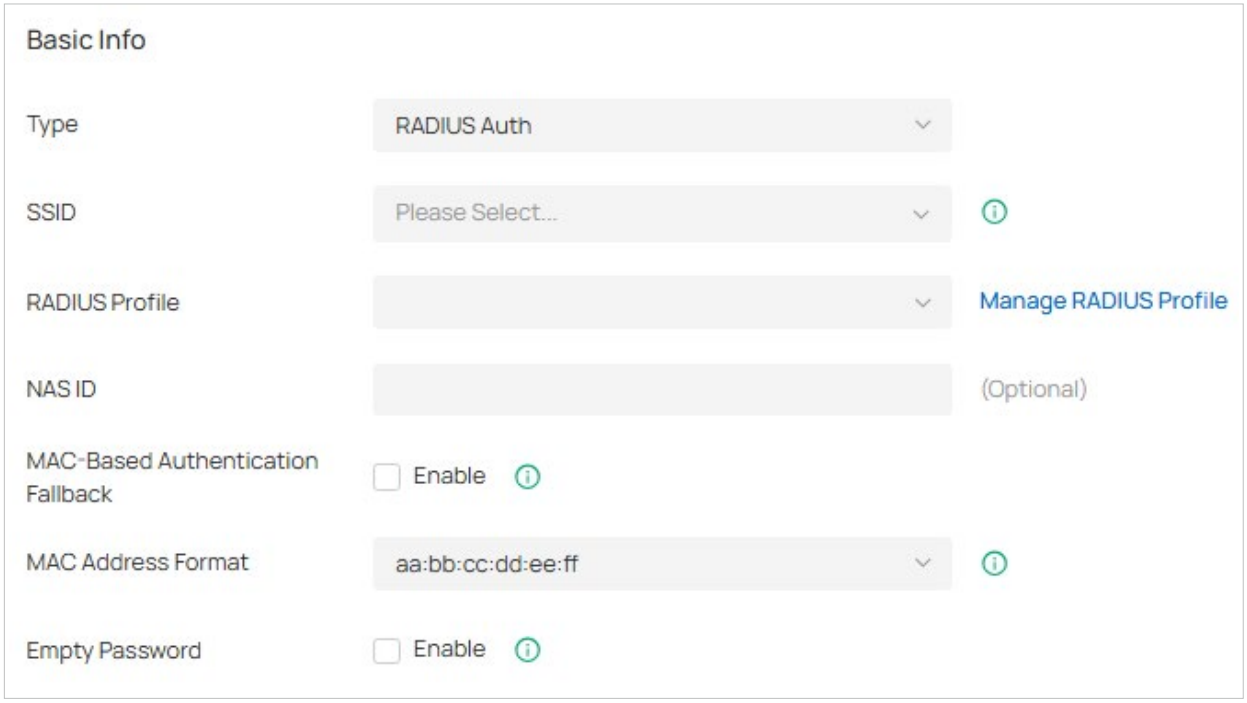
Both MAC-Based Authentication and Portal authentication can authenticate wireless clients. If both are configured on a wireless network, a wireless client needs to pass MAC-Based Authentication first and then Portal authentication for internet access. You can enable MAC-Based Authentication Fallback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

Configuration

1. Go to Network Config > Authentication > MAC-Based Authentication. Click to enable MAC-Based Authentication.



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



Type	Select RADIUS Auth or LDAP Auth for MAC-Based Authentication.
SSID	Select one or more SSIDs for MAC-based authentication to take effect.

RADIUS Auth

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.

LDAP Auth

LDAP Profile	Select the LDAP profile you have created. If no LDAP profiles have been created, click Create New LDAP Profile from the drop-down list or Manage LDAP Profile to create one. The LDAP profile records the information of the LDAP server which acts as the authentication server during MAC-Based 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.

Chapter 19

Configure Network Profiles

Profiles section is used to configure and record your custom settings for application configurations. After creating the profiles, you can apply them to multiply configurations, saving you from repeatedly setting up the same information.

This chapter guides you on how to configure network profiles with the Fusion gateway. The chapter includes the following sections:

19. 1 Create Groups

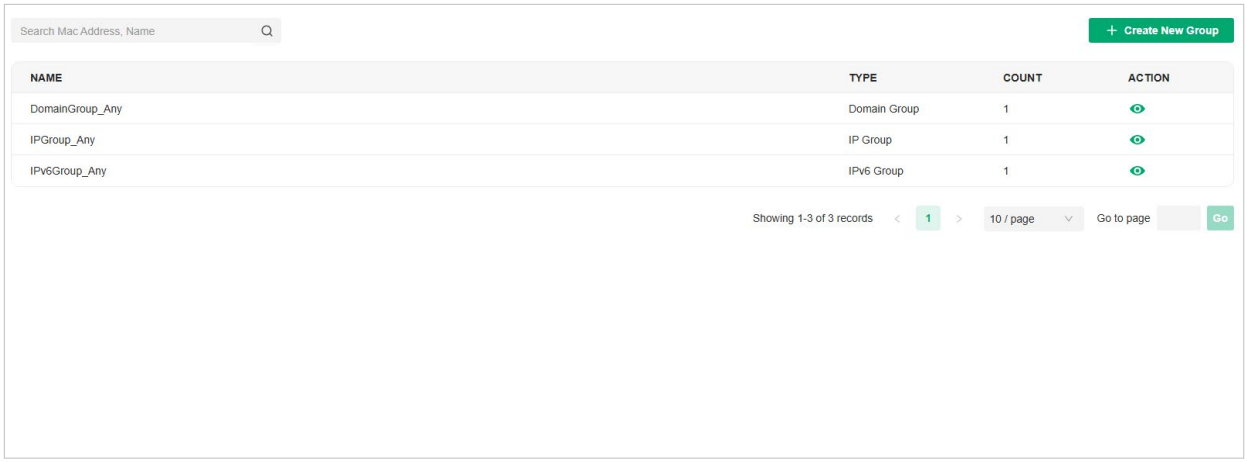
Overview

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

Configuration

To configure the group profiles, follow these steps:

1. Go to Network Config > Profile > Groups.
2. Click Create New Group to add a new group profile.



3. Enter a name, select the type, and configure the corresponding parameters for the new group profile.

- **To create an IP group:**

  Choose the IP Group type and specify IP subnets.

- **To create an IPv6 group:**

  Choose the IPv6 Group type and specify IPv6 addresses.

- **To Create an IP-Port group:**

  Choose the IP-Port Group type and specify the IP-Port type and ports, while it is optional to specify IP subnets. If you only specify ports without entering any IP subnets, it means the group contains the specified ports for all IP addresses.

- **To create an IPv6-Port group:**

  Choose the IPv6-Port Group type and specify the IP-Port type and ports, while it is optional to specify IPv6 addresses. If you only specify ports without entering any IPv6 addresses, it means the group contains the specified ports for all IPv6 addresses.

- **To configure a MAC group:**

  Choose the MAC Group type and add MAC addresses in the MAC Address List.

- **To configure a location group:**

  Choose the Location Group type and select locations. You can enter a description for identification.

- **To configure a domain-port group:**

  Choose the Domian-Port Group type and specify the domain names and ports. You can specify up to 16 domain names for the group. The domain name can be complete, such as www.baidu.com and www.twitter.com; it can also contain wildcards, such as *.google.com, which will match domain names such as www.google.com, pam.google.com and google.com in special cases. Enter one or more ports from 0 to 65535, such as 1,10-20. Empty value means any port.

- **To configure a domain group:**

  Choose the Domian Group type and specify the domain names. You can specify up to 16 domain names for the group. The domain name can be complete, such as www.baidu.com and www.twitter.com; it can also contain wildcards, such as *.google.com, which will match domain names such as www.google.com, pam.google.com and google.com in special cases.

- **To configure an OUI profile group:**

  Choose the OUI Profile Group type and add OUIs in the OUI List.

4. Click Apply to save the entry.

   You can view and edit the list, and export the MAC group if needed. You can apply the customized profiles during application configuration.

19. 2 Create Time Range Profiles

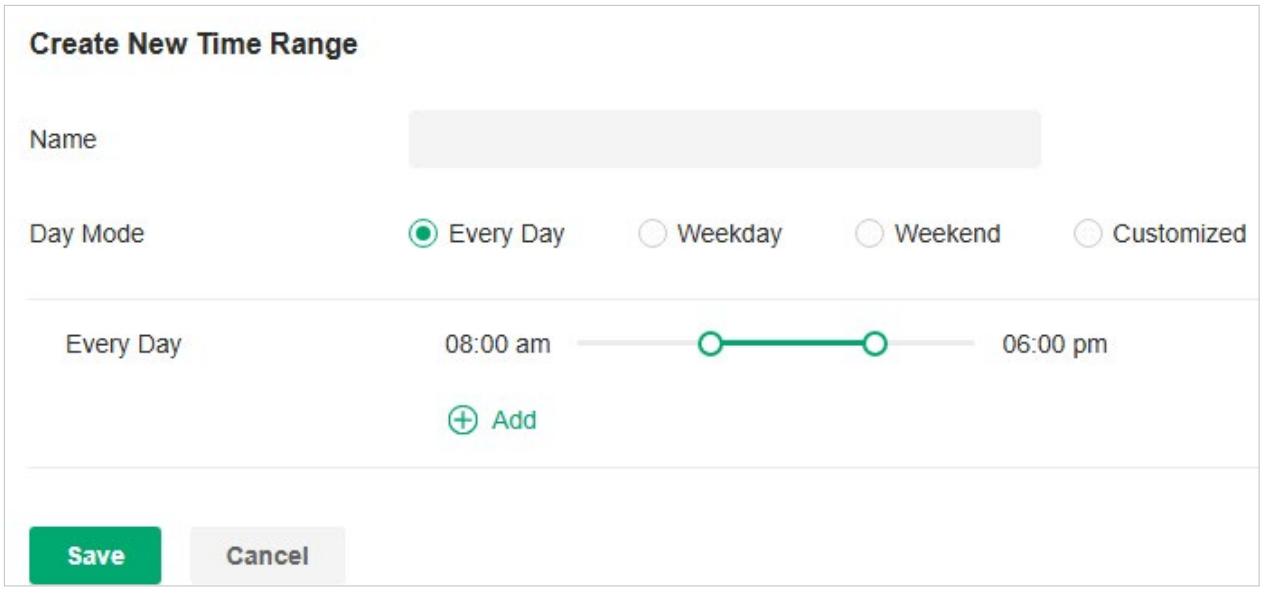
Overview

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.

Configuration

To configure the time range profiles, follow these steps:

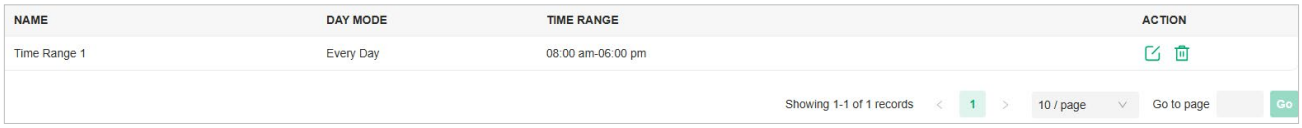
1. Go to Network Config > Profile >Time Range.
2. Click Create New Time Range to add a new time range entry. By default, there is no entry in the list.



3. Enter a Name for the new entry, select the Day Mode, and specify the time range. Click +Add to add a new time period.

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 network is open all day by default.

4. Save the entry. Now you can apply the customized profiles during application configuration.



19. 3 Create Rate Limit Profiles

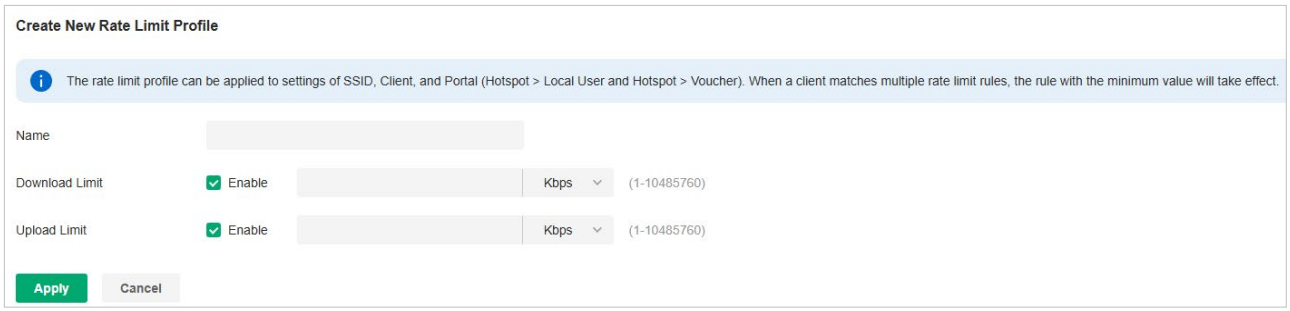
Overview

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. Go to Network Config > Profile > Rate Limit.
2. By default, there is an entry with no limits, and it can not be deleted. You can click Create New Rate Limit Profile to add a new group entry.



3. 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 such as Portal and Wireless Settings.

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.

4. Click Apply to save the entry. Now you can apply the customized profiles during application configuration.

19. 4 Create PPSK Profiles

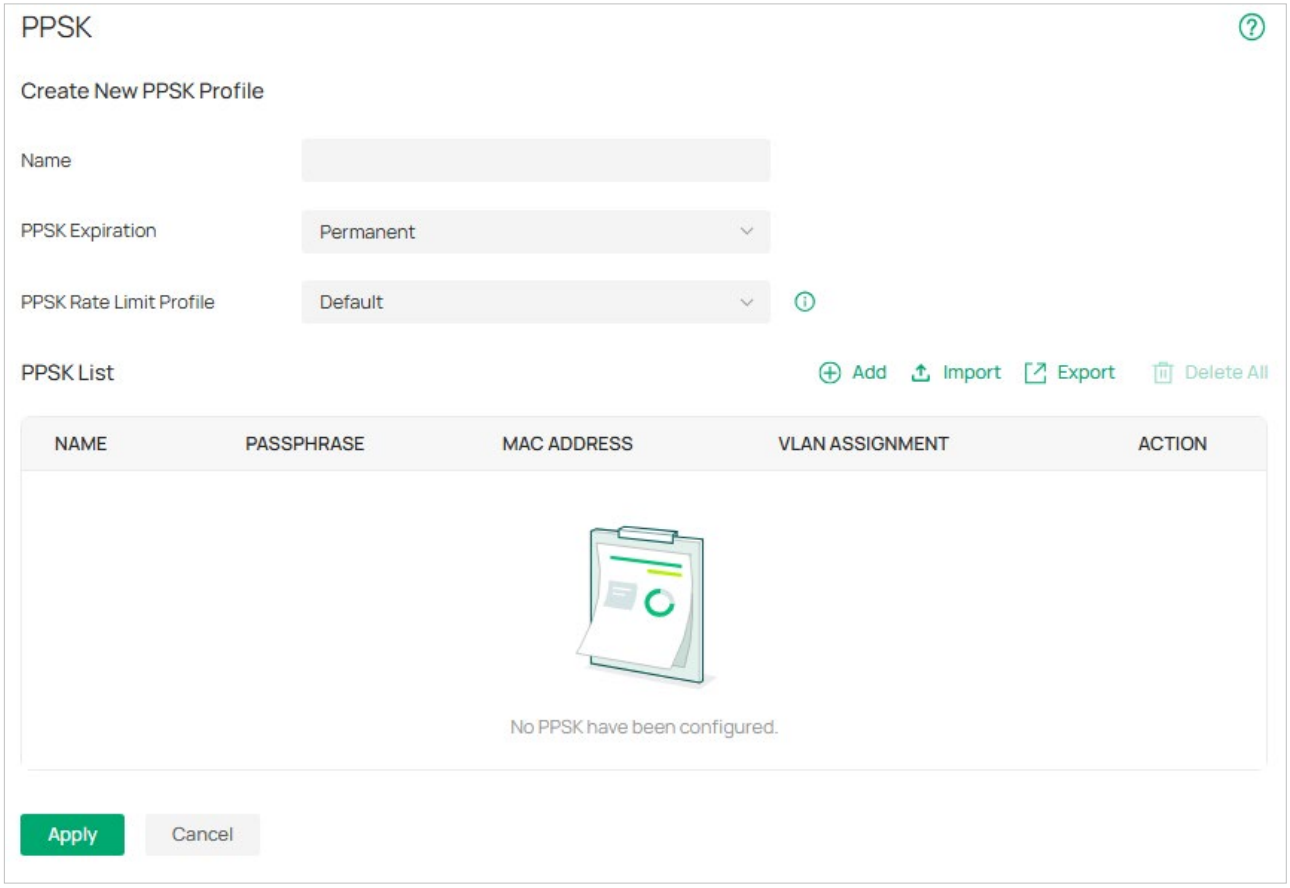
Overview

PPSK is a security solution for you to manage individual client devices 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 a PPSK list and apply it to multiple wireless networks, saving you from repeatedly setting up the same information.

Configuration

To configure the PPSK profiles, follow these steps:

1. Go to Network Config > Profile > PPSK. Click Create New PPSK Profile to add a new PPSK profile .



2. Enter a name for the new profile. Set the PPSK expiration and specify the PPSK Rate Limit Profile.

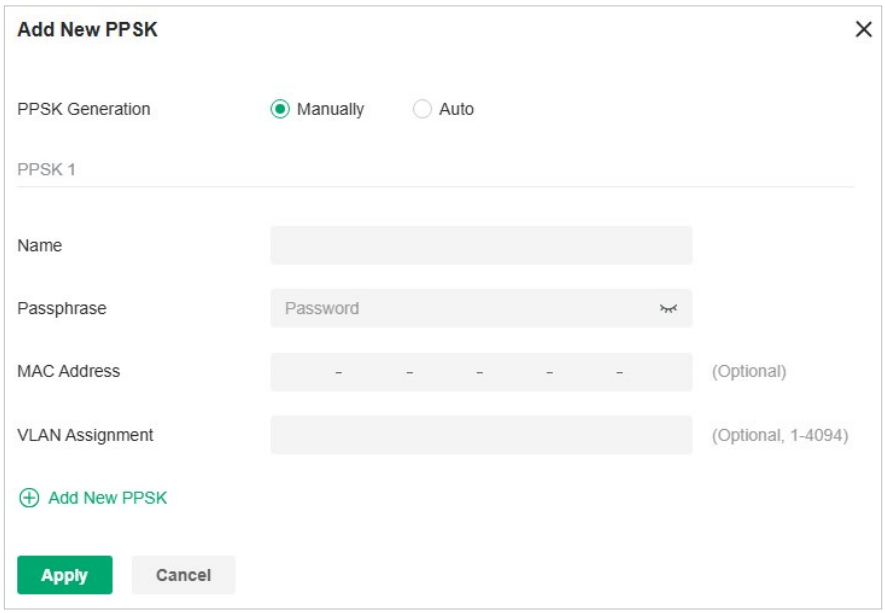
Name	Enter a name to identify the RADIUS entry.

PPSK Expiration	Sets the time range during which clients can access the network via PPSK. Permanent: Clients can permanently access the network via PPSK. Valid Dates: Clients can access the network via PPSK during the specified dates. Start: Time when access begins. End: Time when access ends. Validity Length: Clients can access the network via PPSK for a set time period. Validity After ID Creation: Time when access begins. Daily: Clients can access the network via PPSK during a set time period each day. Start Time: Time when access begins each day. End Time: Time when access ends each day.
PPSK Rate Limit Profile	Specify a profile to limit the upload and download rates of clients accessed via PPSK, ensuring balanced bandwidth usage. You can use the default profile or create a custom one. Download Limit: Set the download rate for each client accessed via PPSK to receive traffic. Upload Limit: Set the upload rate for each client accessed via PPSK to transmit traffic.

3. Add new entries to the PPSK profile.

- **Method 1: Add entries manually**

  Click Add and select Manually for PPSK Generation. Configure the parameters.



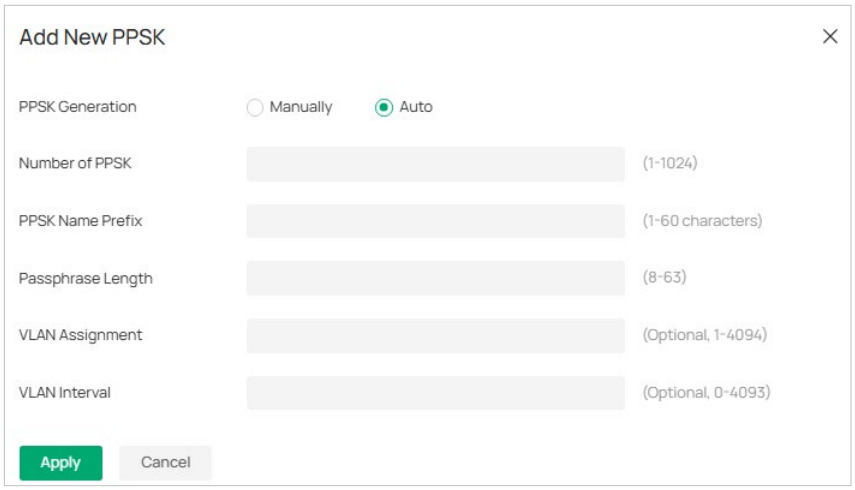
Name	Enter a name to identify the created PPSK.
Passphrase	Enter a passphrase, and the client will use the passphrase for authentication.
MAC Address	(Optional) Enter the MAC address of the device that can use the passphrase for authentication.

VLAN Assignment	(Optional) Enter the VLAN ID, and the client who uses the passphrase for authentication will be assigned to the specified VLAN.

Apply the settings. The new PPSK entry will be created.

- **Method 2: Add entries automatically**

  Click Add and select Auto for PPSK Generation. Configure the parameters and apply the settings.

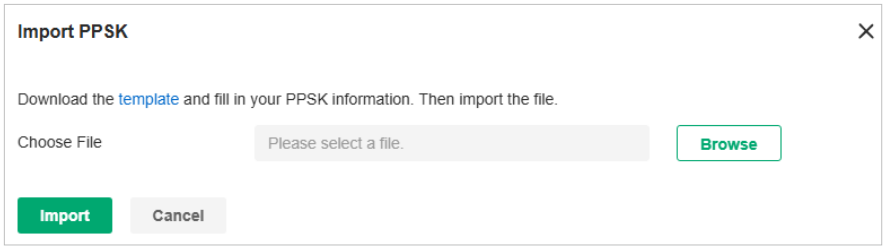


Number of PPSK	Enter the number of PPSK entries to create.
PPSK Name Prefix	Enter the prefix of the names for the created PPSK entries.
Passphrase Length	Enter the passphrase length.
VLAN Assignment	(Optional) Enter the VLAN ID, and the client who uses the passphrase for authentication will be assigned to the specified VLAN.
VLAN Interval	(Optional) Specify the step size between VLAN IDs.

Apply the settings. New PPSK entries will be created automatically.

- **Method 3: Export and Import entries in batch**

  After creating PPSK entries, you can click Export to save them to a file locally, then access another application and click Import to import them in batches from the file.



4. Click Apply to save the entry. Now you can apply the customized profiles during application configuration.

19. 5 Create RADIUS Profile Profiles

Overview

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

In authentication services including 802.1X, Portal and MAC-Based Authentication, compatible 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.

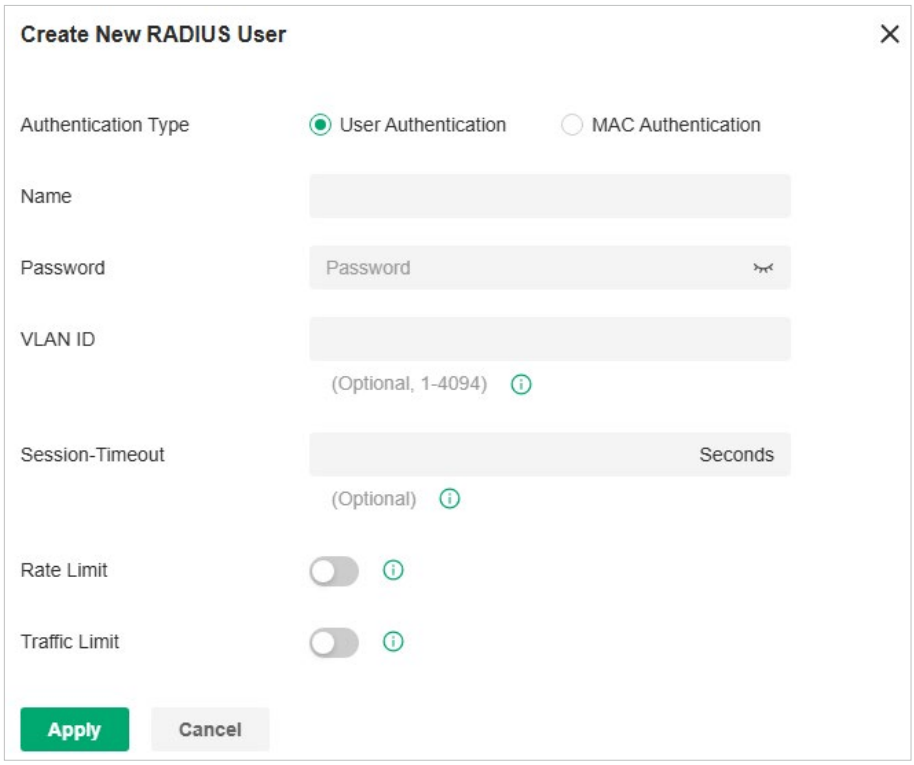
Configuration

- **Configure the Built-in RADIUS Profile**

  a. Go to Network Config > Profile > RADIUS Profile.

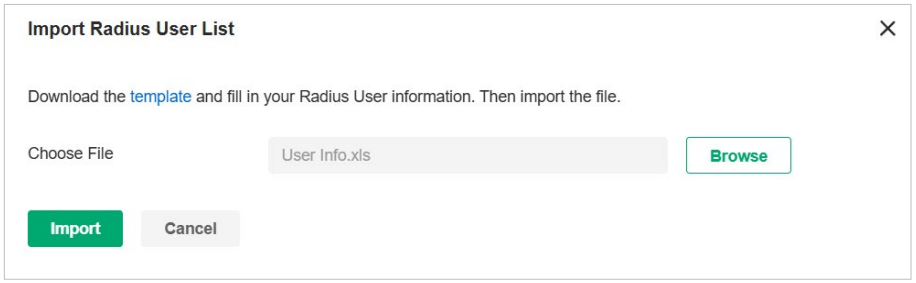
  b. The Fusion gateway provides a Built-in RADIUS Profile. Click the edit icon of the profile, then add or import RADIUS users.

  To add a new RADIUS user, click Add New RADIUS User and configure the parameters.



Authentication Type	Select the Authentication Type. User Authentication: Select this option and enter the user Name and Password for authentication. MAC Authentication: Select this option and enter the MAC Address for authentication.
VLAN ID	Enter a VLAN ID to assign VLANs to users.
Session-Timeout	Configure the authentication expiration time for users.
Rate Limit	When enabled, you can set limits for Uplink Rate and Downlink Rate of each client to balance bandwidth usage. This function applies to the portal service only.
Traffic Limit	When enabled, you can set limits for Uplink Traffic and Downlink Traffic of each client. This function applies to the portal service only.

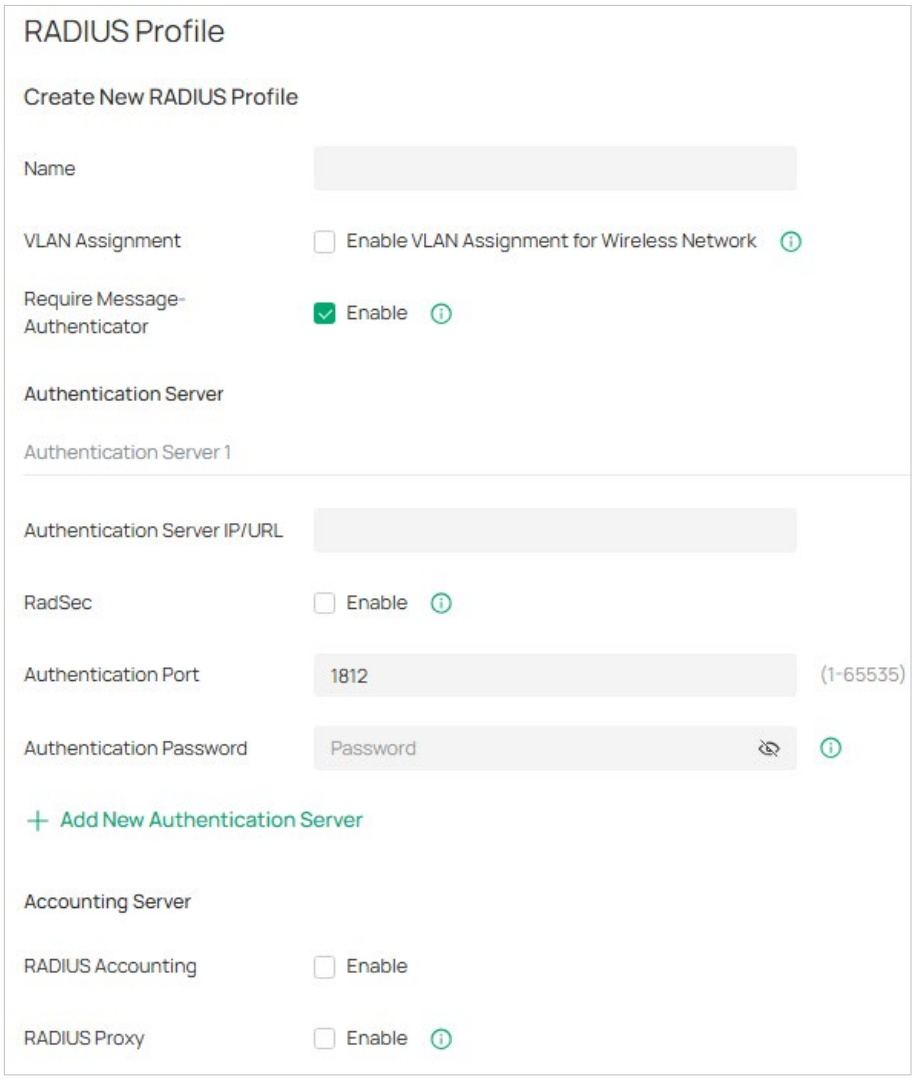
To import RADIUS users in batches, click Import, download the template and fill in your Radius User information. Then import the file.



- **Create New RADIUS Profile**

a. Go to Network Config > Profile > RADIUS Profile.

b. Click Create New RADIUS Profile. Configure the parameters and save the settings.



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.
Require Message-Authenticator	When enabled, the Client verifies the Message-Authenticator field in requests to enhance authentication security. Please ensure the server supports Message Authenticator.
Authentication Server IP/URL	Enter the IP/URL address of the authentication server.

RadSec	RadSec secures RADIUS communications. If enabled, a TLS-encrypted transmission tunnel will be established between the client and the RADIUS server to transmit RADIUS messages. RadSec 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. If there are old devices in the device list that do not support this feature, it is recommended to configure a backup server that is not enabled with this feature.
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 network 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 APs 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, network 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/ URL	Enter the IP/URL 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 network devices and the RADIUS accounting server.
Radius Proxy	With this option enabled, the Controller will act as a proxy to forward the device's authentication messages to the corresponding RADIUS server.
RADIUS CoA	If enabled, TP-Link devices will act as a RADIUS Dynamic Authorization Server and will respond to RADIUS Change-of-Authorization and Disconnect messages sent by the RADIUS servers. This option is only supported by AP PPSK, AP MAC-Based Authentication, and AP WPA-Enterprise.
CoA Password	CoA password is used to authenticate CoA and Disconnect messages sent by the RADIUS servers. The password must be the same as the secret used by RADIUS servers to send the CoA and Disconnect messages.

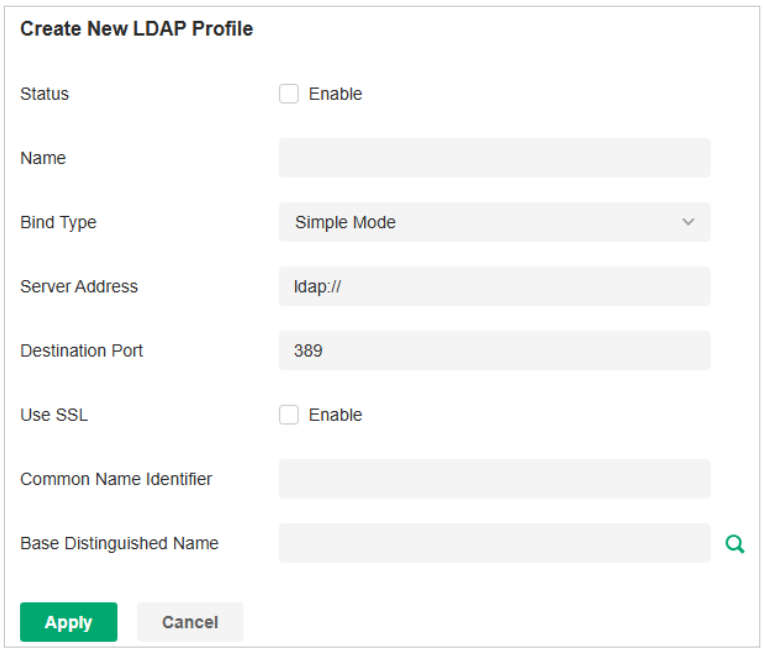
19. 6 Create LDAP Profiles

Overview

The Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for maintaining and accessing directory information over a network. LDAP Authentication allows you to bind the device to an LDAP server and use that server to authenticate LAN clients. Google LDAP profile is designed for use with Google Workspace's Secure LDAP.

Configure a Common LDAP Profile

1. Go to Network Config > Profile > LDAP Profile.
2. Click Create New LDAP Profile to add a new profile .



3. Configure the parameters.

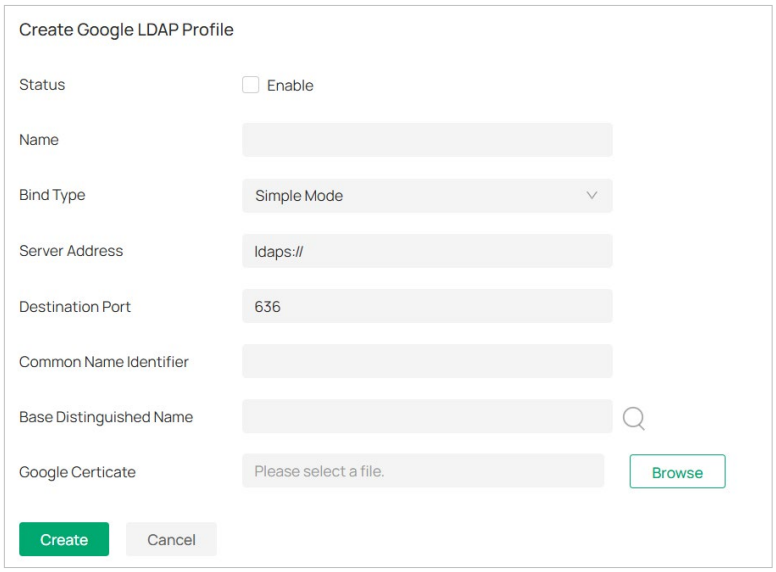
Status	Check the box to enable LDAP Authentication.
Name	Specify the profile name.
Bind Type	Select the LDAP Authentication mode: Anonymous Mode, Simple Mode, or Regular Mode.
Server Address	Enter the IP address of the LDAP server.
Destination Port	Enter the port ID of the LDAP server. By default, the port ID is 389 when SSL is disabled and 636 when SSL is enabled.
Use SSL	Determine whether to use SSL for LDAP communication.

Regular DN	Specify the distinguished name (DN) of the administrator account. This parameter is required in Regular mode.
Regular Password	Specify the password of the administrator account. This parameter is required in Regular mode.
Common Name Identifier	Specify the common name for user authentication. It is usually “cn”. Determine based on the actual situation of the directory.
Base Distinguished Name	Specify the user identifier for user authentication. You can click the icon next to it to search and select from the LDAP directory tree.
Additional Filter	Specify the filter for user authentication. It is not supported in Simple Mode and is optional in other modes.
Group Distinguished Name	Specify the group identifier for user authentication. It is not supported in Simple Mode and is optional in other modes.

4. Click Apply to save the profile. Now you can select the predefined entry of LDAP profile when configuring rules of related modules like LDAP Server.

Configure a Google LDAP Profile

1. Download the Google Certificate.
   a. Sign in to your Google Admin console.
   b. Go to Apps > LDAP.
   c. Select a client.
   d. Click the Authentication card.
   e. Click GENERATE NEW CERTIFICATES.
   f. Download the certificate from the Certificates window.
2. Go to Network Config > Profile > LDAP Profile > Google LDAP Profiles.
3. Click Create Google LDAP Profile to add a new profile .



4. Configure the parameters.

Status	Check the box to enable LDAP Authentication.
Name	Specify the profile name.
Bind Type	Select the LDAP Authentication mode: Simple Mode or Regular Mode.
Server Address	Enter the IP address of the LDAP server.
Destination Port	Enter the port ID of the LDAP server. By default, the port ID is 636.
Common Name Identifier	Specify the common name for user authentication. It is usually “uid”. Determine based on the actual situation of the directory.
Base Distinguished Name	Specify the user identifier for user authentication. You can click the icon next to it to search and select from the LDAP directory tree.
Google Certificate	Upload the Google certificate you downloaded.

5. Click Apply to save the profile. Now you can select the predefined entry of LDAP profile when configuring rules of related modules like LDAP Server.

19. 7 Configure APN Profiles

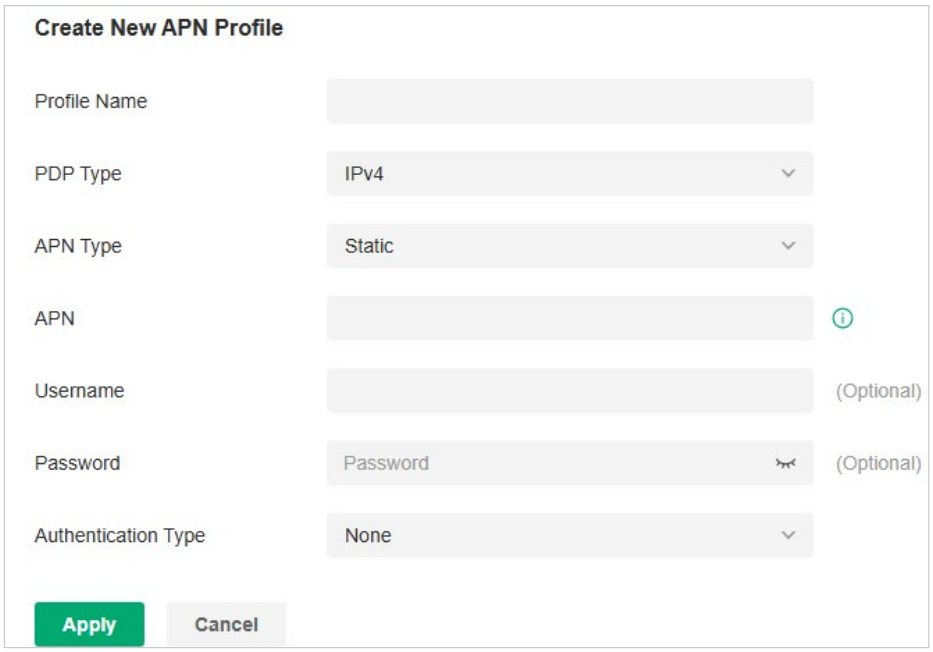
Overview

APN is a network access technology required when using the SIM card to access the internet. It determines which access method the SIM card uses to access the internet.

Configuration

To configure the APN profiles, follow these steps:

1. Go to Network Config > Profile > APN Profile.
2. Click Create New APN Profile to add a new profile .



3. Configure the parameters.

Profile Name	Specify the name of the profile.
PDP Type	Select the PDP (Packet Data Protocol) type: IPv4, IPv6, or IPv4 & IPv6.
APN Type	Select the APN type: Static or Dynamic.
APN	When APN Type is Static, specify the APN (access point name) provided by your ISP.
Username	Enter the username provided by your ISP. This field is case-sensitive.
Password	Enter the password provided by your ISP. This field is case-sensitive.

Authentication Type	Some ISPs need a specific authentication type, please confirm it with your ISP or keep the default value. None: No authentication is required. PAP: Password Authentication Protocol. The protocol allows a device to establish authentication with a peer using a two-way handshake. Select this option if your ISP requires this authentication type. CHAP: Challenge Handshake Authentication Protocol. The protocol allows a device to establish authentication with a peer using a three-way handshake and periodically checking the peer's identity. Select this option if your ISP requires this authentication type.

4. Click Apply to save the profile. Now you can select the predefined entry of APN profile when configuring rules of related modules.

19. 8 Configure Certificate Profiles

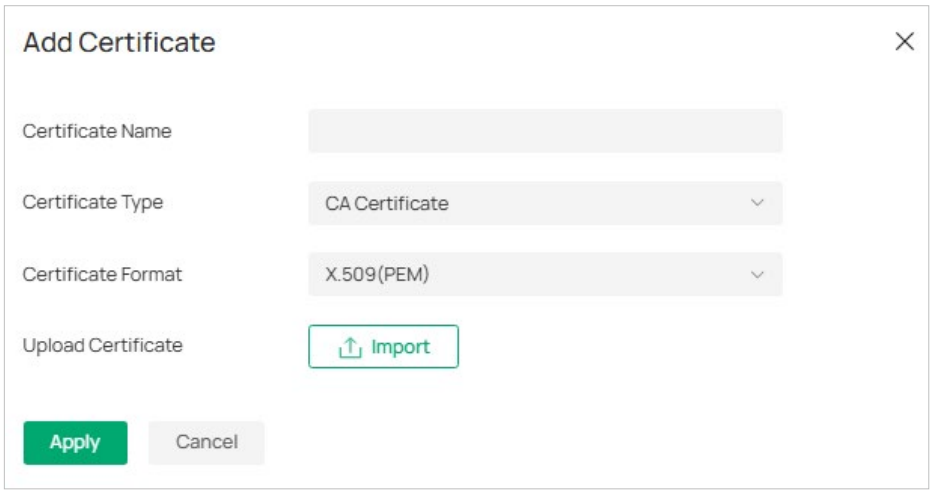
Overview

In the Certificate Profile, you can add and manage CA certificates, client certificates, client private keys and passwords. After adding a certificate profile, you can apply it when configuring features requiring this certificate, saving you from repeated uploads. For example, after adding a CA certificate profile, you can enable RADSEC and select this profile when configuring RADIUS servers to quickly bind this certificate.

Configuration

To configure the certificate profiles, follow these steps:

1. Go to Network Config > Profile > Certificate Profile.
2. Click Add Certificate to add a new certificate.



3. Configure the parameters.

Certificate Name	Specify the name of the certificate.
Certificate Type	Select the type of the certificate. CA Certificate: The CA certificate or self-signed certificate. Client Certificate: The certificate issued by CA or generated locally and sent to the server for identity authentication. Select this option after enabling two-way authentication.
Client Private Key	When the Client Certificate type is selected, click to import the client private key file. The key will be used to encrypt information in the certificate verification message, and the server will use the public key in the client certificate for authentication and decryption.
Password	If the Client Private Key is encrypted, enter the Client Private Password for parsing.

Certificate Format	Select the format of the certificate. The CA certificate supports the X.509(PEM) and X.509(DER) formats. Other certificates only support the X.509(PEM) format.
Upload Certificate	Click to import the certificate file.

4. Click Apply to save the certificate profile.

Chapter 20

Configure the SD-WAN

This chapter will introduce how to configure the SD-WAN to easily connect multiple gateways of sites.

It includes the following sections:

20. 1 Introduction to SD-WAN

Omada SD-WAN (Software-Defined Wide Area Network) connects your branch networks through secure, automated tunnels with centralized cloud management and high reliability. Now you can choose a SD-WAN type that fits your network deployment.

- **Fast Deployment**

  Create a Full Mesh or Hub-Spoke SD-WAN linking all your sites in just a few clicks — no manual VPN setup required.

- **Secure & Reliable**

  Build encrypted site-to-site tunnels with centralized management and guaranteed reliability.

- **License-Free Cloud Management**

  Manage, monitor, and maintain your WAN from the Omada Cloud — with no recurring fees or complex setup.

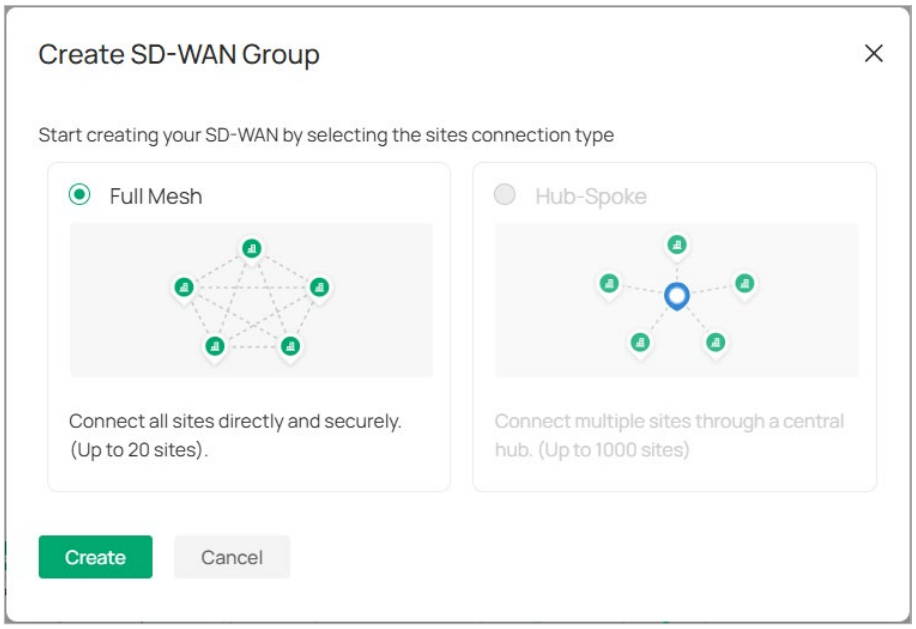
Requirements

To use SD-WAN, ensure the following:

- At least one gateway in your network is configured with a public IP address.
- The WAN networks of the gateways have not enable DMZ.
- The network segments in the network do not conflict with each other or the LAN of other sites.

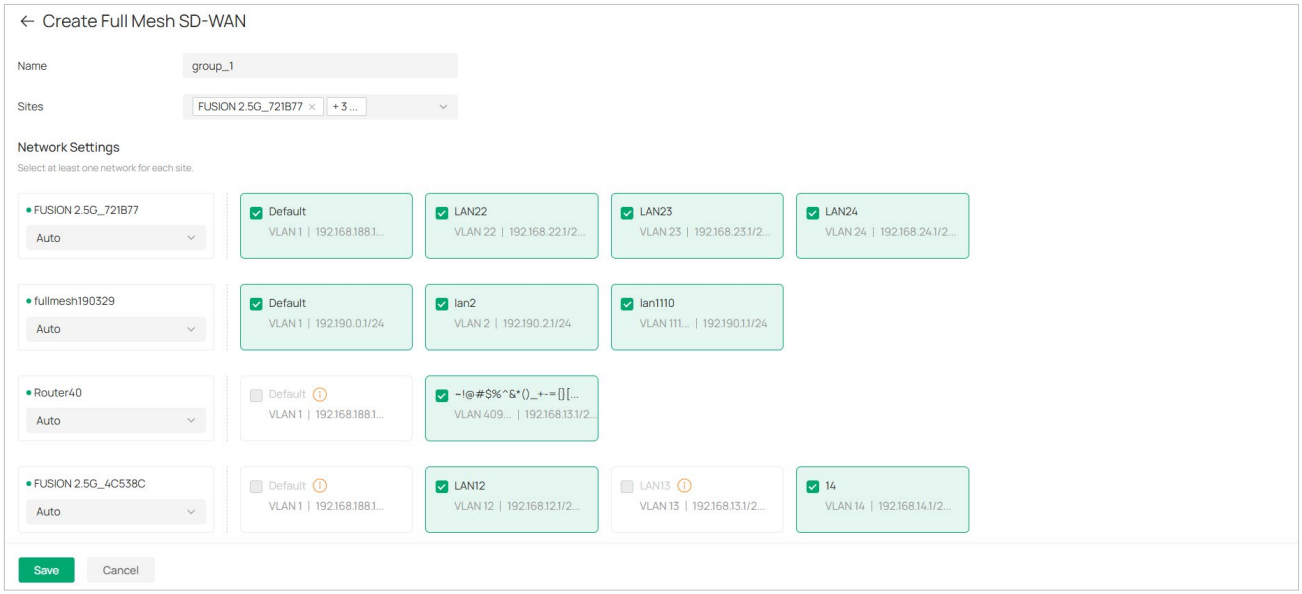
20. 2 Configure the SD-WAN

1. Launch a web browser and enter https://omada.tplinkcloud.com in the address bar. Enter your TP-Link ID and password to log in.
2. Select Fusion Systems from the drop-down list in the top left. Go to SD-WAN.
3. Create a SD-WAN group.
4. Select the site connection type, then click Create. Currently only Full Mesh SD-WAN is supported.

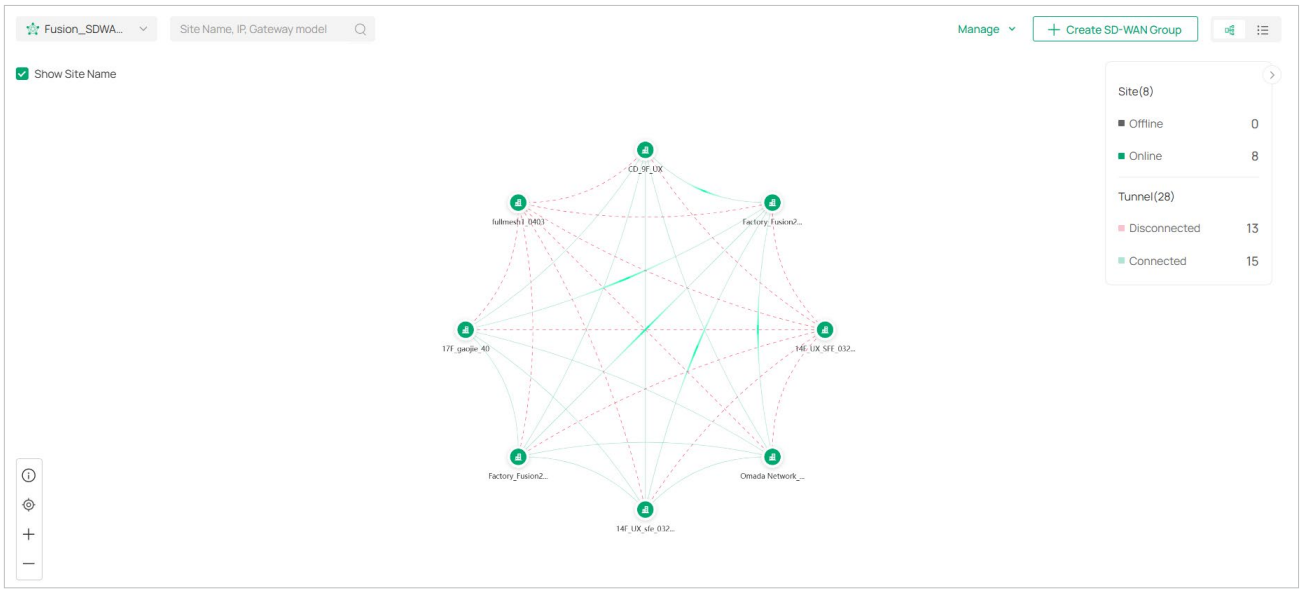


Full Mesh	All sites connect to each other directly with branch-to-branch communication, reducing latency for voice/video and enhancing performance, ideal for decentralized architectures.
Hub-Spoke	A hub on the core site connects all spokes and responsible for network control, routing, and traffic forwarding. This simplifies security policy management but introduces latency and potential bottlenecks.

5. Specify the group name, select the sites to connect, then select at least one network for each site.

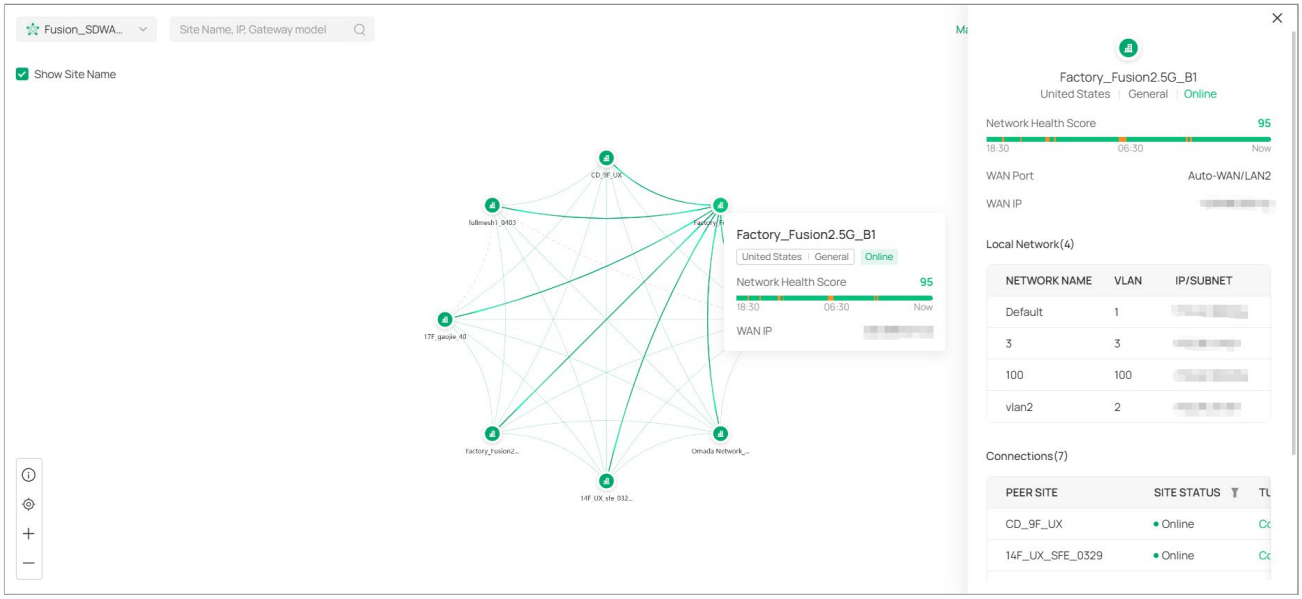


6. Save the settings. The SD-WAN group will be displayed.



Show Site Name	Check the box to show the site names or deselect the box to hide the site names.
	Click to view the map legend, fit the map to the screen, zoom in/out the map.
Manage	Click to edit or delete the group.
Create SD-WAN Group	Click to add a new group.
	Click to switch between the topology and list views.

You can hover your mouse over a site to view its basic information, or click a site to view more details.



Chapter 21

Configure the Hotspot

This chapter guides you on how to configure the hotspot. This chapter includes the following sections:

21. 1 Overview

Hotspot is a portal management system for centrally monitoring and managing the clients authorized by portal authentication.

To access the system, go to Hotspot.

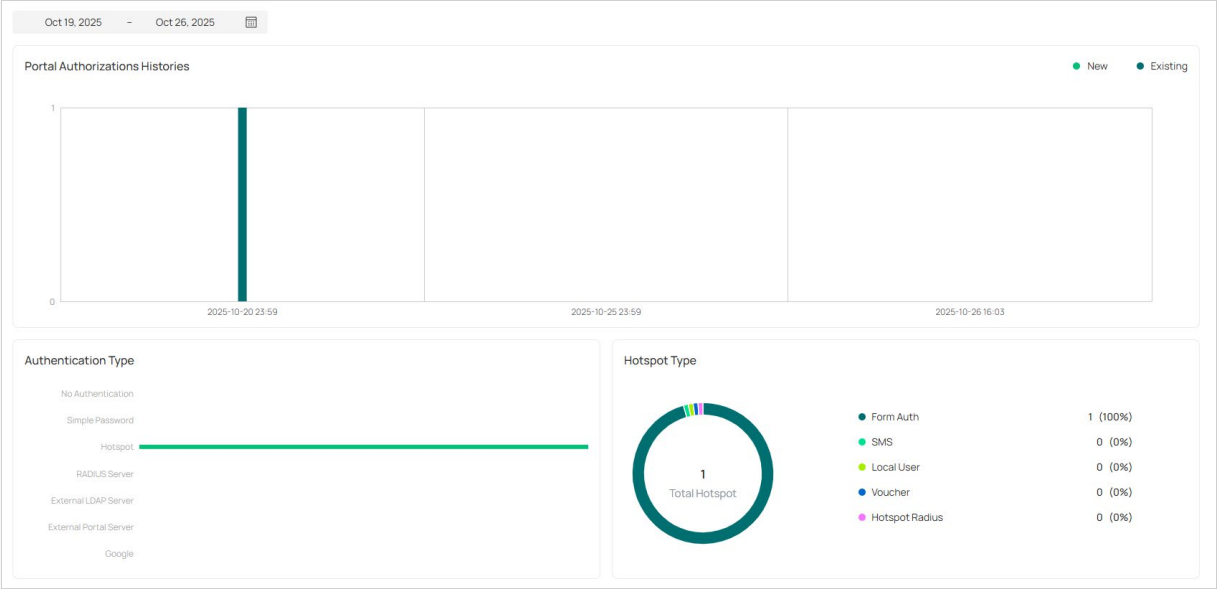
The following tabs are provided in the system for a easy and direct management.

Dashboard	Monitor portal authorizations at a glance through different visualizations.
Authorized Clients	View the records of the connected and expired portal clients.
Vouchers	Create vouchers for Portal authentication, and view and manage the related information.
Local Users	Create local user accounts for Portal authentication, view their information, and manage them.
Form Auth Data	Customize your survey contents and publish it to collect data.
Operators	Create operator accounts for Hotspot management, view their information, and manage them.

21. 2 Dashboard

In the Dashboard, you can monitor portal authorizations at a glance through different visualizations.

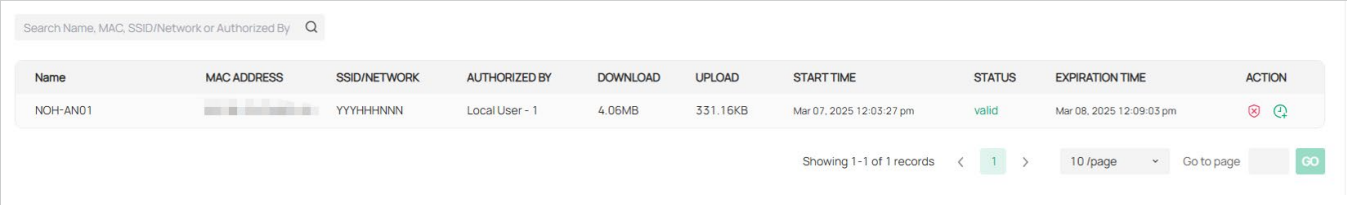
To open the dashboard, click Hotspot in the sidebar, then click Dashboard. Specify the time period to view portal authorization histories.



21. 3 Authorized Clients

The Authorized Clients tab is used to view and manage the clients authorized by portal system, including the expired clients and the clients within the valid period.

To open the list of Authorized Clients, click Hotspot in the sidebar, then click Authorized Clients. You can search certain clients using the search box, view their detailed information in the table, and manage them using the action column.



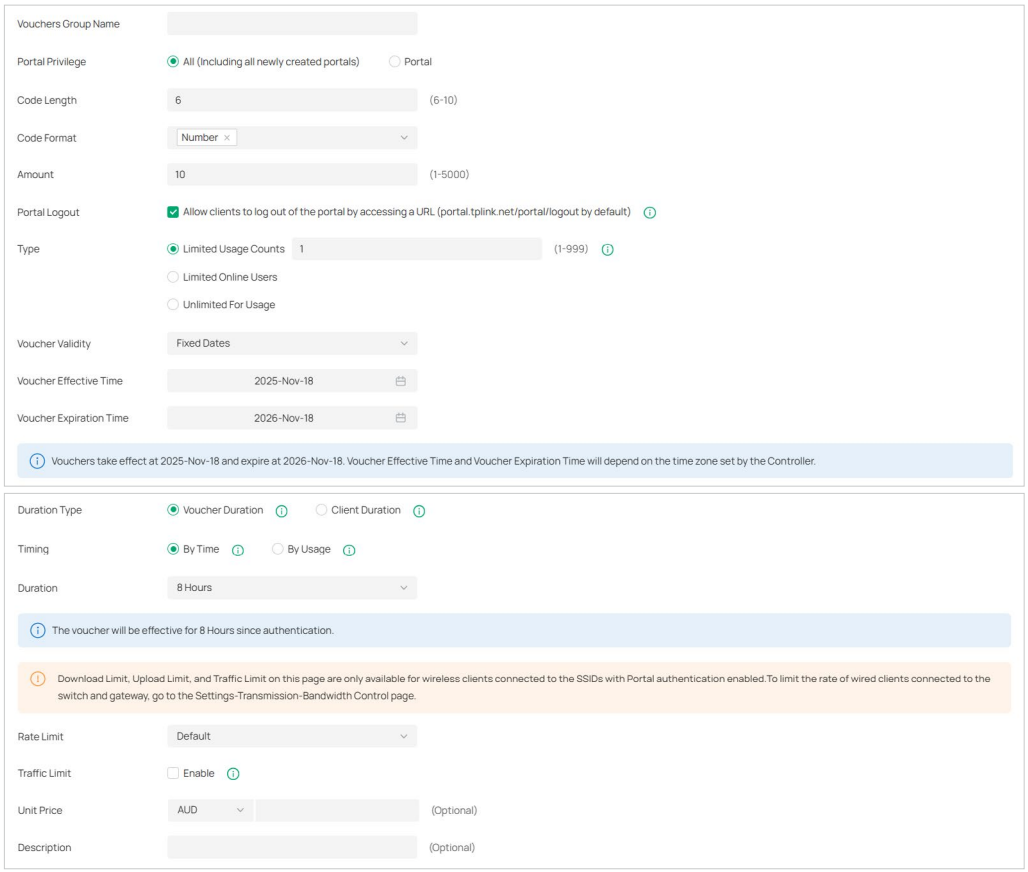
	Click to extend the valid period of the authorized client. You can choose the preset time length or set a customized period based on needs.
	Click to disconnect the authorized client(s). If you disconnect an authorized client, the client needs to be re-authenticated for the next connection.
	Click to delete the expired client from the list.

21. 4 Vouchers

The Vouchers tab is used to create vouchers and manage unused voucher codes. With voucher configured and codes created, you can distribute the voucher codes generated by the controller to clients for them to access the network via portal authentication.

Follow the steps below to create vouchers for authentication:

1. Click Hotspot in the sidebar, then click Vouchers > Voucher Groups.
2. Click Create Vouchers Group on the upper-right.
3. Configure general voucher settings and click Save.

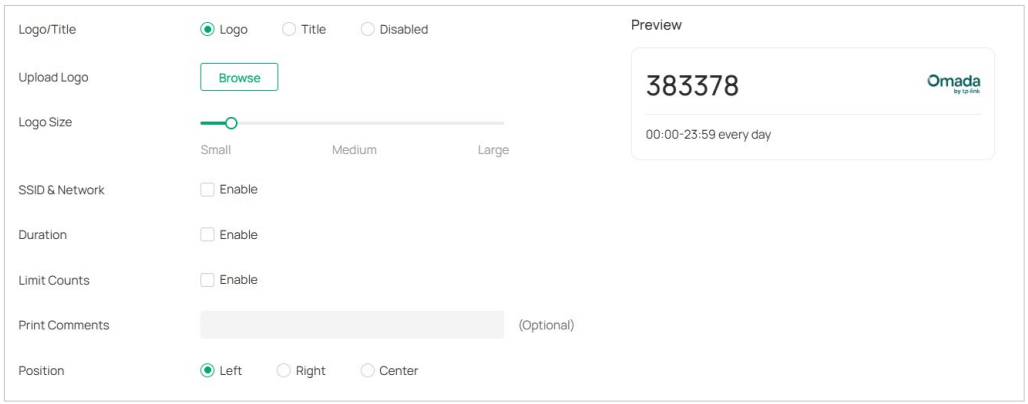


Vouchers Group Name	Enter a name to identify the group.
Portal Privilege	All: The vouchers will take effect for all voucher type portals, including newly created ones. Portal: Select the portal for which the vouchers will take effect.
Code Length	Specify the length of the code(s) from 6 to 10 digits.
Code Format	Choose whether the voucher code is generated by numbers, letters, or a mixture.
Amount	Specify the number of voucher codes you want to create.

Portal Logout	Check the box to allow clients to log out of the portal by accessing a URL (portal.tplink.net/portal/logout by default). You can change the default URL by editing Portal Logout Domain in Settings > System Settings > Access Config. Some devices may require firmware update to support Portal Logout. Please refer to Configuration Result for details.
Type	Select a type to limit the usage counts or the number of authorized users of a voucher code. Limited Usage Counts: The voucher code can only be used for a limited number of times within its valid period. Limited Online Users: The voucher code can be used for an unlimited number of times within its valid period, but only a limited number of wireless clients can access the network with this voucher code at the same time. Unlimited For Usage: The voucher code can be used for an unlimited number of times within its valid period.
Voucher Validity	Specify the validity of vouchers in the group: Permanent: Vouchers will be valid permanently. Fixed Dates: Vouchers will be valid during the start and end dates you specify. Scheduled: Vouchers will be valid according to the schedule you set.
Duration Type	Specify whether to limit the voucher duration or client duration. Voucher Duration: Configure the duration for the voucher. Clients can use the voucher for the specified time duration (e.g., 8 hours after the first use). After reaching the voucher duration, the voucher will expire whether used or not. Client Duration: Configure the duration for the client. The client can use vouchers for the specified time duration (e.g., 8 hours after the first use). After reaching the client duration, the client will expire and cannot use the vouchers to access the network.
Timing	By time: The voucher code takes effect within a fixed period of time after authentication. By Usage: The voucher code takes effect according to the actual time used by the client.
Duration	Select the valid period for the voucher code(s).
Rate Limit	Select an existing rate limit profile, create a new rate limit profile or customize the rate limit for the voucher codes. Custom: Specify the download/upload rate limit based on needs. Download/Upload Limit: Click the checkbox and specify the rate limit for download/upload for wireless clients using the voucher code(s). The value of the download and upload rate can be set in Kbps or Mbps. **Note:** Rate Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to Network Config >Traffic Management > Gateway QoS > Bandwidth Control.

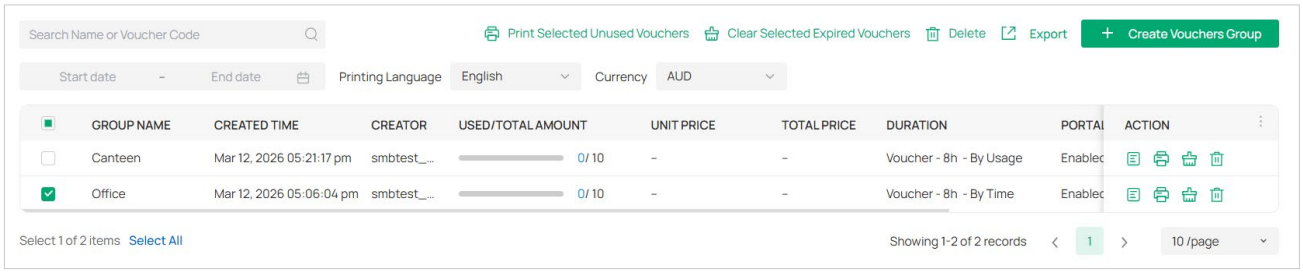
Traffic Limit	Click the checkbox and specify the daily/weekly/monthly/total traffic limit for the voucher, and the value of the traffic limit can be set in MB or GB. Once the limited is reached, the client(s) can no longer access the network using the voucher. **Note:** Traffic Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to Network Config >Traffic Management > Gateway QoS > Bandwidth Control.
Unit Price (Optional)	Set the amount and currency type for the voucher (for statistical purposes only).
Description (Optional)	Enter notes for the created voucher code(s), and the input description is displayed in the voucher list under the voucher tab.

4. Configure voucher pattern settings, preview it, then click Save.



Logo/Title	Choose whether to display a logo or title on the vouchers. Logo: Upload a logo and adjust its size to display the logo on the vouchers. Title: Enter a title and adjust its size to display the title on the vouchers. Disabled: No logo or title will be displayed on the vouchers.
SSID & Network	Enable this option and select the SSID or network to display if needed.
Duration	Enable this option to display the voucher validity duration if needed.
Limit Counts	Enable this option to display the voucher limit counts if needed.
Print Comments	Enter print comments if needed and the comments will be printed when you print the created voucher codes.
Position	Choose the position to display the voucher code.

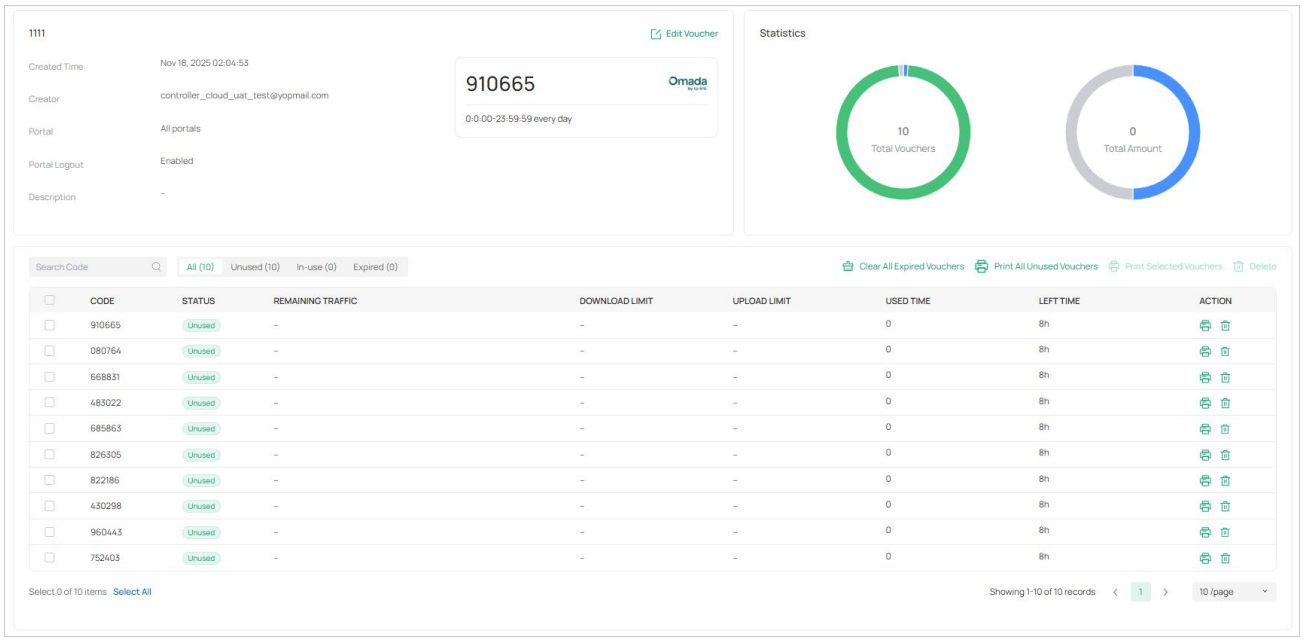
5. The voucher group is generated.



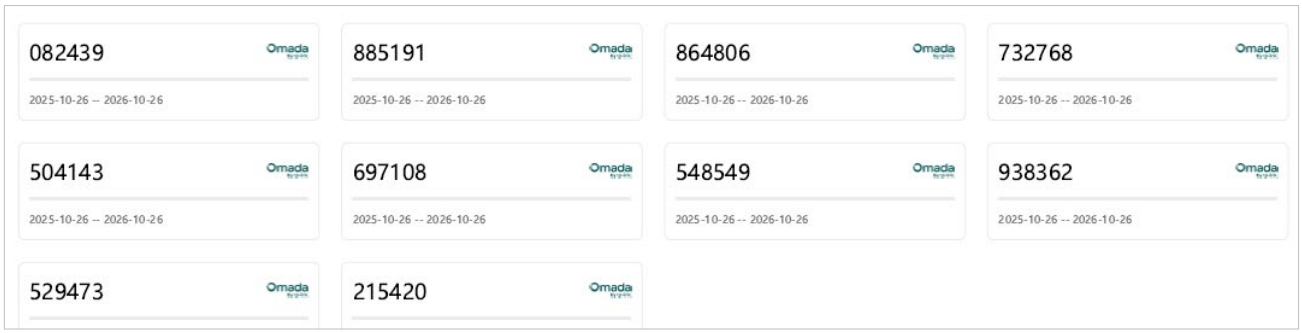
2	The voucher code can be used for an unlimited number of times within its valid period, but only a limited number of wireless clients can access the internet with this voucher code at the same time. The number on the right shows the limited number of users.
2	The voucher code can only be used for a limited number of times within its valid period. The number on the right shows the limited number of authentication times.

In the voucher group list, you can:

- Click the Details icon in the Action column to view the voucher codes. If you want to change the voucher pattern settings, click Edit Voucher.

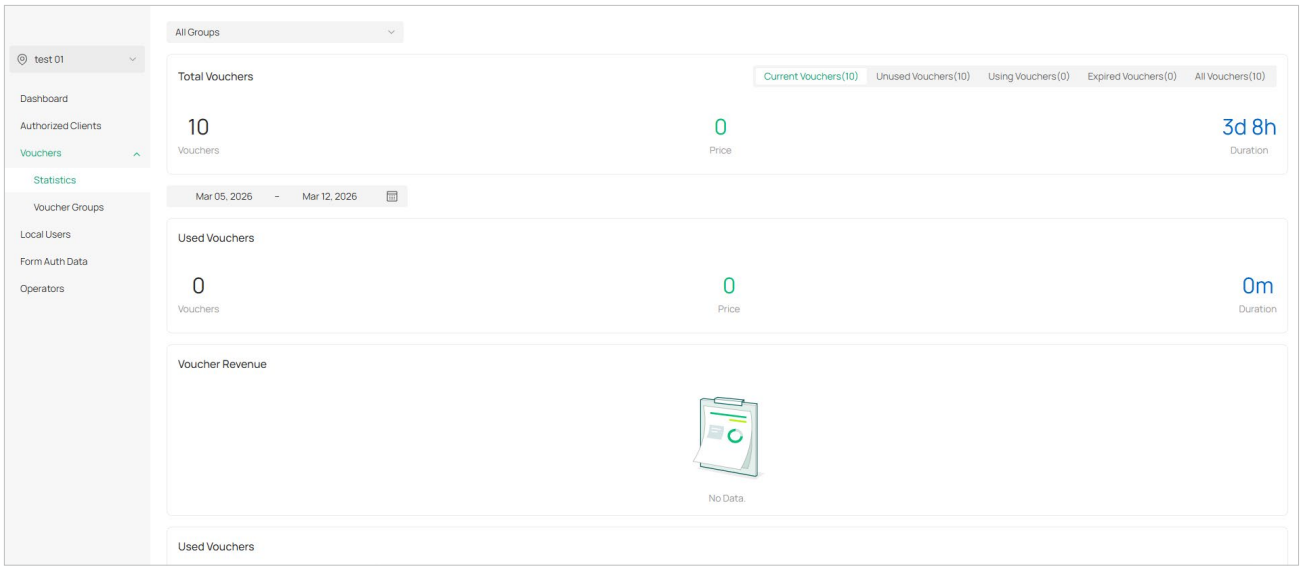


- Click the Print icon to print unused vouchers of a voucher group, or select multiple voucher groups and click Print Selected Unused Vouchers for print them in batches.



- Click the Clear icon to clear expired vouchers of a single group, or select multiple groups and click Clear Selected Expired Vouchers for batch clear.
- Click the Delete icon to delete a single group, or select multiple groups and click Delete for batch delete.
- Select multiple groups and click Export Vouchers to export their vouchers.

6. Distribute the vouchers to clients, and then they can use the codes to pass authentication. If a voucher code expires, it will be automatically removed from the list.
7. Go to the Vouchers > Statistics page. You can select All Groups or a specific group from the drop-down list to view voucher statistics.



21. 5 Local Users

The Local Users tab is used to create user accounts for authentication. With the Local User configured, clients are required to enter the username and password to pass the authentication. You can create multiple accounts and assign them to different users.

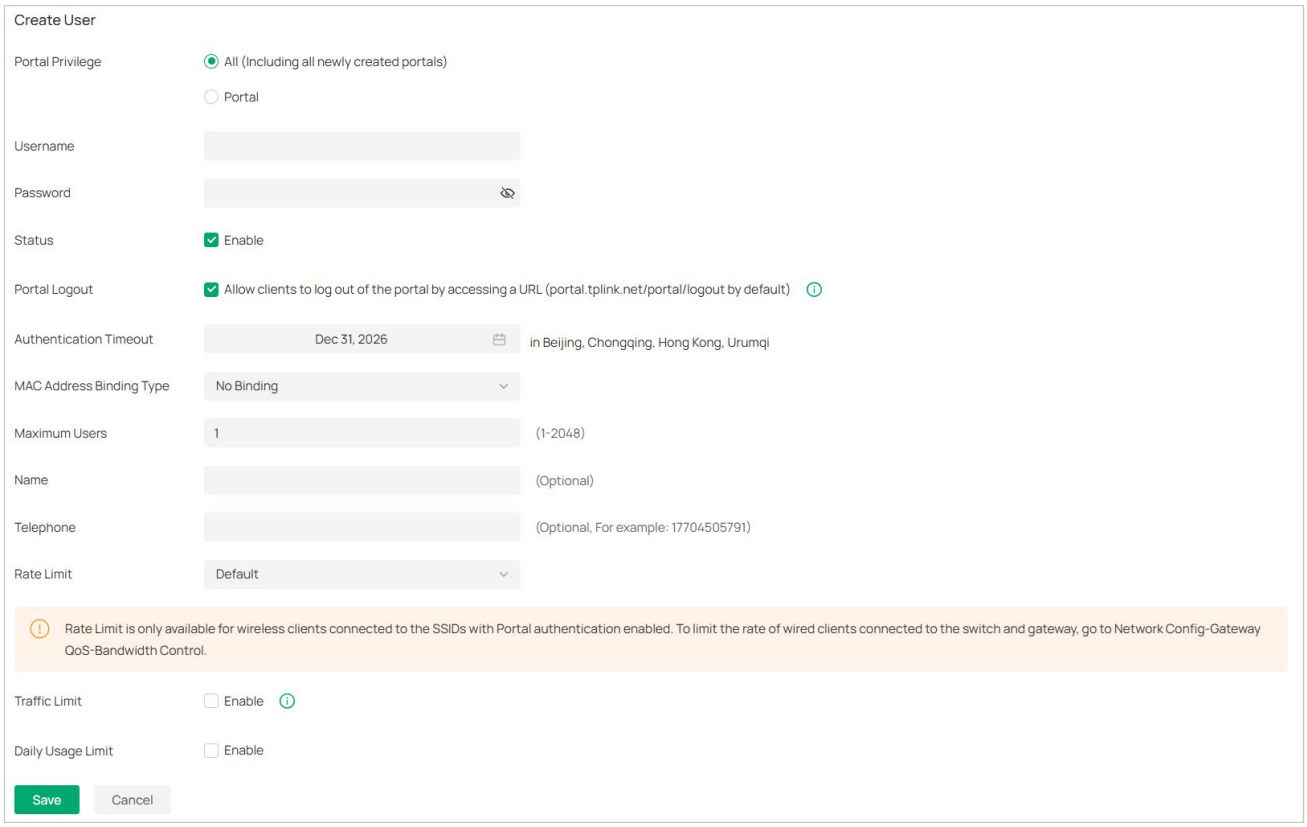
There are two ways to create local user accounts: create accounts on the page and import from a file.

To create local user accounts, follow the steps below.

1. Click Hotspot in the sidebar, then click Local Users.
2. Create Local User accounts through either of the following ways.

- **Create Local User accounts**

  Click Create User on the upper-right, and the following window pops up. Configure the following parameters and click Save.



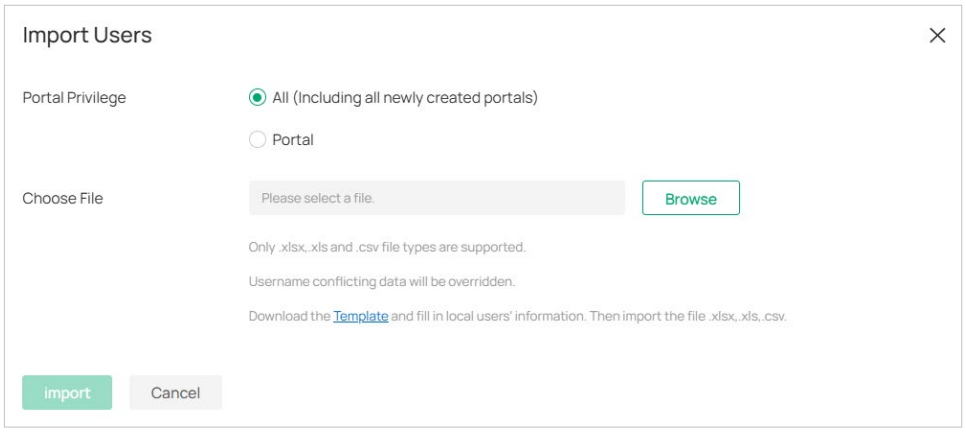
Portal Privilege	All: The local user will take effect for all portals, including newly created ones. Portal: Select the portal for which the local user will take effect.
Username	Specify the username. The username should be different from the existing ones, and it is not editable once it is created.
Password	Specify the password. Local users are required to enter the username and password to pass authentication and access the network.
Status	When the status is enabled, it means the user account is valid. You can disabled the user account, and enable it later when needed.

Portal Logout	Check the box to allow clients to log out of the portal by accessing a URL (portal.tplink.net/portal/logout by default). You can change the default URL by editing Portal Logout Domain in Settings > System Settings > Access Config. Some devices may require firmware update to support Portal Logout. Please refer to Configuration Result for details.
Authentication Timeout	Specify the authentication timeout for local users. After timeout, the users need to log in again on the authentication page to access the network.
MAC Address Binding Type	There are three types of MAC binding: No Binding, Static Binding and Dynamic Binding. No Binding: No MAC address is bound to the local user account. Static Binding: Bind a MAC address to this user account manually. Then only the user with the this MAC address can use the username and password to pass the authentication. Dynamic Binding: The MAC address of the first user that passes the authentication will be bound to this account. Then only this user can use the username and password to pass the authentication.
Maximum Users	Specify the maximum number of users that can use this account to pass the authentication.
Name (optional)	Specify a name for identification.
Telephone (optional)	Specify a telephone number for identification.
Rate Limit	Select an existing rate limit profile, create a new rate limit profile or customize the rate limit for the local users. Custom: Specify the Download Limit and Upload Limit based on needs.
Traffic Limit	Click the checkbox and specify the daily/weekly/monthly/total traffic limit for the local user account, and the value of the traffic limit can be set in MB or GB. Once the limited is reached, the user(s) can no longer access the network using this account. **Note:** Traffic Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to Network Config >Traffic Management > Gateway QoS > Bandwidth Control.

- **Create Local User accounts from files**

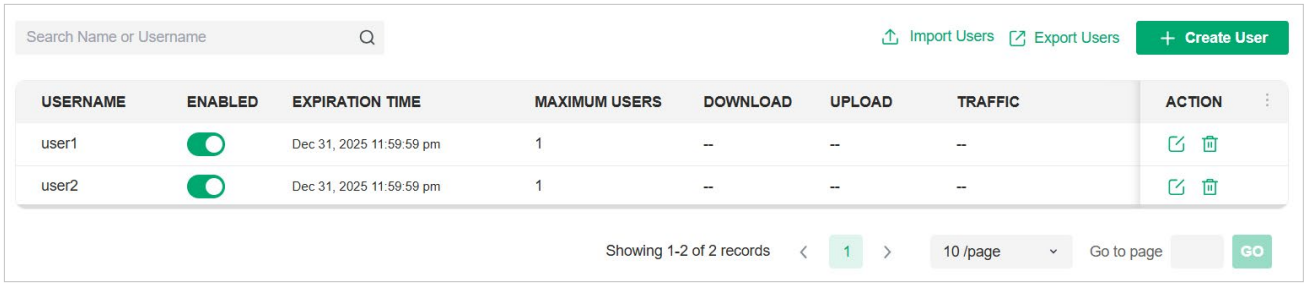
  Click Import Users on the upper-right, and the following window pops up. Click Template to download the template and fill in local users' information. Then click Browse, select the file, and click Import.

To see required parameters and corresponding explanation, refer to Create Local User accounts. Note that the imported file will override the current user data.



Portal Privilege	All: The local users will take effect for all portals, including newly created ones. Portal: Select the portal for which the local users will take effect.

3. The local user account(s) will be created and displayed in the module. You can view the information of the created local users, search certain accounts through the name, and use icons for management.



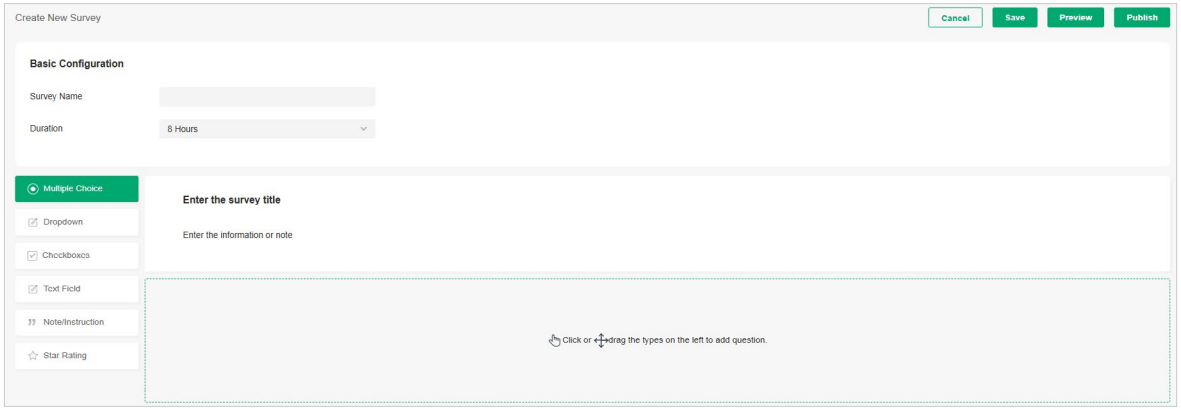
Import Users	Click to add local user(s) from files in the format of CVS or Excel. It is recommended when you need to create local users in batches. Select the portals based on needs, and the local users will be imported to the chosen portal. Note that the imported file will override the current user data.
Export Users	Click to export the local user(s) to files in the format of CVS or Excel. Select the portals based on needs, and the local users of the chosen portal will be exported.
	Click to edit the parameters for the local user.
	Click to delete the local user.

21. 6 Form Auth Data

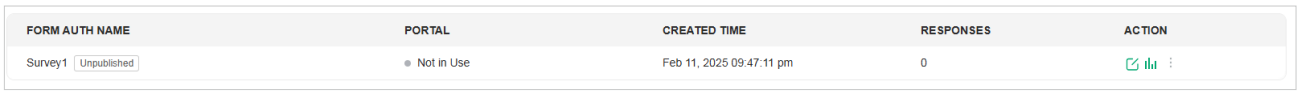
The Form Auth Data tab is used to create and manage surveys. You can customize your survey contents and publish it to collect data.

To create surveys, follow the steps below.

1. Click Hotspot in the sidebar, then click Form Auth Data.
1. Click Create New Survey and the following window pops up.



2. Specify the survey name and duration, then customize the contents.
3. Preview and save the settings or publish the survey.
4. The surveys are created and displayed in the table. You can use icons for management and click the ellipse icon for more management options.

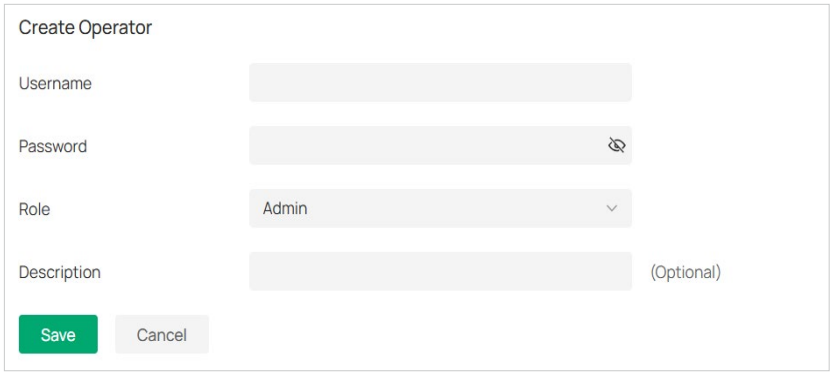


21.7 Operators

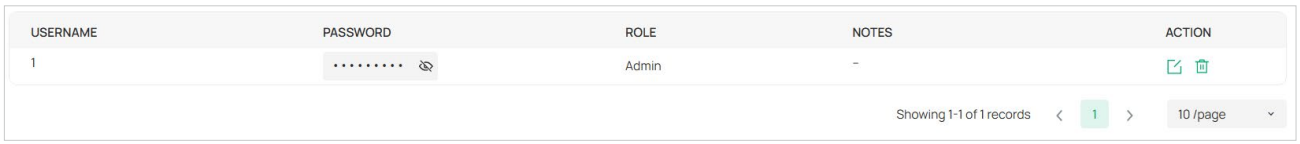
The Operators tab is used to manage and create operator accounts that can only be used to remotely log in to the Hotspot system and manage vouchers and local users. The operators have no privileges to create operator accounts, which offers convenience and ensures security for client authentication.

To create operator accounts, follow the steps below.

1. Click Hotspot in the sidebar, then click Operators.
2. Click Create Operator on the lower-left, and the following window pops up.



3. Specify the username, password, and role for the operator account. Admin role has read and write permissions, while Viewer role has read-only permissions.
4. (Optional) Enter a description for identification.
5. The operator accounts are created and displayed in the table. You can view the information of the create operator accounts on the page, search certain accounts through the name and notes, and use icons for management.



6. Then you can use an operator account to log in to the Hotspot system:

   Visit the URL **https://Fusion gateway's domain name or IP/ControllerID/login#hotspot** (for example: **https://192.168.188.1/d3eab5ad8771ff8c1e50b68c171d209e/login#hotspot**), and use the operator account to enter the Hotspot system.

Chapter 22

Maintain the Network

This chapter guides you on how to maintain the network to ensure the stability and security of network operations. This chapter includes the following sections:

22. 1 Maintain the Network with Tools

The Fusion gateway provides many tools for you to analyze your network:

- **Network Check**

  Test the device connectivity via ping, traceroute, DNSLookup, or ARP Table.

- **Packet Capture**

  Capture packets for network troubleshooting.

- **Terminal**

  Open Terminal to execute CLI or Shell commands.

- **Cable Test**

  Perform cable test to check the cable issues.

- **Interference Detection**

  Scan for interference in the environment and obtain channel occupancy information.

- **Remote Access**

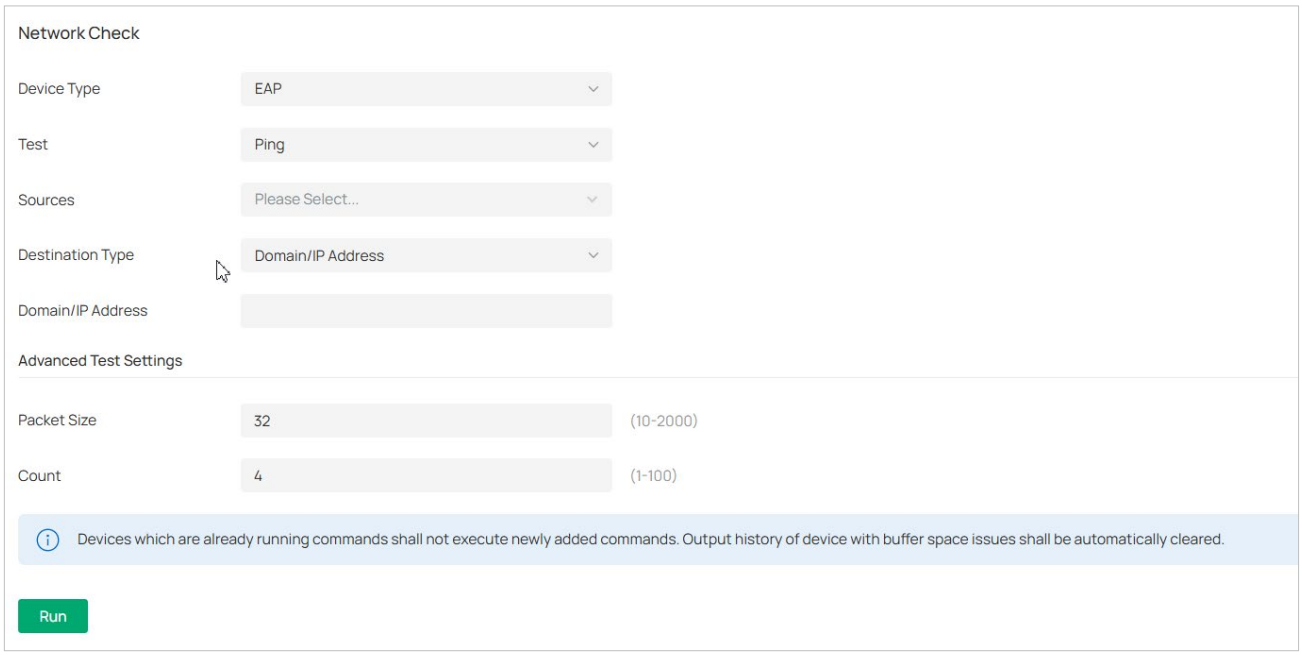
  Allows easy access to internal network devices from an external network using adopted Omada devices.

Note:

Firmware updates are required for earlier devices to support these tools.

22. 1. 1 Network Check

1. Go to Network Tools > Network Check.
2. Configure the test parameters.



Device Type	Select the device type to perform a test.
Test	Choose a tool to test the device connectivity. Ping: Tests the connectivity between the specified sources and destination, and measures the round-trip time. Traceroute: Displays the route (path) the specified sources have passed to reach the specified destination, and measures transit delays of packets across an Internet Protocol network. DNS Lookup: Helps find DNS records of a domain name. ARP Table: Helps check the ARP table of the device.
Sources	Select one or multiple devices to perform a test.
Destination Type	Select the destination type and specify the destination to test. The options vary with the test type. For the Ping test, you can specify the Domain/IP Address or Client. For the Traceroute test, you can specify the Domain/IP Address. For the DNSLookup test, you can specify the Domain.
Advanced Test Settings	(Only for the Ping test) Packet Size: Specify the size of ping packets. Count: Specify the number of ping packets.

Note:

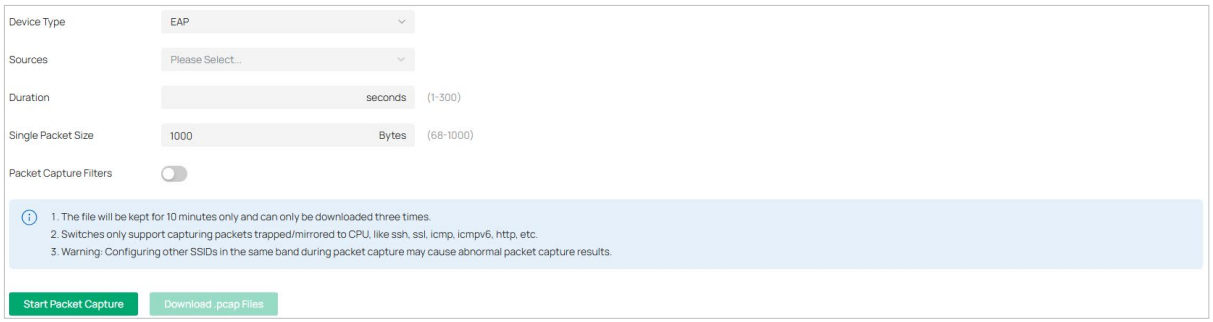
- Devices which are already running commands shall not execute newly added commands.
- Output history of device with buffer space issues shall be automatically cleared.

3. Click Run to perform the test. You can view the test result in the Device Output section.

You can click the Send Email/Download/Enlarge Font icons above the test result field to email the test logs to a mailbox, download the test logs locally, or adjust the text font size.

22. 1. 2 Packet Capture

1. Go to Network Tools > Packet Capture.
2. Configure the parameters for packet capture.



Device Type	Select the device type to capture packets.
Sources	Select one or multiple devices to capture packets.
Interface Type	Select the interface type to capture packets. Wired: If selected, select the Port to capture packets and select the Capture Mode. Wireless: If selected, select Band and SSID / Interface to capture packets. **Note:** The following configurations will affect packet capturing on a wireless interface : • If a certain band is turned off, packets on the SSIDs of the corresponding band will not be captured. • If a WLAN schedule is configured, packets outside the schedule will not be captured. • If a certain SSID is turned off, packets on the SSID will not be captured.
Capture Mode	Select a mode to capture packets: Local: The device executes the packet capture locally. The captured packets are packaged and stored in the internal directory of the device. You can download the file from the Fusion gateway web page. Stream: The device does not save the packet capture files to the device's internal storage, thereby avoiding memory consumption. Packets captured by the device can be displayed in real-time using packet capture tools such as Wireshark, enabling real-time viewing and analysis of the captured packets.
Duration	Specify the duration for packet capture.
Single Packet Size	Specify the size of a single captured packet. It cannot exceed 1 MB.
Packet Capture Filters	(Optional) Enter the filters to capture packets. Supported filters include: host, src, dst, tcp port, tcp src port, tcp dst port, udp port, udp src port, udp dst port, ether host, ether src, ether dst Combination of operators "and", "or", "(" and ")" is supported between multiple filter items. For example: (src 192.168.0.1 and tcp port 80) or (src 192.168.0.1 and tcp port 90) (src 192.168.0.1 and tcp src port 80) or (dst 192.168.0.1 and tcp dst port 90) ether src A0:00:00:04:C5:84 and ether dst A0:00:00:04:C5:85 Note: host: host address, src: source, dst: destination, ether: ethernet address (MAC address)

3. Click Start Packet Capture to capture packets. After packets are captured, you can click Download

.pcap Files to download them.

Note:

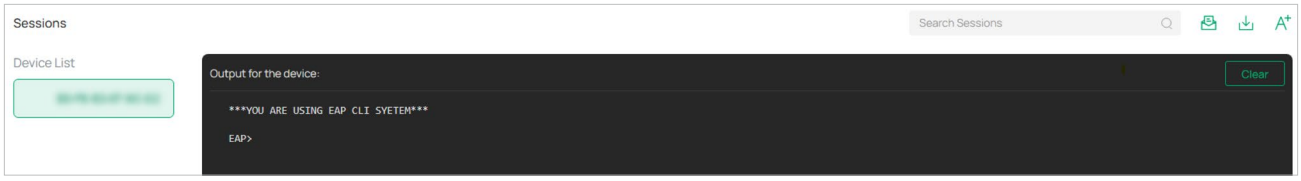
- The file will be kept for 10 minutes only and can only be downloaded three times.
- Switches only support capturing packets trapped/mirrored to CPU, like ssh, ssl, icmp, icmpv6, http, etc.
- Warning: Configuring other SSIDs in the same band during packet capture may cause abnormal packet capture results.

22. 1. 3 Terminal

1. Go to Network Tools > Terminal.
2. Configure the parameters.

Device Type	Select the device type to run CLI or Shell commands.
Sources	Select one or multiple devices to test.

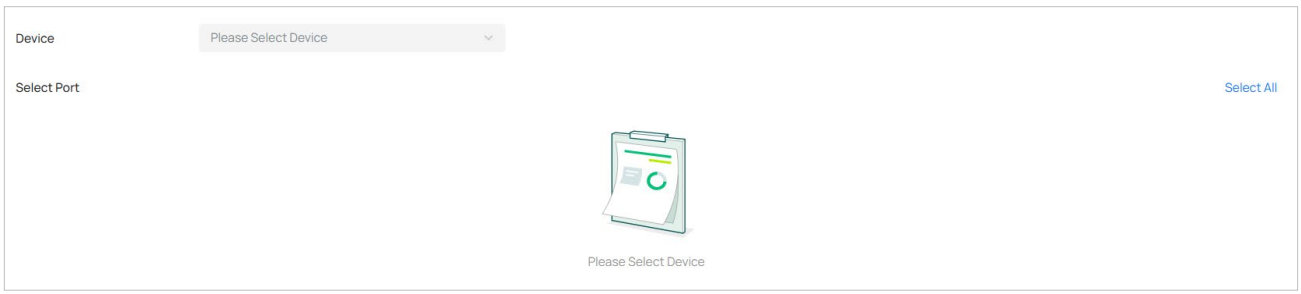
3. Click Open Terminal. Now you can run CLI or Shell commands.



You can click the Send Email/Download/Enlarge Font icons above the test result field to email the test logs to a mailbox, download the test logs locally, or adjust the text font size.

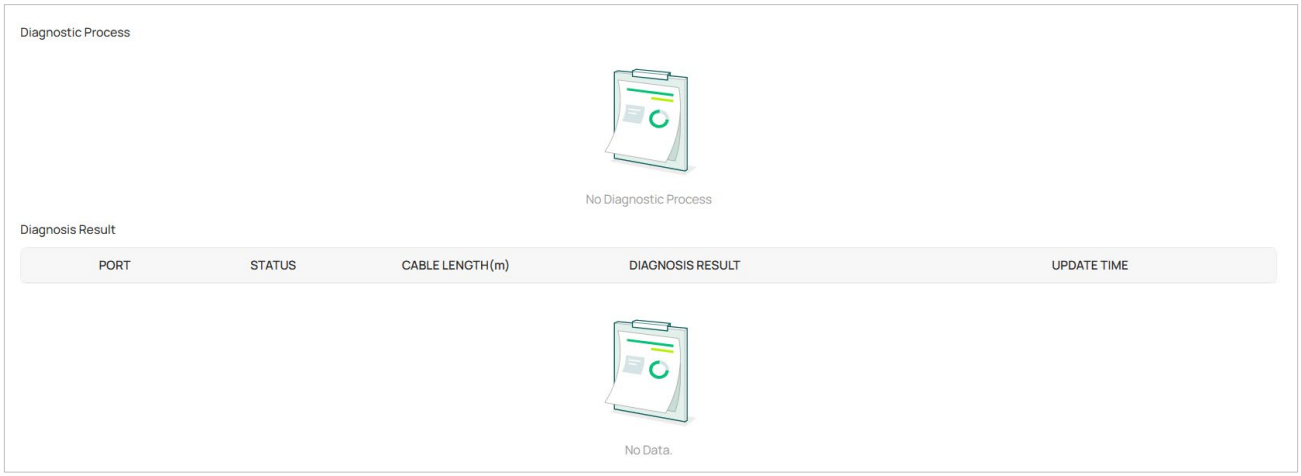
22. 1. 4 Cable Test

1. Go to Network Tools > Cable Test.
2. Configure the parameters.



Device	Select the device in the pop-up window to run the cable test.
Select Port	Select the port of the device to run the cable test.

3. After running the cable test, you can check the diagnostic process and results below.



22. 1. 5 Interference Detection

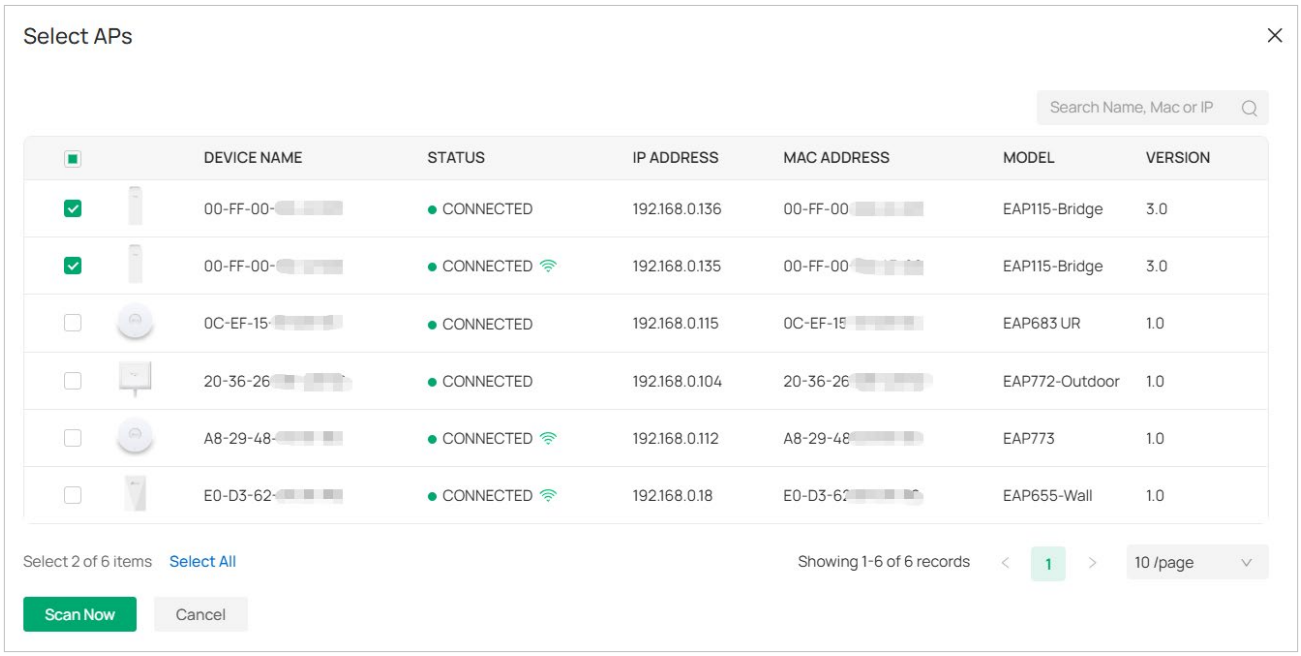
Interference Detection is used to scan for interference in the environment and obtain channel occupancy information. After the scan is complete, it generates scan results that include channel utilization information and Wi-Fi interference source information.

There are two ways to configure the interference detection function: one for a single device and the other for multiple devices.

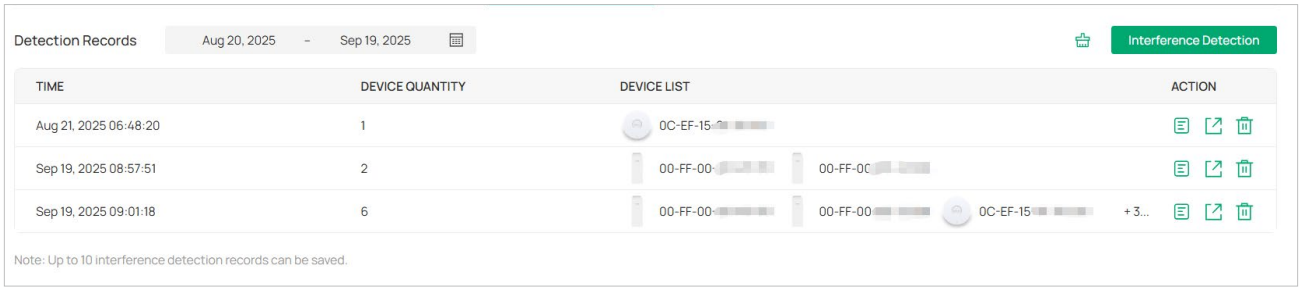
Method 1: Configure Interference Detection for Multiple Devices

Note: After the scan is complete, a scan result entry will be generated and retained as a historical record that can be exported.

1. Go to Network Tools > Interference Detection.
2. Click the Interference Detection button.
3. In the pop-up window, select the devices to scan, and click Scan Now to start scanning.



The Interference Detection page will display the detection records. You can click the Export icon of a record to export it if needed.



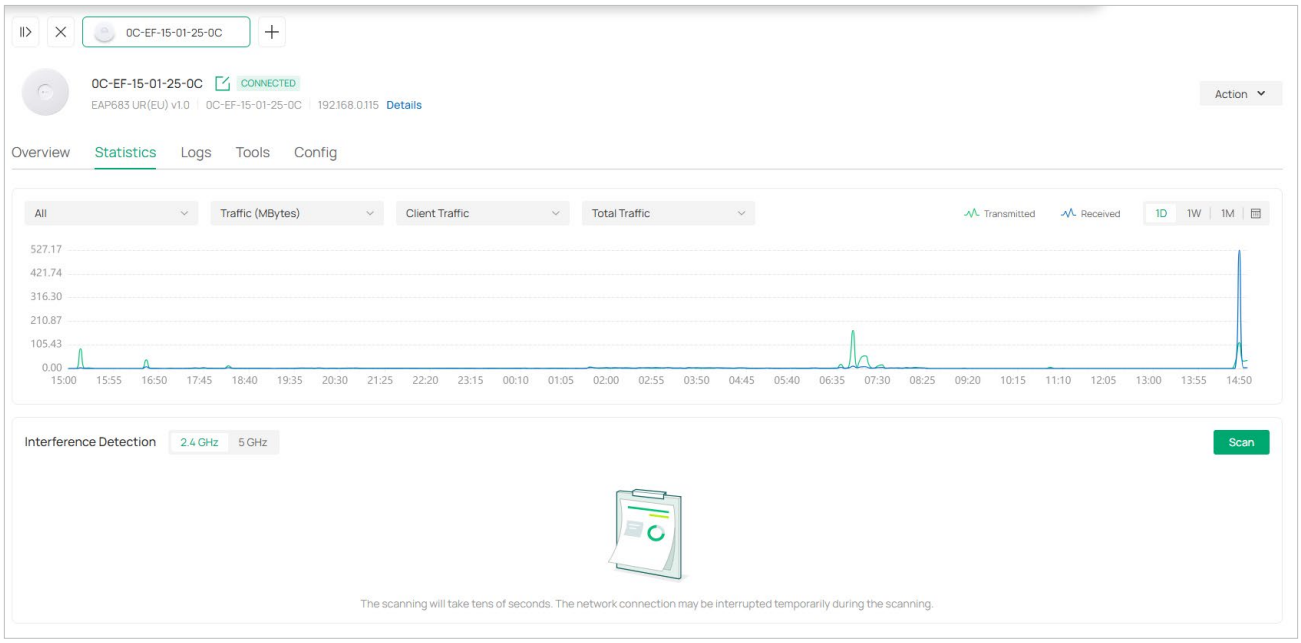
4. Click the Detail icon of a record to view the detailed results.

   You can select All AP to view all device results or select a specific device to view its result. Click the band to view each band's result.

Method 2: Configure Interference Detection for a Single Device

Note: After the scan is complete, a scan result entry will be generated and overwrite the old entry, and the historical scan results will not be retained.

1. Go to Devices > Device List, click the target AP, and click Manage Device.
2. Go to Statistics > Interference Detection. Click Scan to start scanning.

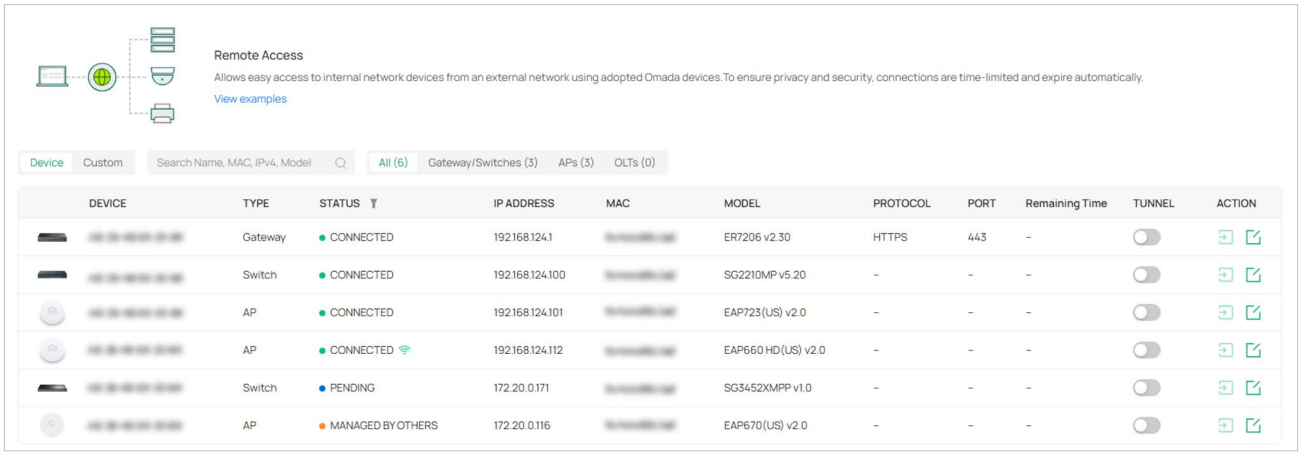


3. Wait for the scan to complete and the results will be displayed.

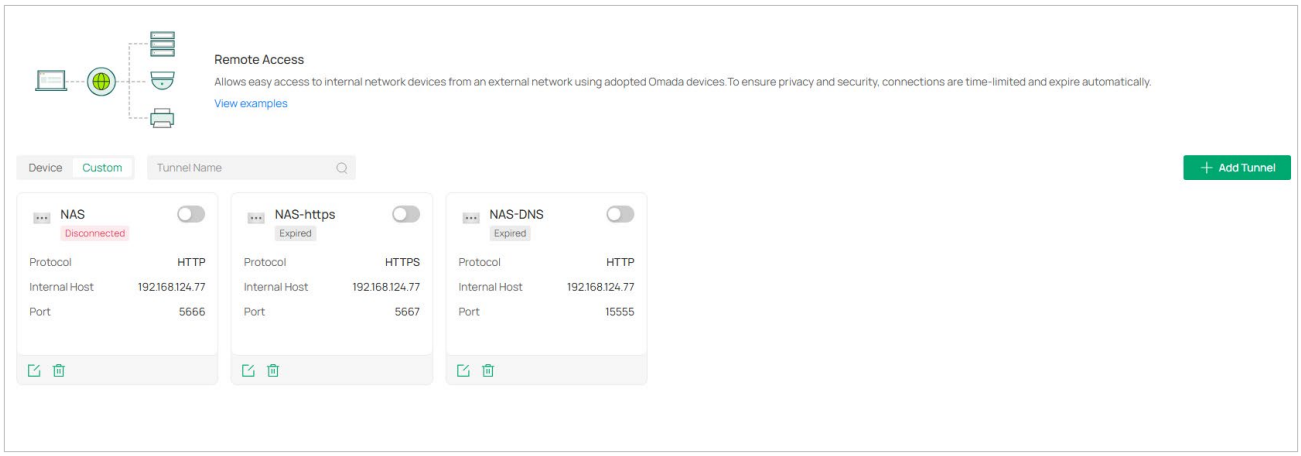
22. 1. 6 Remote Access

Remote Access allows easy access to internal network devices from an external network using adopted Omada devices. To ensure privacy and security, connections are time-limited and expire automatically.

1. Go to Network Tools > Remote Access.
2. In the Device tab, you can click the button in the TUNNEL column or the icon to enable the remote access for a specified device and configure the parameters. After editing and saving the configuration, the tunnel's valid period will be recalculated.



3. In the Custom tab, you can click + Add Tunnel to to create a tunnel manually and configure the parameters. You can also edit or delete an exsiting tunnel. After editing and saving the configuration, the tunnel's valid period will be recalculated.



Tunnel Name	Specify the name of the Tunnel.
Status	Enable/Disable the Tunnel.
Protocol	For Software Fusion gateway/Hardware Fusion gateway, the protocol types include HTTP and HTTPS. For Cloud-Based Fusion gateway, the protocol types include HTTP, HTTPS, SSH, and Telnet.
Internal Host	You can manually enter an IP address, or use Select Online Clients to automatically enter the IP of the currently online client.
Port	Each protocol has a default port, which will be automatically filled in after selection. If the device uses a non-default port, you can manually modify the port value.
Valid Period	By default, the tunnel is valid for 3 hours. It can be manually set to any duration between 1 and 24 hours.

22. 2 Maintain PoE Devices with IntelliRecover

Overview

IntelliRecover is a self-healing feature designed to automatically recover frozen or unresponsive PDs (Powered Devices), such as PoE switches or APs, by power cycling the specific PoE port they are connected to.

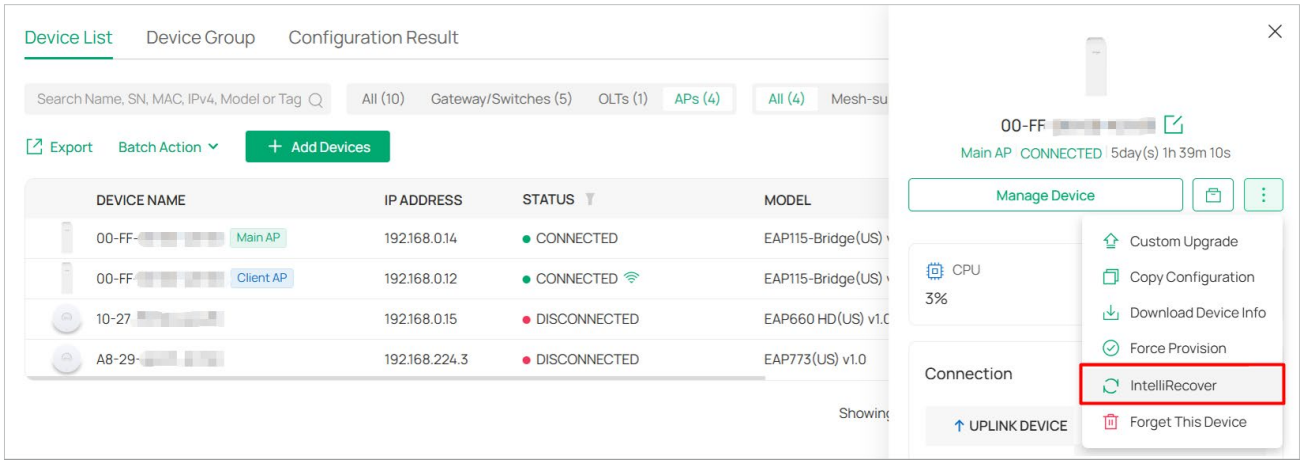
Network Preparation:

- A PoE Switch that can be managed by the Fusion gateway;
- APs, security devices, or clients powered by the PoE switch.

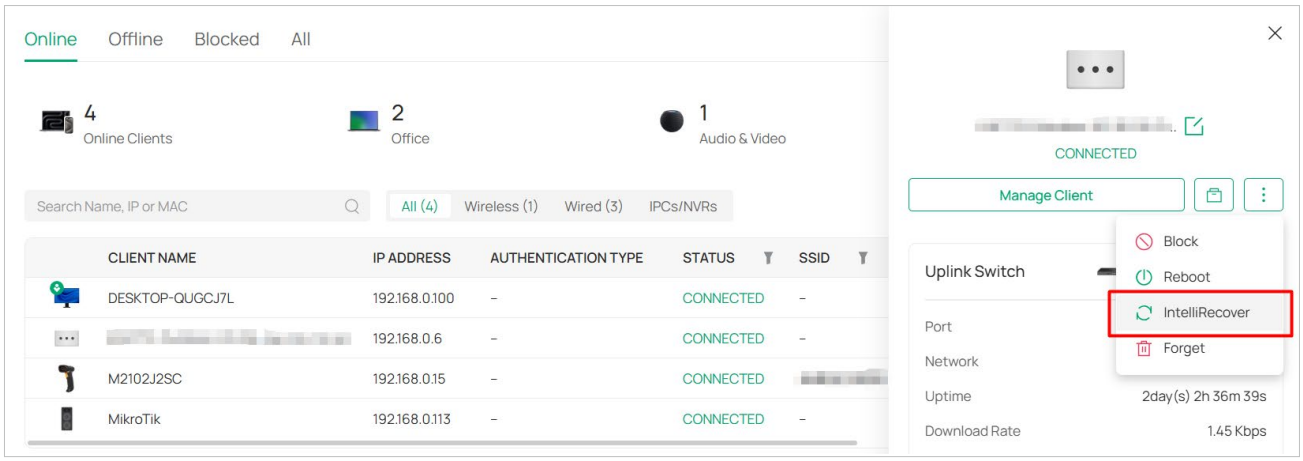
Configuration

To configure IntelliRecover, follow these steps:

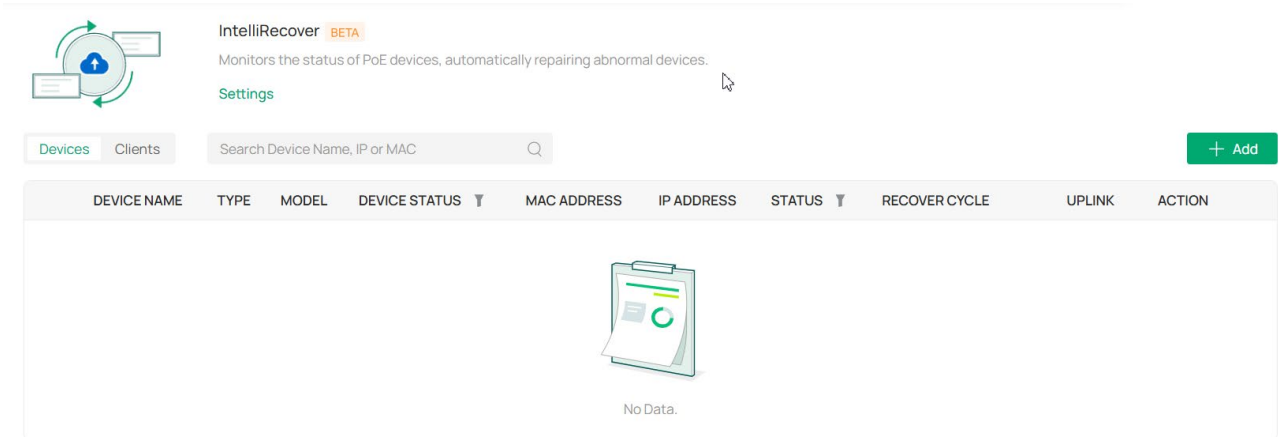
1. Go to Devices. After adopting the PoE switch, and the AP or security device directly connected to the PoE switch, click the AP or security device to open its Properties window. Click ⋮ then click IntelliRecover to enable the function for the device so that it can be added to the monitoring list.



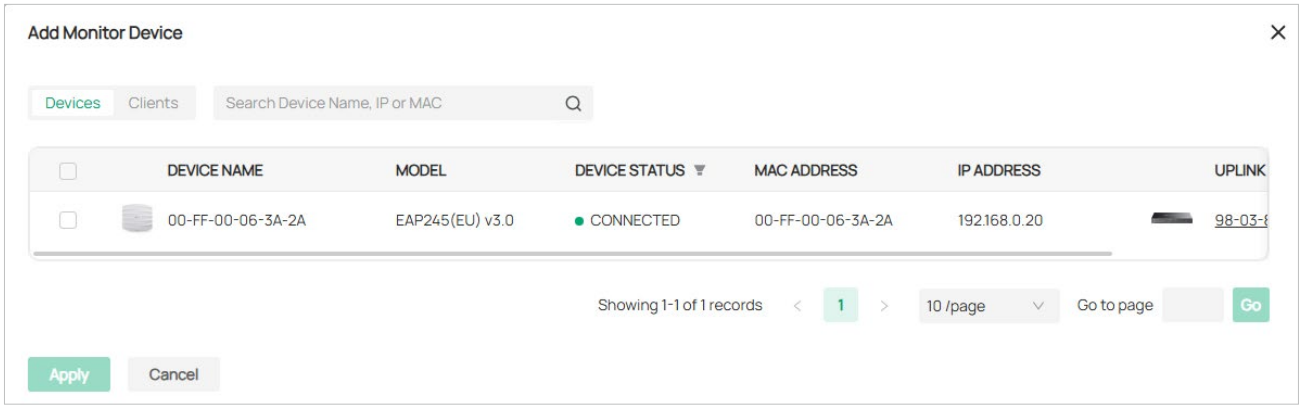
2. Go to Clients. Click the client device to open its Properties window. Click ⋮ then click IntelliRecover to enable the function for the client so that it can be added to the monitoring list.



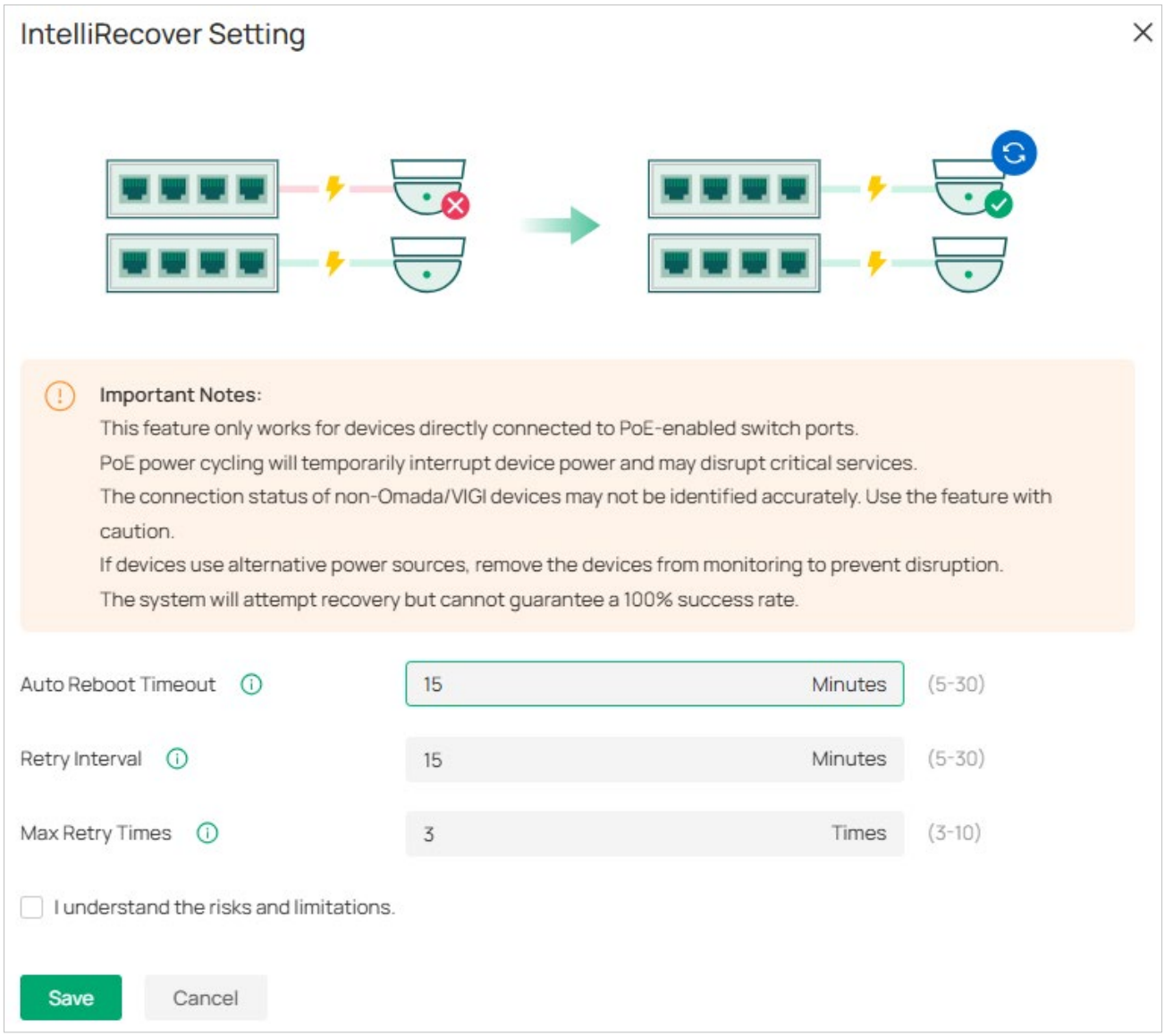
3. Go to the IntelliRecover page. Click Add to add the devices or clients to the monitoring list.



4. Select the devices or clients to be monitored and click Apply.



5. Enable IntelliRecover and enter the Settings window.



Auto Reboot Timeout	Defines the duration the system waits after detecting a device failure before initiating an automatic reboot. Enter a value between 5–30 minutes.
Retry Interval	Specifies the waiting period between consecutive reboot attempts if the initial recovery fails. Enter a value between 5–30 minutes.
Max Retry Times	Sets the maximum number of automatic power-cycle attempts the system will perform before ceasing recovery efforts. Enter a value between 3–10 times.

6. After the configuration, when the monitored device goes offline, the switch PoE port connected to the device will be automatically rebooted and a log will be generated. You can also click the Reboot PoE Port icon in the Action column to manually reboot the PoE Port.


Devices
Clients
00-FF-00-06-3A-2A
+ Add
DEVICE NAME
TYPE
MODEL
DEVICE STATUS
MAC ADDRESS
IP ADDRESS
STATUS
RECOVER CYCLE
UPLINK
Reboot PoE Port
00-FF-00-06-3A-2A
AP
EAP245(EU) v3.0
CONNECTED
00-FF-00-06-3A-2A
192.168.0.20
Monitoring
0
98-03-8E-EC-57-53 - Port 3
Showing 1-1 of 1 records
1
10 /page
Go to page
Go

Chapter 23

Manage Accounts

This chapter gives an introduction to different user levels of Fusion gateway accounts and guides you on how to create and manage them. It includes the following sections:

23. 1 Introduction to User Accounts

The Fusion gateway offers multiple levels of access available for users: **Owner**, **Super Admin**, **Admin**, and **Viewer**. You can also create new account roles and customize their permissions to access different features.

Since the Fusion gateway can be accessed both locally and via cloud access, users can be further grouped into local users and cloud users.

Multi-level administrative account presents a hierarchy of permissions for different levels of access to the Fusion gateway as required. This approach ensures security and gives convenience for management.

Moreover, in the user accounts list of the Owner/Super Admin, all accounts it created will be displayed. The accounts created by each administrator will be hidden by default, making the interface more systematic and to the point.

- **Owner**

The Owner has access to all features.

The account who first launches the Fusion gateway will be the Owner (used to be recognized as Main Admin in earlier Fusion gateway versions). It cannot be changed and deleted.

- **Super Admin**

The Super Admin can manage all the other roles (except Owner) and the privileges of most features.

- **Admin**

Admins have no permission to some modules, mainly including cloud access, migration, and auto-backup. They have read-only permission to some modules, such as custom account roles.

Admins can be created and deleted by the Owner/Super Admin and Admins.

- **Viewer**

Viewers can view the status and settings of the network, and change the settings in Hotspot Manager.

The entrance to Account page is hidden for viewers, and they can be created or deleted by the administrators.

- **Custom roles**

Custom roles can be configured to access different features.

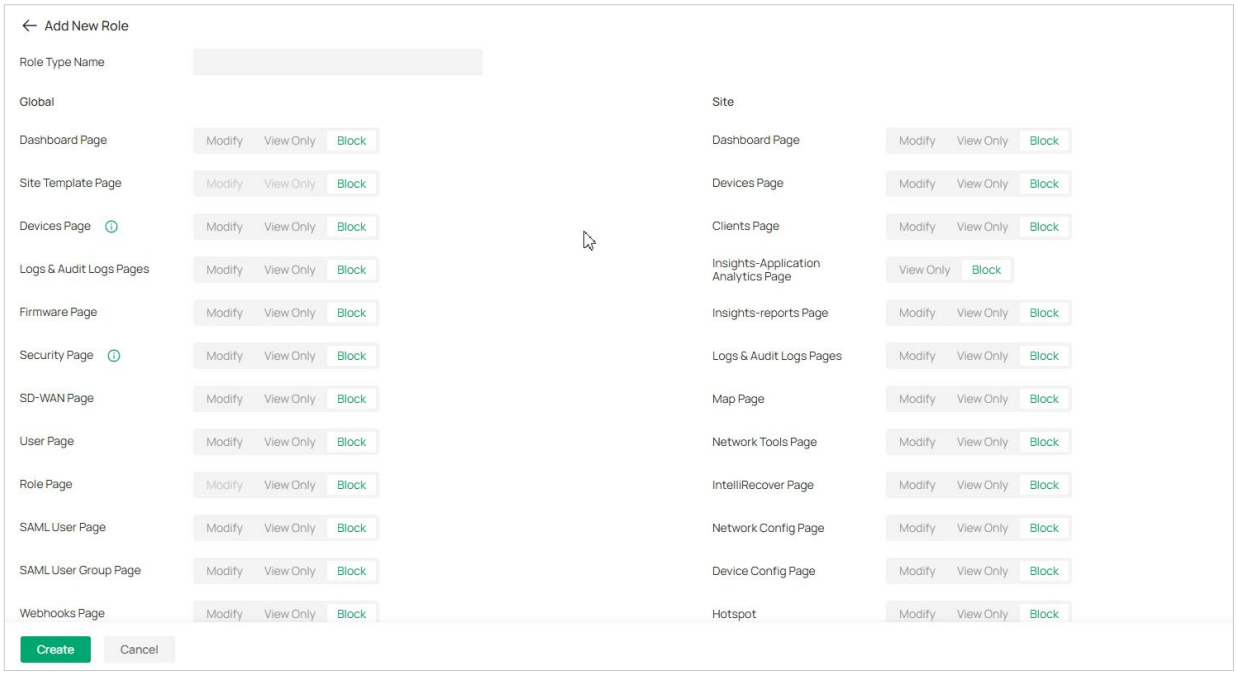
They can be created or deleted only by the Owner/Super Admin.

Note:

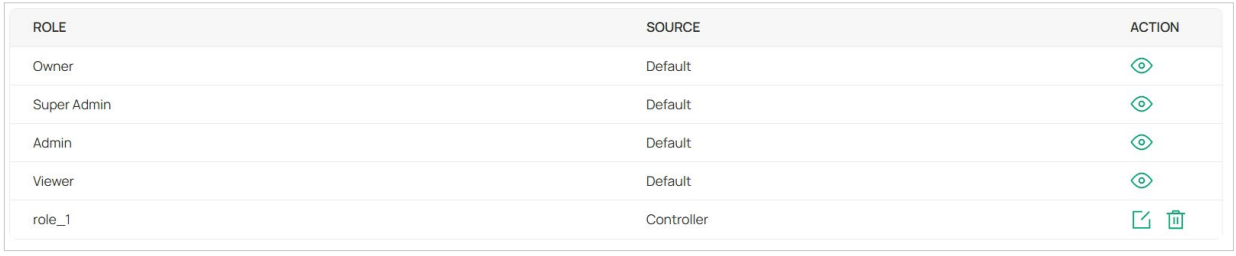
Please upgrade Omada APP to version 4.6 or later, otherwise you may not be able to log in with the accounts bound with customized roles.

23. 2 Create and Manage Roles

1. Go to Accounts > Role. The Fusion gateway offers four levels of default roles: **Owner**, **Super Admin**, **Admin**, and **Viewer**.
2. If you want to create a custom role, click Add New Role.
3. Specify the role type name and customize the permissions for the role. Click Create.



4. The new role will be displayed in the role list.



If you want to edit/delete a custom role, click the Edit/Delete icon in the ACTION column.

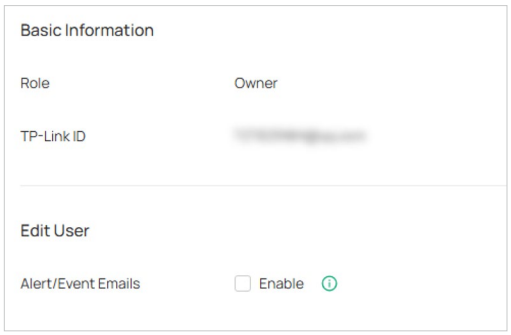
23. 3 Create and Manage Local User Accounts

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

23. 3. 1 Edit the Owner Account

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

1. Go to Accounts > User.
2. Click the Edit icon in the ACTION column and enter your current password to view or change your account.
3. Check and edit the account information. Click Save.

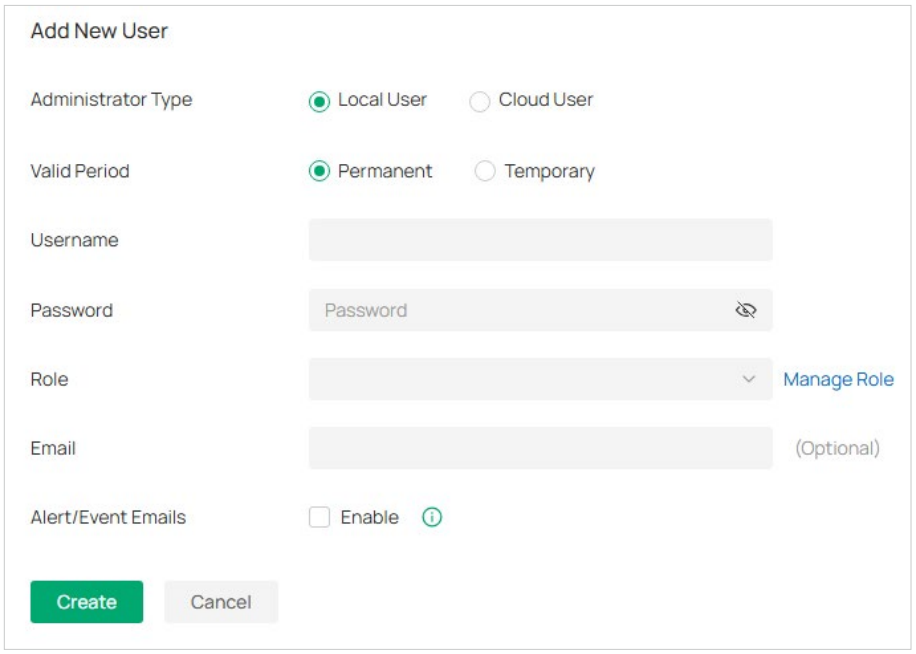


Alert/Event Emails	With Alert/Event Emails enabled, the controller will send the user emails about alerts and events.

23. 3. 2 Create and Manage Other Local Accounts

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

1. Go to Accounts > User. Click Add New User.
2. Select Local User for the administrator type. Specify the parameters and click Create.



Administrator Type	Select the type of user to create. Local User: Set the login username and password to create a user account for local access. Cloud User: Specify a TP-Link ID to invite a user for cloud access.
Valid Period	Set the user account's validity period. Permanent: The user account's permissions will be permanent unless modified or deleted. Temporary: The user account's will have permissions are valid only for the set period.
Username	Specify the username for local login.
Password	Specify the password for local login.
Role	Bind a role to customize the feature access permissions to of the user account.
Email	Enter the email address to receive alerts and events.
Alert/Event Emails	With Alert/Event Emails enabled, the controller will send the user emails about alerts and events

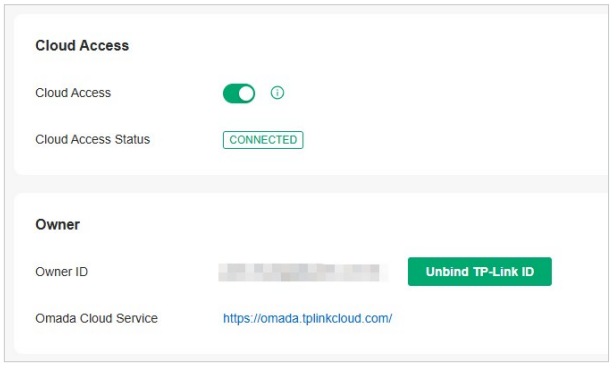
23. 4 Create and Manage Cloud User Accounts

A Cloud-Based Fusion gateway enables cloud access by default and automatically sets up the cloud Owner. An on-premise Fusion gateways automatically sets up the cloud Owner if you have enabled cloud access and bound the Fusion gateway account with a TP-Link ID in the quick setup. The username and password is the same as that of the TP-Link ID. The cloud Owner is cannot be deleted, and it can create, edit, and delete other levels of user accounts.

23. 4. 1 Set Up the Cloud Owner Account

For an on-premise Fusion gateway, if you have not enabled the cloud access and bound the Fusion gateway with a TP-Link ID in quick setup, you can follow the steps below to set up the cloud Owner:

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

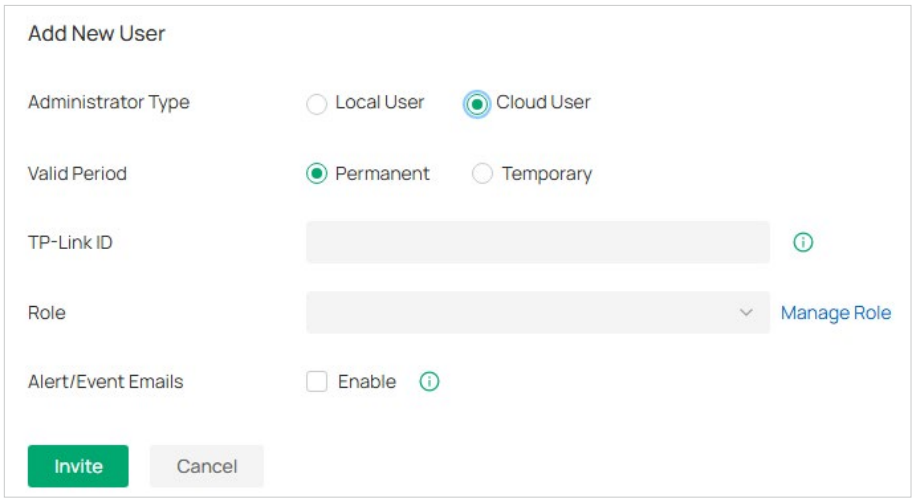


2. Go to Accounts > User. A cloud Owner with the same username as the TP-Link ID will be automatically created. The Cloud Owner cannot be deleted. You can log in with the cloud Owner when the cloud access is enabled.

23. 4. 2 Create and Manage Other Cloud Accounts

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

1. Go to Accounts > User. Click Add New User.
2. Select Cloud User for the administrator type. Specify the parameters and click Invite.



Administrator Type	Select the type of user to create. Local User: Set the login username and password to create a user account for local access. Cloud User: Specify a TP-Link ID to invite a user for cloud access.
Valid Period	Set the user account's validity period. Permanent: The user account's permissions will be permanent unless modified or deleted. Temporary: The user account's will have permissions are valid only for the set period.
TP-Link ID	Enter the email address of the user you wish to invite to send an invitation. If the email address has been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation. If the email address has not been registered, it will receive an invitation to regist. After finishing registration, it will automatically become a valid cloud user.
Role	Bind a role to customize the feature access permissions to of the user account.
Alert/Event Emails	With Alert/Event Emails enabled, the controller will send the user emails about alerts and events

23. 5 Manage User Accounts Across Fusion Gateways

Overview

If you have multiple Fusion gateways, Account Manager allows you to centrally manage user accounts across Fusion gateways, assign users, enforce permissions, and streamline onboarding through Cloud Portal.

To use Account Manager, ensure your Fusion gateways meet the following requirements:

Fusion gateway Type: Omada On-Premises Networking Fusion gateways only.

Version Required: v5.15.20 or later.

Status: Fusion gateways must be online.

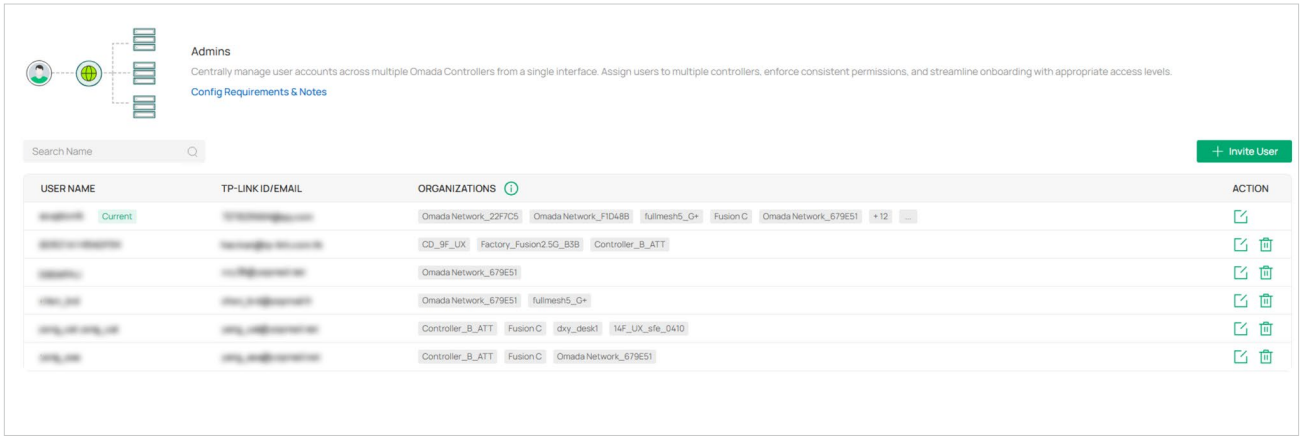
Cloud Access: Must be enabled.

Notes:

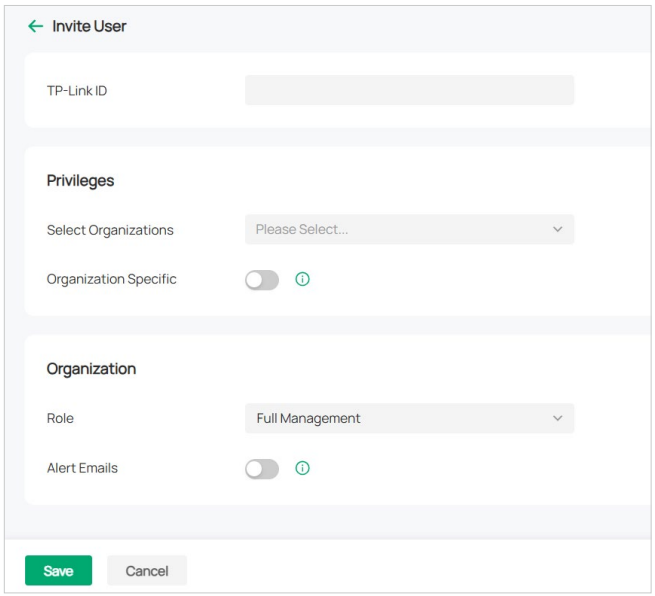
- For MSP Fusion gateways, permissions are applied at the MSP level.
- Account Manager currently supports Full Management (Super Admin) and View Only (Viewer) permissions.

Configuration

1. Launch a web browser and visit https://omada.tplinkcloud.com. Enter your TP-Link ID and password to log in. If you do not have a TP-Link ID, create a TP-Link ID first.
2. Go to Admins. The user accounts of all Fusion gateways managed by the current TP-Link ID will listed. The organization column displays the status of organization invitation: yellow text indicates that the user has been invited but not yet agreed, and gray text indicates that the user has agreed to join.



3. If you want to invite a user to help manage a Fusion gateway organization, click Invite User and configure the parameters.



TP-Link ID	Enter the TP-Link ID of the user you want to invite. If the email address has already been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation. If the email address has not been registered, it will receive an invitation email for registration. After finishing registration, it will automatically becomes a valid cloud user.
Select Organizations	Select one or multiple Fusion gateway organization that the invited user can manage.
Organization Specific	Enable this option if you selected multiple Fusion gateway organizations and want to configure the roles and alert settings for them separately.
Role	Set the permissions for the user: Full Management (Super Admin) or Viewer (View Only).
Alert Emails	With Alert Emails enabled, the organization will send the user emails about alerts.

Chapter 24

Configure Controller Settings

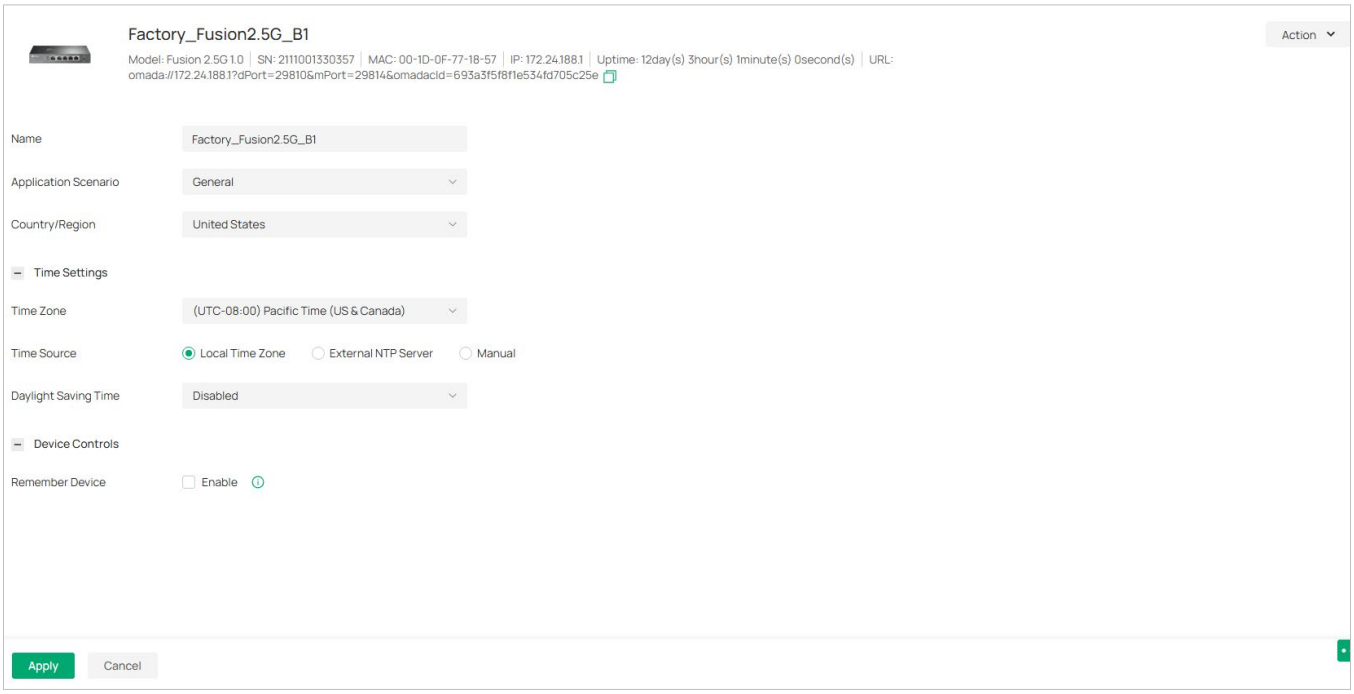
Controller settings control the appearance and behavior of the controller and provide methods of data backup, restoration, migration, and more. The chapter includes the following sections:

24. 1 System Settings

Go to Settings > System Settings.

24. 1. 1 OS Settings

In OS Settings, you can view the general information about your Fusion gateway status. You can also manage the gateway and configure its general settings here. Click Action in the upper right corner, you can choose to reboot or reset the device from the drop-down list.

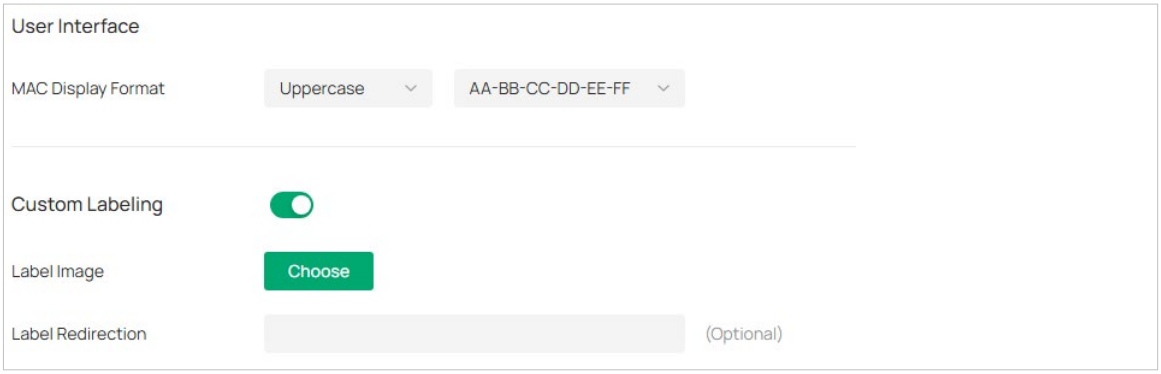


Name	Specify a name to identify the Fusion gateway.
Application Scenario	Specify the application scenario or create a new scenario based on needs.
Country/Region	Select the country/region of the Fusion gateway.
Time Zone	Select the time zone of the Fusion gateway.
Time Source	Choose the time synchronization method Local Time Zone: Use the time zone External NTP Server: Enter the IP address(es) of the NTP (Network Time Protocol) server. NTP server assigns network time to the EAP devices. Manual: Manually set the accurate time of the Fusion gateway

Daylight Saving Time	Enable the feature if your country/region implement DST. There are three modes for DST: Disabled, Auto, Mannual Time Offset: Specify 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.
Remember Device	When enabled, the Fusion gateway will remember all devices in the controller. After device reset and power-on, the Fusion gateway will automatically adopt the device if the Fusion gateway can find it.

24. 1. 2 User Interface

In User Interface, you can customize the User Interface settings of the Fusion gateway.

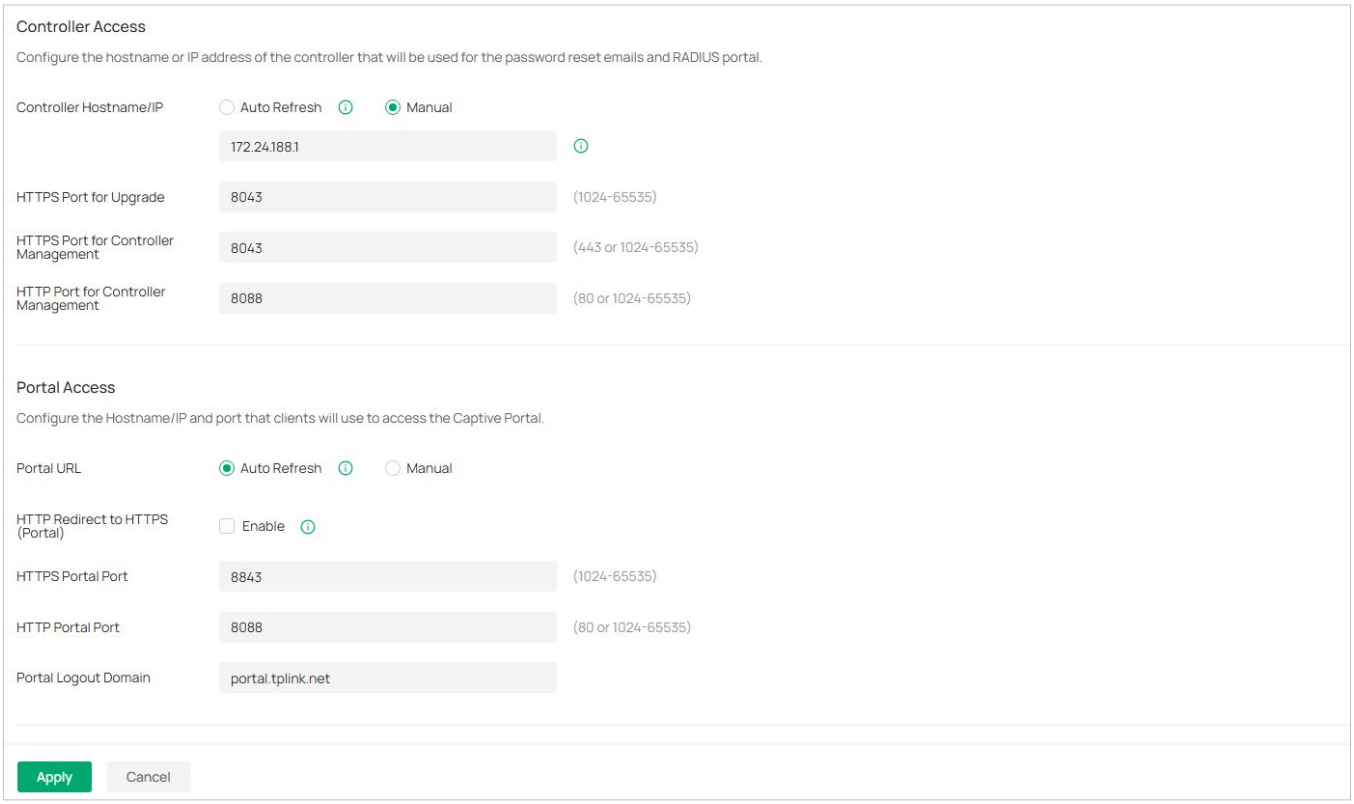


Refresh Interval	Specify the interval to automatically refresh the UI interface. Note that this feature is only available on Omada Local.
MAC Display Format	Specify the format to display MAC addresses, including: (1) Device and Client MAC addresses in the controller web and Omada app (2) Device and Client MAC addresses returned by the Open API (3) Device and Client MAC addresses in the exported data (such as CSV, XLSX, Email) of devices, clients, events, and others (4) MAC addresses for the RADIUS Portal and RADIUS Server to submit authentication and billing requests, such as Calling-Station-ID and Called-Station-ID (5) apMac, gatewayMac, and clientMac parameters filled in the URL redirected to the third-party Portal Web Server when using External RADIUS Portal and External Portal Server
Custom Labeling	When enabled, you can upload a private labeling image to replace the current labeling on the controller web page, and modify the redirect URL.

Label Image	Click to upload the labeling image. Only PNG, JPG, JPEG, and BMP images are supported. The image size should be less than 2MB.
Label Redirection	Specify the hyperlink URL to redirect after clicking the labeling image.

24. 1. 3 Access Config

In Access Config, you can configure the controller's access settings, device management access settings for access control.

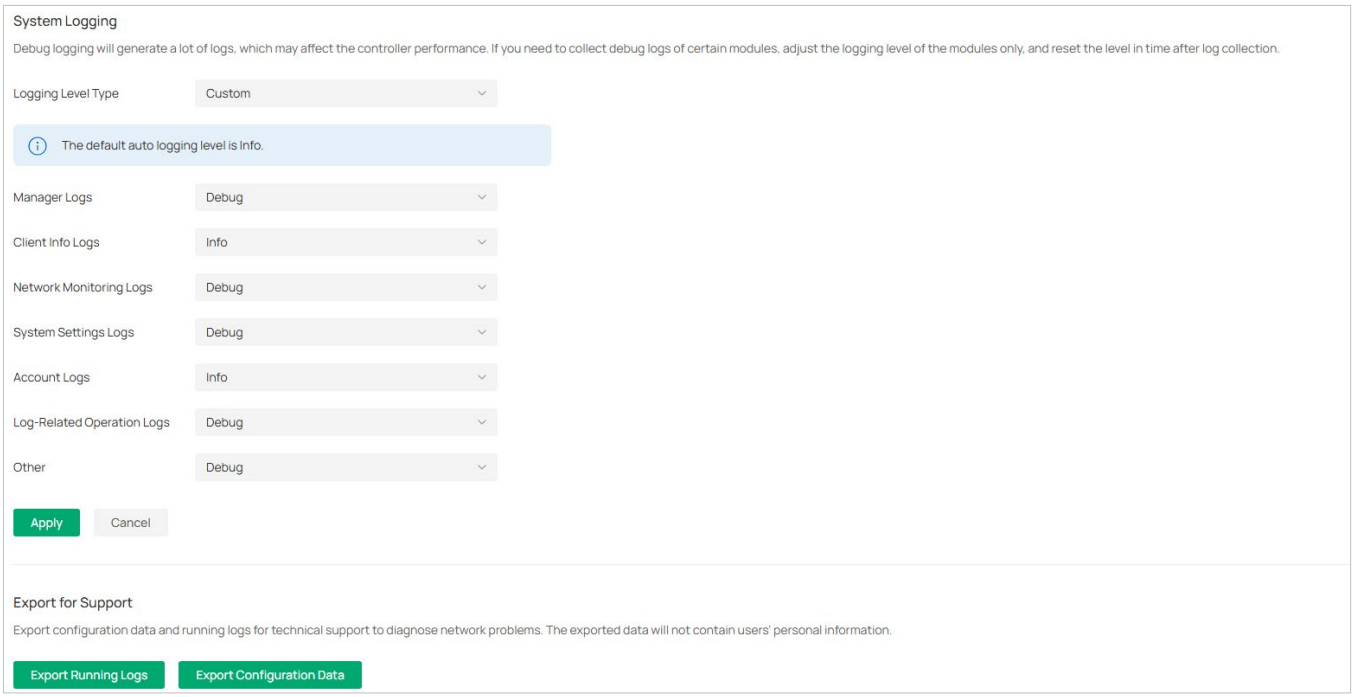


Controller Hostname/IP	Specify the hostname or IP address for the controller which will be used as the controller URL in the notification email for resetting your controller password. You can keep it default, and the IP address recognized by the controller will be used as the controller URL. Auto Refresh: When selected, the Controller Hostname/IP automatically changes with the system IP address. Manual: When selected, you need to enter the hostname or IP address of the Controller.
HTTPS Port for Upgrade	Specify the HTTPS port used by the controller for upgrade.
HTTPS Port for Controller Management	Specify the HTTPS port used by the controller for management. After setting the port, you can visit https://[Omada Controller Host's IP address or URL]:[HTTPS Port] to log in to the Omada Controller.

HTTP Port for Controller Management	Specify the HTTP port used by the controller for management. After setting the port, you can visit http://[Omada Controller Host's IP address or URL]:[HTTP Port] to log in to the Omada Controller.
Portal URL	Select a method to configure the URL of the Portal. Auto Refresh: When selected, the device will automatically use the actual IP address of the Controller as the Portal URL. Manual: When selected you need to enter a domain name or IP address that clients can access controller internal portal web pages.
HTTP Redirect to HTTPS (Portal)	When enabled, clients will be redirected to Captive Portal using HTTPS instead of HTTP.
HTTPS Portal Port	Specify the HTTPS port used by the controller for portal authentication.
HTTP Portal Port	Specify the HTTP port used by the controller for portal authentication.
Portal Logout Domain	Specify the domain used by clients to log out of Portal authentication.
Device Management Access	When enabled, the controller will apply the Device Management Hostname/IP to managed devices for remote management. This feature is currently not supported on gateways and OLTs.
Device Management	When enabled, the controller will apply the specified Hostname/IP address as the Inform URL/IP to managed devices at remote sites. This will overwrite the device settings if they were manually set before adoption. Agile (Easy-Managed) Switches do not support this function.
Device Web Access	This function controls whether HTTP/HTTPS access to the web pages of managed Omada devices is available or not. If it is turned off, HTTP/HTTP access to the devices' web pages will be unavailable.

24. 1. 4 Diagnostics

In Diagnostics, you can configure system logging level type and export support data to help diagnose network problems.



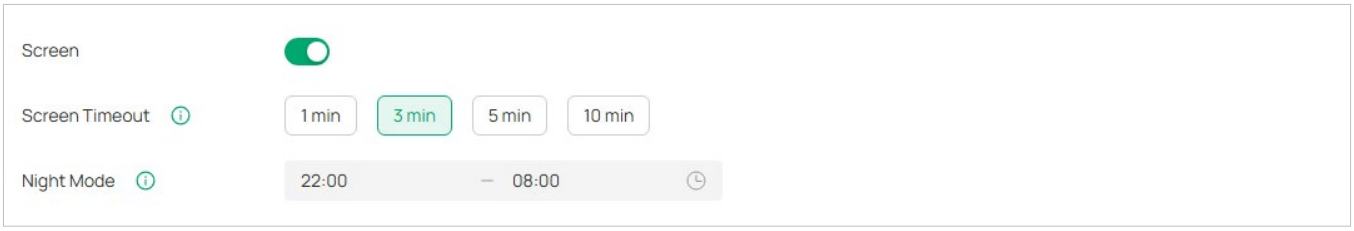
Logging Level Type	Choose whether to customize the log level.
Manager Logs	Select the log level of the manager module, which mainly includes device management and controller-related configurations.
Client Info Logs	Select the log level of the client info module, which mainly includes functions related to client monitoring.
Network Monitoring Logs	Select the log level of the network monitoring module, which mainly includes functions related to data monitoring.
System Setting Logs	Select the log level of the system setting module, which mainly includes system data related functions.
Account Logs	Select the log level of the account module, which mainly includes account-related functions.
Log-related Operation Logs	Select the log level of the log-related operation module, which mainly includes related functions of the log page.
Others	Select the log level of other modules.
Export for Support	Click export button to export configuration data or running logs for technical support to diagnose network problems.

24. 1. 5 Screen Settings

In Screen Settings, you can configure the display settings for the fusion gateway screen.

Note:

- To ensure reliability, the screen turns off automatically after extended inactivity.



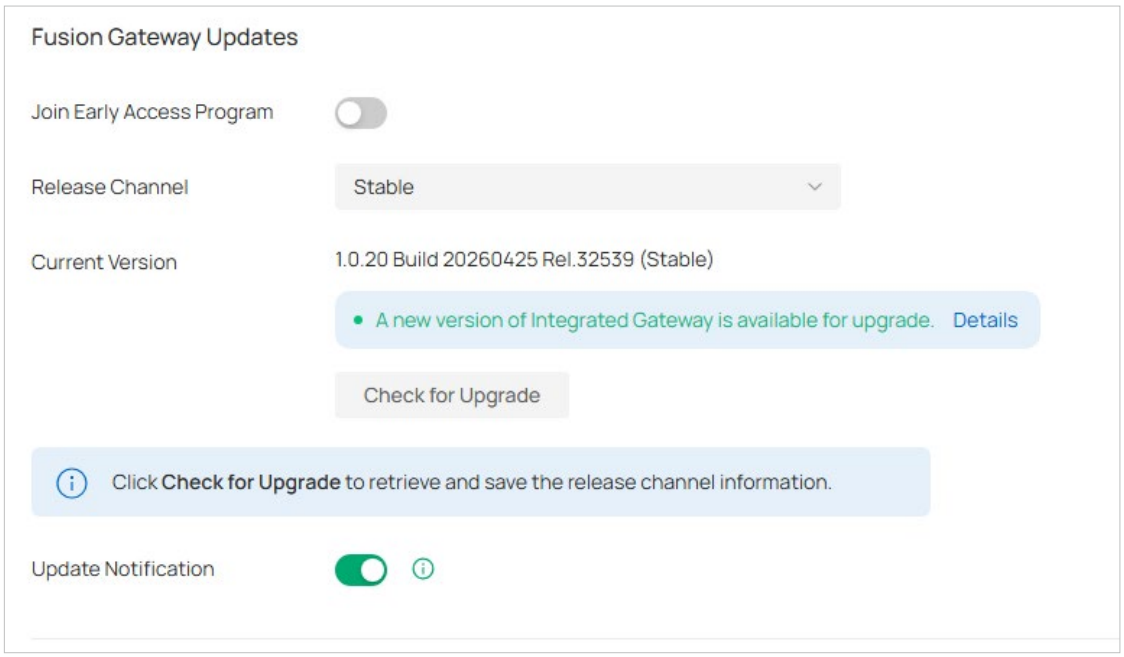
Screen	Enable or disable the fusion gateway screen display.
Screen Timeout	Set the duration of inactivity before the screen enters screensaver mode or turns off.
Night Mode	During the specified time range, the screen turns off after inactivity and will not wake up from alerts.

24. 1. 6 Advanced Settings

In Advanced Settings, you can proceed with Fusion gateway updates and configure HTTPS Certificate.

- Fusion Gateway Updates

  In Fusion Gateway Updates, you can check for gateway updates.

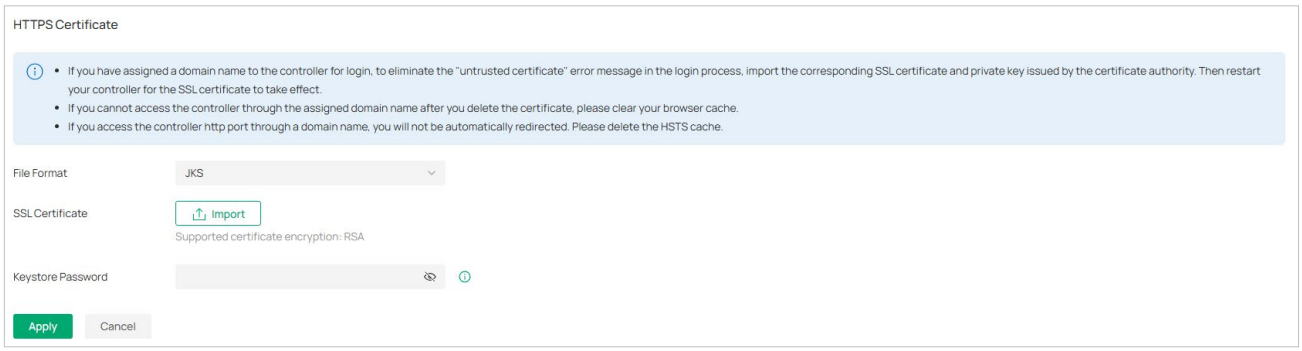


Join Early Access Program	By joining this program, you can check for firmware in the Release Channel > Beta for upgrading, so you can try out in-development features and help improve them.
Release Channel	You can select the Release Channel of the controller to check whether the corresponding Channel has a newer version.
Current Version	Displays the current version of the fusion gateway.

Manual Upgrade	Manually upload a firmware file to upgrade the fusion gateway.
Update Notification	When enabled, the system will notify when a new firmware version is available.

■ HTTPS Certificate

In HTTPS Certificate, you can assign a domain name to the controller for login to eliminate the error message of "untrusted certificate".



File Format	Select the format of the certificate file to be imported.
SSL Certificate	Import the SSL certificate to create an encrypted link between the controller and server. JKS: Import your SSL certificate and enter the keystore password if your SSL certificate has the keystore password. Otherwise, leave it blank. PFX: Import your SSL certificate and enter the private key password if your SSL certificate has the private key password. Otherwise, leave it blank. PEM: Import your SSL certificate and SSL Key.
Keystore Password	If the certificate you imported has a password, enter the password here.

Note:

- If you have assigned a domain name to the controller for login, to eliminate the "untrusted certificate" error message in the login process, import the corresponding SSL certificate and private key issued by the certificate authority. Then restart your controller for the SSL certificate to take effect.
- If you cannot access the controller through the assigned domain name after you delete the certificate, please clear your browser cache.
- If you access the controller http port through a domain name, you will not be automatically redirected. Please delete the HSTS cache.

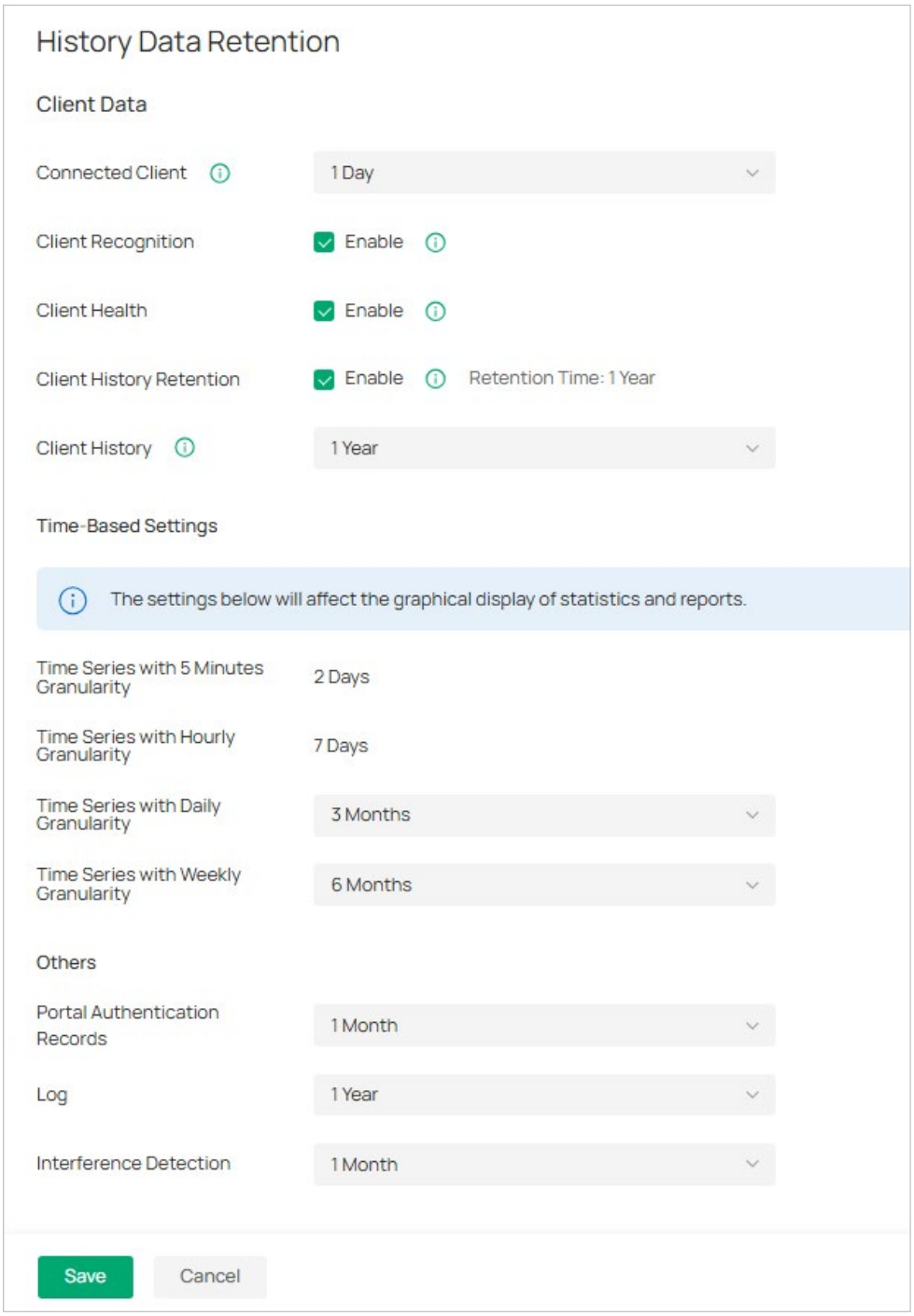
■ Join the User Experience Improvement Program

By joining this program, you have fully read and understood our User Experience Improvement Program Policy. You can opt out of the program at any time.

24. 2 History Data Retention

In History Data Retention, you can specify how the Fusion gateway retains its data..

Go to Settings > History Data Retention.



Connected Client	Specify the retention time of connected client data.
Client Recognition	This function controls whether to identify the type, vendor, and model information of clients in the network.

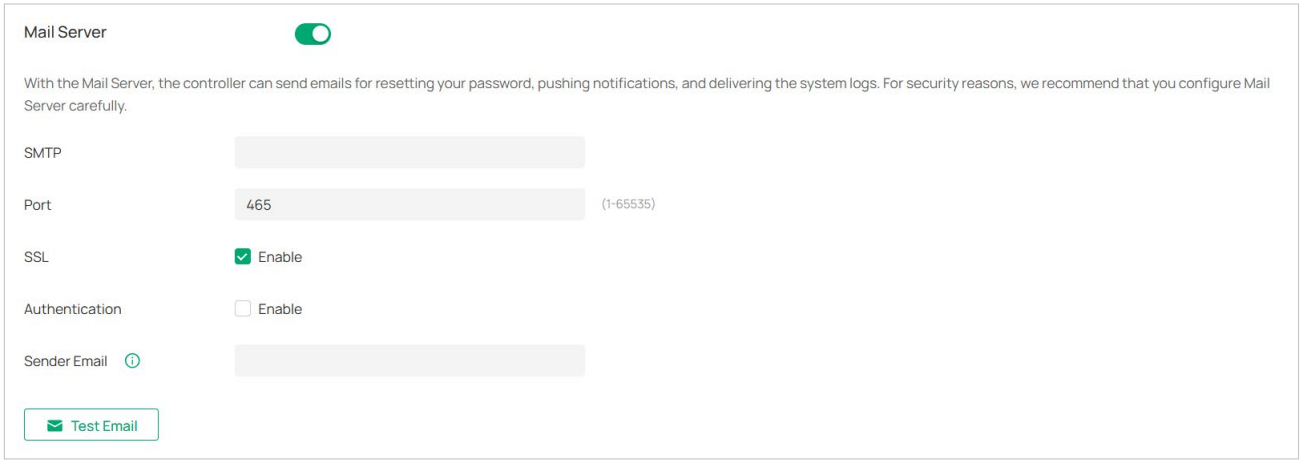
Client Health	This function controls whether to display and record health statistics of clients in the network.
Client History Retention	This function controls whether to retain online and offline records of clients in the network.
Client History Data	Specify the retention time of client online and offline records.
Client History	Specify the retention time of client online and offline records.
Time Series with 5 Minutes Granularity	Displays the retention time of AP, switch, gateway, and client data. Corresponding to 5-minute statistics.
Time Series with Hourly Granularity	Displays the retention time of AP, switch, gateway, and client data. Corresponding to hourly statistics.
Time Series with Daily Granularity	Specify the retention time of AP, switch, gateway, and client data. Corresponding to daily statistics.
Time Series with Weekly Granularity	Specify the retention time of client data. Corresponding to weekly statistics.
Portal Authentication Records	Specify the retention time of portal authorization records.
Log	Specify the retention time of logs.
Interference Detection	Specify the retention time of scanned Interference Detection. Corresponding to Tools-Interference Detection.

24. 3 Server Settings

On the Server Settings page, You can manage the Server configuration of the controller. In the Mail Server section, you can configure the controller to send emails for resetting your password, pushing notifications, and delivering system logs. The mail server feature works with the SMTP (Simple Mail Transfer Protocol) service provided by an email service provider.

Configuration

1. Go to Settings > Server Settings. Enable the SMTP (Simple Mail Transfer Protocol) Service in your email account. For details, refer to the instructions of your email service provider.
2. Enable Mail Server and configure the parameters.



SMTP	Enter the URL or IP address of the SMTP server according to the instructions of your email service provider.
Port	Configure the port used by the SMTP server according to the instructions of the email service provider.
SSL	Enable or disable SSL according to the instructions of your email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between the controller and the SMTP server
Authentication	Enable or disable Authentication according to the instructions of your email service provider. If Authentication is enabled, the SMTP server requires the user name and password for authentication. Username: When Authentication is enabled, enter your email address as the username. Authorization Code: When Authentication is enabled, enter the authentication code as the password, which is provided by the email service provider when you enable the SMTP service.
Sender Email	Specify the sender address of the email. If you leave it blank, the controller will uses your email address as the sender address.
Test Emal	Specify an email address to send a test email to check the mail server configuration.

24. 4 Platform Integration

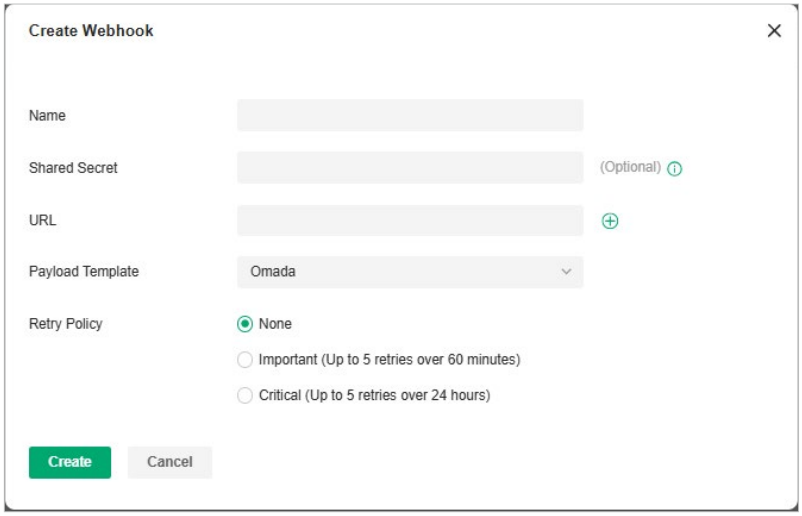
24. 4. 1 Open API

Overview

Webhook is an API concept and one of the usage paradigms of microservice APIs. It is also called a reverse API, that is, the front end does not actively send requests, but is completely pushed by the back end. In Omada, Webhook is used for the active push function of messages such as alerts.

Configuration

1. Go to Settings > Platform Integration > Webhooks.
2. Click Create New Webhook.



Name	Specify the Webhook entry name.
Shared Secret	Authentication secret key. It is generated by the system by default. You can also modify it manually.
URL	Specify the Webhook URL address.
Payload Template	Please select a template for message push.
Webhook ID	Displays the Webhook ID automatically generated.
Last Update	Displays the time when the content of the Webhook entry was last modified.
Retry Policy	Specify the Webhook retry policy, including None (no retry), Important (up to 5 retries over 60 minutes), and Critical (up to 5 retries over 24 hours).
Test	Test the connectivity of the Webhook entry.

Dispatch Logs	View the dispatch log of the Webhook entry.

3. Save the settings. The webhook entry will be added.

You can click the icon in the ACTION column to test the connectivity, view the dispatch logs, and edit, or delete the Webhook entry.

24. 5 Backup & Restore

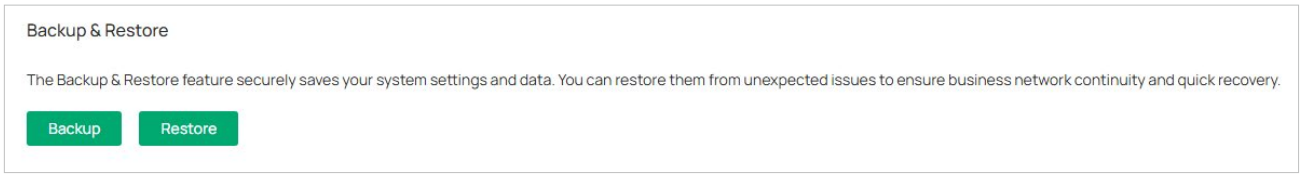
Overview

Backup & Restore allows you to back up and restore configurations to prevent data loss. Meanwhile, you can also set a schedule for the controller to back up configurations and data automatically at the specified time, so you can restore them when needed.

Configuration

■ Configuring Backup & Restore

1. Go to Settings > Backup & Restore. In the Backup & Restore section, select the information and time range for backup files and download the files.
2. When needed, select the backup file in your computer to restore the information.



- Backup:

Backup Contents	Select the contents you want to include in the backup file. Configuration File: Export the configuration data. The configuration file can be used for restoring the configuration. Data: Export the data only, such as logs and client records. These content cannot be used for restoration.
Retained Data Backup	Select the time range in the drop-down list, and the data within the time range and controller settings will be saved in the backup file. If you select Settings Only, only the settings will be saved.
Export	Select where you want to export the data. Export to Downloads:Export and save the data locally. Export to File Server: Export and save the data to a file server. Select the desired file server type (FTP / TFTP / SFTP / SCP) and configure the parameters.

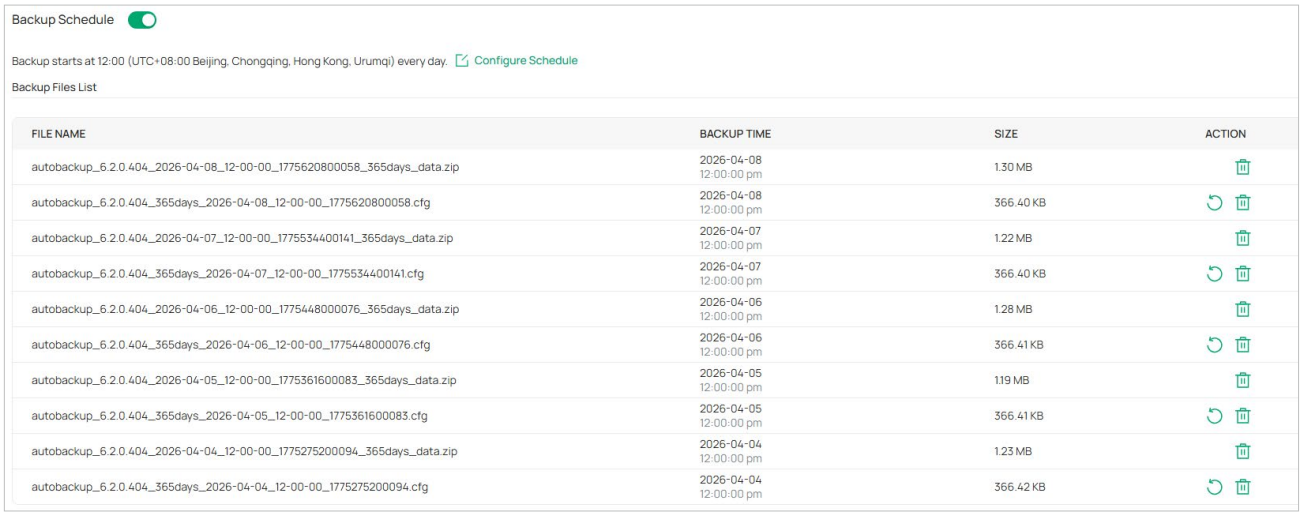
- Restore:

Import	Select where you store the restore file. Import from Local File:Import the data locally. Import from File Server: Import the data from a file server. Select the desired file server type (FTP / TFTP / SFTP / SCP) and configure the parameters.

Restore	Select the backup file to restore the information.

Configuring Backup Schedule

1. Go to Settings > Backup & Restore. In the Backup Schedule section, enable backup schedule and configure the parameters.
2. Restore or delete the backup files when needed.



Note:

The backup files cannot be exported when the gateway is managed via cloud.

Repeat	Specify the schedule cycle (Daily, Weekly, Monthly, or Yearly).
Month&Date/Date/Day	Specify the day or date on which the backup schedule starts.
Retained Data Backup	Select the length of time in days that data will be backed up. 7 Days/30 Days/60 Days/90 Days/180 Days/365 Days: Back up the data in the recent days. All Time: (Only for Software Controller) Back up all data in the controller.
Start Time	Specify the time at which the backup schedule starts.
Retained Data Backup	Select the length of time that data will be backed up. Settings Only: Back up controller settings only. 7 Days/1 Month/2 Months/3 Months/6 Months/1 Year: Back up the data in the recent 7 days/1 month/2 months/3 months/6 months/1 year. All Time: (Only for Omada Controller) Back up all data in the controller.

Storage	Select where you want to save the backup file. Save to Controller Storage: The backup file will be saved as a local file. Save to File Server: The backup file will be saved in the specified file server. Four types of file server are available: FTP, TFTP, SFTP, and SCP.
Type	Specify the file server you are using.
Server Hostname/IP	Specify the Hostname/IP corresponding to the file server.
Port	Specify the port corresponding to the file server.
FTP Username	Specify the username of the FTP file server.
FTP Password	Specify the password of the FTP file server.
SFTP Username	Specify the username of the SFTP file server.
SFTP Password	Specify the password of the SFTP file server.
SCP Username	Specify the username of the SCP file server.
SCP Password	Specify the password of the SCP file server.
File Path	Specify the file path.

24. 6 Migration

Migration allows administrators to migrate all the configurations and data from the current Fusion gateway to another Fusion gateway with the same version. Quick and easy migration makes it convenient to transfer settings and data, which saves you time from setting the same configurations.

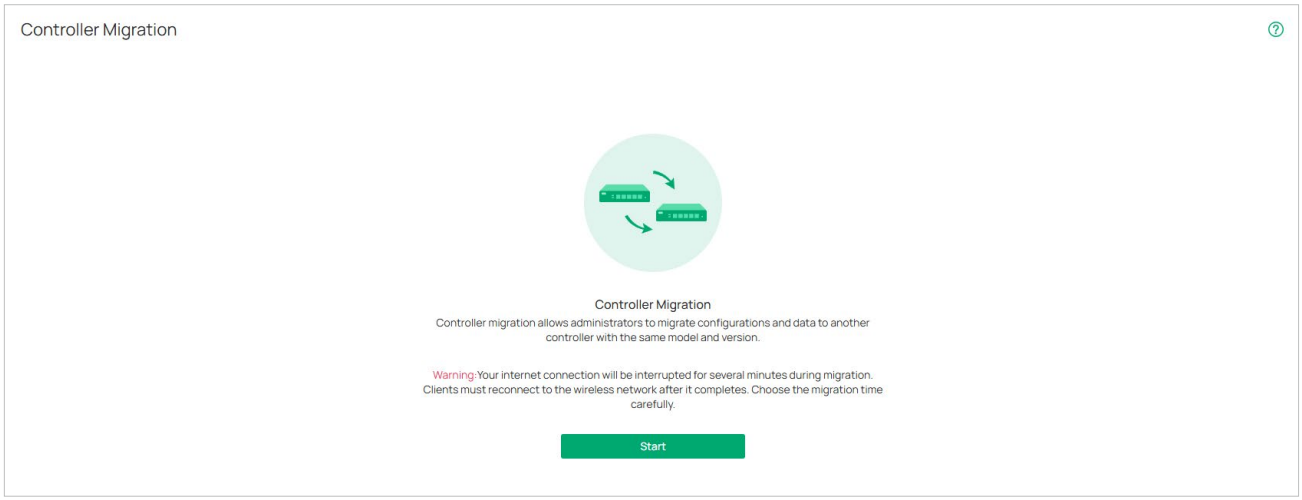
Configuration

Note:

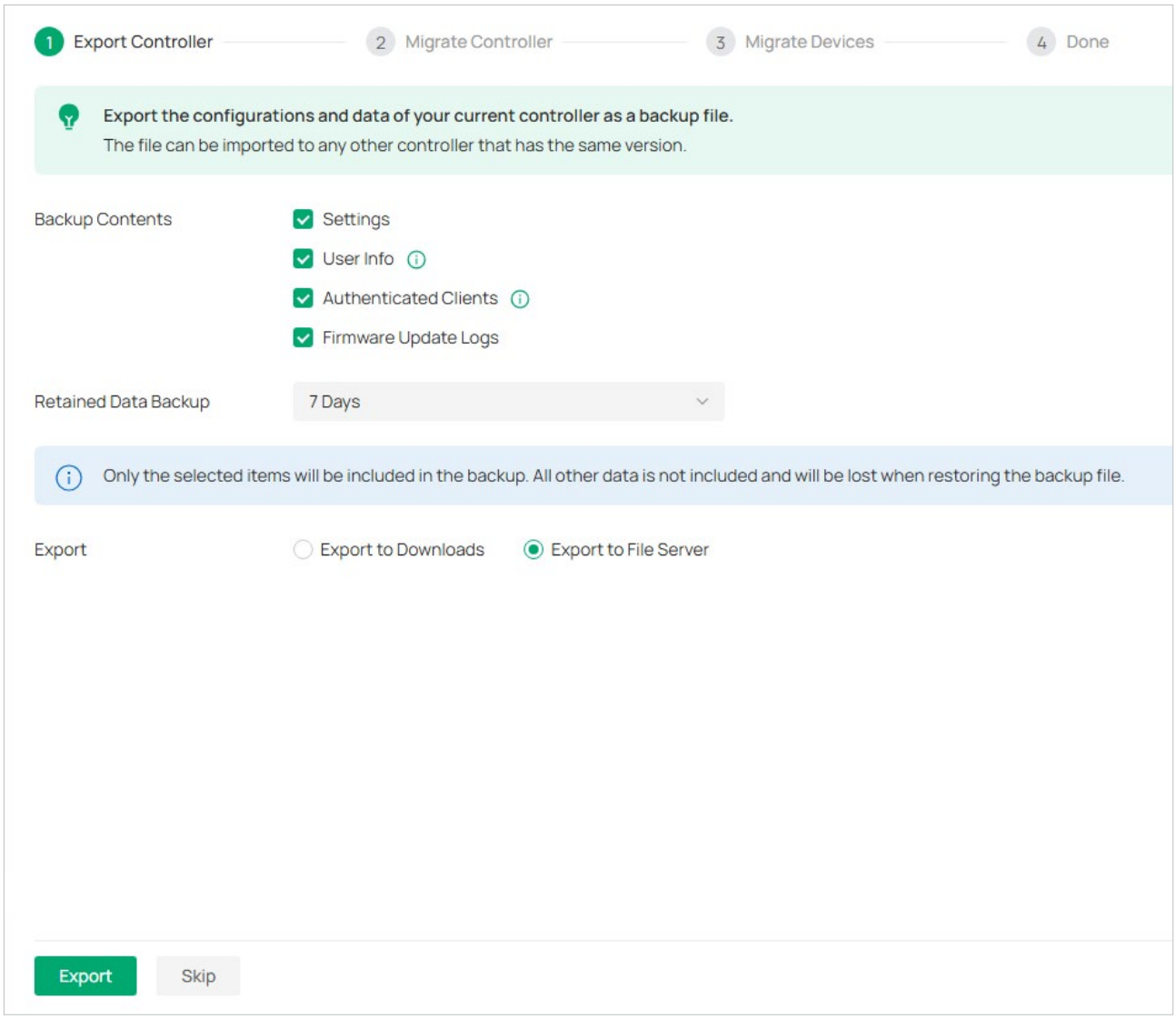
Your internet connection will be interrupted for several minutes during migration. Clients must reconnect to the wireless network after it completes. Choose the migration time carefully.

Step1: Export Controller

1. Go to Settings > Migration. Click the start button on the following page.

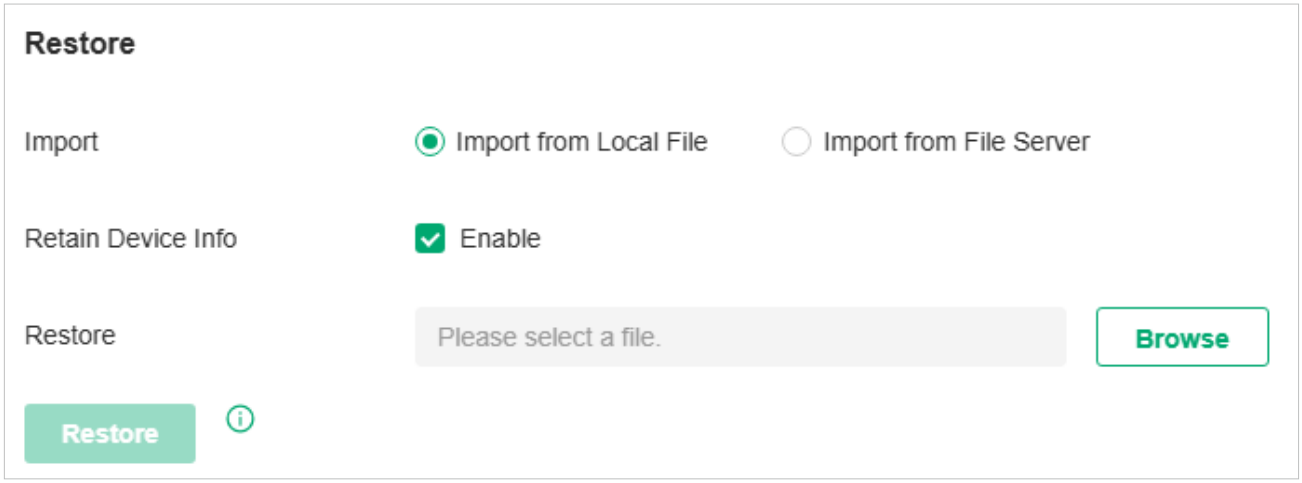


2. Select the length of time in days that data will be backed up in the Retained Data Backup, and where you want to export and save the data. Click Export to export the configurations and data of your current controller as a backup file. If you have backed up the file, click Skip.



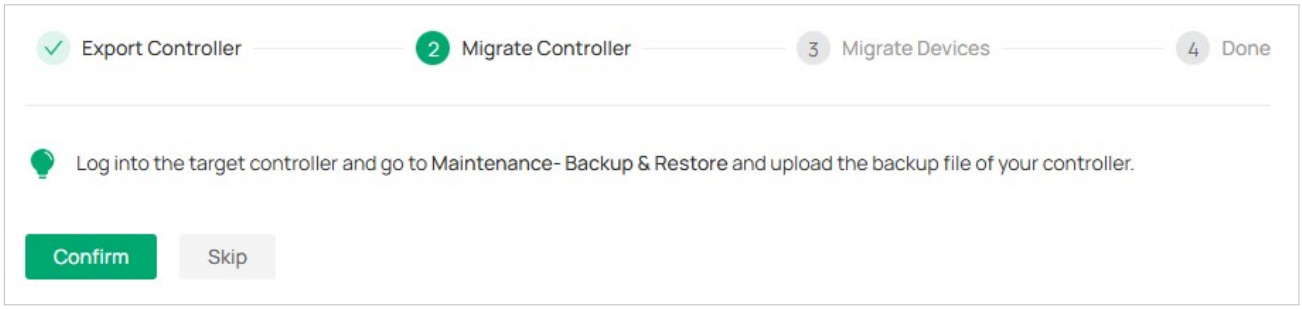
Step2: Migrate Controller

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



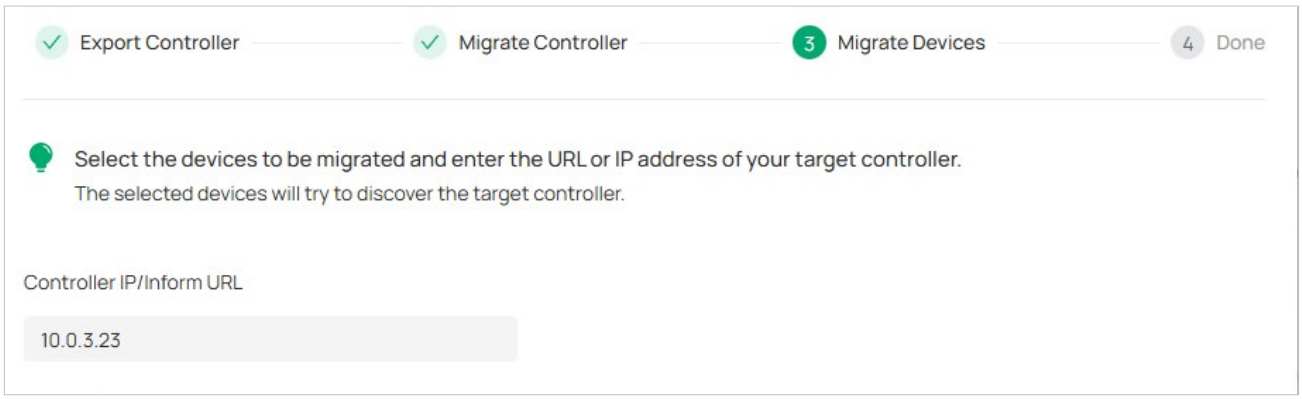
2. After the file has been imported to the target controller, go back to the previous controller and click

Confirm.



Step3: Migrate Devices

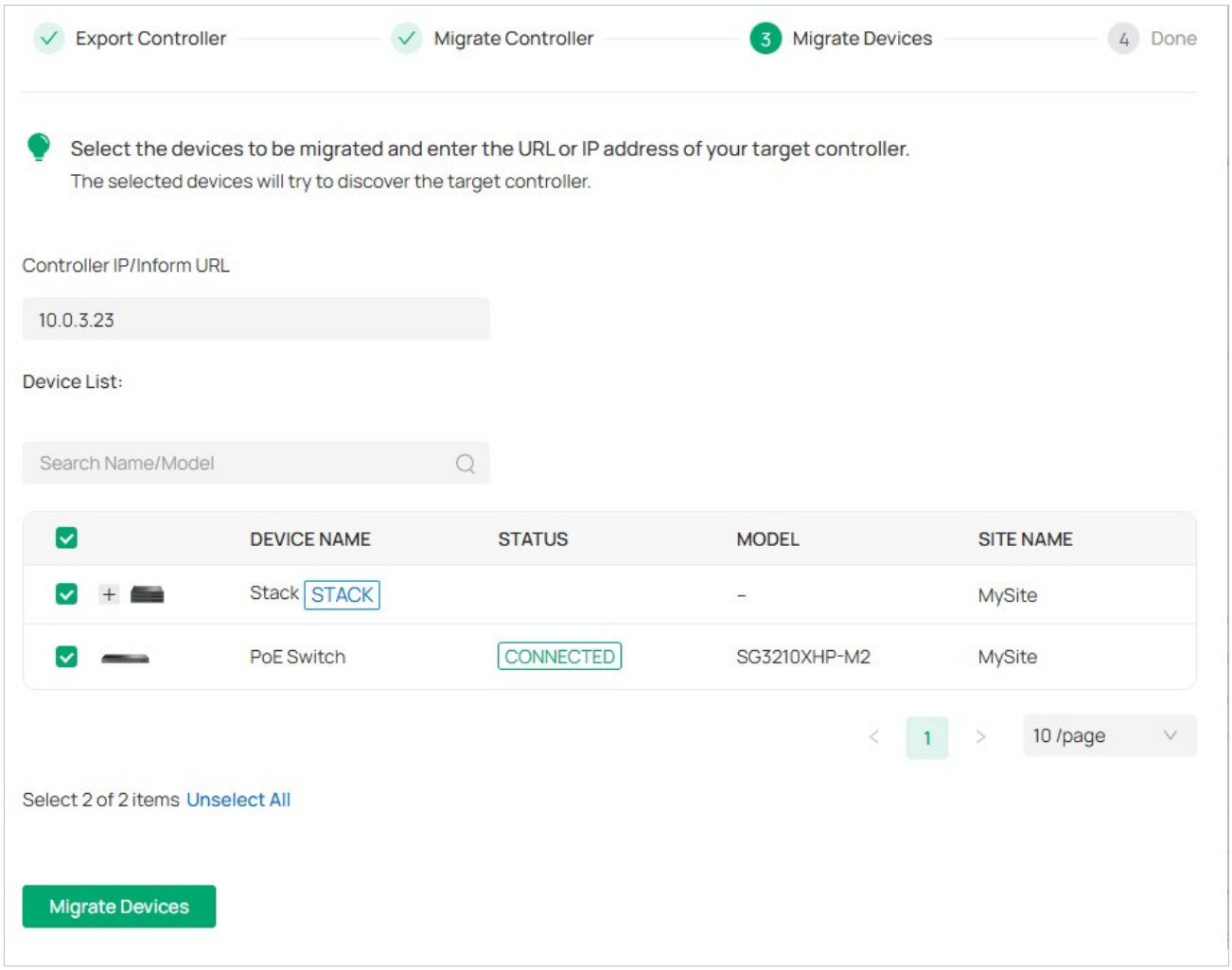
1. Enter the IP address or URL of your target controller into Controller IP/Inform URL input filed. In this case, the IP address of the target controller is 10.0.3.23.



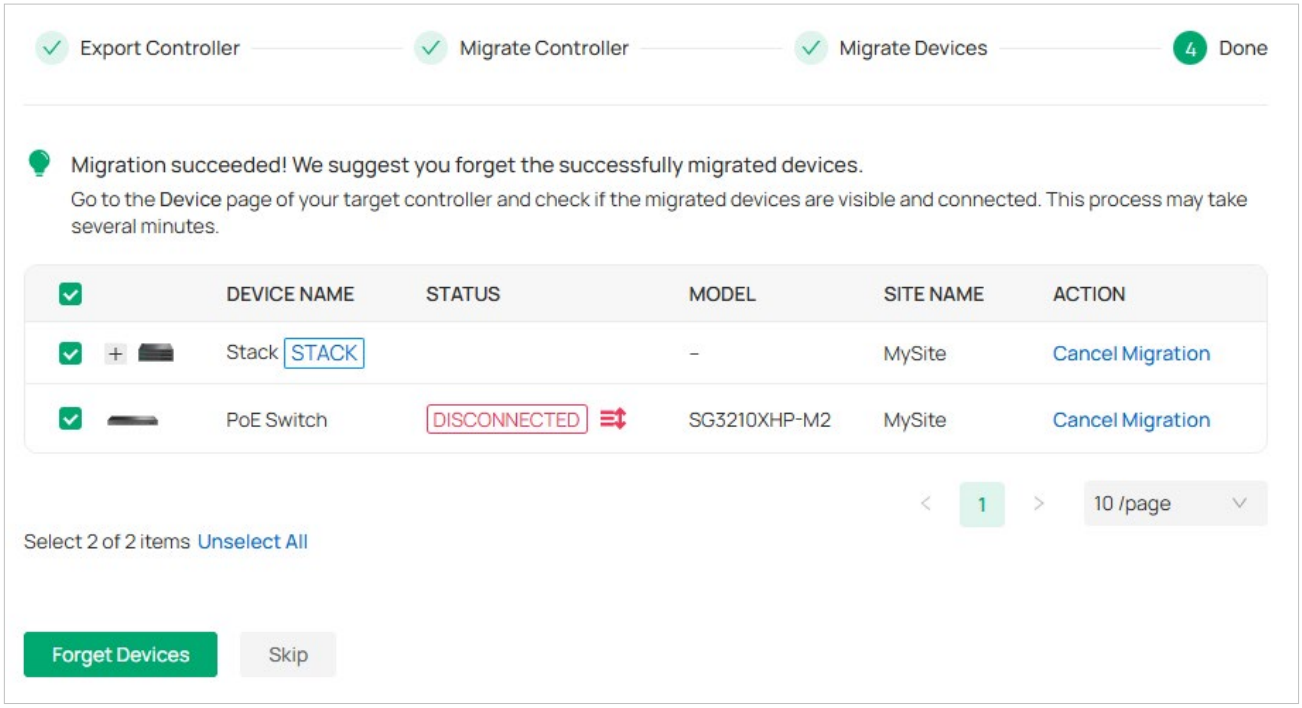
Note:

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

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



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



When the migration process is completed, all the configuration and data are migrated to the target controller.

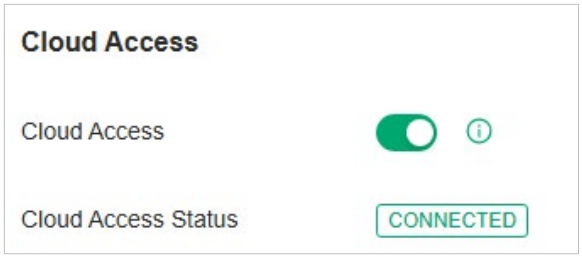
24. 7 Cloud Access

Overview

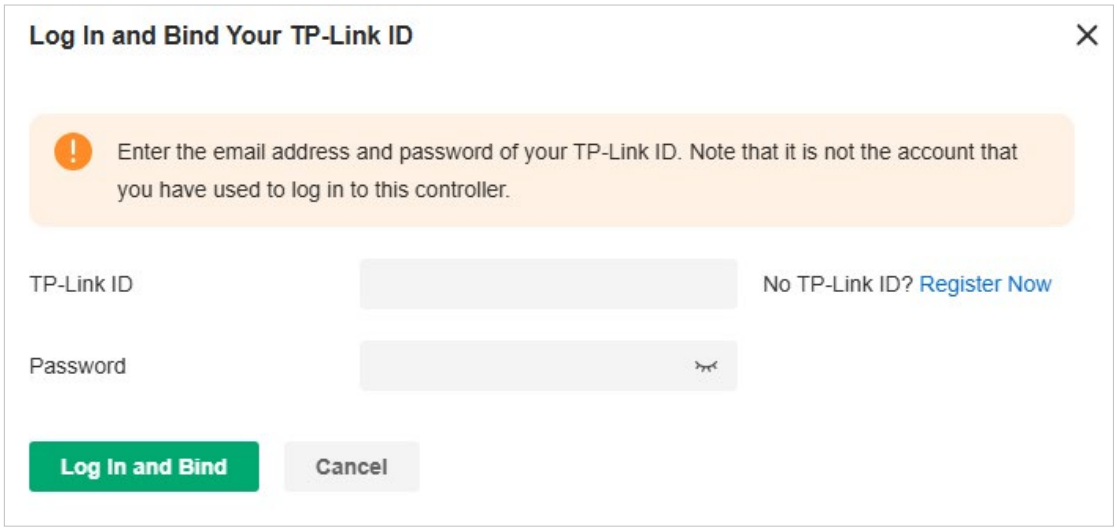
With Cloud Access, it is convenient to centrally manage the entire network at any time and from anywhere, as long as you have access to the internet.

Configuration

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



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



3. Access the Fusion gateway through Omada Cloud Service.

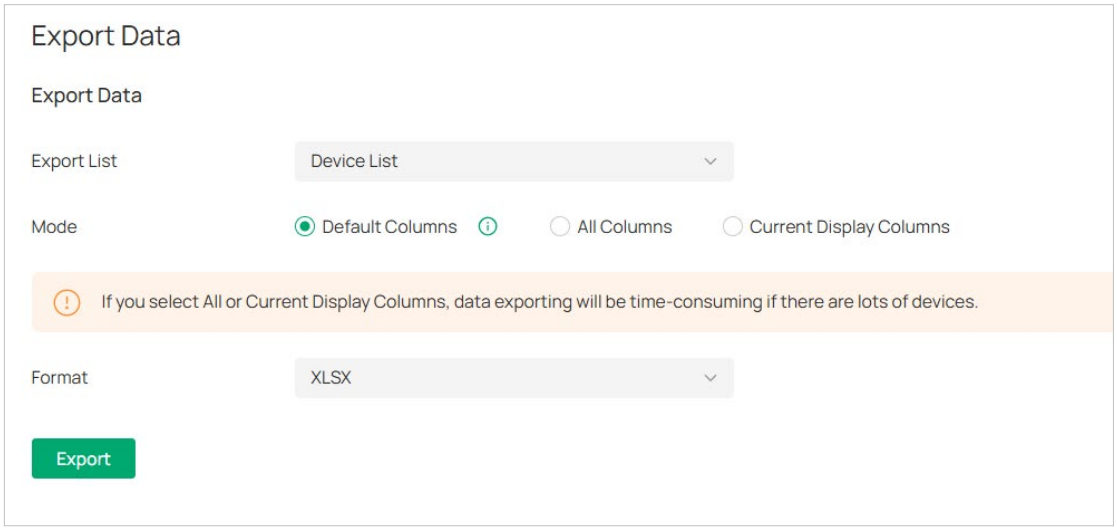
24. 8 Export Data

Overview

You can export the data of the Fusion gateway to monitor or debug the connected devices.

Configuration

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



Export List	Device List: Export the list of managed devices. Client List (All): Export the list of all clients that are connected to the networks. Alert & Event List: Export the list of the alerts and events. Audit Log List: Export the list of the audit logs. Authorized Client List: Export the list of authorized clients. Voucher Codes: Export the list of the voucher codes. Client Connection Records: Export the list of the client connection records. Threat Management: Export the list of the threat management data.
Mode	Select the columns to export. We recommend selecting Default Columns, which include commonly needed columns such as DEVICE NAME, MAC ADDRESS, MODEL, etc. If you select All Columns or Current Display Columns, data exporting will be time-consuming if there are lots of devices.
Format	The data can be exported to the file in the format of .CSV or .XLSX.