User Guide

Omada Central Essentials

© 2025 TP-Link 1900000201 V5.15

About this Guide

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

In this guide, the following conventions are used:

Controller	Stands for the Omada Central Essentials.
Gateway/Router	Stands for the Omada Gateway/Router.
Switch	Stands for the Omada Switch.
AP	Stands for the Omada 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

About this Guide

1.Omada Central Essentials Solution Overview

1. 1 Overview 2
1. 2 Core Components 3

2.Get Started with Omada Central Essentials

2. 1 Set Up Your Omada Central Essentials 7
2. 2 Navigate the Controller UI 9
2. 3 Configure Controller Settings 15
2. 3. 1 Organization Status 15
2. 3. 2 Organization Settings 15
2. 3. 3 UI Interaction 17
2. 3. 4 Account Security 18
2. 3. 5 Migration 19
2. 4 Manage Account 24
2. 4. 1 Introduction to User Accounts and Role 24
2. 4. 2 Create and Manage User Accounts 25

3.Manage and Configure Sites

3. 1 Create Sites 28
3. 2 Configure Site Settings 32
3. 2. 1 Site Configuration 32
3. 2. 2 General Config 34
3. 2. 3 Wireless Features 35
3. 2 4 Device Account 37

4.Manage, Configure, and Monitor Devices

4. 1 Adopt Devices 40
4. 2 Introduction to the Devices Page 46
4. 3 Configure and Monitor Gateways 51
4. 3. 1 Configure the Gateway 51
4. 3. 2 Monitor the Gateway 63
4. 4 Configure and Monitor Switches 64

4. 4 1 Configure Switches 64
4. 4. 2 Monitor Switches 90
4. 5 Configure and Monitor APs 95
4. 5. 1 Configure APs 96
4. 5. 2 Monitor APs 107
4. 6 Configure and Manage Bridge Groups 118
4. 6. 1 Introduction to Bridge 118
4. 6. 2 Create a Bridge Group 118
4. 6. 3 Configure and Monitor the Bridge Group 119

5.Configure the Network with Omada Central Essentials

5. 1 Quick Config in Home Page 121
5. 2 Configure Wired Networks 126
5. 2. 1 Set Up an Internet Connection 127
5. 2. 2 Configure LAN Networks 149
5. 2. 3 Configure LAN DNS 165
5. 3 Configure Wireless Networks 167
5. 3. 1 Set Up Basic Wireless Networks 167
5. 3. 2 Advanced Settings 172
5. 3. 3 WLAN Schedule 175
5. 3. 4 802.11 Rate Control 176
5. 3. 5 Multicast/Broadcast Management 177
5. 4 Network Security 179
5. 4. 1 ACL 179
5. 5 Transmission 185
5. 5. 1 Routing 185
5. 5. 2 NAT 188
5. 5. 3 Bandwidth Control 192
5. 6 Configure VPN 196
5. 6. 1 WireGuard VPN 196
5. 7 Configure VoIP 199
5. 7. 1 Call Settings 199
5. 7. 2 VoIP Devices 204
5. 7. 3 Telephone Book 206
5. 7. 4 Call Logs 207
5. 7. 5 Voice Mail 208
5. 7. 6 Call Forwarding 209
5. 8 Services 212

5. 8. 1 DHCP Reservation 212
5. 8. 2 Dynamic DNS 214
5. 8. 3 SSH 217
5. 9 Authentication 219
5. 9. 1 Portal 219
5. 9. 2 Past Portal Authorizations 226
5. 10 Create Profiles 227
5. 10. 1 Groups 227
5. 10. 2 Time Range 229
5. 10. 3 Rate Limit 230
5. 10. 4 APN Profile 231

6.Monitor the Network

6. 1 View the Status of Network with Dashboard 234
6. 1. 1 Page Layout of Dashboard 234
6. 1. 2 Explanation of Widgets 236
6. 2 Monitor the Network with Map 250
6. 2. 1 Topology 250
6. 2. 2 Heat Map 252
6. 3 View Statistics During Specified Period with Insight 260
6. 3. 1 Port Forwarding Status 260
6. 3. 2 Dynamic DNS 261
6. 4 View and Manage Logs 262
6. 4. 1 Alerts 262
6. 4. 2 Events 264
6. 4. 3 Notifications 265
6. 5 Audit Logs 268
6. 6 Monitor the Network with Tools 269
6. 6. 1 Network Check 269
6. 6. 2 Terminal 271
6. 6. 3 Cable Test 271
6. 7 IntelliRecover 273

7.Monitor and Manage the Clients

7. 1 Manage Wired and Wireless Clients in Clients Page 277
7. 1. 1 Introduction to Clients Page 277
7. 1. 2 Using the Clients Table to Monitor and Manage the Clients 277
7. 1. 3 Using the Properties Window to Monitor and Manage the Clients 279

7. 2 Manage Client Authentication in Hotspot 283
7. 2. 1 Dashboard 283
7. 2. 2 Authorized Clients 283
7. 2. 3 Voucher Groups 284
7. 2. 4 Form Auth Data 288
7. 2. 5 Operators 289

Chapter 1

Omada Central Essentials Solution Overview

Omada Central Essentials is a free and easy version of Omada Central. It offers free, easy-to-use cloud-based centralized management and monitoring for the Omada networking system, covering access points, switches, and gateways, ideal for surveillance networks and small businesses.

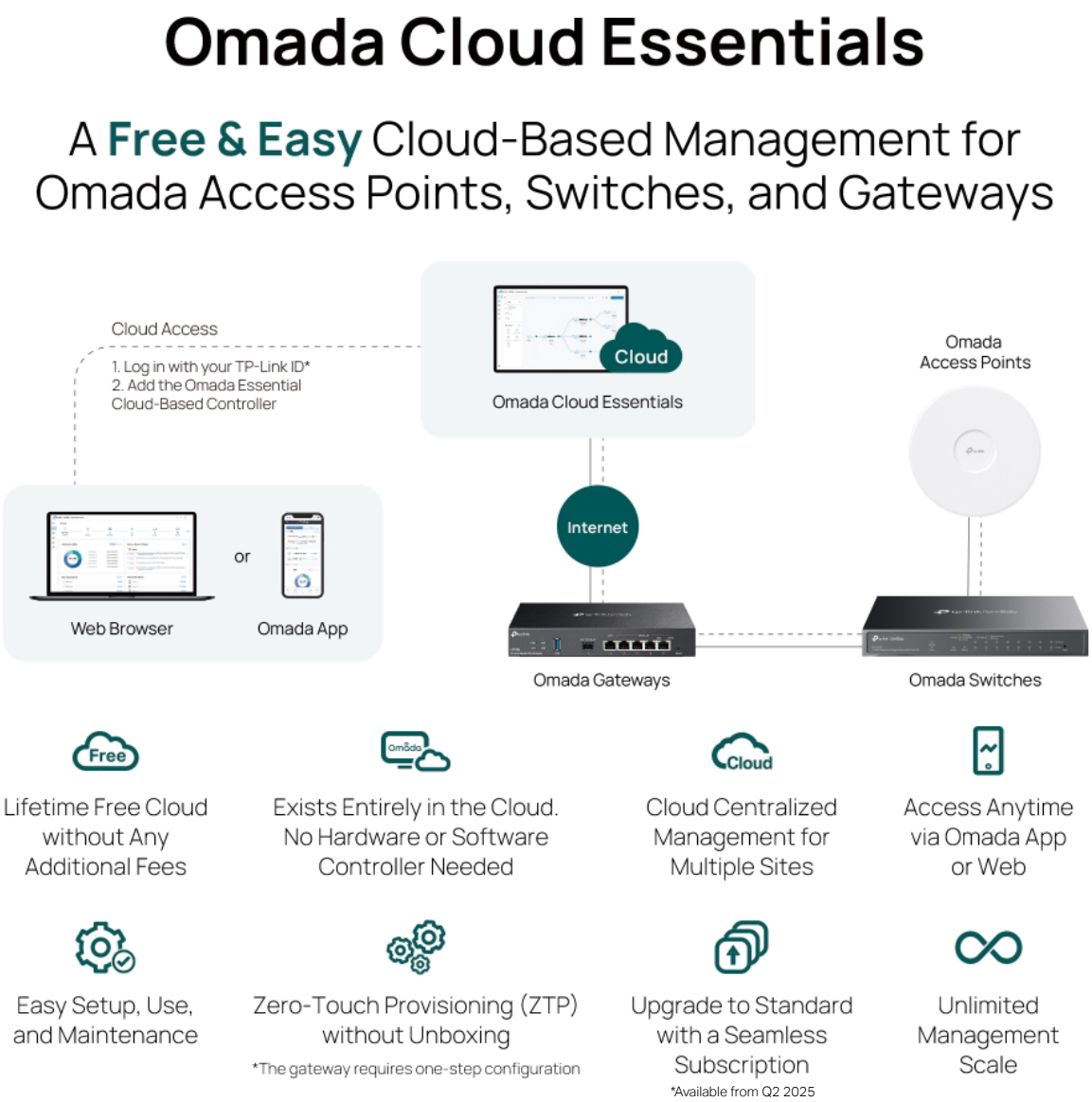
The chapter includes the following sections:

- 1. 1 Overview
- 1. 2 Core Components

1. 1 Overview

Omada Central Essentials is a free and easy version of Omada Central. It offers free, easy-to-use cloud-based centralized management and monitoring for the Omada networking system, covering access points, switches, and gateways, ideal for surveillance networks and small businesses.

This figure shows a sample architecture of an Omada Central Essentials network:



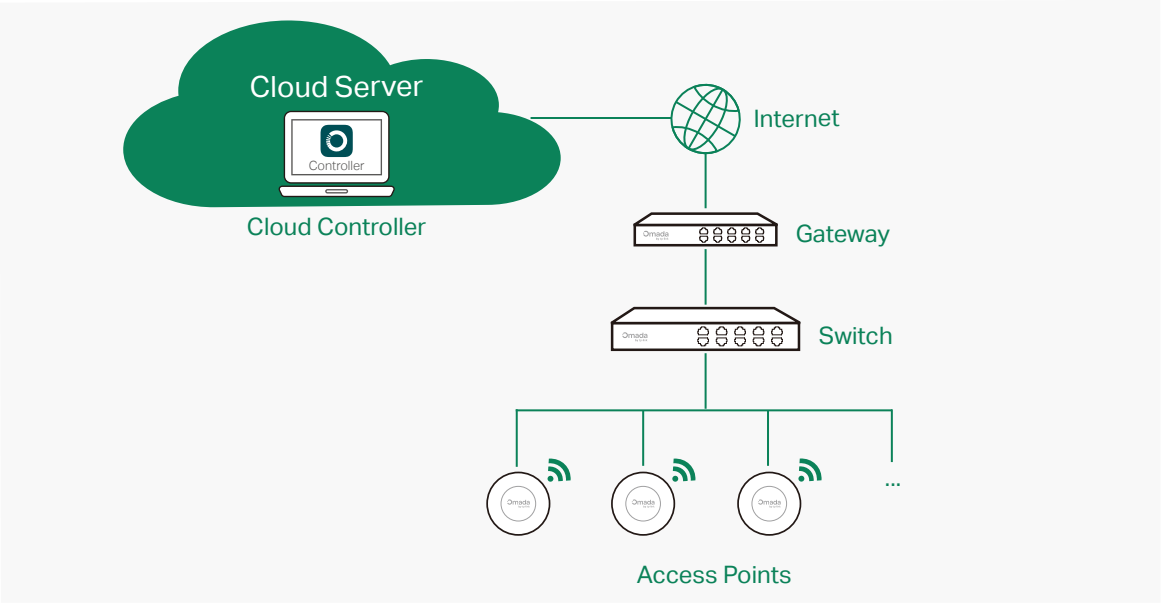
1. 2 Core Components

An Omada Central Essentials network consists of the following core components:

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

Omada Central Essentials

Omada Central Essentials is deployed on the Omada Cloud server, providing free services. You can configure and manage the devices via the cloud service, and you need not purchase an additional hardware device or install the software on the host.



Gateways

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

Managing the gateway centrally through Omada Central Essentials is available on certain models only. For more information, refer to https://www.omadanetworks.com/omada-sdn/product-list/.

Switches

Omada Switch provides high-performance and enterprise-level security strategies and lots of advanced features, which is ideal access-edge for the SDN network.

Managing the switch centrally through Omada Central Essentials is available on certain models only. For more information, refer to https://www.omadanetworks.com/omada-sdn/product-list/.

Access Points

Omada Access Point provides business-class Wi-Fi with superior performance and range

which guarantees reliable wireless connectivity for the SDN network.

Managing the access points centrally through Omada Central Essentials is available on certain models only. For more information, refer to https://www.omadanetworks.com/omada-sdn/product-list/.

Chapter 2

Get Started with Omada Central Essentials

This chapter guides you on how to get started with Omada Central Essentials to configure the network. The chapter includes the following sections:

- 2.1 Set Up Your Omada Central Essentials
- 2. 2 Navigate the Controller UI
- 2. 3 Configure Controller Settings
- 2. 4 Manage Account

2. 1 Set Up Your Omada Central Essentials

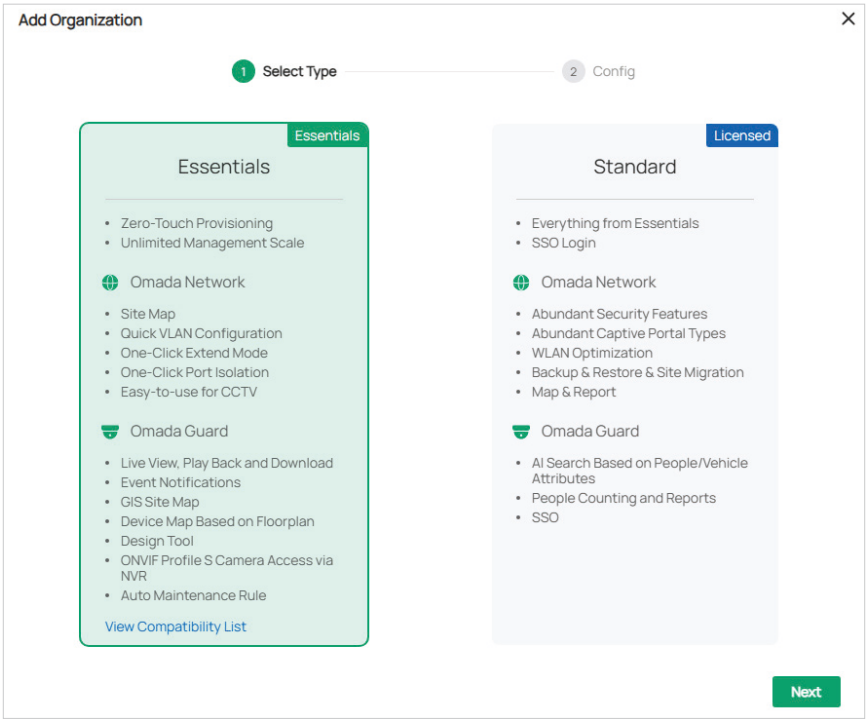
The Omada Central Essentials solution offers easy and free management of essential features.

View the compatible device list below to see if your devices can be centrally managed by the Omada Essential Cloud-Based Controller:

https://www.omadanetworks.com/omada-cloud-essentials/product-list/

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

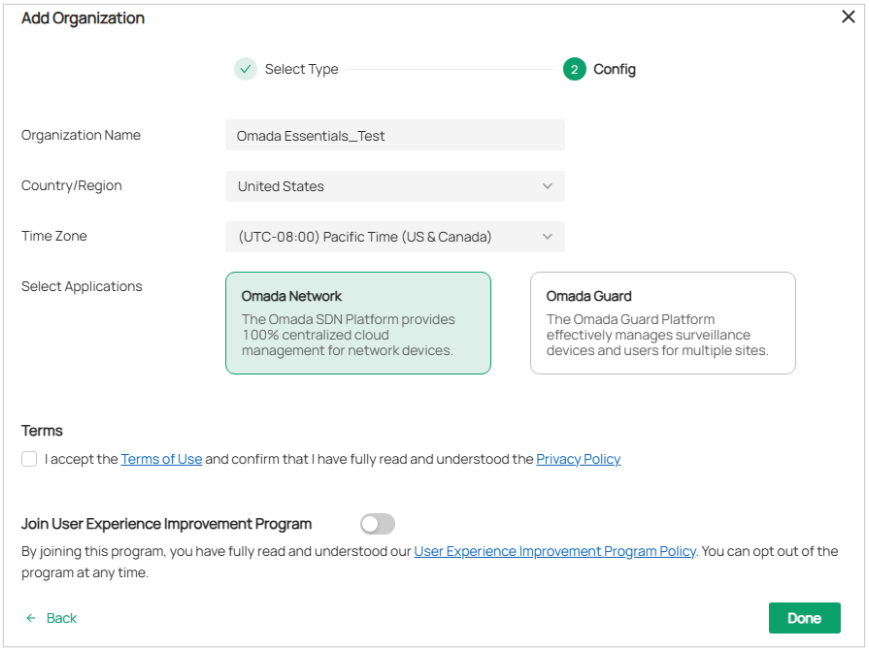
1. Launch a web browser and enter https://omada.tplinkcloud.com in the address bar. Enter your TP-Link ID and password to log in. If you do not have a TP-Link ID, create a TP-Link ID first.
2. On the Cloud-Based Systems page, click Add Organization and select Essentials.
   - Omada Central Essentials: for easy and free management of essential features.
   - Omada Central Standard: for basic and advanced features through subscription-based licensing. (For guidance on Omada Central Standard, refer to Omada SDN Controller_User Guide.)



3. Select Omada Network and follow the instructions to complete the setup process.

   • Omada Network: The Omada SDN Platform provides 100% centralized cloud management for network devices.

   • Omada Guard: The Omada Guard Platform effectively manages surveillance devices and users for multiple sites. (For guidance on Omada Guard, refer to the user guide of Omada Guard.)



4. Add devices with the serial number, make sure the devices are online and in factory default.

2. 2 Navigate the Controller UI

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

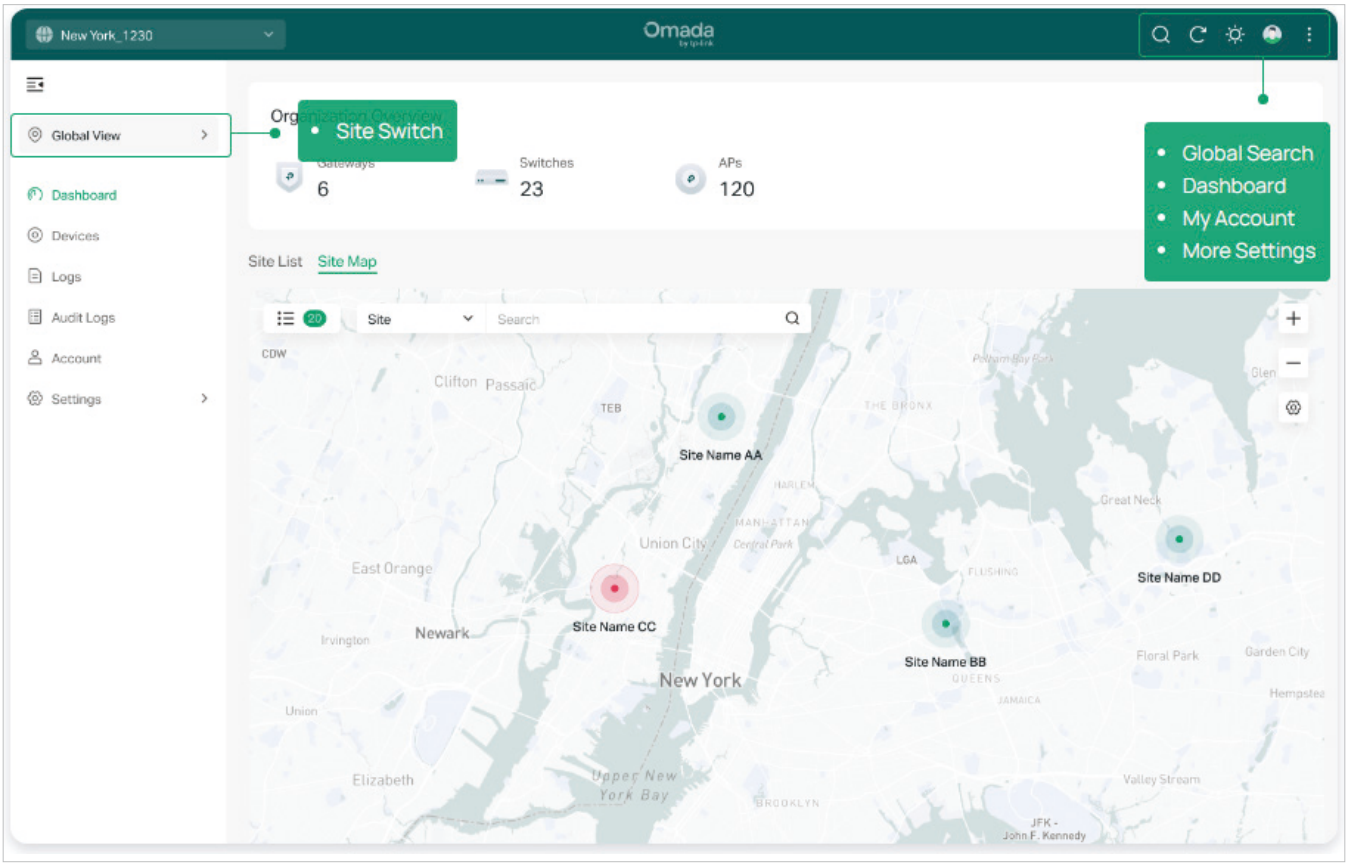
Note:

Features available in the Omada SDN Controller may vary due to your region, controller type and version, and device model.

■ Global Overview

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

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



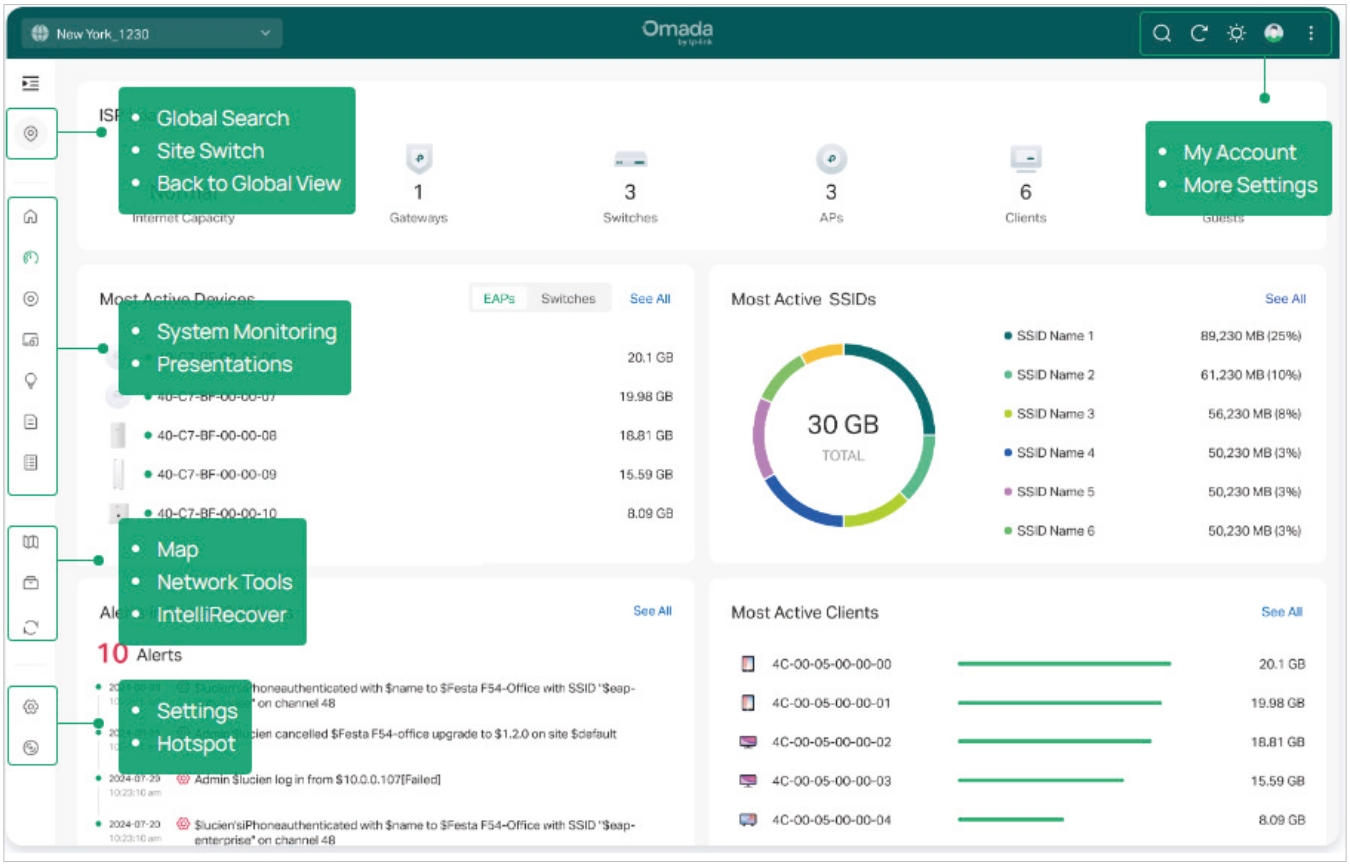
■ Site Overview

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

- Monitoring—Keep you informed of accurate, real-time status of every network device

and client.

- Settings—Configure all your network devices centrally.



■ Network Monitoring

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

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

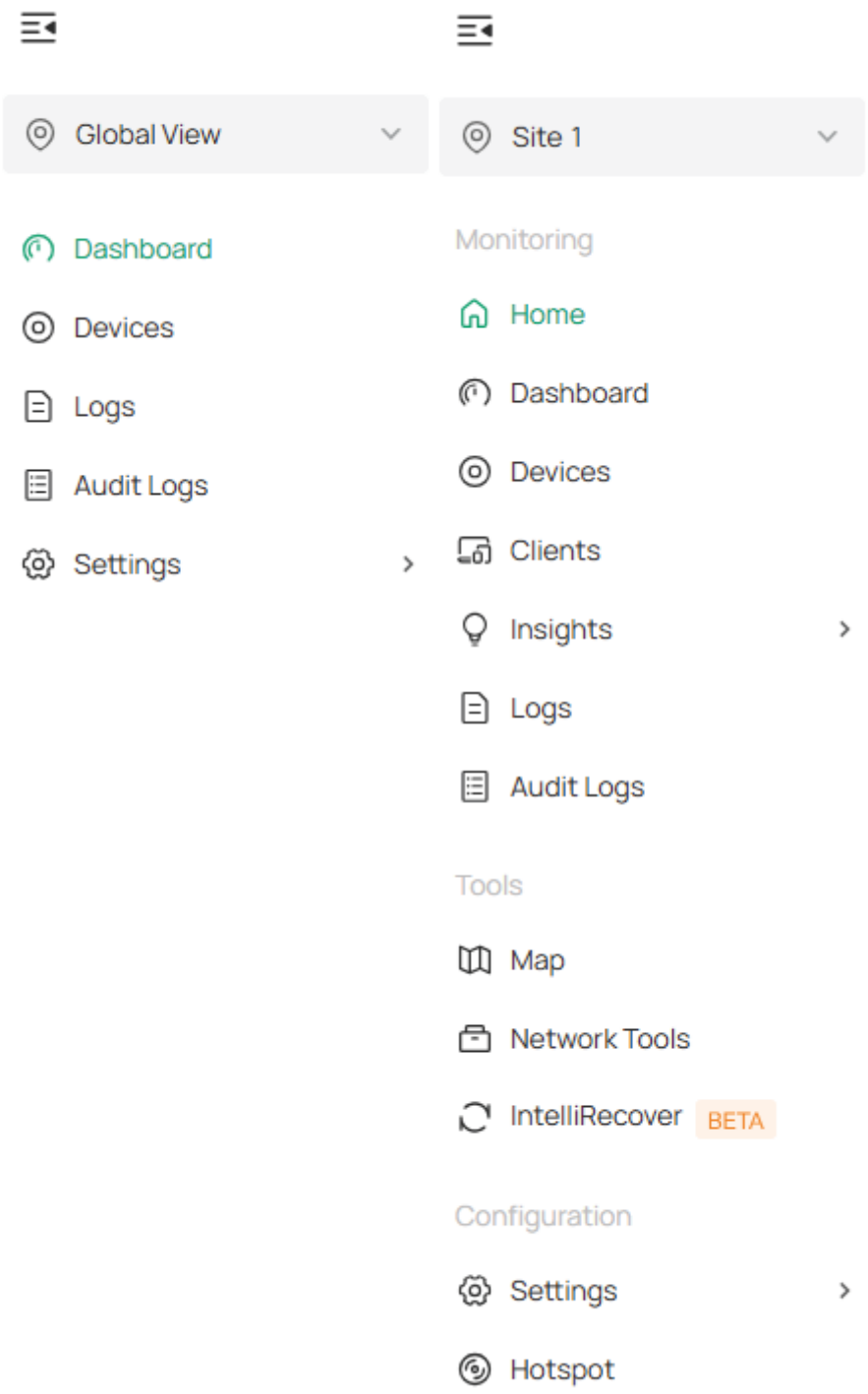
The elements in the top right corner of the screen give quick access to:



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.Z **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.

The left-hand navigation bar provides access to



Global/Site View Drop-down List	Allows you to access the Global View or access a site quickly. Global View: Know the status of your Site at a glance, and manage sites in the platform. Site View: Know the status of your network at a glance, gain insights, and manage network devices all in the platform.
Dashboard	Displays a summarized view of the network status through different visualizations. The customizable and widget-driven dashboard is a powerful tool that arms you with real-time data for monitoring the network. With the drag and drop feature, you can modify your dashboard and re-arrange it to let you track all the important metrics.
Devices	Displays all TP-Link devices discovered on the site and their general information. This list view can change depending on your monitoring need through customizing the columns. You can click any device on the list to reveal the Properties window for more detailed information of each device and provisioning individual configurations to the device.
Clients	Displays a list view of wired and wireless clients that are connected to the network. This list view can change depending on your monitoring need through customizing the columns. You can click any clients on the list to reveal the Properties window for more detailed information of each client and provisioning individual configurations to the client.
Insights	Displays a list of statistics of your network device, clients and services during a specified period. You can change the range of date in one-day increments.
Logs	Shows log lines about varied activities of users, devices, and systems events, such as administrative actions and abnormal device behaviors. Comprehensive logs make historical information more accurate, readily accessible, and usable, which allows for proactive troubleshooting. And you can determine alert-level events and enable pushing notifications.
Audit Logs	Records information about which accounts have accessed the site, and what operations they have performed during a given period of time.
Map	Generates the system topology automatically and you can look over the provisioning status of devices. By clicking on each node, you can view the detailed information of each device. You can also upload images of your location for a visual representation of your network.
Network Tools	Provides various network tools for you to test the device connectivity, capture packets for troubleshooting, and open Terminal to execute CLI or Shell commands.
IntelliRecover	Monitors the status of PoE devices, automatically repairing abnormal devices.

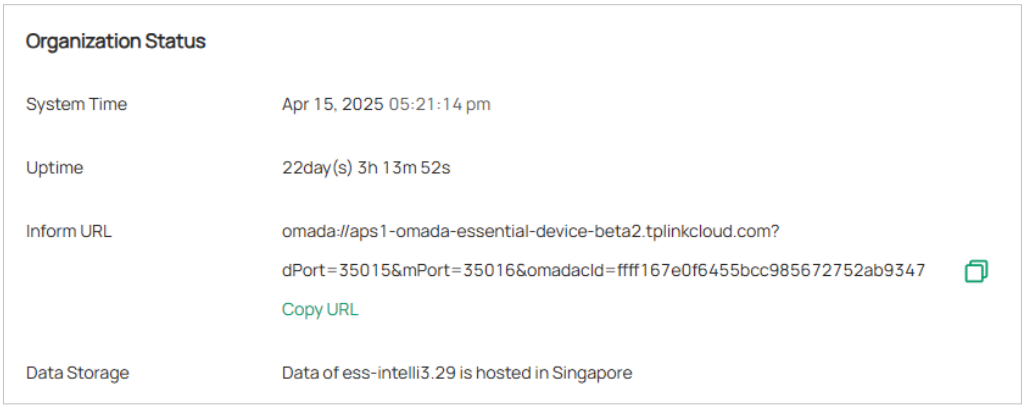
Settings	Allows you to provision and configure all your network devices on the same site in minutes and maintain the controller system for best performance.
Hotspot	Allows you to centrally monitor and manage the clients authorized by portal authentication.

2. 3 Configure Controller Settings

2. 3. 1 Organization Status

Launch the organization and access the Global View. Go to Settings > Organization Status.

In Organization Status, you can view the organization-related information and status.

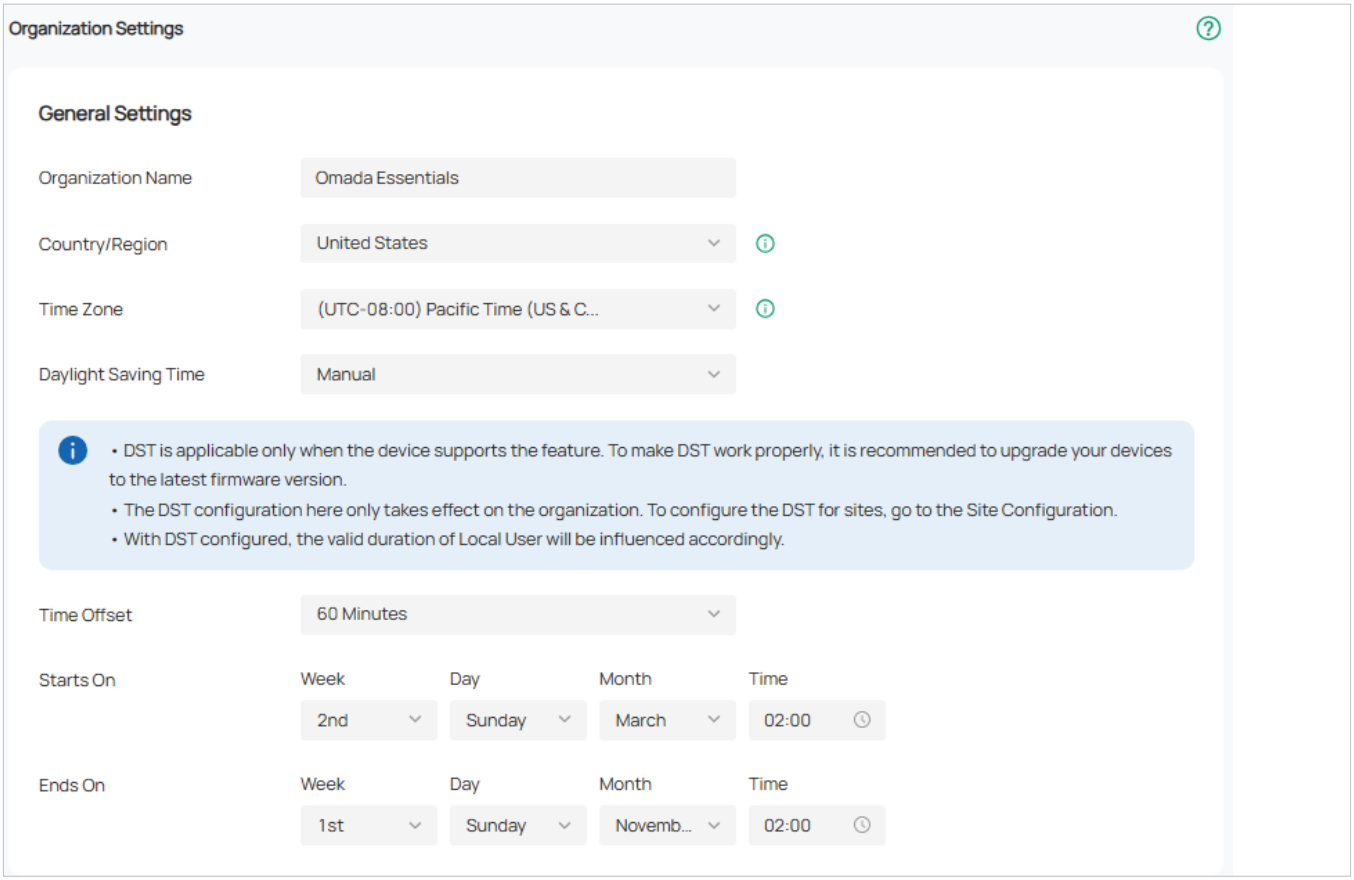


System Time	Displays the system time of the organization. The system time is based on the time zone which you configure. To configure the time zone, go to Settings > Organization.
Uptime	Displays how long the organization has been working.
Inform URL	Displays customer's device management address, used for device discovery or device migration.
Data Storage	Displays where the user data is hosted.

2. 3. 2 Organization Settings

Launch the organization and access the Global View. Go to Settings > Organization Settings.

In General Settings, you can configure general settings of the organization.



Organization Name	Specify the Organization Name to identify the organization.
Country/Region	Select the location of the organization. The configuration here only takes effect on the organization. To configure the Country/Region for sites, go to the Site Configuration.
Time Zone	Select the Time Zone of the organization according to your region. For organization settings, time is displayed based on the Time Zone. The configuration here only takes effect on the organization. To configure the Time Zone for sites, go to the Site Configuration.
Daylight Saving Time	Enable the feature if your country/region implements DST.
Time Offset	Select the time added in minutes when Daylight Saving Time starts.
Starts On	Specify the time when the DST starts. The clock will be set forward by the time offset you specify.

Ends On	Specify the time when the DST ends.The clock will be set back by the time offset you specify.

In Services, you can configure client idle threshold.

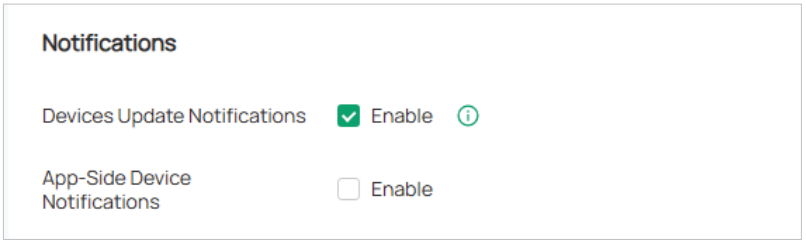


Client Idle Threshold	The organization will consider a client offline (thus disconnect it) when it is idle for longer than the specified threshold. If the specified threshold is too short, clients may be disconnected frequently.

2. 3. 3 UI Interaction

Launch the organization and access the Global View. Go to Settings > UI Interaction.

In Notifications, you can enable the notification features to receive notifications of the device activities.



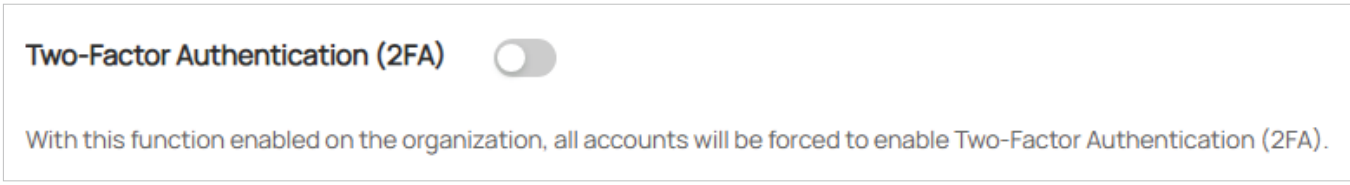
Devices Update Notification	With this feature enabled, you will receive an update notification when a new firmware version for your device is available.
App-Side Device Notifications	With this function enabled, the Organization will send notifications to the app when your devices go online or offline.

2. 3. 4 Account Security

Launch the organization and access the Global View. Go to Settings > Account Security.

■ Two-Factor Authentication (2FA)

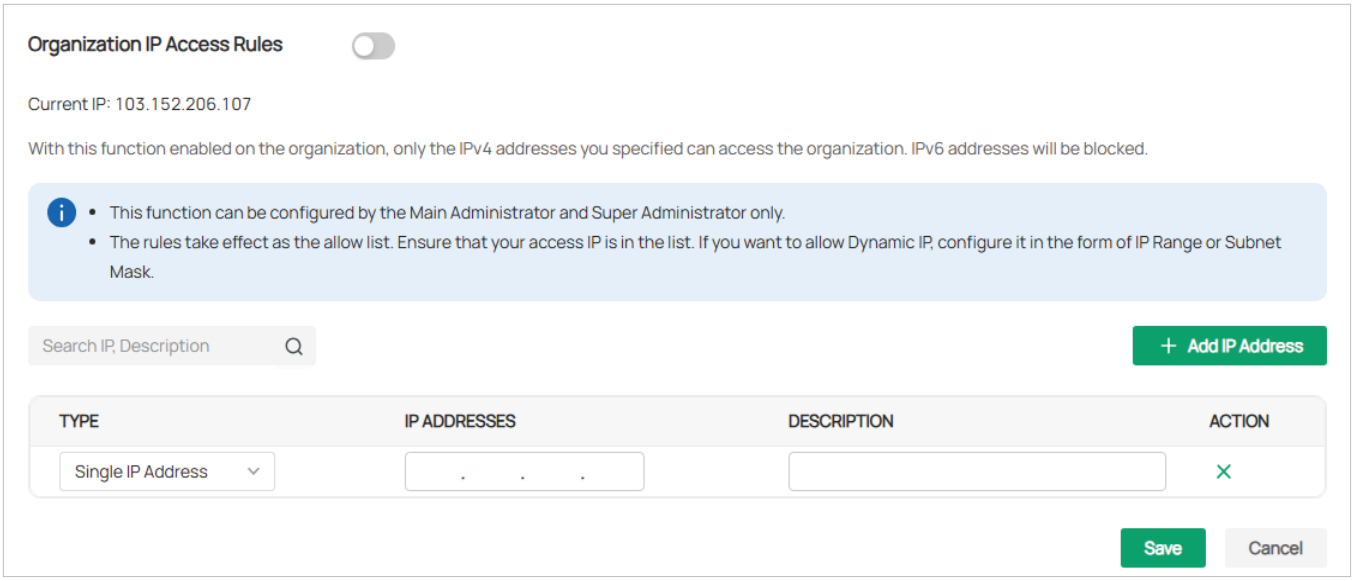
You can enable Two-Factor Authentication (2FA) to improve the security of the organization.



Two-Factor Authentication (2FA)	This function improves the security of the controller by requiring two factors of identification to access resources and data. With this function enabled, all accounts will be forced to enable 2FA upon user login. You can also enable 2FA for accounts on the Admin > User page.

■ Organization IP Access Rules

You can enable Organization IP Access Rules, so that only the IPv4 addresses you specified can access the controller locally. IPv6 addresses will be blocked.



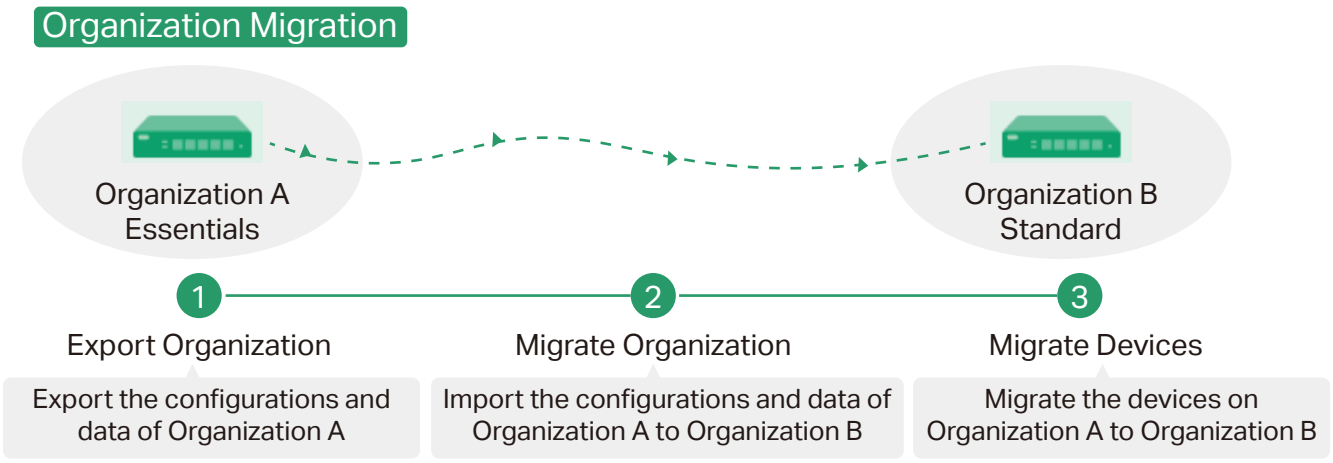
Type	Specify the IP address type: Single IP Address, Single Subnet Mask, or IP Range.
IP Addresses	Specify the IP addresses that are allowed to access the controller.
Description	Enter a description for identification.

2. 3. 5 Migration

Migration services allow users to migrate the configurations and data to any other organization.

Organization Migration allows the administrators to migrate all the configurations and data from the current Essentials organization to a Standard organization. The quick and easy migration makes it convenient to transfer the settings and data, which saves the time from setting the same configurations.

The process of migrating configurations and data can be summarized in three steps: Export Organization, Migrate Organization and Migrate Devices.



Step 1: Export Organization

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

Step 2: Migrate Organization

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

Step 3: Migrate Devices

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

To migrate your controller, follow these steps below.

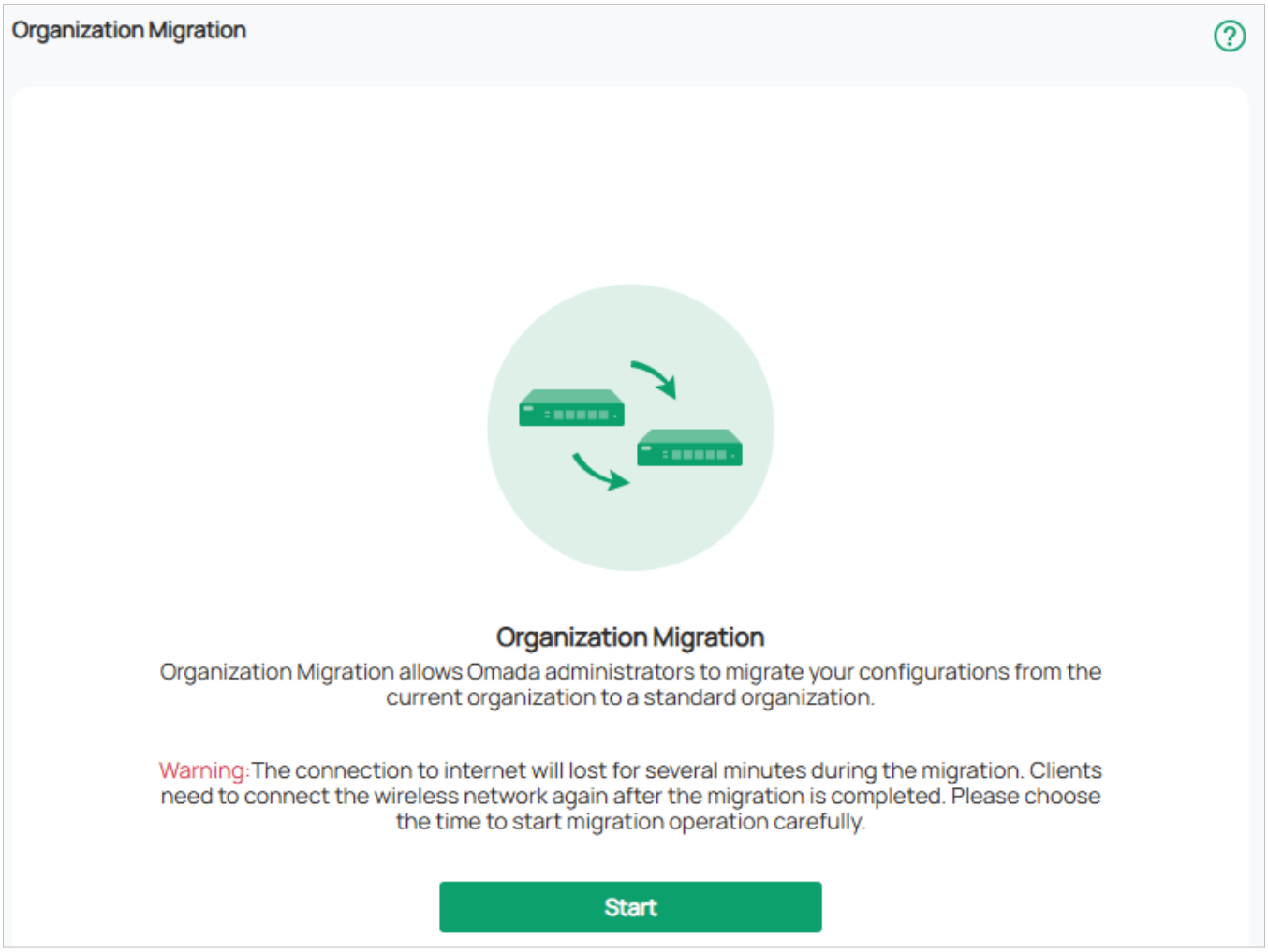
Note:

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

- Configuration Steps:

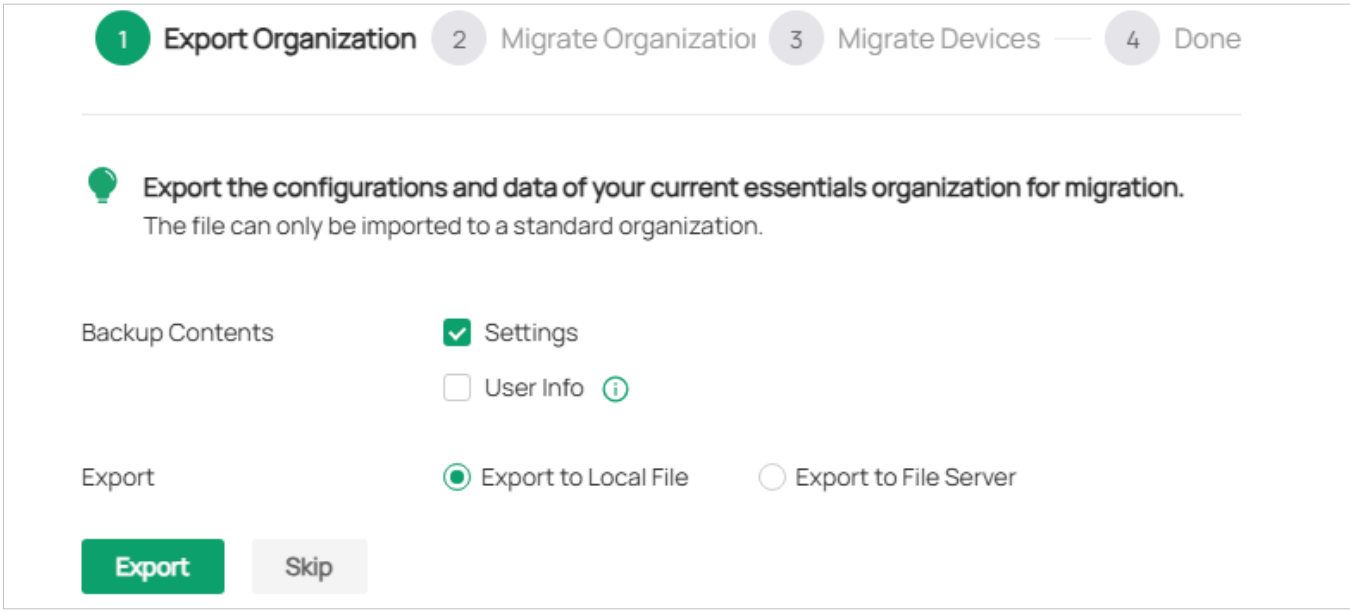
Step 1: Export Organization

1. Launch the organization and access the Global View. Go to Settings > Migration. Click the start button on the following page.



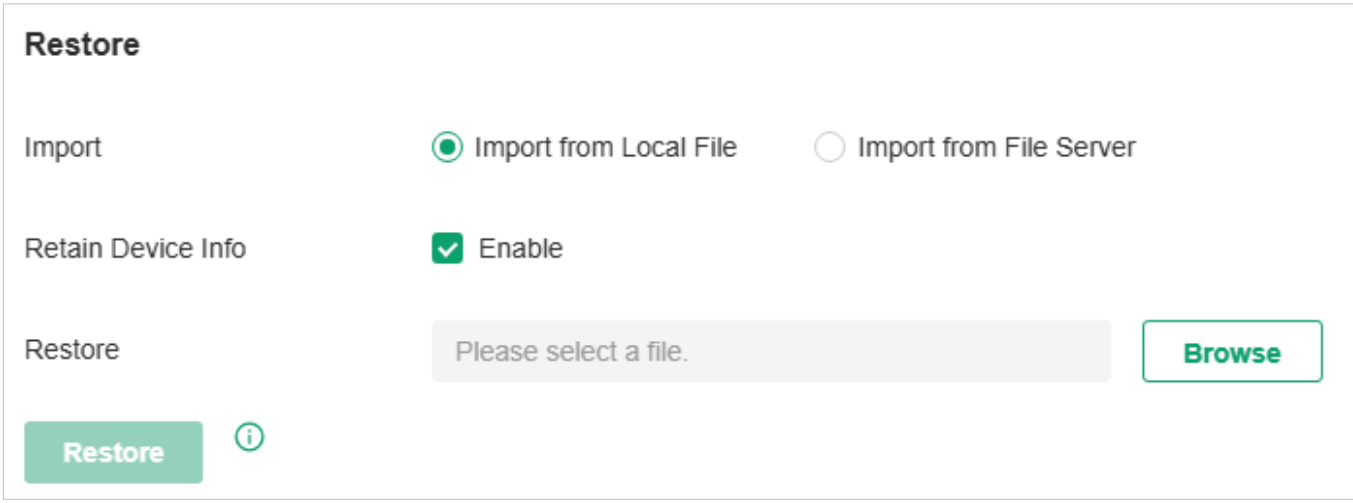
2. Select the backup contents and where you want to export and save the data. Click Export to export the configurations and data of your current organization as a backup file. If you

have backed up the file, click Skip.

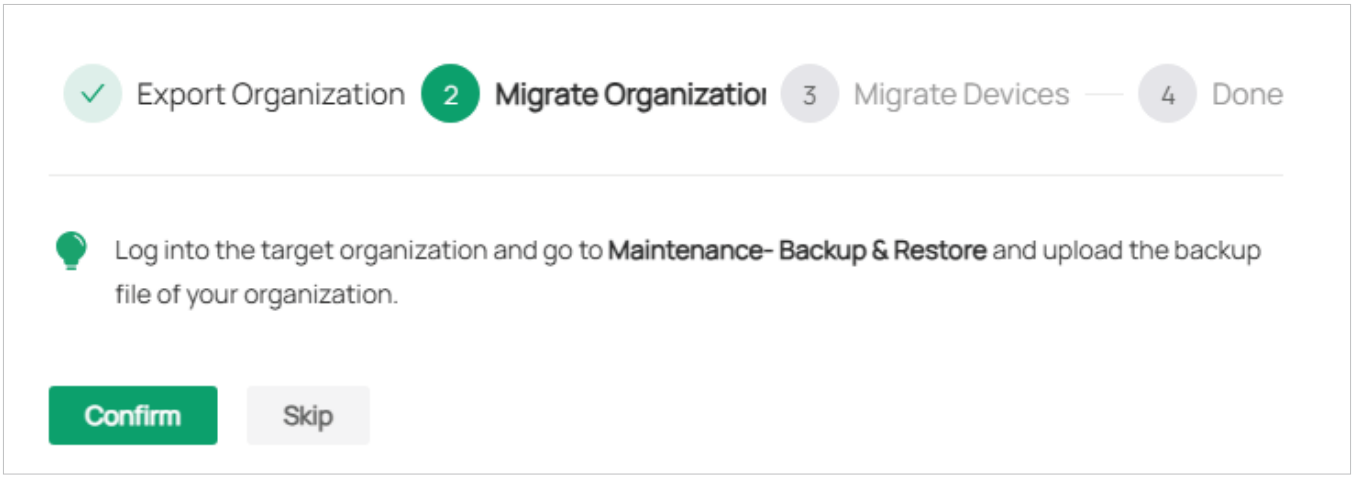


Step 2: Migrate Organization

1. Log in to the target organization. Launch the organization and access the Global View. Go to Settings > Maintenance > Restore. Click Browse to locate and choose the backup file of the previous organization. Then click Restore to upload the file.

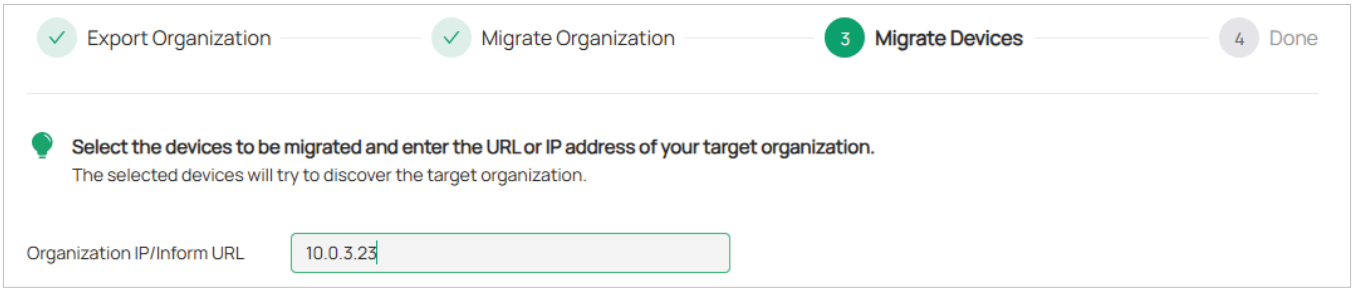


2. After the file has been imported to the target organization, go back to the previous organization and click Confirm.



Step 3: Migrate Devices

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

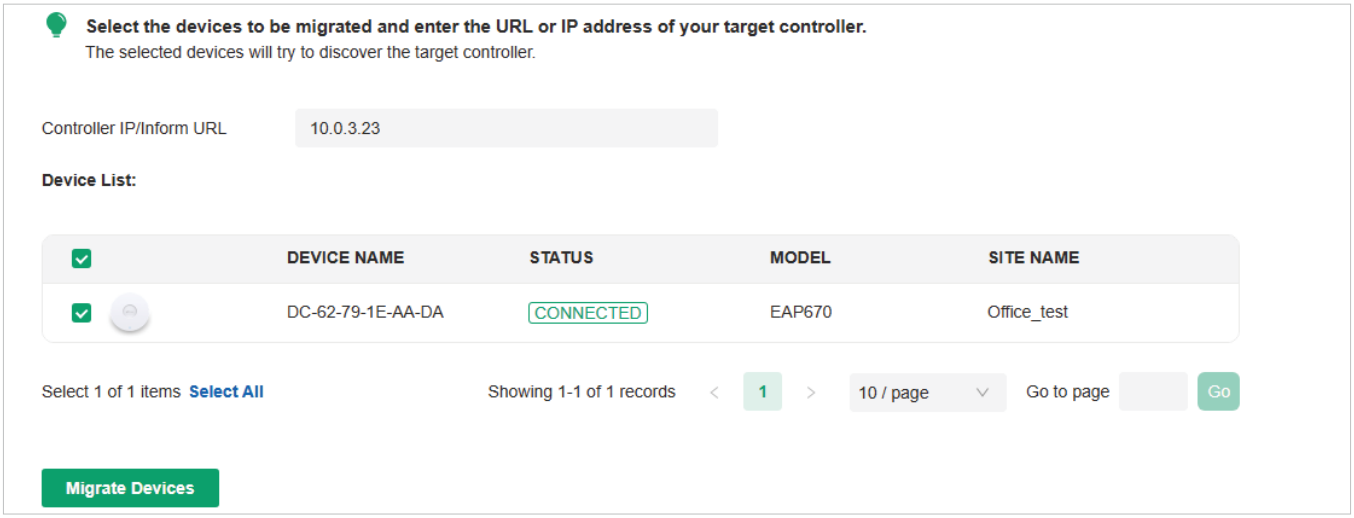


Note:

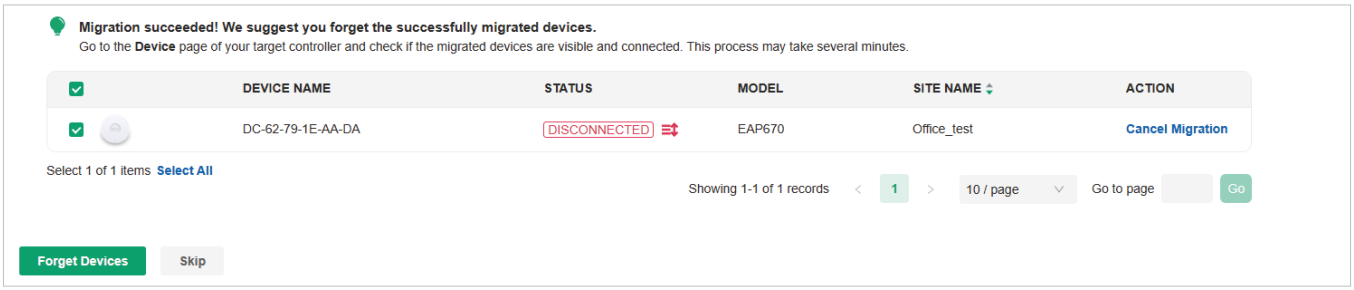
Make sure that you enter the correct IP address or URL of the target organization to establish the communication between managed devices and your target organization. Otherwise the managed devices cannot be adopted by the target organization.

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 organization.



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



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

2. 4 Manage Account

2. 4. 1 Introduction to User Account and Role

- User

The Omada Essential Cloud-Based Controller offers multiple levels of access available for users: **Owner**, **Super Administrator**, **Administrator**, and **Viewer**. You can also create new account roles and customize their permissions to access different features.

Multi-level administrative account presents a hierarchy of permissions for different levels of access to the controller as required. This approach ensures security and gives convenience for management.

Moreover, in the user accounts list of the Owner/Super Administrator, 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.

- Role

In Account > Role, four roles corresponding to the user accounts are displayed. You can view the details or permissions of each role.

- Owner

The Owner has access to all features.

The account who first launches the controller will be the Owner (used to be recognized as Main Administrator in earlier controller versions). It cannot be changed and deleted.

- Super Administrator

The Super Administrator can manage all the other roles (except Owner) and the privileges of most features.

- Administrator

Administrators have no permission to some modules, mainly including cloud access, migration, auto-backup and global view logs. They have read-only permission to some modules, such as global view license management and custom account roles.

Administrators can be created and deleted by the Owner/Super Administrator and

Administrators.

- Viewer

Viewers can view the status and settings of the network, and change the settings in Hotspot Manager.

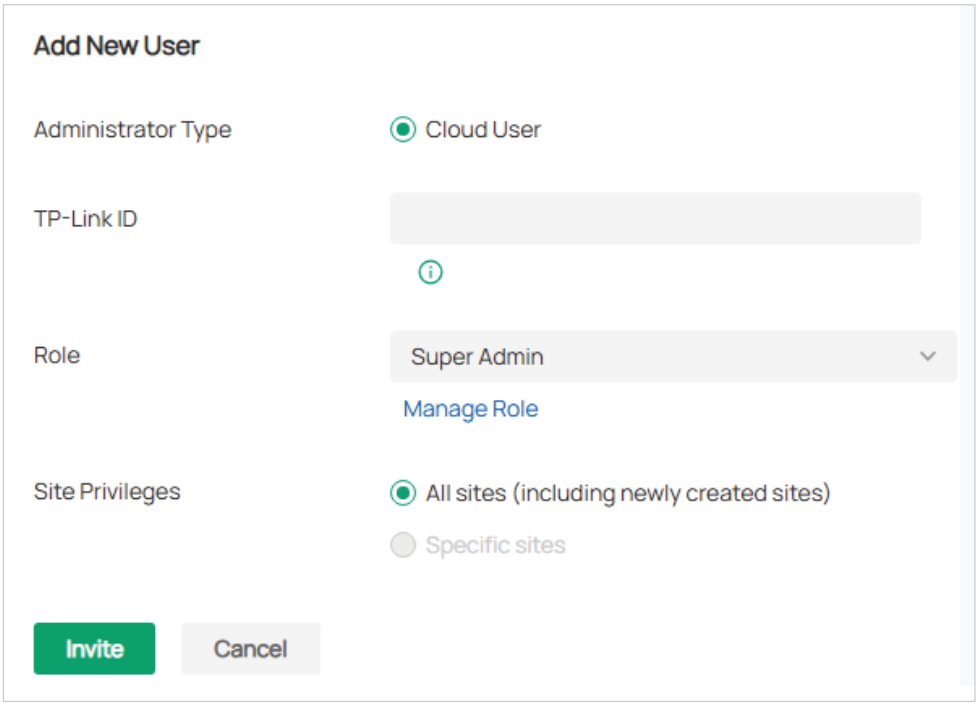
The entrance to Account page is hidden for viewers, and they can be created or deleted by the administrators.

2. 4. 2 Create and Manage User Accounts

The Controller automatically sets up the Owner, which cannot be deleted. The Owner can create, edit, and delete other levels of cloud user accounts.

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

1. Launch the controller and access the Global View. Go to Accounts > User.
2. Click Add New User.
3. Specify the parameters and click Invite.



TP-Link ID	Enter an email address of the created cloud user, and then an invitation email will be sent to the email address. If the email address has already been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation. If the email address has not been registered, it will receive an invitation email for registration. After finishing registration, it will automatically becomes a valid cloud user.
Role	Select a role for the created cloud user. Super Administrator: This role can manage all the other roles (except Owner) and the privileges of most features. Administrator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete main administrator and other administrator accounts. Viewer: This role can view the information of the sites chosen in the site privileges. It can only edit itself.
Site Privileges	Assign the site permissions to the created cloud user. All sites (including newly created sites): The created user has device permissions in all sites, including all new-created sites. Specific sites: The created user has device permission in the sites that are selected. Select the sites by checking the box before them.

Chapter 3

Manage and Configure Sites

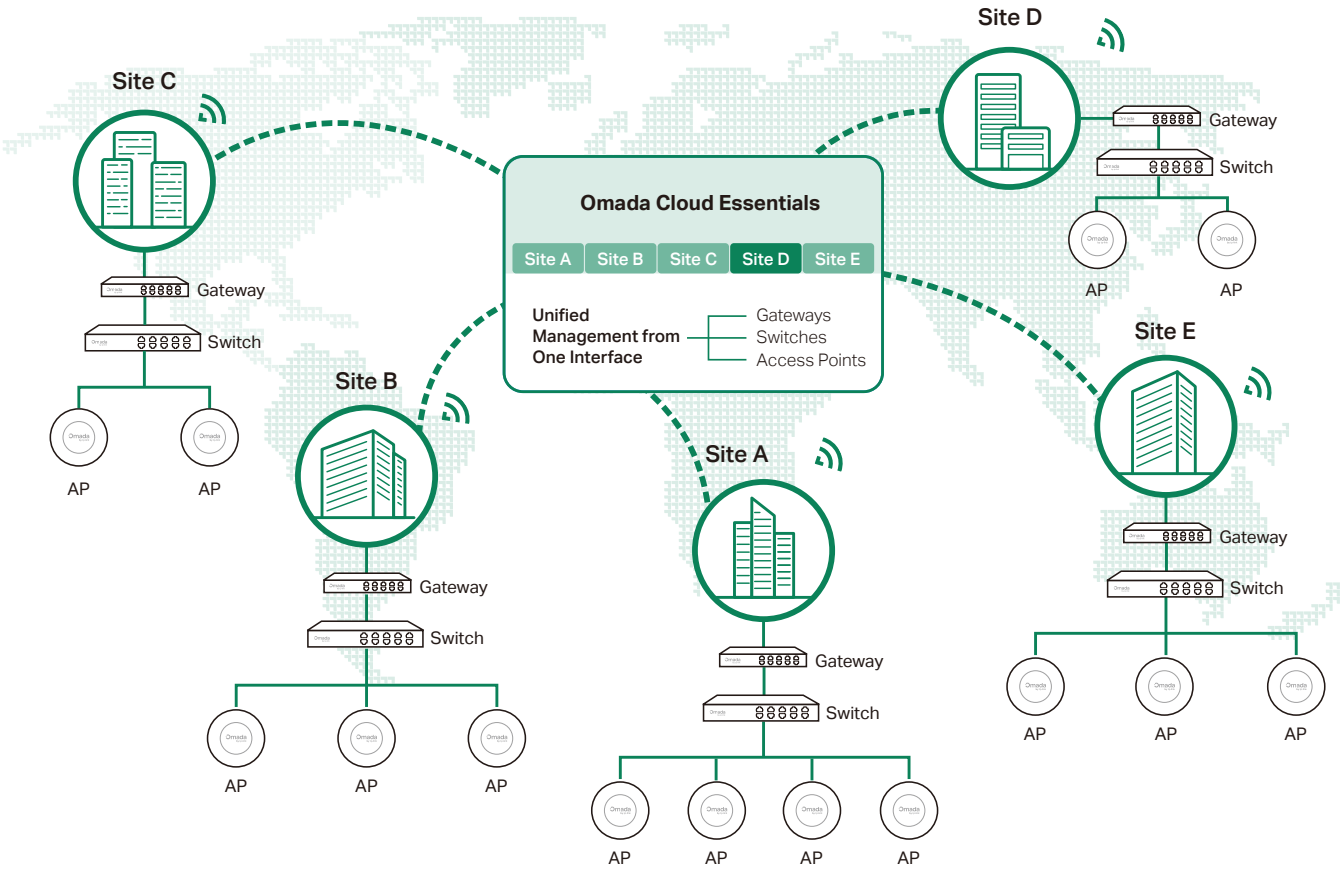
Start managing your network by creating and configuring sites so that you can configure and monitor your devices centrally while keeping things organized. The chapter includes the following sections:

- 3. 1 Create Sites
- 3.2 Configure Site Settings

3. 1 Create Sites

Overview

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



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

Configuration

To create and manage a site, follow these steps:

1) Create a site.

2) View and edit the site.

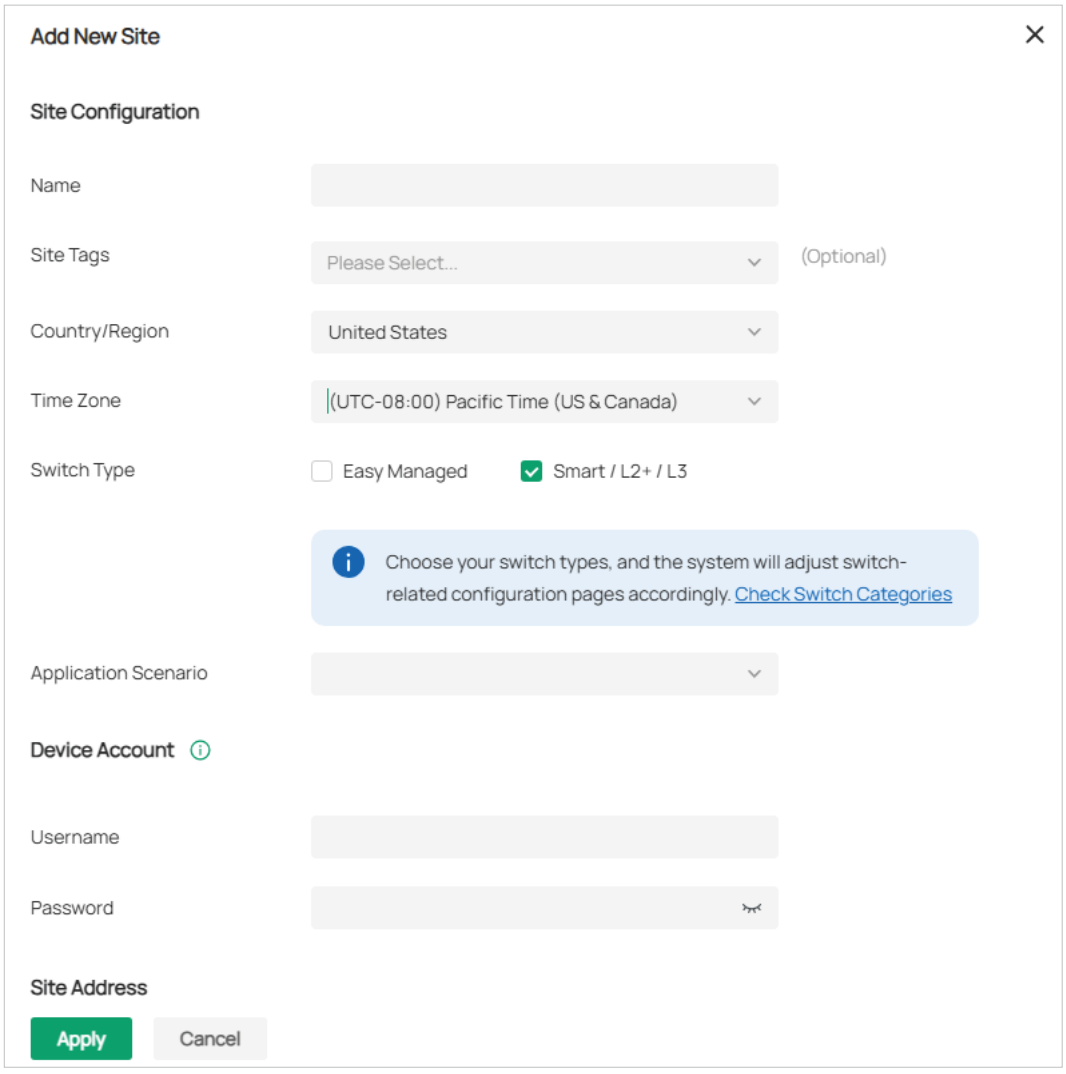
3) Access the site.

Step 1: Create a Site

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

- Create a site from scratch

1. Launch the controller and access the Global View.
2. Go to Dashboard > Site List and click Add New Site.



3. Enter a Site Name to identify the site, and configure other parameters according to actual site needs and location.
4. Create a device username and password for login to newly adopted devices.

5. Click Apply. The new site will be added to the Site List.

- Copy an existing site

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

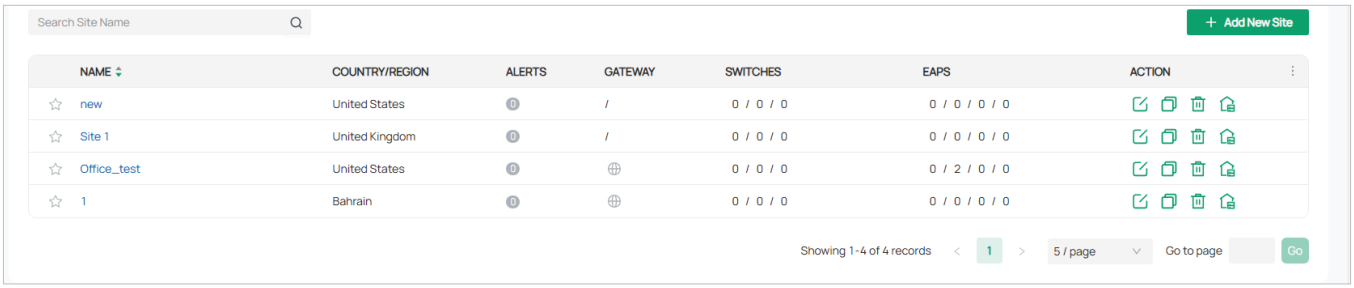
1. In the Site List, click the Copy icon in the ACTION column of the site which you want to copy.



2. Enter a Site Name to identify the new site.
3. Click Apply. The new site will be added to the Site List.

Step 2: View and Edit the Site

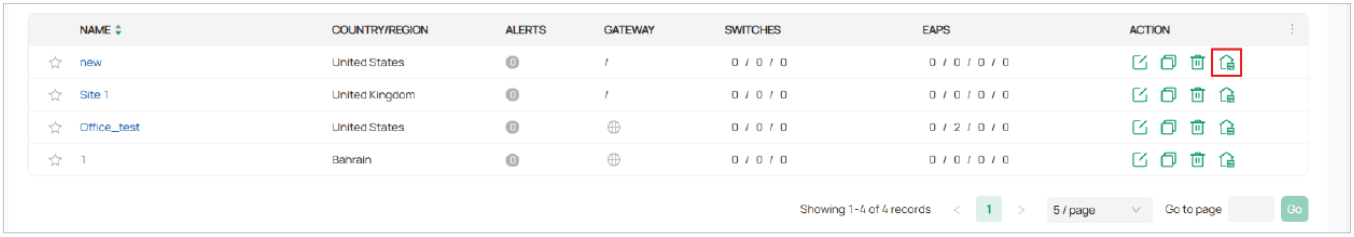
After you create the site, you can view the site status in the Site List. You can click the icons in the ACTION column to edit, copy, delete and launch the site.



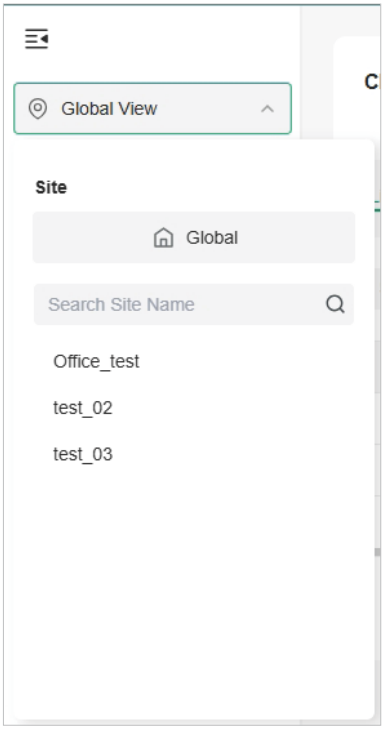
Step 3: Access the Site

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

Click the Launch icon in the ACTION column of the site to access the site.



Alternatively, select the site from the Global/Site View drop-down list in the left of the page.



Note:

Configuration items in Global View will be applied to the whole system while configuration items in Site View will be applied to the site which you are currently in.

3. 2 Configure Site Settings

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

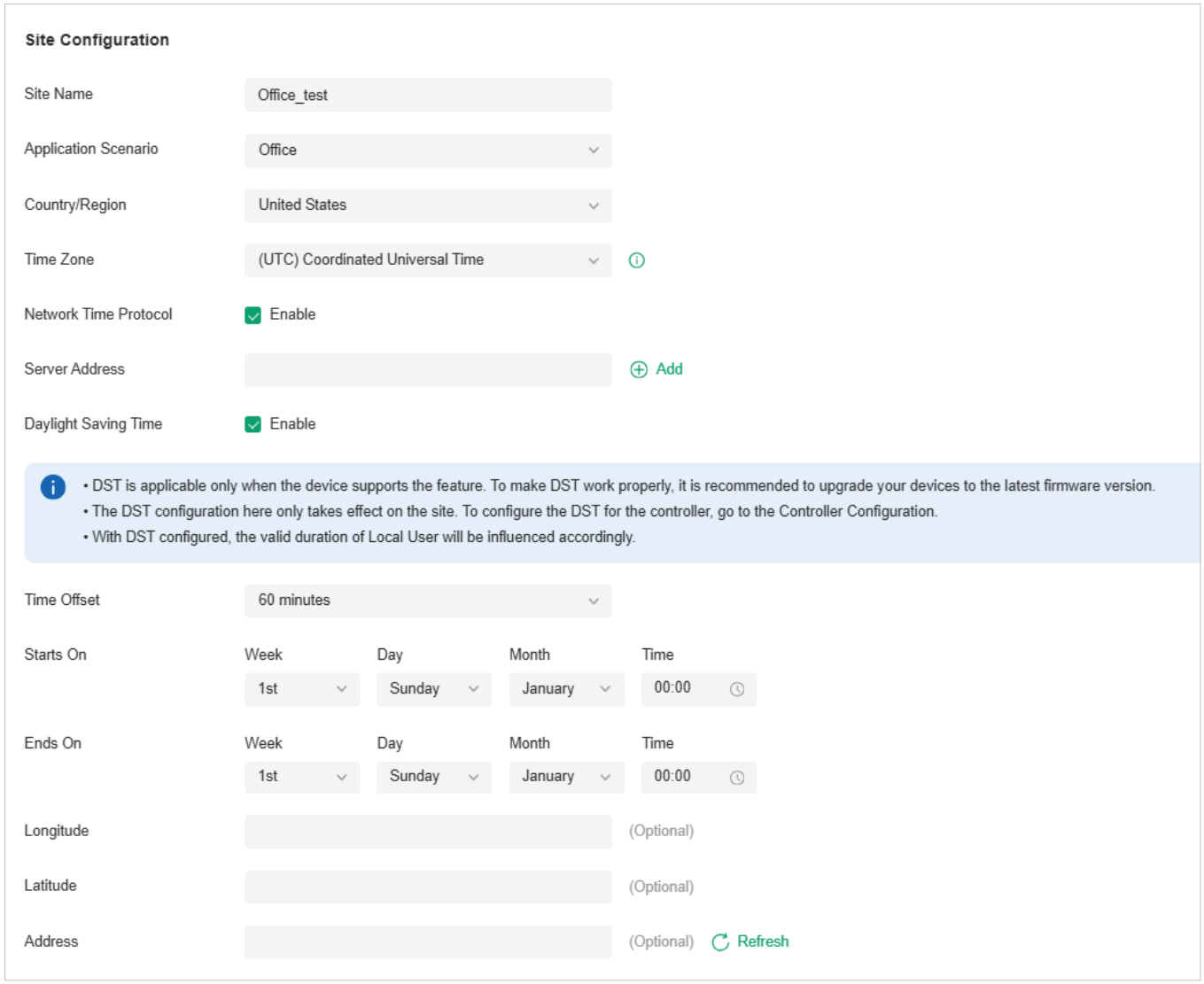
3. 2. 1 Site Configuration

Overview

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

Configuration

Launch the controller and access a site. Go to Settings > General Settings > Site Settings, and configure the following information of the site in Site Configuration. Click Save.



Site Name	Specify the name of the current site. It should be no more than 64 characters.
Application Scenario	Specify the application scenario of the site. To customize your scenario, click Create New Scenario in the drop-down list.
Country/Region	Select the location of the site.
Time Zone	Select the time zone of the site.
Network Time Protocol	Enter the IP address(es) of the NTP (Network Time Protocol) server. NTP server assigns network time to the EAP devices.
Daylight Saving Time	Enable the feature if your country/region implements DST.
Time Offset	Select the time added in minutes when Daylight Saving Time starts.

Starts On	Specify the time when the DST starts. The clock will be set forward by the time offset you specify.
Ends On	Specify the time when the DST ends.The clock will be set back by the time offset you specify.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.

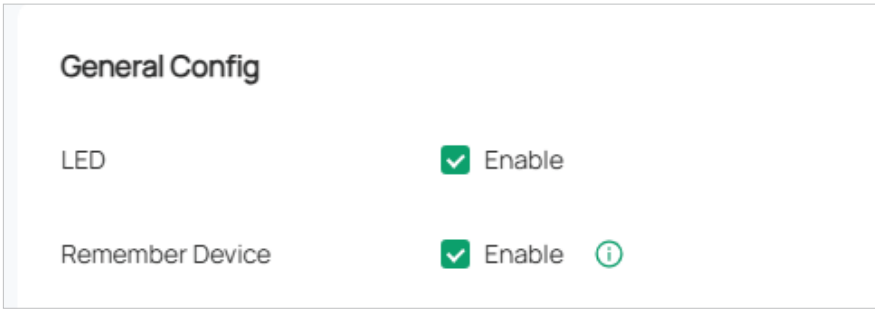
3. 2. 2 General Config

Overview

In General Config, you can control the LED status of devices in the site and remember all devices in the site.

Configuration

Launch the controller and access a site. Go to Settings > General Settings > Site Settings, and configure the following features for the current site in General Config. Click Save.



LED	Enable or disable LEDs of all devices in the site. By default, the device follows the LED setting of the site it belongs to. To change the LED setting for certain devices, refer to Manage, Configure, and Monitor Controller-Managed Devices.
Remember Device	When enabled, the controller will remember all devices in the site. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.

3. 2. 3 Wireless Features

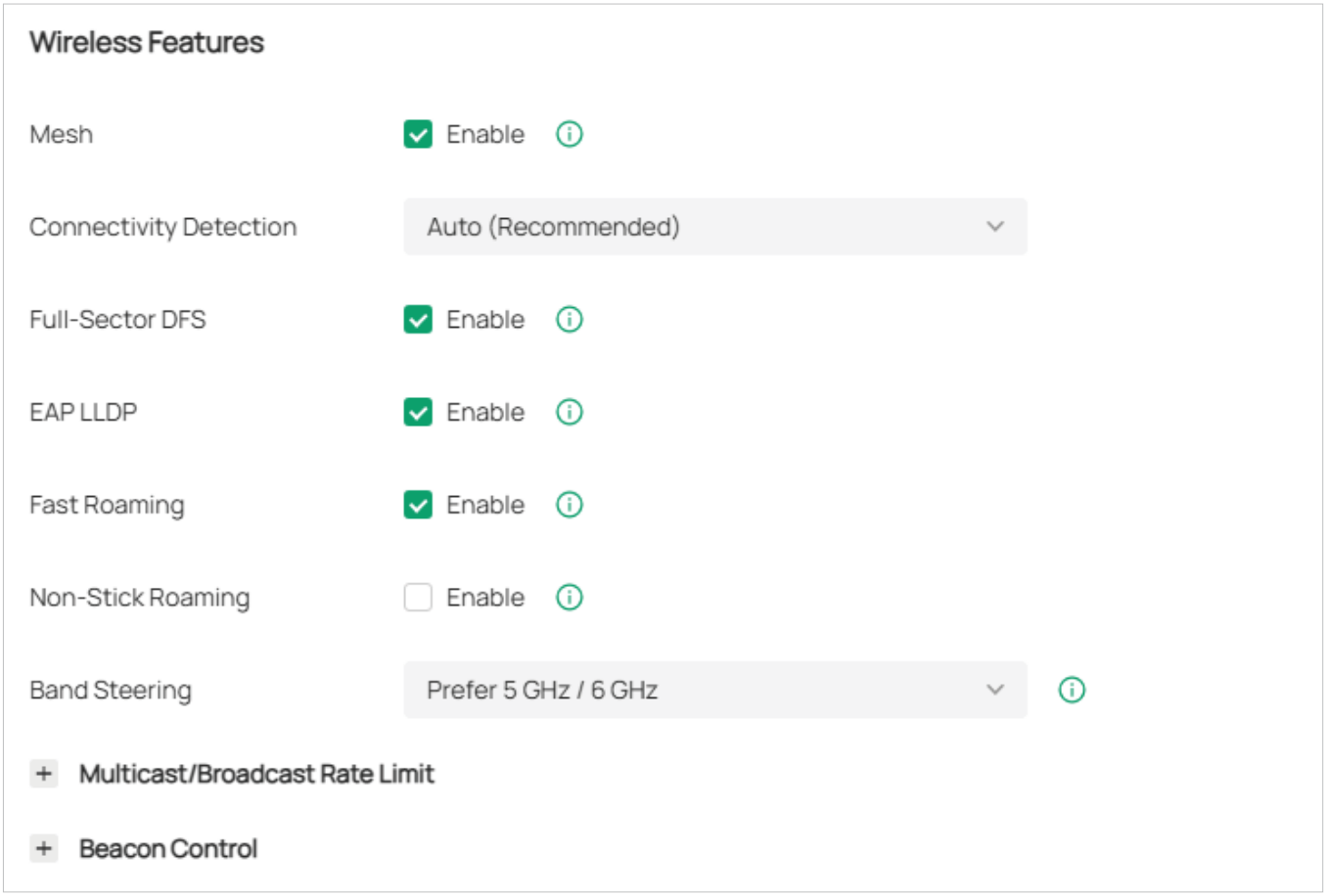
Overview

Wireless features include Mesh, Auto Failover, Connectivity Detection, Full-Sector DFS, EAP LLDP, Fast Roaming, Non-Stick Roaming, Band Steering, Multicast/Broadcast Rate Limit and Beacon Control. They are applicable to APs and wireless gateways/routers. 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.

Configuration

Launch the controller and access a site. Go to Settings > General Settings > Site Settings, and configure the following features in Wireless Features. Click Save.



Mesh	When enabled, APs supporting Mesh can establish the mesh network at the site.
Connectivity Detection	(For APs in the mesh network) Specify the method of Connection Detection when mesh is enabled. In a mesh network, the APs can send ARP request packets to a fixed IP address to test the connectivity. If the link fails, the status of these APs will change to Isolated. Auto (Recommended): Select this method and the mesh APs will send ARP request packets to the default gateway for the detection. Custom IP Address: Select this method and specify a desired IP address. The mesh APs will send ARP request packets to the custom IP address to test the connectivity. If the IP address of the AP is in different network segments from the custom IP address, the AP will use the default gateway IP address for the detection.
Full-Sector DFS	(For APs in the mesh network) With this feature enabled, when radar signals are detected on current channel by one AP, the other APs in the mesh network will be also informed. Then all APs in the mesh network will switch to an alternate channel. To enable this feature, enable Mesh first.
EAP LLDP	Click the checkbox to enable EAP LLDP (Link Layer Discovery Protocol) for device discovery and auto-configuration of VoIP devices.
Fast Roaming	With this feature enabled, wireless clients that support 802.11k/v can improve fast roaming experience when moving among different APs and wireless gateways/routers. By default, it is disabled. This feature is available for some certain 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.
Band Steering	Band steering can adjust the number of clients in 2.4 GHz, 5 GHz and 6 GHz bands to provide better wireless experience. When enabled, multi-band clients will be steered to the 5 GHz and 6 GHz band according to the configured parameters. This function can improve the network performance because the 5 GHz and 6 GHz band supports a larger number of non-overlapping channels and is less noisy.

Multicast/ Broadcast Rate Limit	With rate limit configured for Other Multicast, multicast services such as multicast video will be affected.
Beacon Control	Beacons are transmitted periodically by the AP and wireless gateway/ router to announce the presence of a wireless network for the clients. Click ⊞, select the band, and configure the following parameters of Beacon Control. Beacon Interval: Specify how often the APs and wireless gateways/routers send a beacon to clients. By default, it is 100. DTIM Period: Specify how often the clients check for buffered data that are still on the AP or wireless gateway/router awaiting pickup. By default, the clients check for them at every beacon. DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames indicating whether the AP or wireless gateway/router has buffered data for client devices. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend that you keep the default interval, 1. RTS Threshold: RTS (Request to Send) can ensure efficient data transmission by avoiding the conflict of packets. If a client wants to send a packet larger than the threshold, the RTS mechanism will be activated to delay packets of other clients in the same wireless network. We recommend that you keep the default threshold, which is 2347. If you specify a low threshold value, the RTS mechanism may be activated more frequently to recover the network from possible interference or collisions. However, it also consumes more bandwidth and reduces the throughput of the packet. Airtime Fairness: With this option enabled, each client connecting to the AP or wireless gateway/router can get the same amount of time to transmit data so that low-data-rate clients do not occupy too much network bandwidth and network performance improves as a whole. We recommend you enable this function under multi-rate wireless networks.

3. 2. 4 Device Account

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

Launch the controller and access a site. Go to Settings > General Settings > Site Settings, and modify the username and password in Device Account. Click Save and the new username and password are applied to all devices on the site.



Chapter 4

Manage, Configure, and Monitor Controller-Managed Devices

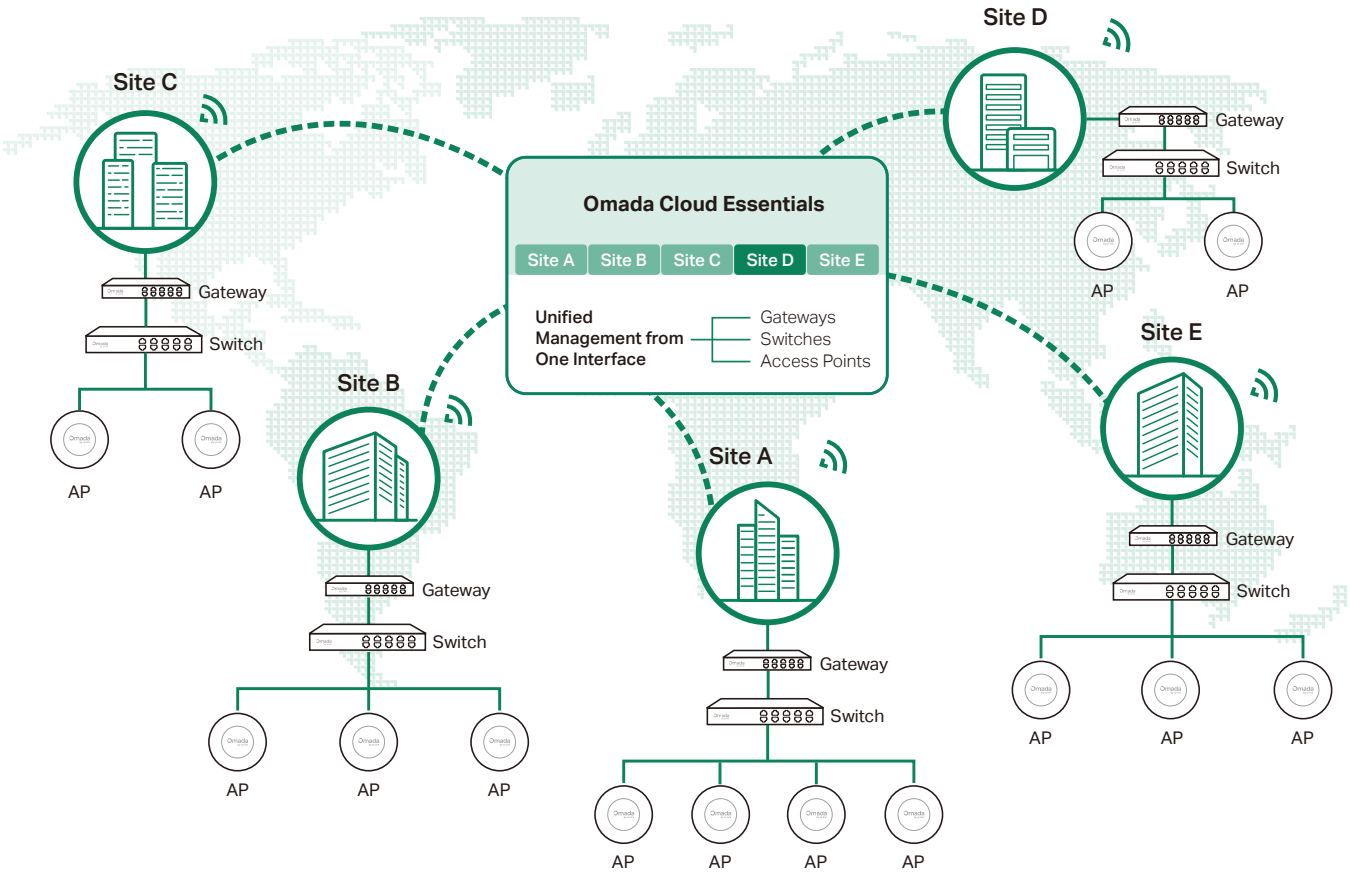
This chapter guides you on how to configure and monitor controller-managed devices, including gateways, switches and APs. You can configure the devices individually or in batches to modify the configurations of certain devices. The chapter includes the following sections:

- 4.1 Adopt Devices
- 4.2 Introduction to the Devices Page
- 4.3 Configure and Monitor the Gateway
- 4.4 Configure and Monitor Switches
- 4.5 Configure and Monitor APs
- 4.6 Create and Manage Bridge Groups

4. 1 Adopt Devices

Overview

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



Configuration

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

1) Connect to the internet.

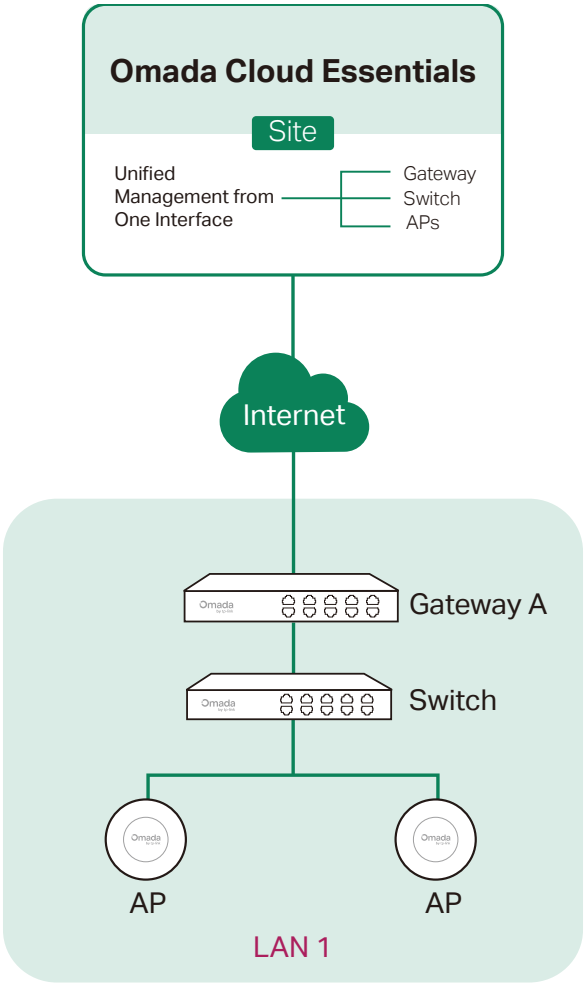
2) Prepare for controller management.

3) Adopt the devices.

Step 1: Connect to the Internet

1. Set up the network.

   Make sure that your devices are connected to the internet.



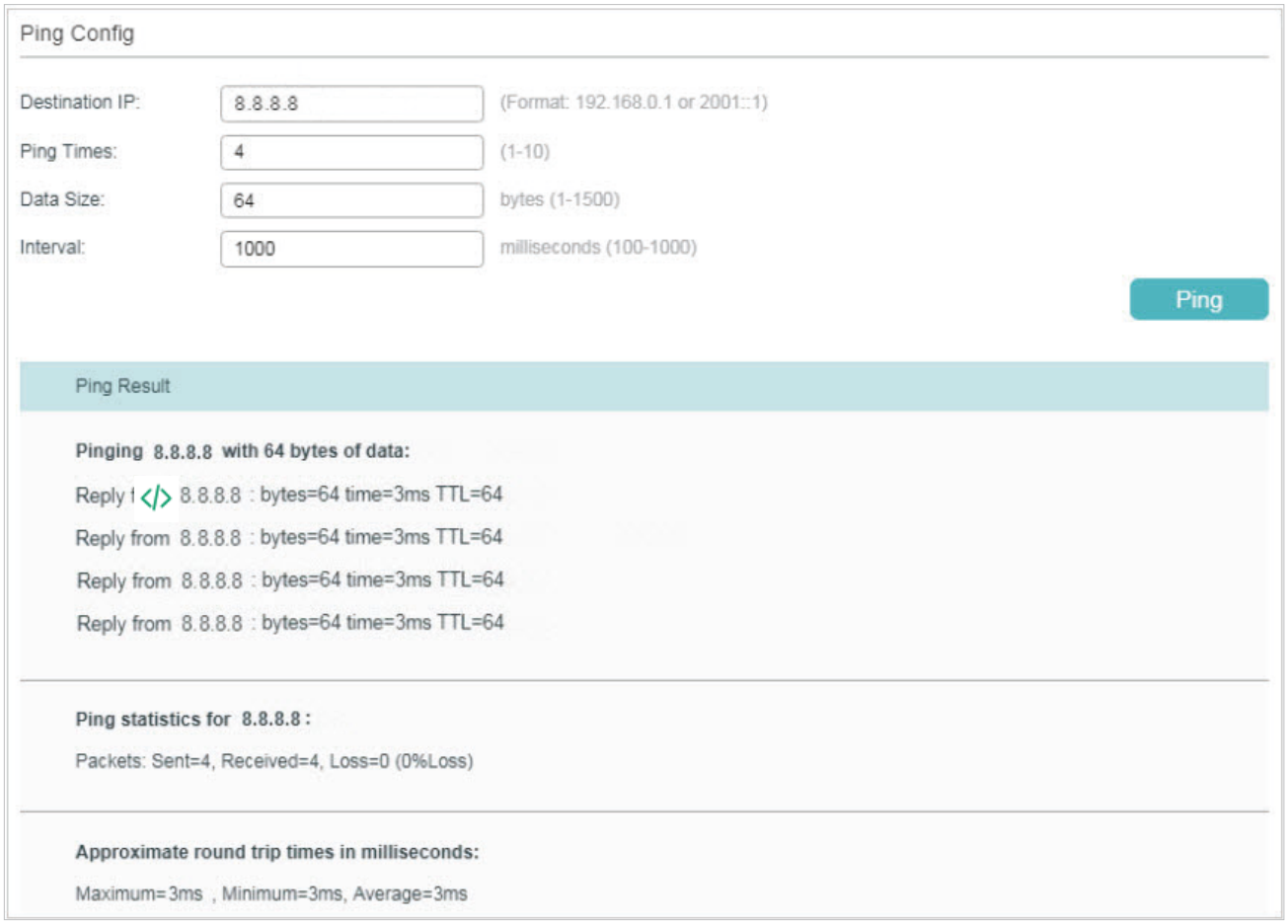
   If you are using firewalls in your network, make sure that the firewall doesn't block traffic from the controller. To configure your firewall policy, you may want to know the URL of the controller. After you open the web page of the controller, you can get the URL from the address bar of the browser.

   Refer to *Which ports do Omada SDN Controller and Omada Discovery Utility use? (above Controller 5.0.15)* to check the port list used by Omada Controller.

2. (Optional) Test the network.

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

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



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

Step 2: Prepare for Controller Management

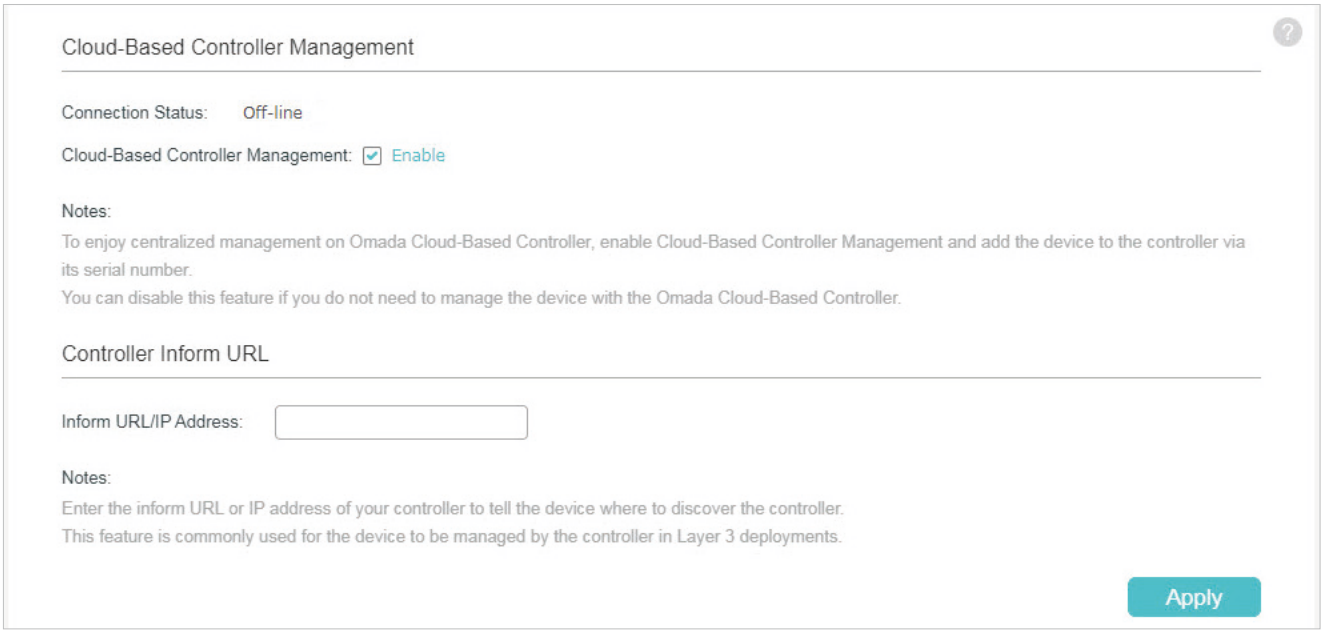
Note:

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

The Cloud-Based Controller Management feature allows the devices to be adopted by the Cloud-Based Controller. Make sure Cloud-Based Controller Management is enabled on the devices. For details, refer to the User Guide of your devices, which can be downloaded from https://support.omadanetworks.com/product/.

Let's take a switch for example. Log into the web page of the switch in Standalone Mode.

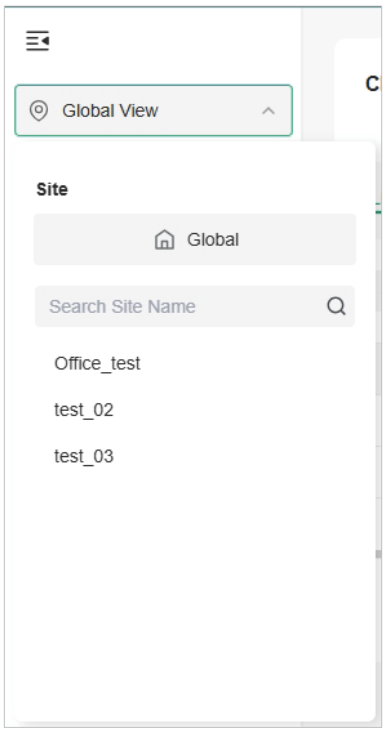
Go to SYSTEM > Controller Settings to load the following page. In Cloud-Based Controller Management, enable Cloud-Based Controller Management and click Apply.



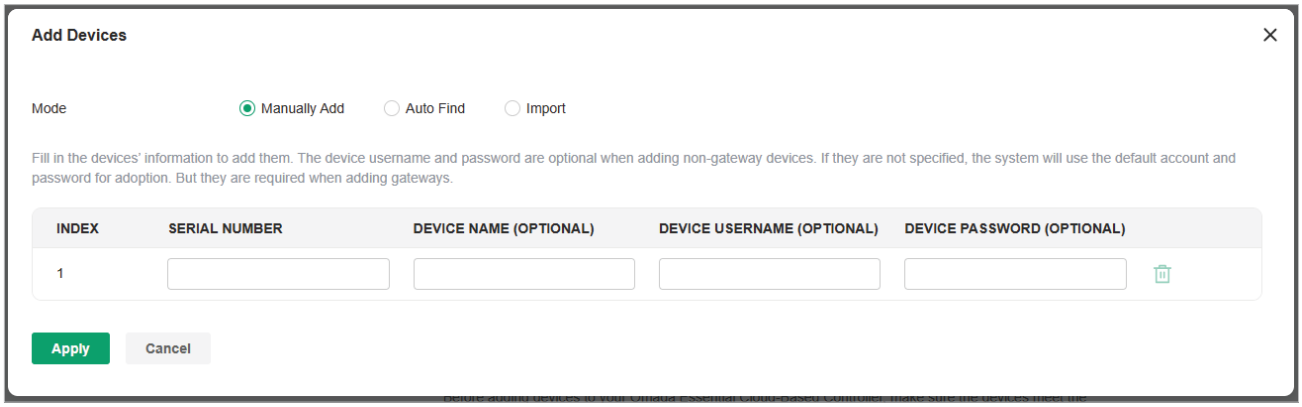
Step 3: Adopt the Devices

1. Ensure your devices are compatible with your Omada Central.
   - Essentials version: https://www.omadanetworks.com/omada-cloud-essentials/product-list/
   - Standard version: https://www.omadanetworks.com/omada-cloud-based-controller/product-list/

2. Launch the controller and access a site.



3. Go to Devices and click Add Devices.



4. Choose a method to add your devices.

- **Manually Add**

Fill in the devices' information to add them. The device username and password are optional when adding non-gateway devices. If they are not specified, the system will use the default account and password for adoption. But they are required when adding gateways.

- **Auto Find**

Automatically find the Omada devices with Inform URL configured to add them.

- **Import**

  Download the template and fill in your devices' information. Then import the file. Up to 1500 devices can be imported at a time.

5. Once the devices are adopted, they are subject to central management in the site.

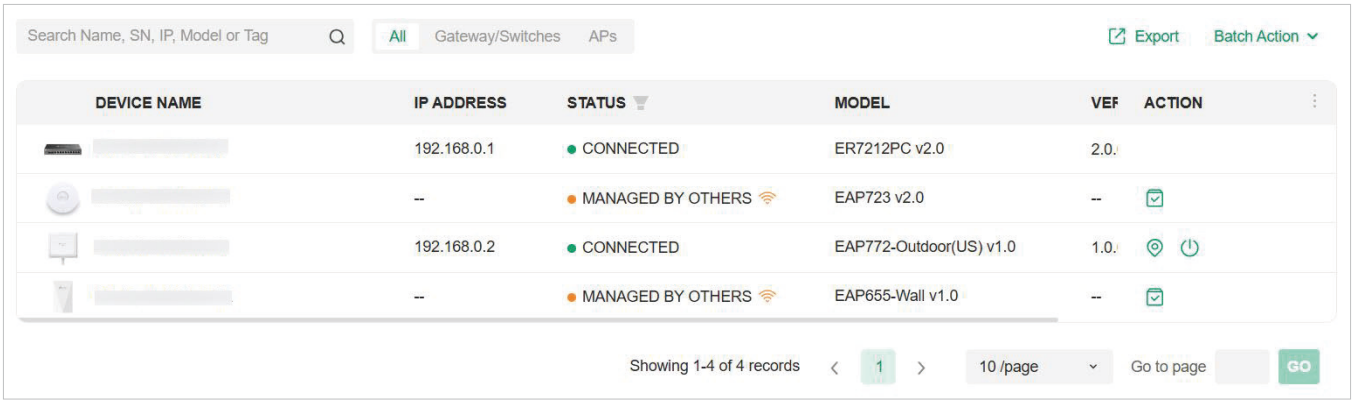
4. 2 Introduction to the Devices Page

The Devices page is further divided into Device List, Device Group, and Configuration Result.

Overview

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

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



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

PENDING	The device is in Standalone Mode or with factory settings, and has not been adopted by the controller. To adopt the device, click , and the controller will use the default username and password to adopt it. When adopting, its status will change from Adopting, Provisioning, Configuring, to Connected eventually.
ISOLATED	(For APs in the mesh network) The AP once managed by the controller via a wireless connection now cannot reach the gateway. You can rebuild the mesh network by connecting it to an AP in the Connected status, then the isolated AP will turn into a connected one. For detailed configuration, refer to Mesh.
CONNECTED	The device has been adopted by the controller and you can manage it centrally. A connected device will turn into a pending one after you forget it.

MANAGED BY OTHERS	The device has already been managed by another controller. You can reset the device or provide the username and password to unbind it from another controller and adopt it in the current controller.
HEARTBEAT MISSED	A transition status between Connected and Disconnected. Once connected to the controller, the device will send inform packets to the controller in a regular interval to maintain the connection. If the controller does not receive its inform packets in a certain time (e.g. in 1 minutes for APs), the device will turn into the Heartbeat Missed status. For a heartbeat-missed device, if the controller receives an inform packet from the device in 5 minutes, its status will become Connected again; otherwise, its status will become Disconnected.
DISCONNECTED	The connected device has lost connection with the controller for more than 5 minutes.
	(For APs in the mesh network) When this icon appears with a status icon, it indicates the 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 about Migration, refer to Migration.

Configuration

- Customize the Column

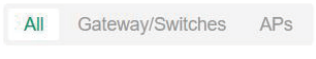
  To customize the columns, click the ellipsis icon next to Action and check the boxes of information type.

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

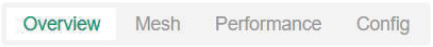
- Filter the Devices

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

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

  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.

If you select the APs tab, another tab bar 

will be available to change the column quickly.

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

- Quick Operations

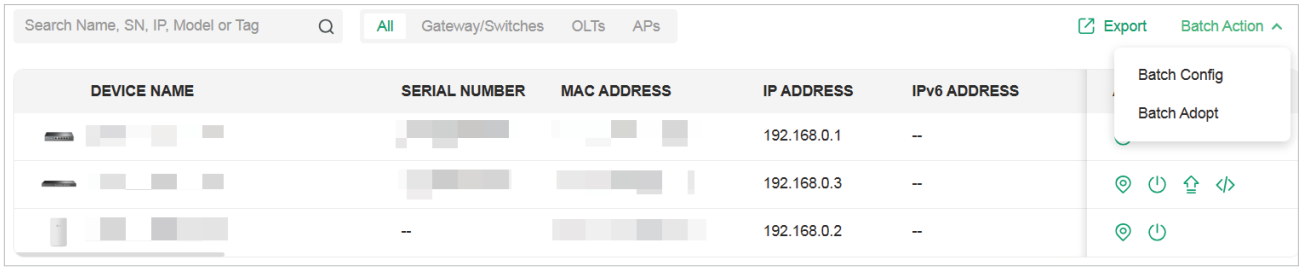
Click the icons in the Header or the Action column to quickly adopt, locate, upgrade, or reboot the device.

Start Rolling Upgrade	Click to upgrade the managed devices in batches.
	Click to check if there is new firmware for the managed devices.
	(For pending devices) Click to adopt the device.
	(For connected switches and APs) Click this icon and the LEDs of the device will flash to indicate the device's location. The LEDs will keep flashing for 10 minutes, or you can click the icon to stop the flashing.
	(For connected devices) Click to reboot the device.
	Click to upgrade the device's firmware version. This icon appears when the device has a new firmware version.

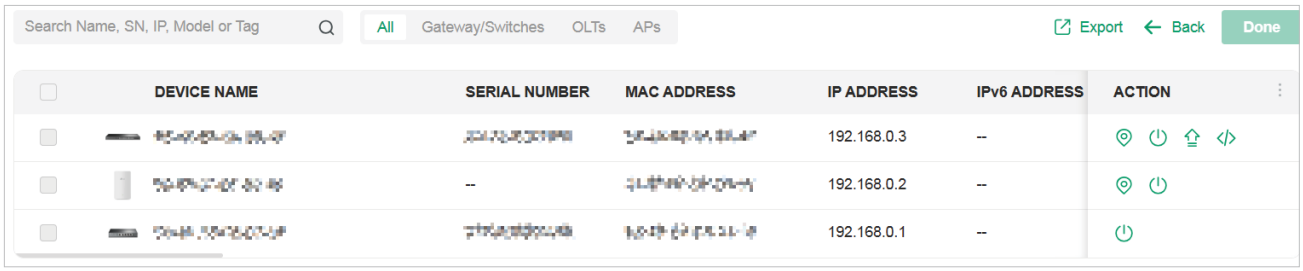
- Batch Edit (for Switches and APs)

After selecting the Gateway/Switches or APs tab, you can adopt or configure the switches or APs in batches. Batch Config is available only for the devices in Connected/Disconnected/

Heartbeat Missed/Isolated status, while Batch Adopt is available for the devices in the Pending/Managed By Others status.

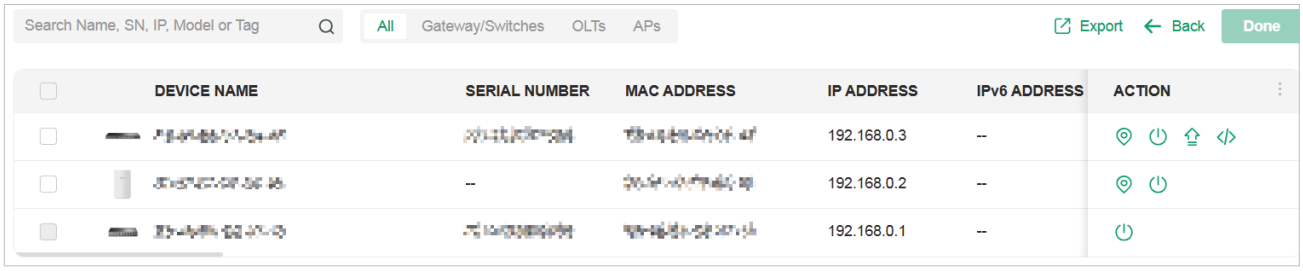


Click Batch Action, select Batch Adopt, click the checkboxes of devices, and click Done. If the selected devices are all in the Pending status, the controller will adopt then with the default username and password. If not, enter the username and password manually to adopt the devices.



Click Batch Action, select Batch Config, click the checkboxes of devices, and click Done. Then the Properties window appears. There are two tabs in the window: Devices and Config. In Devices, you can click the close icon to remove the device from the current batch configuration.

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



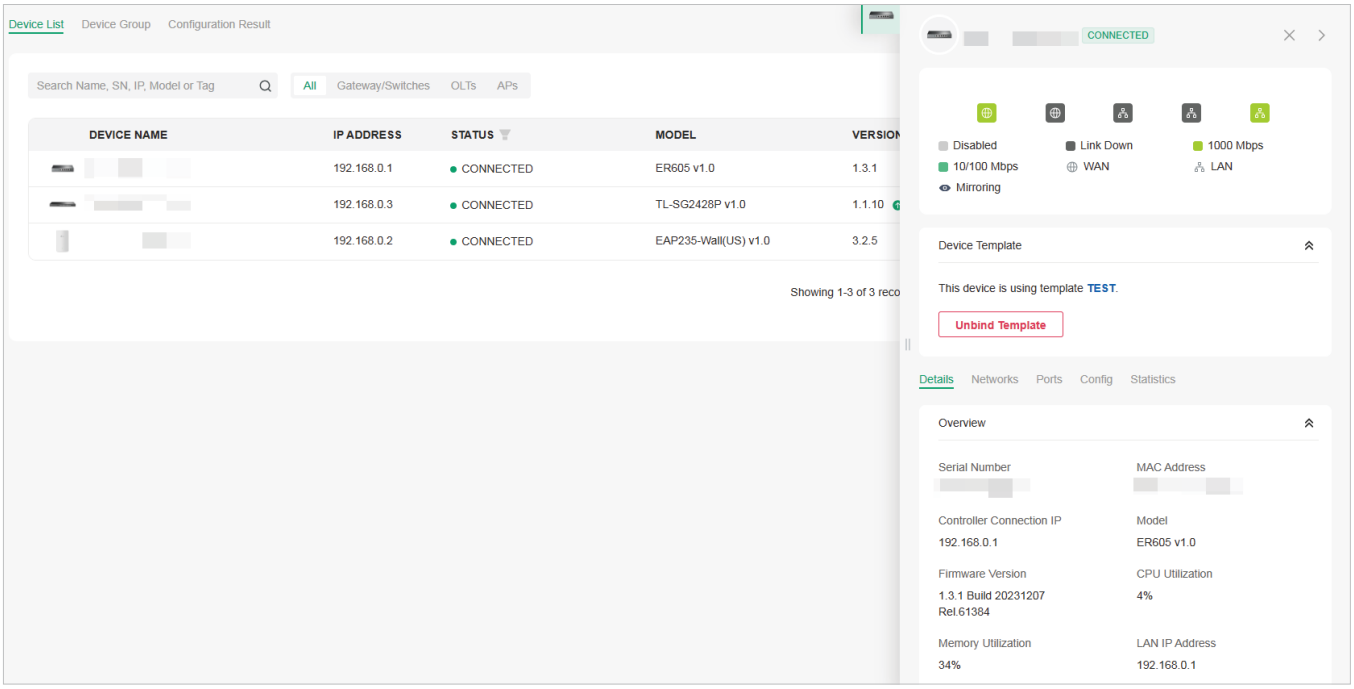
>	Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click <||.
<||	Click to maximize the Properties window. You can also use the icon on pages other than the Devices page.

	Click to close the Properties window of the chosen device(s). Note that the unsaved configuration will be lost.
	The number on the lower-right shows the number of devices in the batch configuration.

4. 3 Configure and Monitor the Gateway

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

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



Note:

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

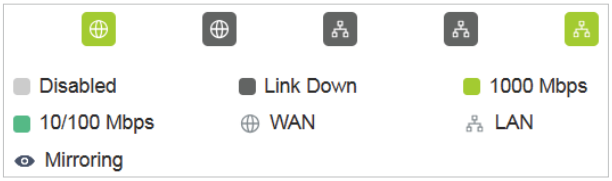
4. 3. 1 Configure the Gateway

In the Properties window, you can view and configure the ports in Ports, and configure the gateway features in Config.

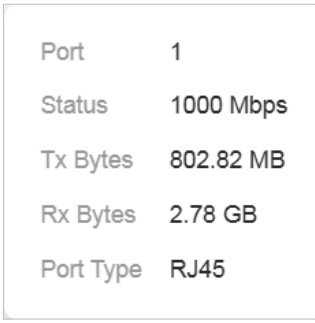
Monitor Panel

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

ports are disabled.

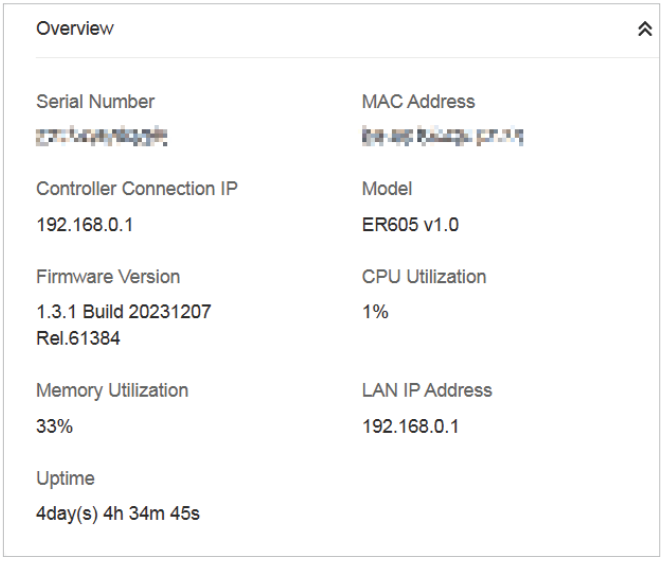


You can hover the cursor over the port icon for more details.



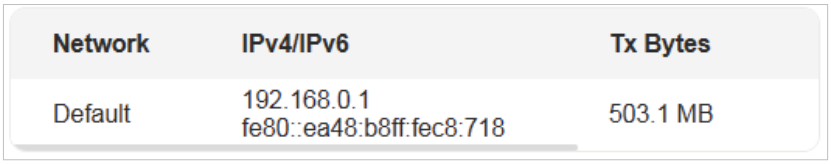
Details

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



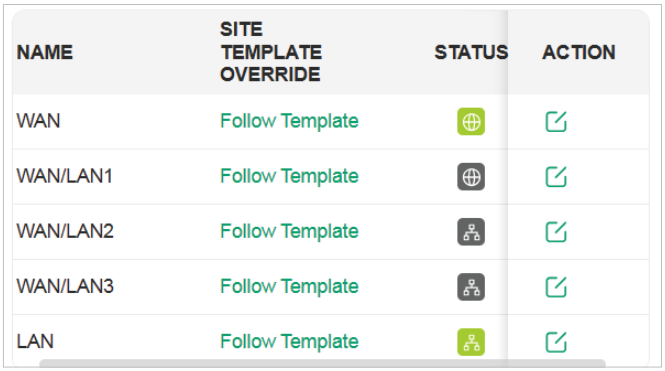
Networks

In Networks, you can view the network information of the router.

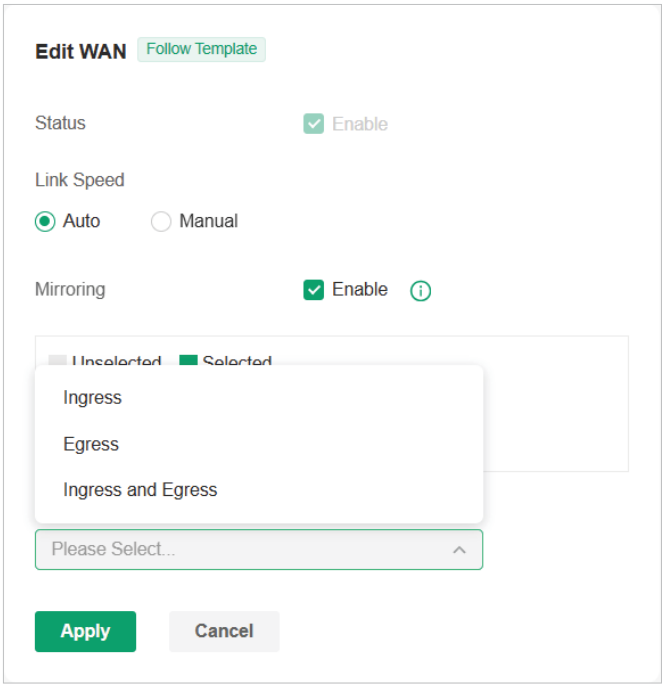


Ports

In Ports, you can view the status and edit settings of the ports.



To configure a port, click the edit icon in the Action column.



Status	Check the box to enable 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.
Mirroring	Mirroring is used to analyze network traffic and troubleshoot network problems. Enable this option to set the edited port as the mirroring port, then specify one or multiple mirrored ports. The gateway will sends a copy of traffics passing through the mirrored ports to the mirroring port.
Mirror Mode	Specify the directions of the traffic to be mirrored. Ingress and Egress: Both the incoming and outgoing packets through the mirrored port will be copied to the mirroring port. Ingress: The packets received by the mirrored port will be copied to the mirroring port. Egress: The packets sent by the mirrored port will be copied to the mirroring port.

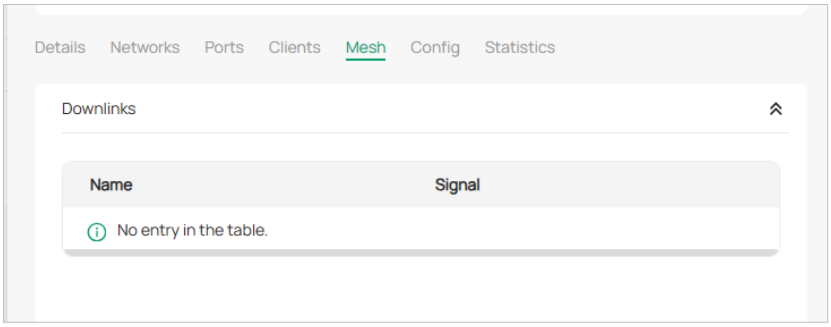
Clients

In Clients, you can view the clients of the router.



Mesh (for wireless routers only)

In Mesh, you can view the mesh downlinks of the router.

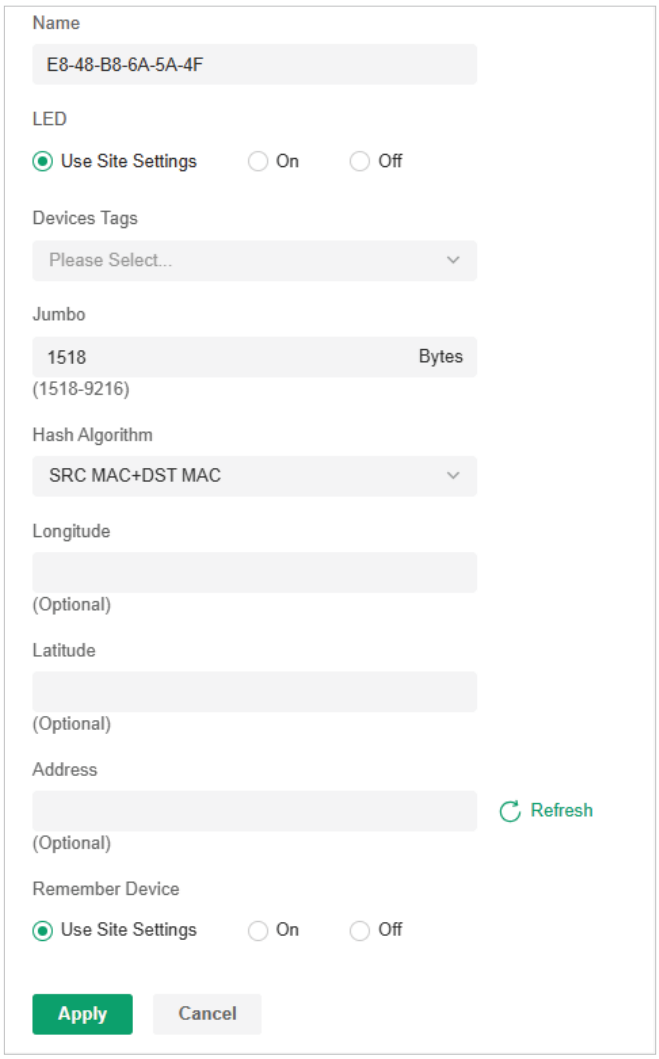


Config

In the Properties window, click Config and then click the sections to configure the features applied to the router.

■ General

In General, you can specify general settings of the router.

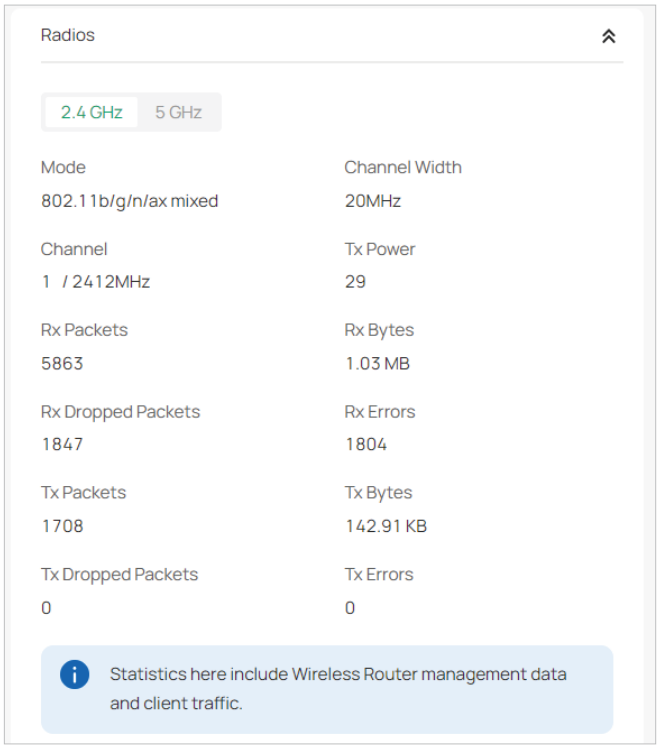


Name	Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. On/Off: The device's LED will keep on/off.
Device Tags	Select a tag from the drop-down list or create a new tag to categorize the device.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.

Remember Device	When enabled, 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.

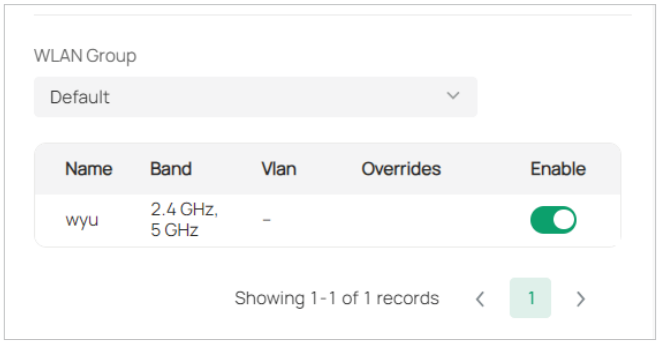
- Radios (for wireless routers only)

  In Radios, you can view the statistics of the wireless router management data and client traffic of each band. Different models support different bands.

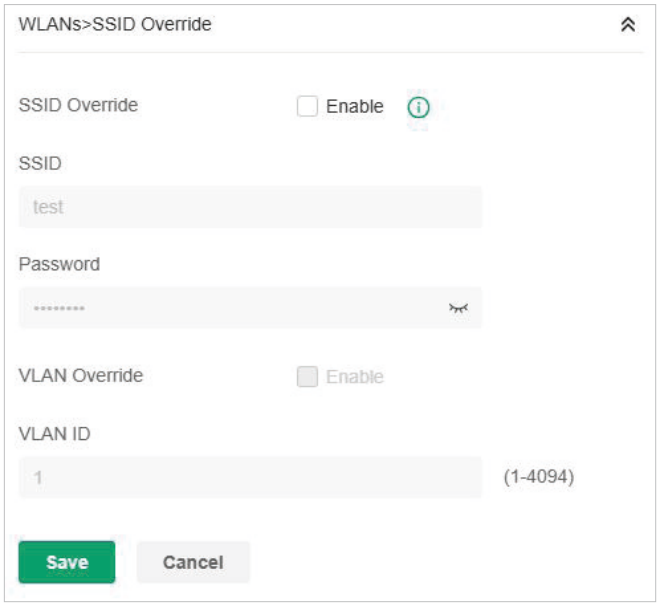


- WLANs

  In WLANs, you can apply the WLAN group to the router and specify a different SSID name and password to override the SSID in the WLAN group. After that, clients can only see the new SSID and use the new password to access the network. To create or edit WLAN groups, refer to Configure Wireless Networks.



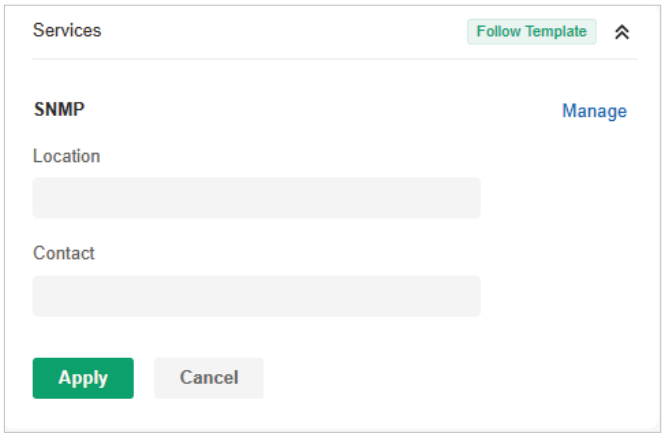
(Only for configuring a single device) To override the SSID, select a WLAN group, click the edit icon in the entry and then the following page appears.



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

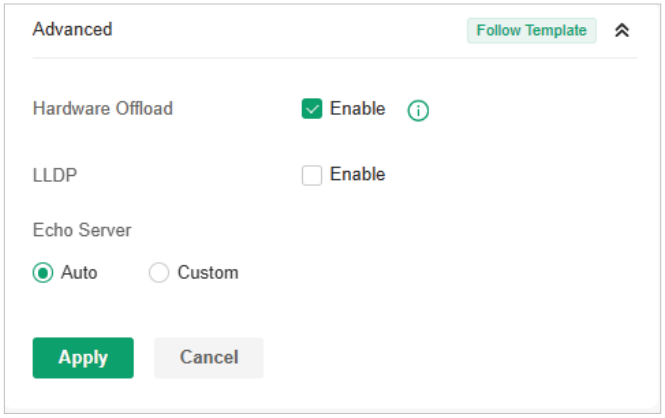
- Services

In Services, you can configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP.



- Advanced

In Advanced, you can configure advanced settings to make better use of network resources.

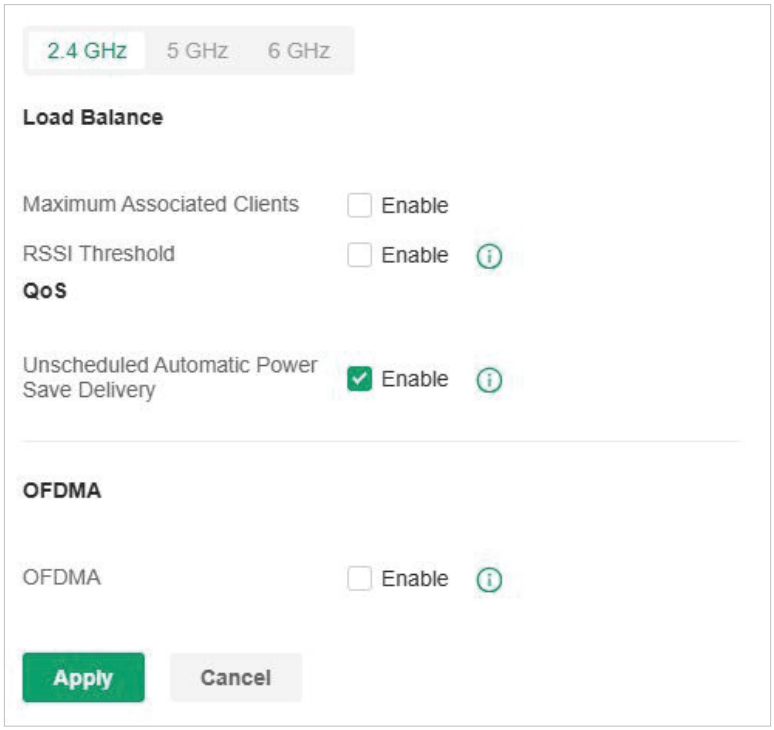


Hardware Offload	Hardware Offload can improve performance and reduce CPU utilization by using the hardware to offload packet processing. Note that this feature cannot take effect if QoS, Bandwidth Control, or Session Limit is enabled. To configure Bandwidth Control and Session Limit for the router, refer to Transmission.
LLDP	LLDP (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.

For a wireless gateway, you can configure Load Balance and QoS to make better use of network resources. Load Balance can control the client number associated to the device,

while QoS can optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media.

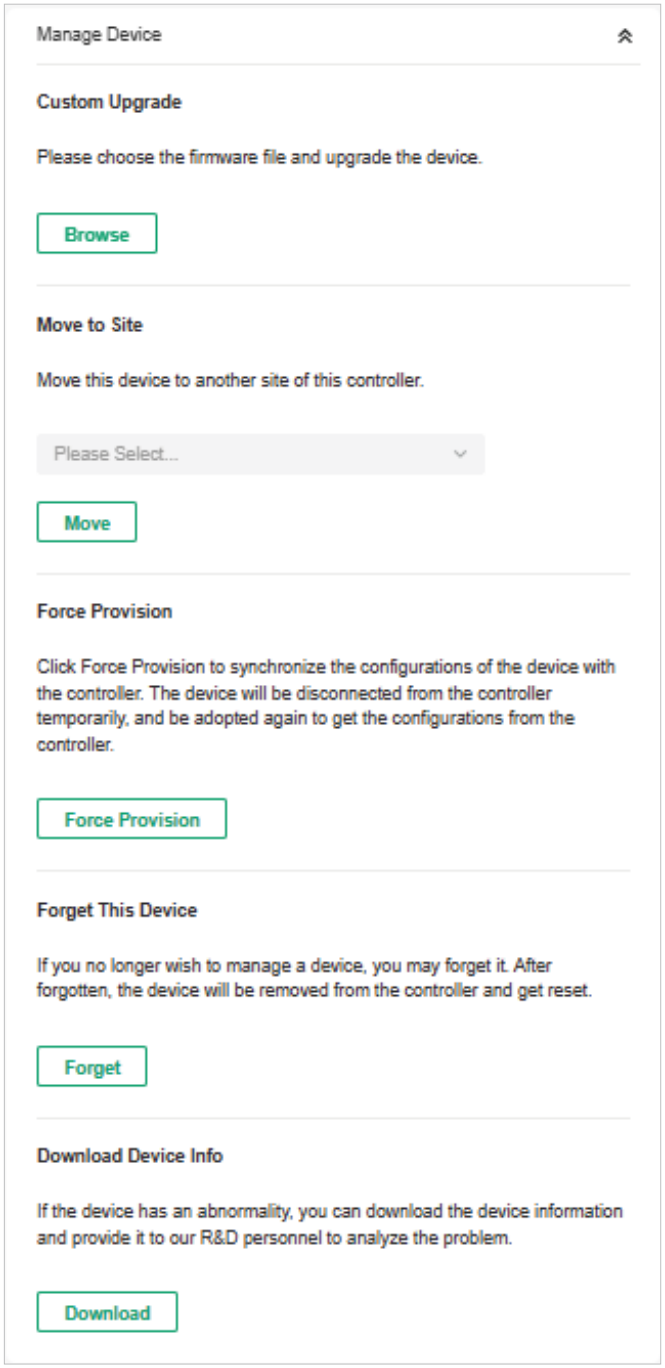
Select each frequency band and configure the following parameters and features.



Max Associated Clients	Enable this function and specify the maximum number of connected clients. If the connected client reaches the maximum number, the 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 the client's signal strength is weaker than the threshold, the client will lose connection with the device.
Unscheduled Automatic Power Save Delivery	When enabled, this function can greatly improve the energy-saving capacity of clients.
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.

■ Manage Device

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

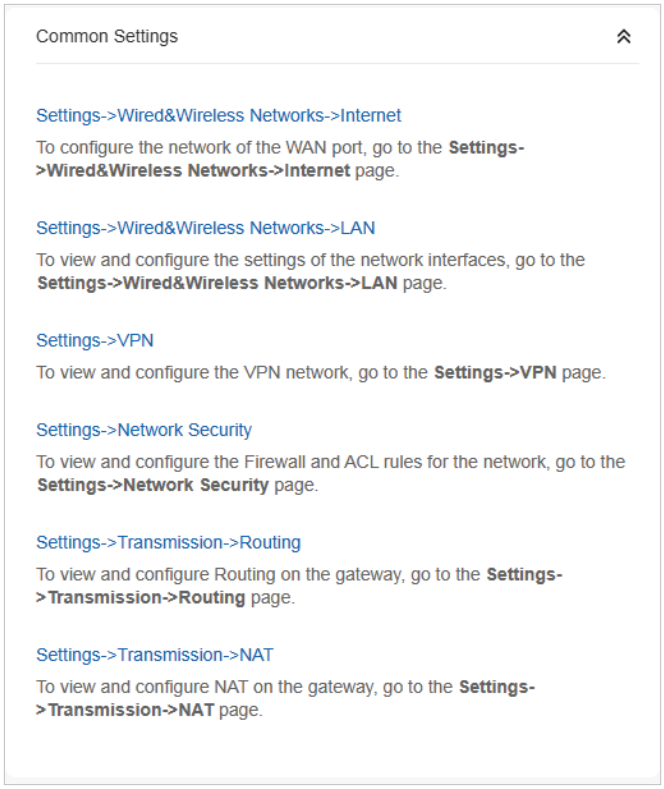


Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.

Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget 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.
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.

- Common Settings

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

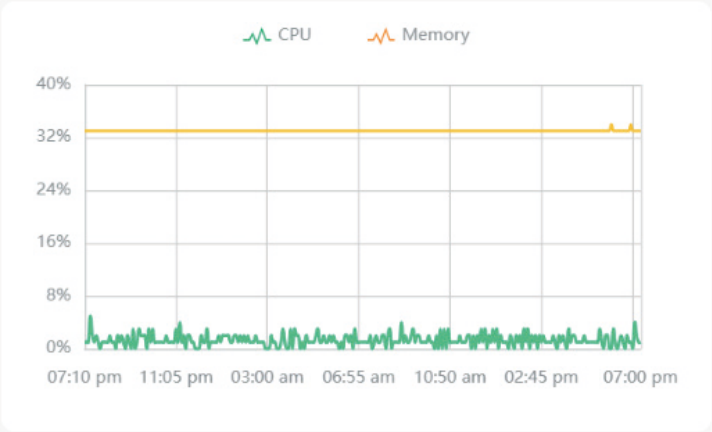


4. 3. 2 Monitor the Gateway

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

Statistics

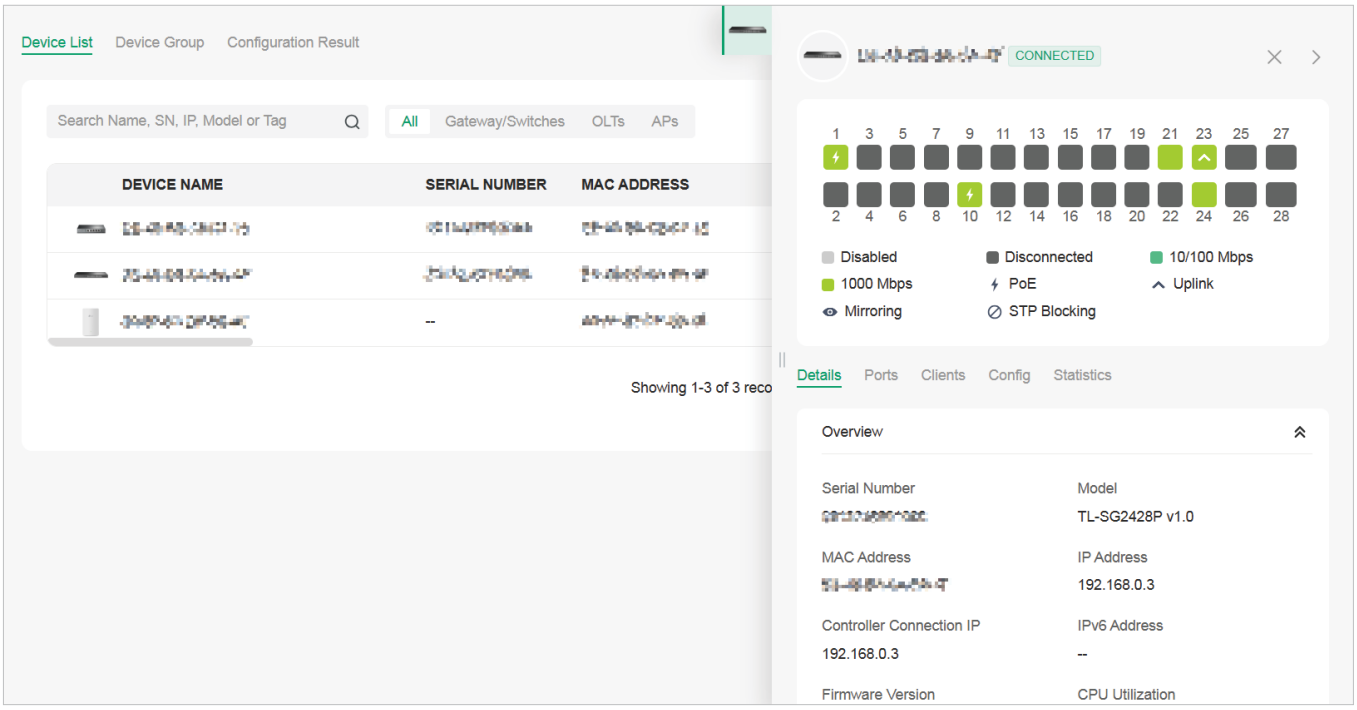
In Statistics, you can monitor the CPU and memory of the device in last 24 hours via charts. To view statistics of the device in a certain period, click the chart.



4. 4 Configure and Monitor Switches

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

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



Note:

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

4. 4. 1 Configure Switches

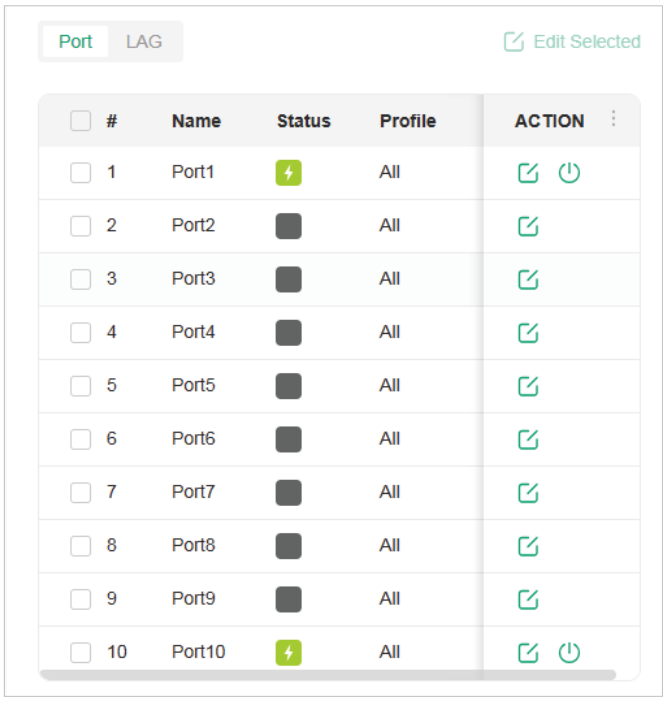
In the Properties window, you can view and configure the profiles applied to ports in Ports, and in Config, you can configure the switch features.

Ports

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

- Ports

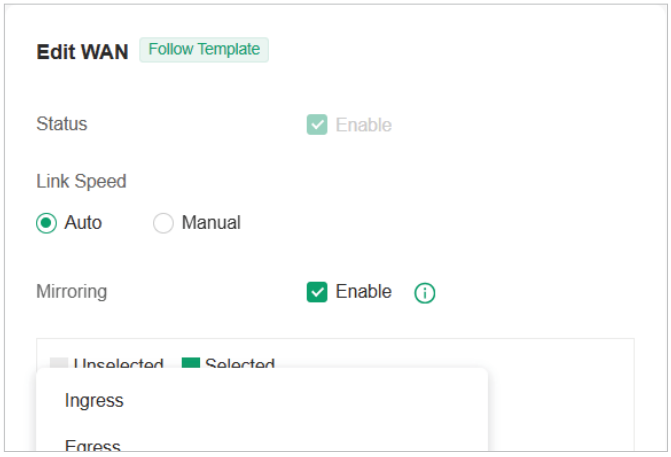
  In Ports, you can view and configure all ports' names and applied profiles.



Status	Displays the port status in different colors. : The port profile is Disabled. To enable it, click the edit icon to change the profile. : The port is enabled, but no device or client is connected to it. : The port is running at 1000 Mbps. : The port is running at 10/100 Mbps.
Profile	Displays the profile applied to the port.

Action	: Click to edit the port name and configure the profile applied to the port. : (For PoE ports) Click to reboot the connected powered devices (PDs).

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

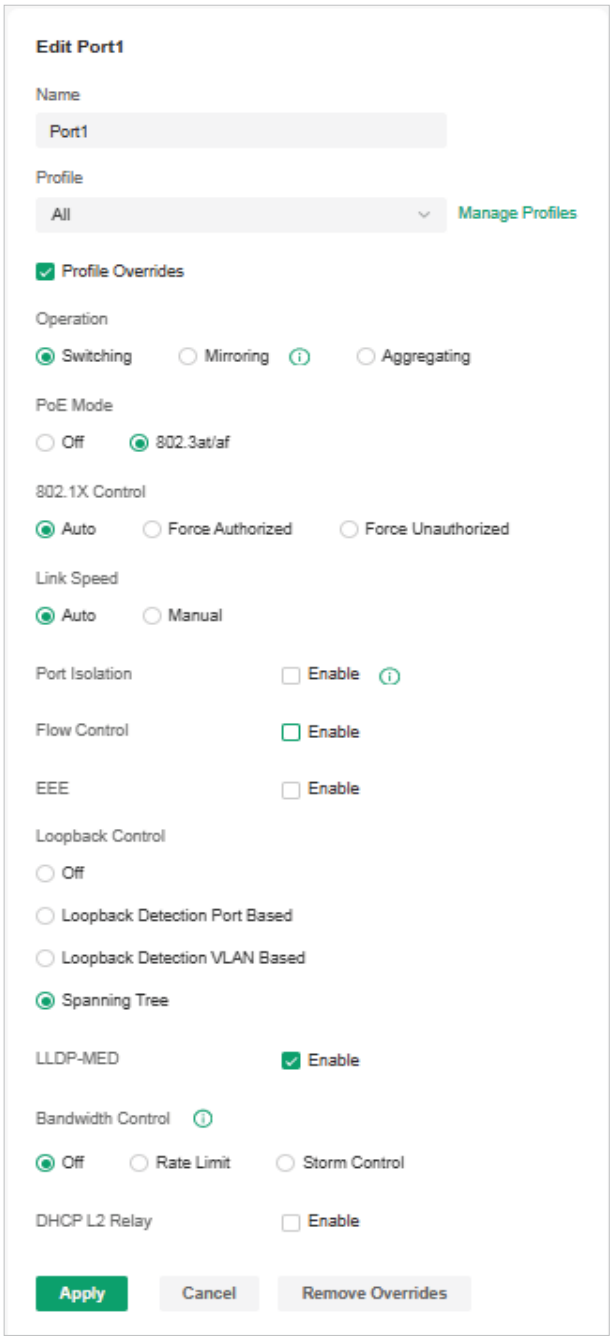


Name	Enter the port name.
Profile	Select the profile applied to the port from the drop-down list. Click Manage Profiles to jump to view and manage profiles. For details, refer to Configure Wired Networks.
Profile Overrides	Click the checkbox to override the applied profile. The parameters to be configured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

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

- Override the Applied Profile

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



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

802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to Settings > Authentication > 802.1X. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, and the client connected to the port cannot authenticate with any means. The switch cannot provide authentication services to the client through the port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.

Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the 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.
LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP (Voice over Internet Protocol) devices.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and specify traffic threshold on each port to make good use of network bandwidth. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the specified rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.

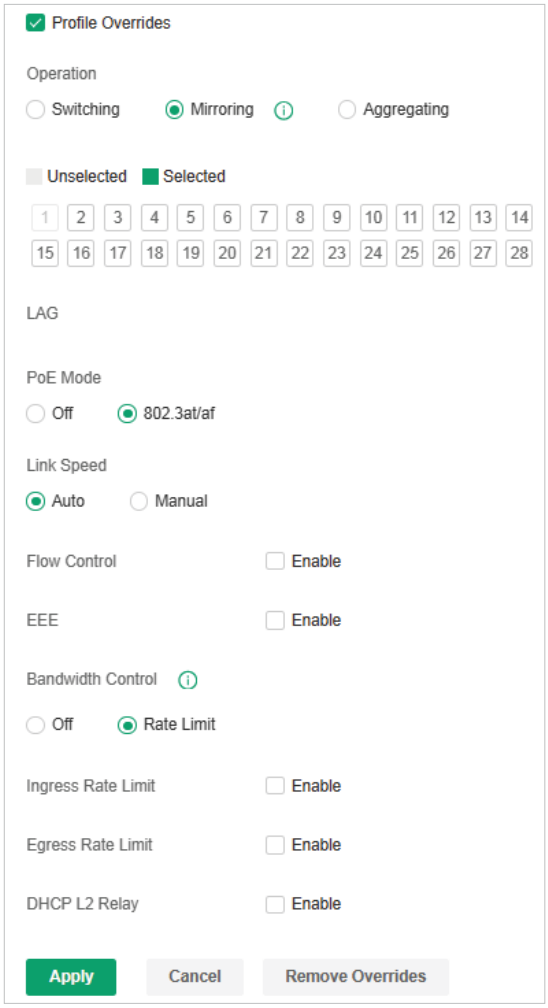
Broadcast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Unknown Unicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
Action	When Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.
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	(Optional) Enter the customized circuit ID. The circuit ID configurations of the switch and the DHCP server should be compatible with each other. If it is not specified, the switch will use the default circuit ID when inserting Option 82 to DHCP packets.
Remote ID	(Optional) Enter the customized remote ID. The remote ID configurations of the switch and the DHCP server should be compatible with each other. If it is not specified, the switch will use its own MAC address as the remote ID.

- Configure a Mirroring Port

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

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

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



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

Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
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.

- Configure a LAG

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

Configuration Guidelines:

Ensure that both ends of the aggregation link work in the same LAG mode. For example, if the local end works in LACP mode, the peer end should also be set as LACP mode.

Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed, duplex, jumbo and flow control mode.

A port cannot be added to more than one LAG at the same time.

LACP does not support half-duplex links.

One static LAG supports up to eight member ports. All the member ports share the bandwidth evenly. If an active link fails, the other active links share the bandwidth evenly.

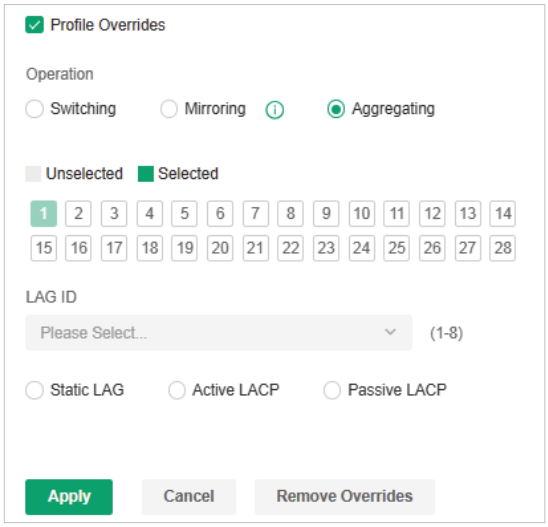
One LACP LAG supports multiple member ports, but at most eight of them can work simultaneously, and the other member ports are backups. Using LACP protocol, the switches negotiate parameters and determine the working ports. When a working port fails, the backup port with the highest priority will replace the faulty port and start to forward data.

The member port of an LAG follows the configuration of the LAG but not its own. Once removed, the LAG member will be configured as the default All profile and Switching operation.

The port enabled with Port Security, Port Mirror, MAC Address Filtering or 802.1X cannot be added to an LAG, and the member port of an LAG cannot be enabled with these functions.

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

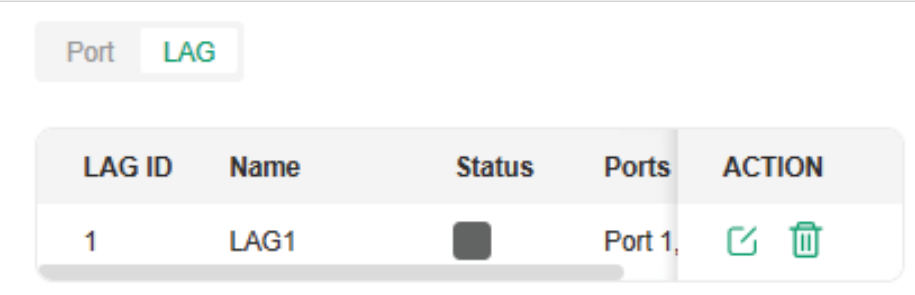
Overrides and all profile configurations become the same as the applied profile. For other parameters, configure them under the LAG tab.



LAG ID	Specify the LAG ID of the LAG. Note that the LAG ID should be unique. The valid value of the LAG ID is determined by the maximum number of LAGs supported by your switch. For example, if your switch supports up to 14 LAGs, the valid value ranges from 1 to 14.
Static LAG	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.

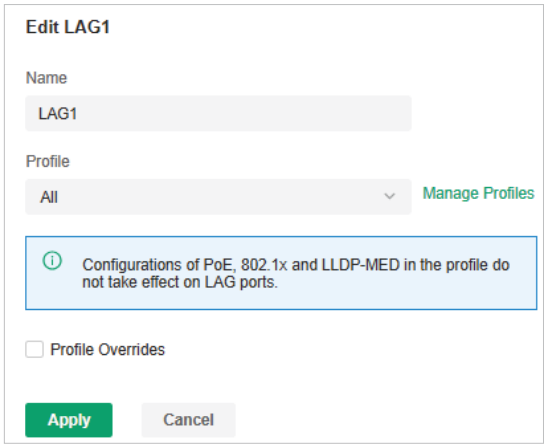
- LAG

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



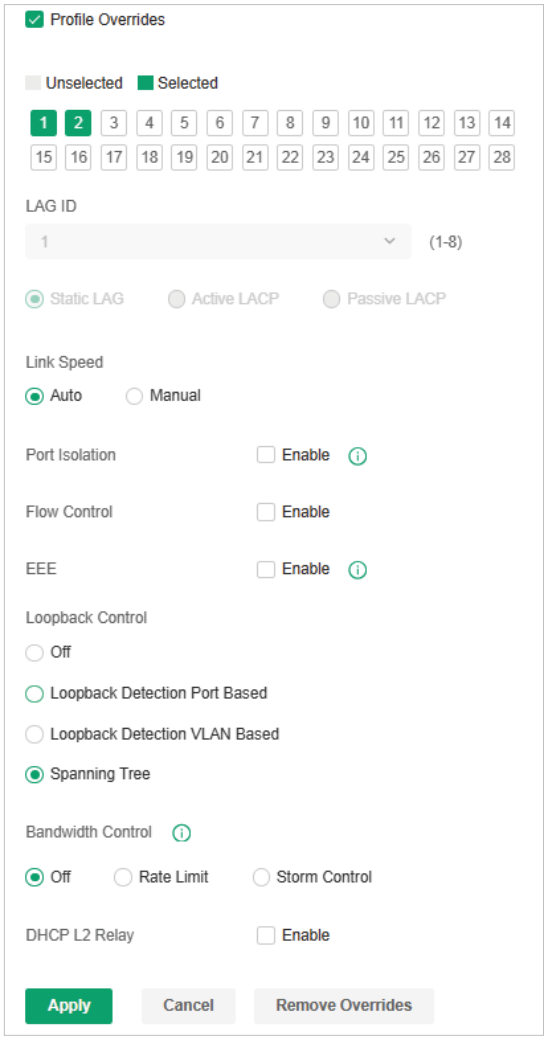
Status	Displays the status in different colors. : The LAG profile is Disable. To enable it, click the edit icon to change the profile. : The port is enabled, but no device or client is connected to it. : The LAG ports are running at 1000 Mbps. : The LAG port are running at 10/100 Mbps.
Ports	Displays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

Click the edit icon to configure the LAG name and the applied profile.



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

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



Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.

EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the 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.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the specified rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.

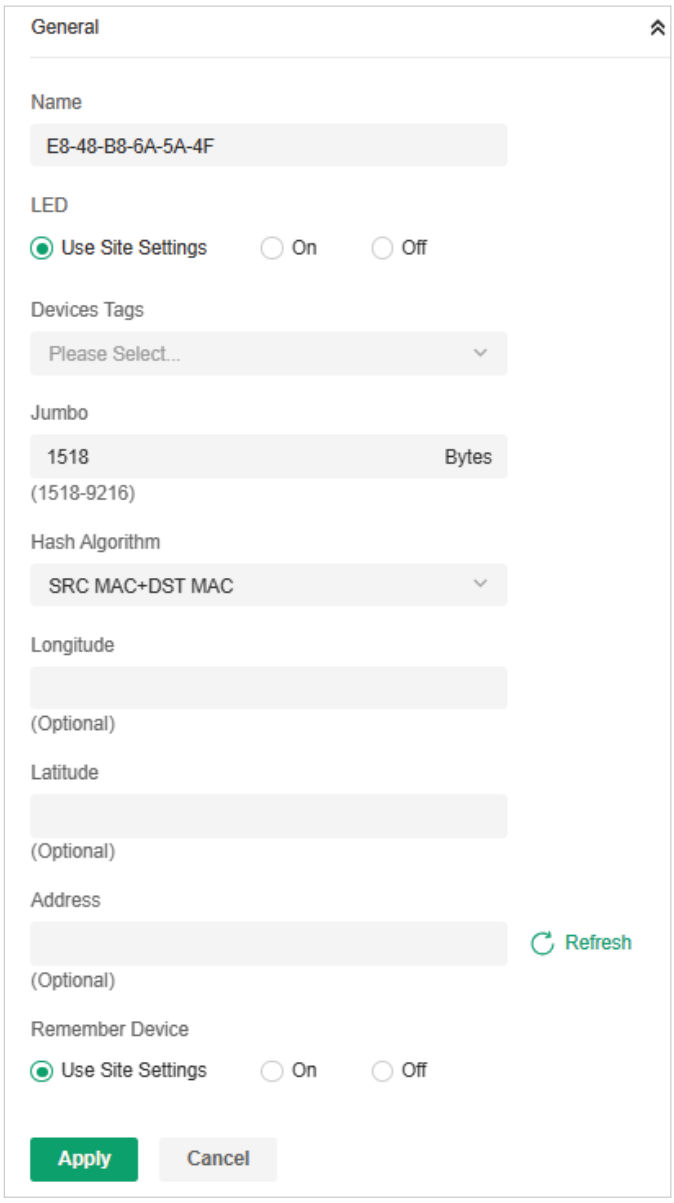
Broadcast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Unknown Unicast Threshold	With Storm Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.
Action	With Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.

Config

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

■ General

In General, you can specify general settings of the switch.

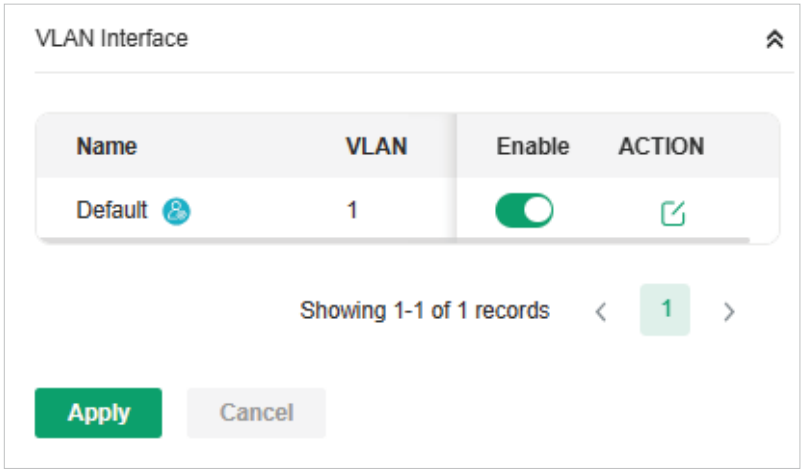


Name	(Only for configuring a single device) Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. On/Off: The device's LED will keep on/off.
Device Tags	Select a tag from the drop-down list or create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

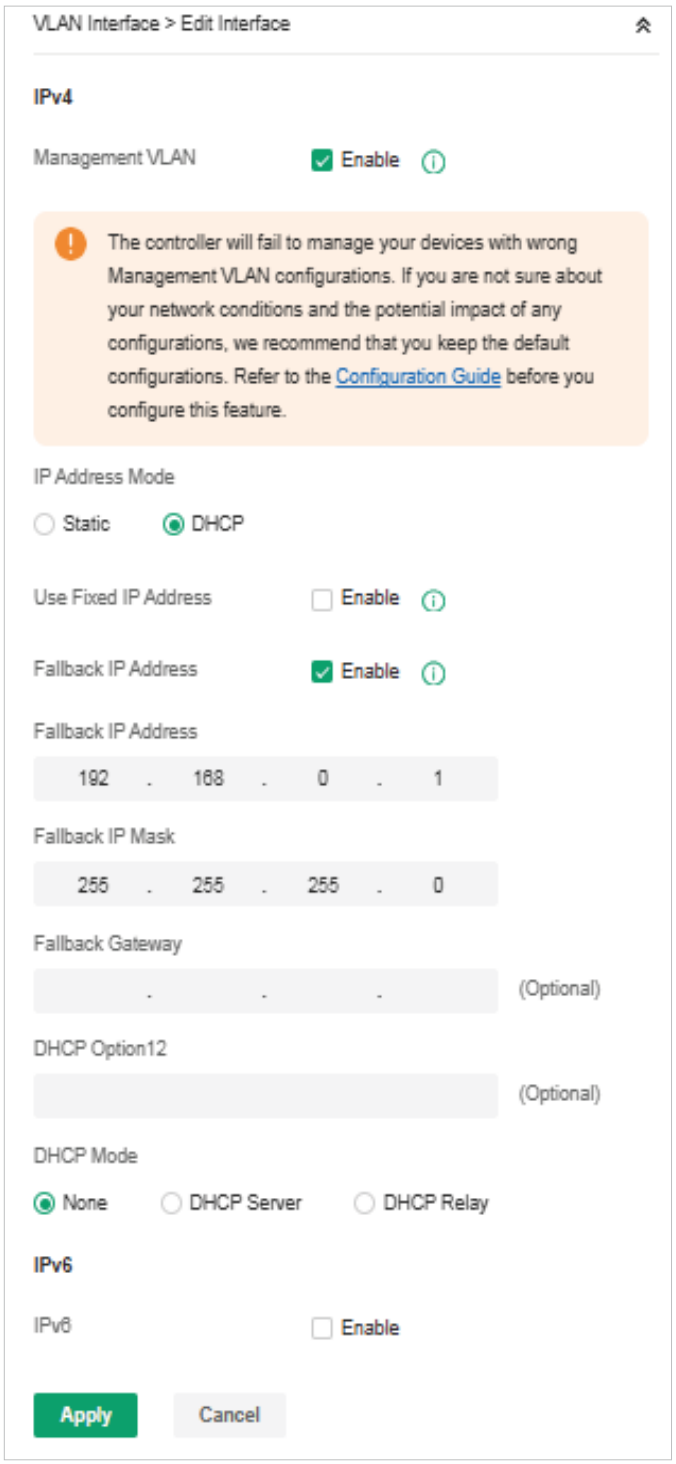
Jumbo	Configure the size of jumbo frames. By default, it is 1518 bytes. Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1518 bytes. If you want the switch supports to transmit frames of which the MTU size is greater than 1518 bytes, you can configure the MTU size manually here.
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.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.
Remember Device	When enabled, 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.

- VLAN Interface

In VLAN Interface, you can configure Management VLAN and different VLAN interface for the switch. The general information of the existing VLAN interface are displayed in the table.



To configure a single VLAN interface, hover the mouse on the entry and click to edit the settings.

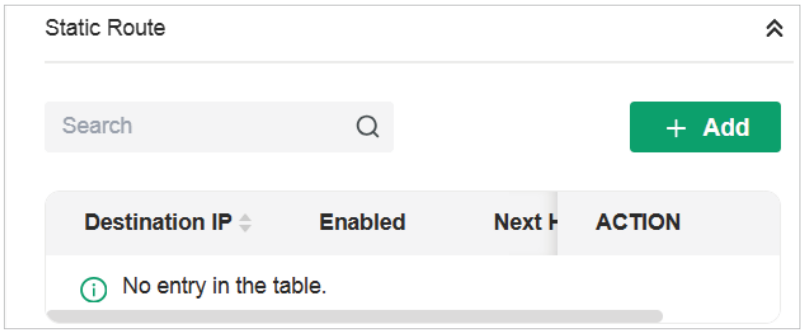


Management VLAN	Click the checkbox if you want to use the VLAN interface as Management VLAN. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
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.

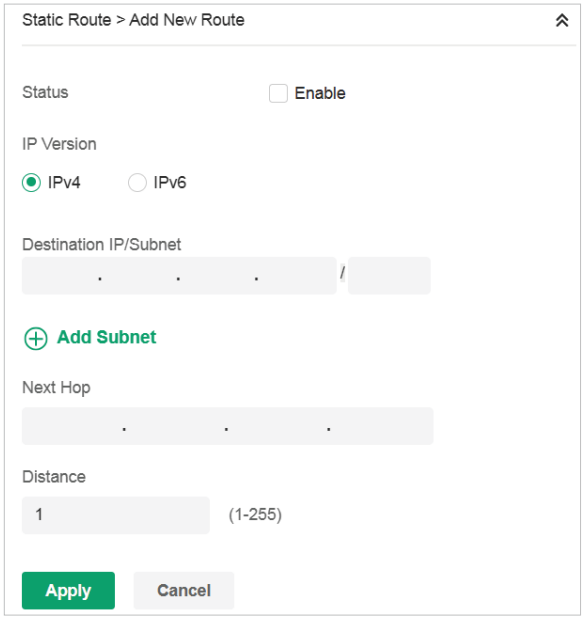
DHCP Mode	Select a mode for the clients in the VLAN to obtain their IP address. None: Do not use DHCP to assign IP addresses. DHCP Server: Assign an IP address to the clients through a DHCP server. When DHCP Server is selected, you can specify the DHCP Range, and the IP addresses in the range can be 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. 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.

- Static Route

In Static Route, you can configure entries of static route for the switch. The general information of the existing static route entries are displayed in the table. For an existing static route, click the edit button to modify the settings, and click the delete button to remove it.



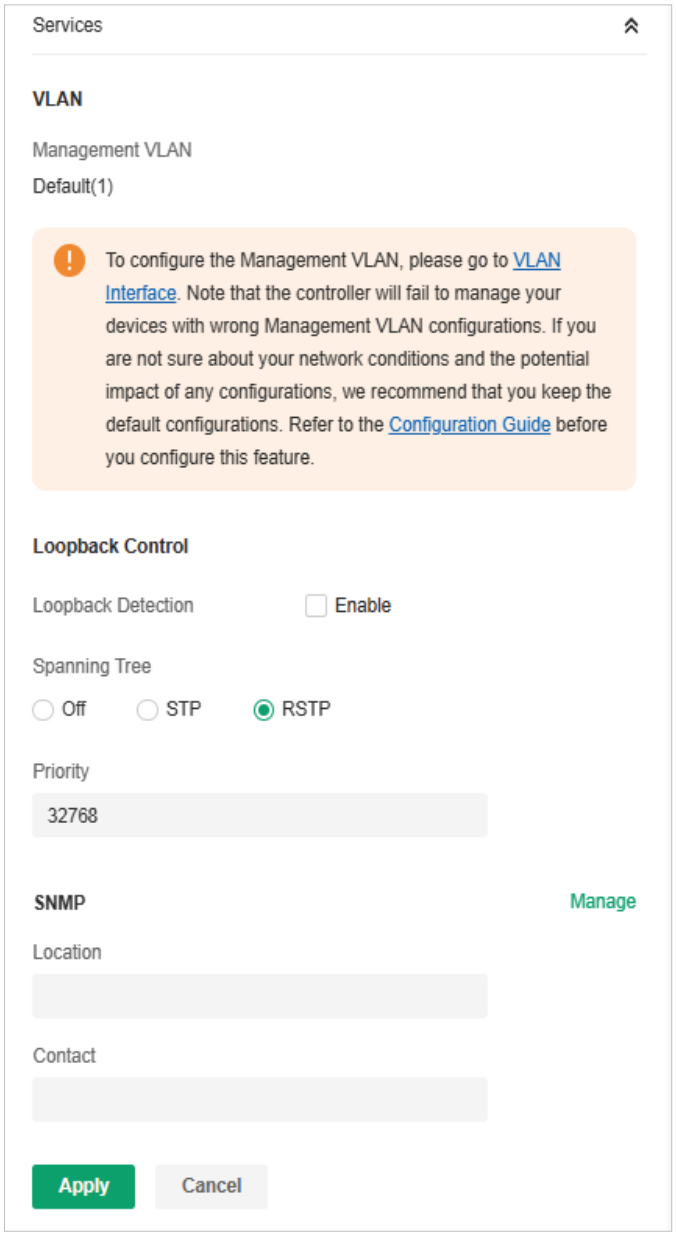
To add a new static route entry, click + Add and configure the parameters.



Status	Click the checkbox to enable or disable the static route.
IP Version	Select IPv4 or IPv6.
Destination IP/ Subnet / Destination IP/ Prefix Length	When IP Version is IPv4, specify Destination IP/Subnet. When IP Version is IPv6, specify Destination IP/Prefix Length. They identify the network traffic which the Static Route entry controls. You can click + Add Subnet to specify multiple entries or click the trash bin icon to delete them.
Next Hop	Specify the IP address for your devices to forward the corresponding network traffic.
Distance	Specify the priority of a static route. It is used to decide the priority among routes to the same destination. Among routes to the same destination, the route with the lowest distance value will be recorded into the routing table.

■ Services

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

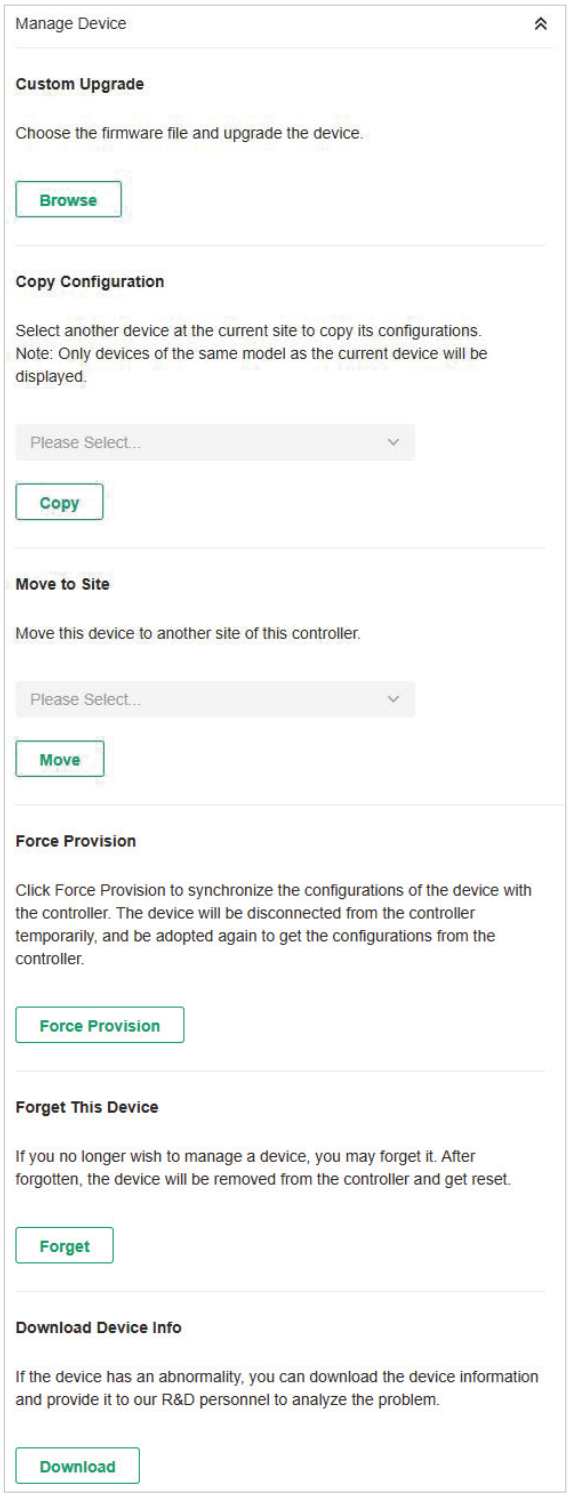


Management VLAN	Display the name of the current Management VLAN. To configure the Management VLAN, please go to Config > VLAN Interface. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.
Loopback Detection	When enabled, the switch checks the network regularly to detect the loopback. Note that Lopback Detection and Spanning Tree are not 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 ree convergence. Priority: When STP/RSTP enabled, specify the priority for the swith in Spanning Tree. In STP/RSTP, the switch with the highest priority will be selected as the root of the spanning tree. The switch with the lower value has the higher priority.

SNMP	(Only for configuring a single device) Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP.

Manage Device

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



Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.
Copy Configuration	Select another device at the current site to copy its configurations.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	(Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget This 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.
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.

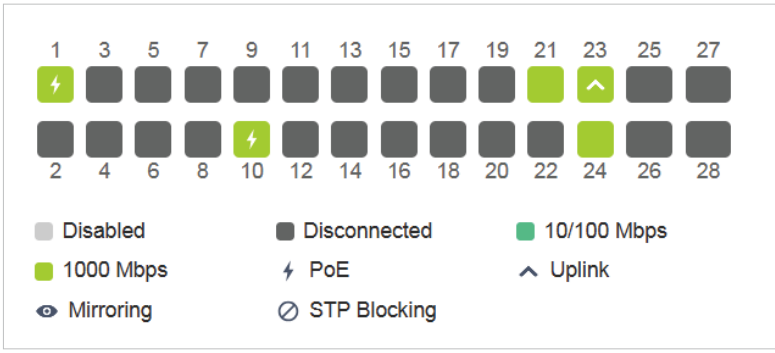
4. 4. 2 Monitor Switches

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

Monitor Panel

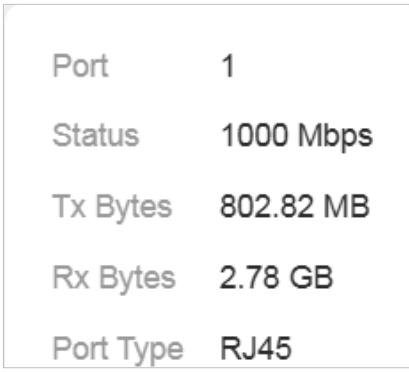
The monitor panel displays the switch's ports and uses colors and icons to indicate the connection status and port type. When the switch is pending or disconnected, all ports are

disabled.



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

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



Status	Displays the negotiation speed of the port.
Tx Bytes	Displays the amount of data transmitted as bytes.
Rx Bytes	Displays the amount of data received as bytes.
Profile	Displays the name of profile applied to the port, which defines how the packets in both ingress and egress directions are handled. For detailed configuration, refer to Create Profiles.
PoE Power	Displays the PoE power supply for the PD device.

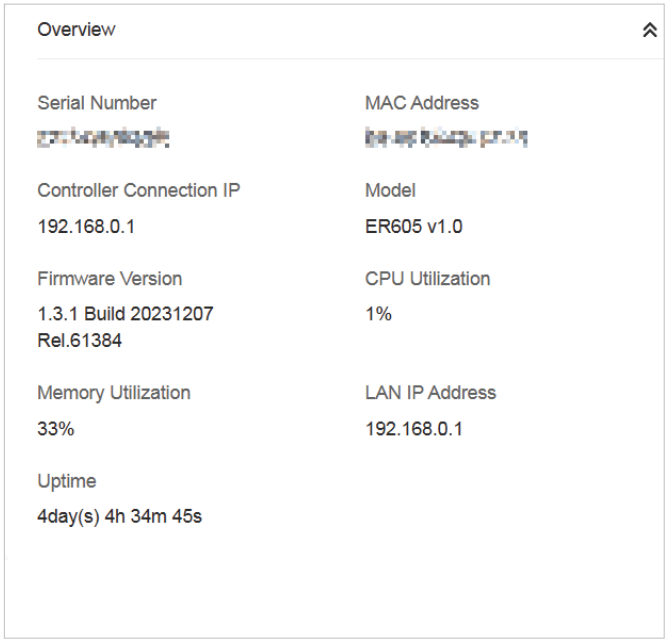
Uplink	Displays the name of device connected to the uplink port.
Mirroring From	Displays the name of port that is mirrorred.
LAG ID	Displays the name of ports that are aggregated into a logical interface.

Details

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

- Overview

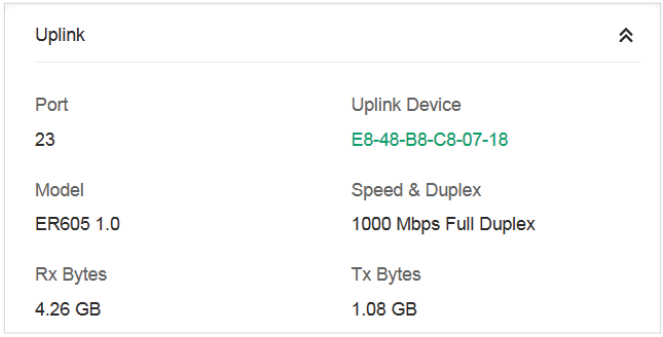
  In Overview, you can view the basic information of the device. The listed information will be varied due to the device's model and status.



- Uplink (Only for the switch connected to a controller-managed router/switch in

Connected status)

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



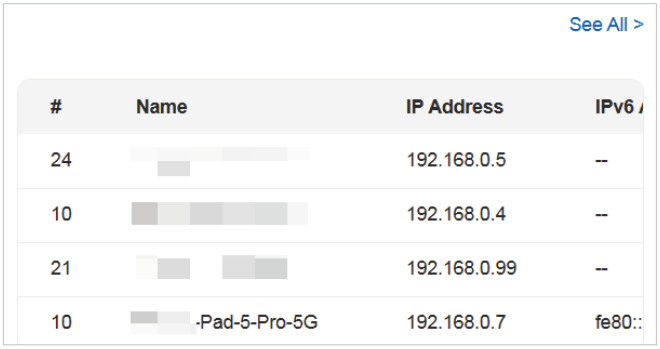
- Downlink (Only for the switch connected to controller-managed devices in Connected status)

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



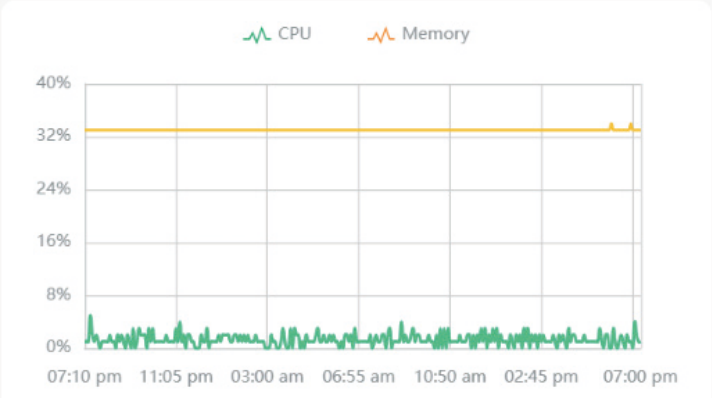
Clients

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



Statistics

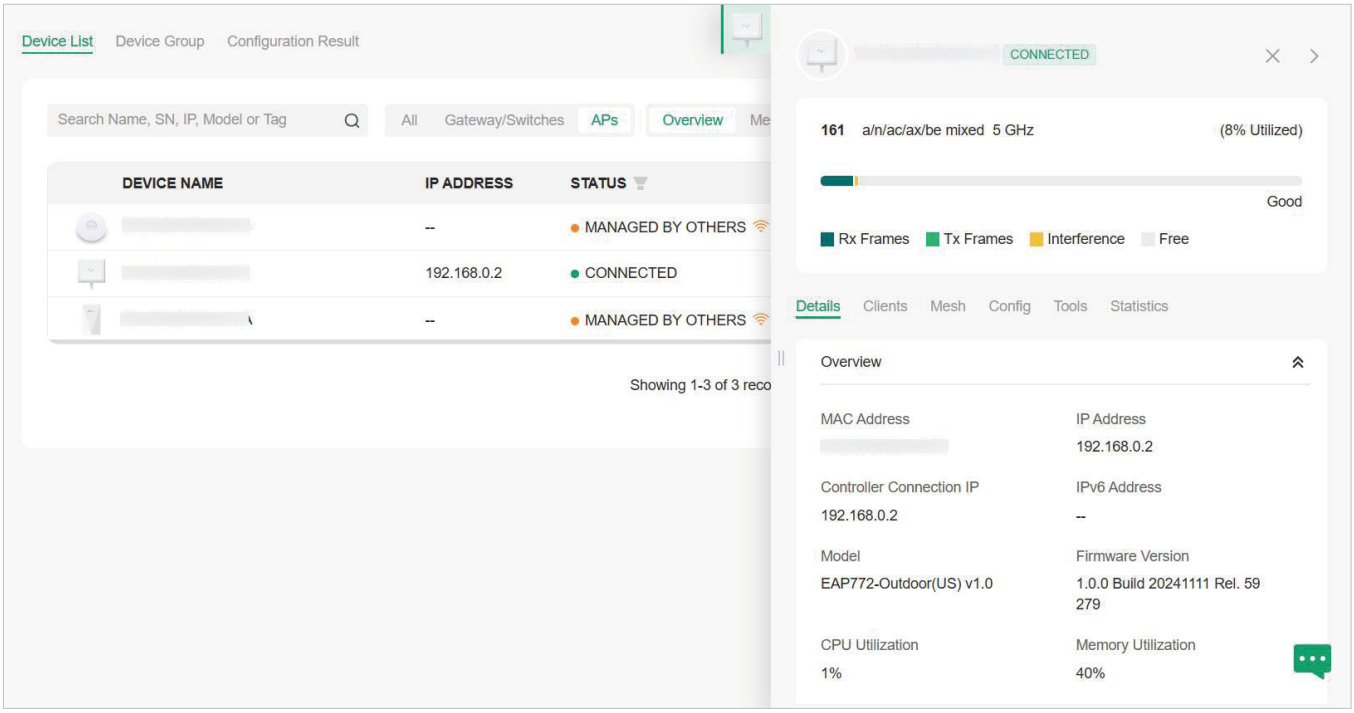
In Statistics, you can monitor the CPU and memory of the device in last 24 hours via charts. To view statistics of the device in certain period, click the chart to jump to View the Statistics of the Network.



4. 5 Configure and Monitor APs

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

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



Note:

The available functions in the window vary due to the model and status of the device.

In Batch Config, you can only configure the selected devices, and the unaltered configurations will keep the current settings.

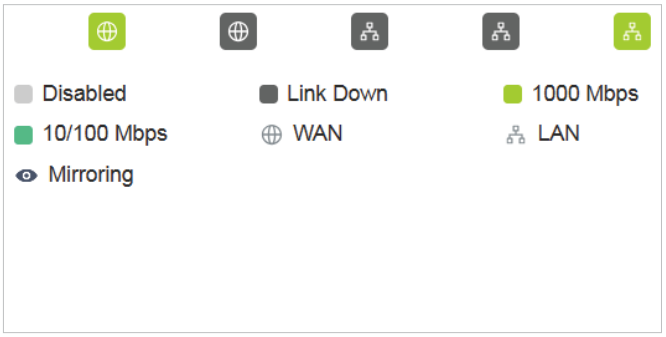
In Batch Config, if some functions, such as the 5 GHz band, are available only on some selected APs, the corresponding configurations will not take effect. To configure them successfully, check the model of selected devices first.

4. 5. 1 Configure APs

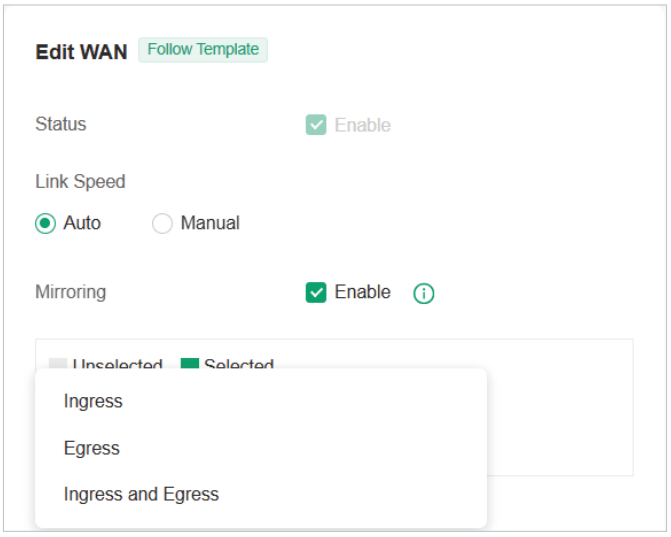
In the Properties window, you can view and configure the ports (only for EAPs with multiple LAN ports) in Ports, and configure the gateway features in Config.

Ports (Only for EAPs with multiple LAN ports)

In Ports, you can view the status and edit settings of the ports.



To configure a port, click the edit button in the Action column.



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 EAP inserts a VLAN tag to the frame based on the PVID before forwarding it.

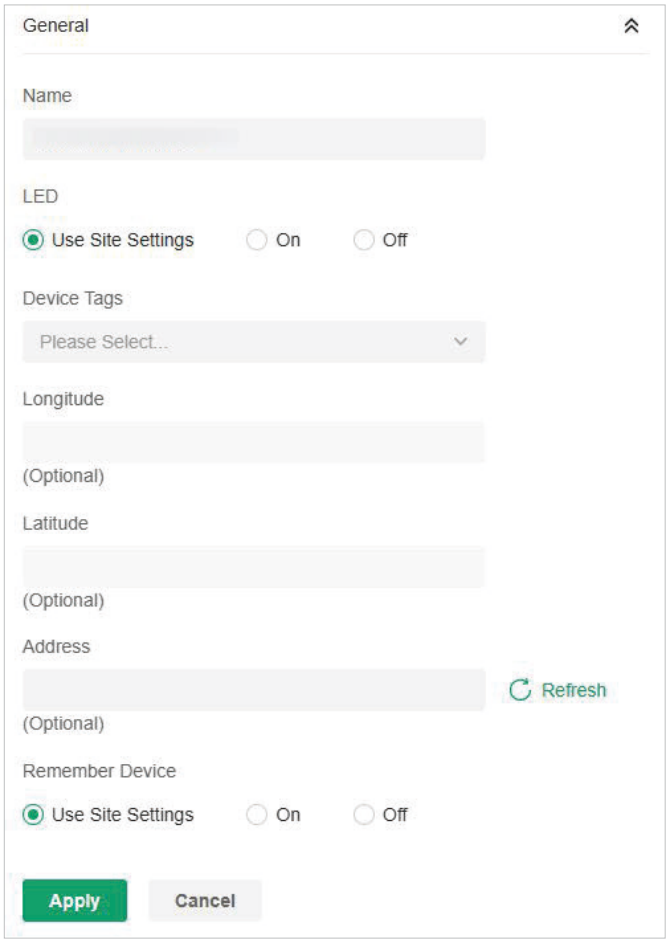
PoE Out	(Only for APs with the PoE out port) Enable this function to supply power to the connected device on this port.

Config

In the Properties window, click Config and then click the sections to configure the features applied to the selected AP(s).

- General

  In General, you can specify general settings of the AP.

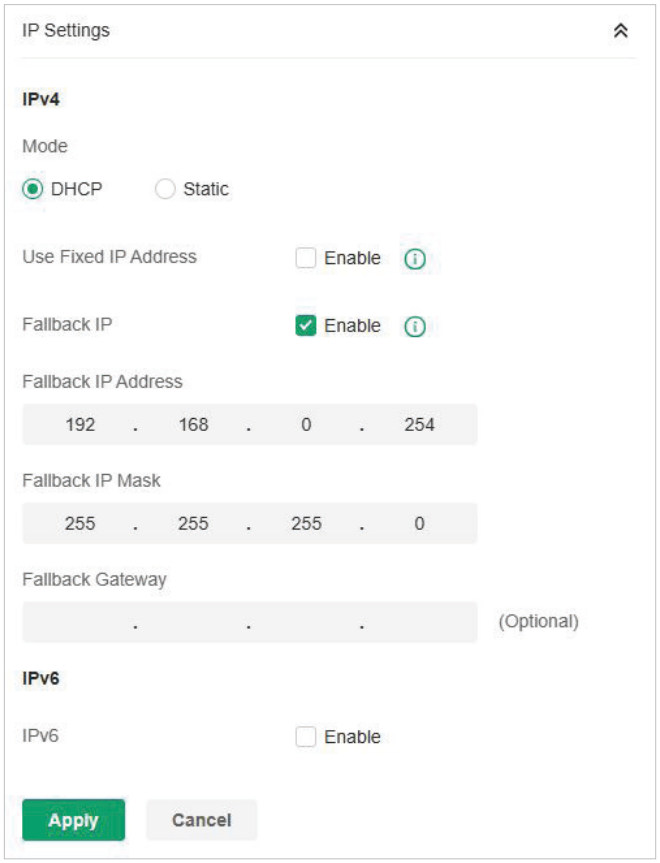


Name	(Only for configuring a single device) Specify a name of the device.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to General Config. On/Off: The device's LED will keep on/off.

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 Tags	Select a tag from the drop-down list or create a new tag to categorize the device.
Longitude / Latitude / Address	Configure the parameters according to where the site is located. These fields are optional.
Remember Device	When enabled, 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.

- IP Settings (Only for configuring a single device)

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



If you select DHCP as the mode, make sure there is a DHCP server in the network and then the device will obtain dynamic IP address from the DHCP server automatically. If you want to let the device use a fixed IP address, you can enable Use Fixed IP Address, and set the network and IP address based on needs. Also, you can set a fallback IP address to hold an

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

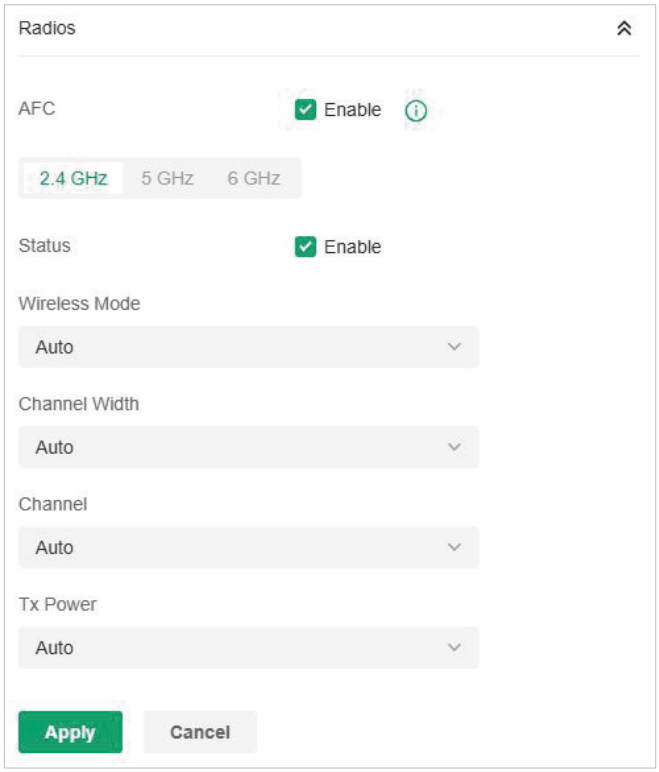
If you select Static as the mode, set the IP address, IP mask, gateway, and DNS server for the static address.

- Radios

In Radios, you can control how and what type of radio signals the AP emits. Select each frequency band and configure the parameters. Different models support different bands.

Note:

The 6 GHz band is only available for certain devices.



AFC	(For Wi-Fi 7 APs of US version) Enable this feature to use the 6GHz band. The AFC (Automated Frequency Coordination) feature adjusts the transmission power of the 6 GHz band according to your geographic location to meet regulatory requirements.
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.

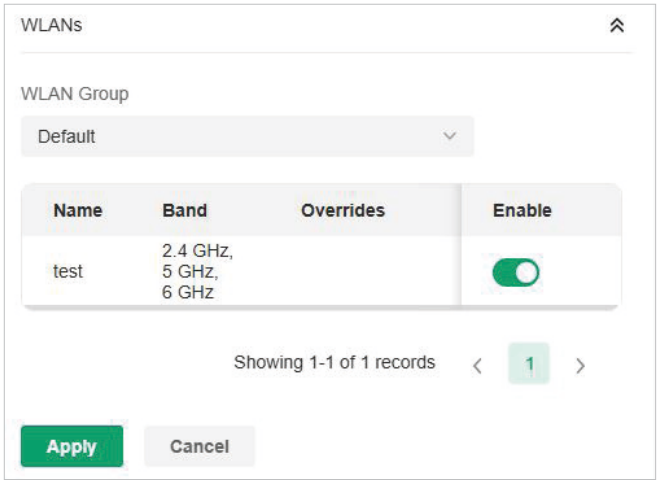
Channel	Specify the operation channel of the AP to improve wireless performance. If you select Auto for the channel setting, the AP scans available channels and selects the channel where the least amount of traffic is detected.
Tx Power	Specify the Tx Power (Transmit Power) in the 4 options: Low, Medium,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

- WLANs

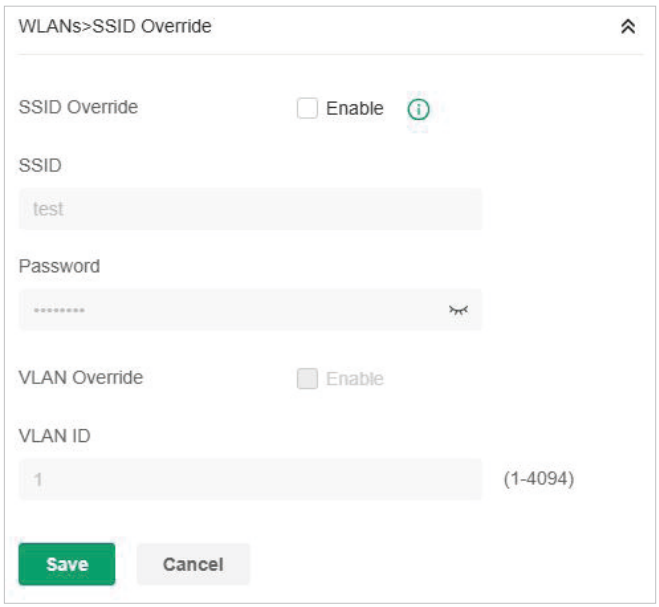
In WLANs, you can apply the WLAN group to the AP and specify a different SSID name and password to override the SSID in the WLAN group. After that, clients can only see the new SSID and use the new password to access the network. To create or edit WLAN groups, refer to Configure Wireless Networks.

Note:

The 6 GHz band is only available for certain devices.



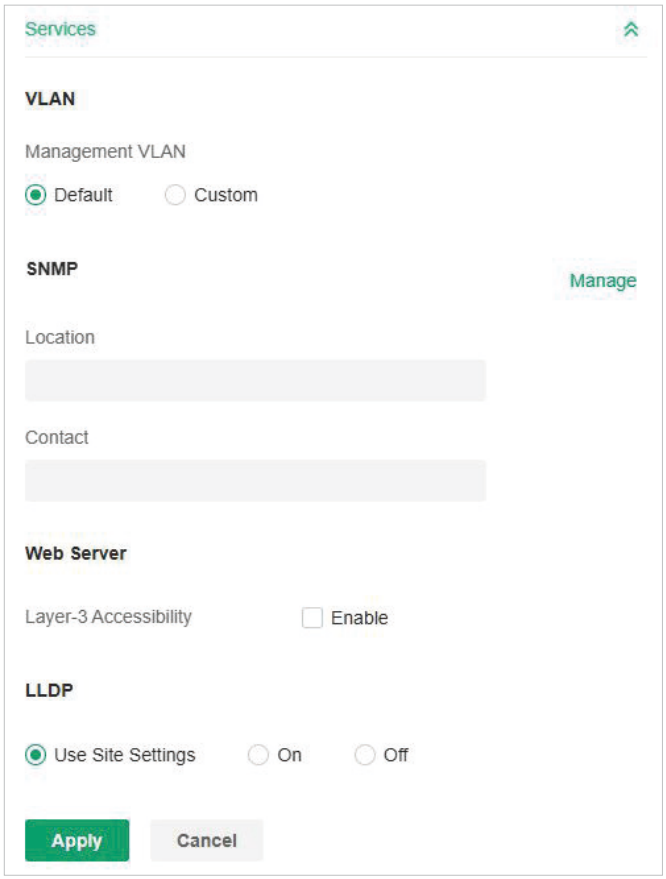
(Only for configuring a single device) To override the SSID, select a WLAN group, click in the entry and then the following page appears.



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

■ Services

In Services, you can enable Management VLAN to protect your network and configure SNMP and web server parameters.

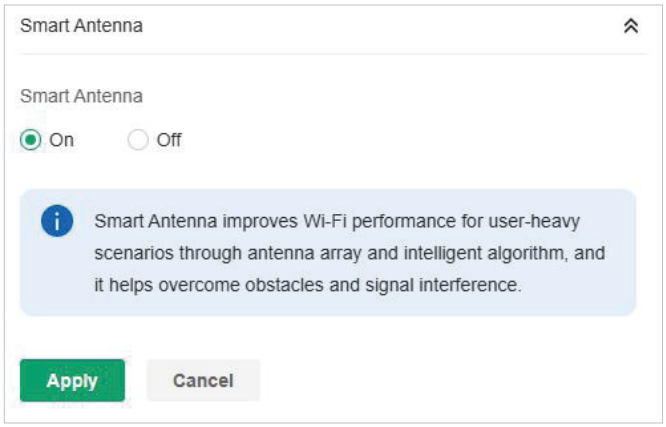


Management VLAN	To configure Management VLAN, create a network in LAN first, and then select it as the management VLAN on this page. For details, refer to Configure Wired Networks. The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands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

Loopback Control	(Only for EAPs 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.
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.

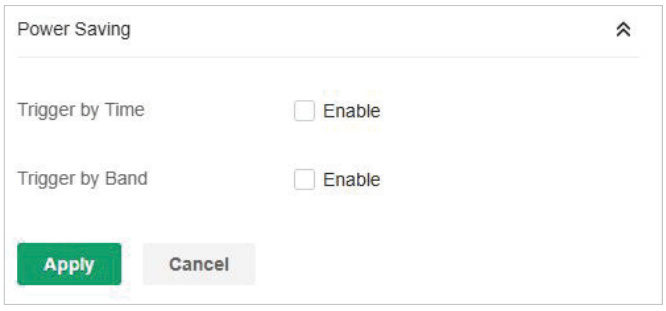
- Smart Antenna (Only for certain models)

  In Smart Antenna, you can turn on the function to improve Wi-Fi performance for user-heavy scenarios through antenna array and intelligent algorithm. This help overcome obstacles and signal interference.



- Power Saving (Only for certain models)

  In Power Saving, you can trigger the power saving mode reduce the AP's power usage.

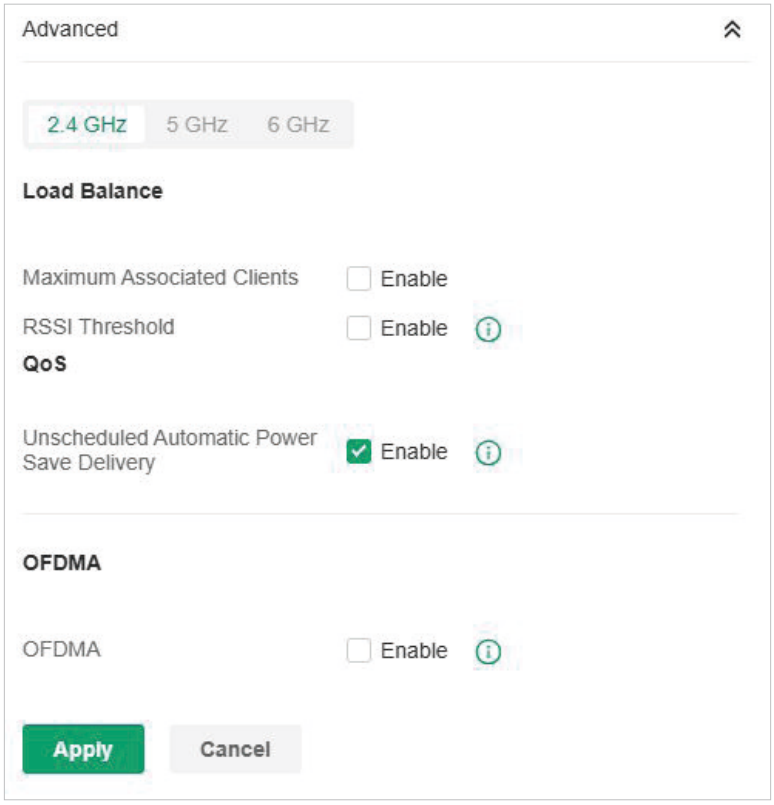


Trigger by Time	With this option enabled, you can specify the start and end time to enable power saving every day within the time period.

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.

- Advanced

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

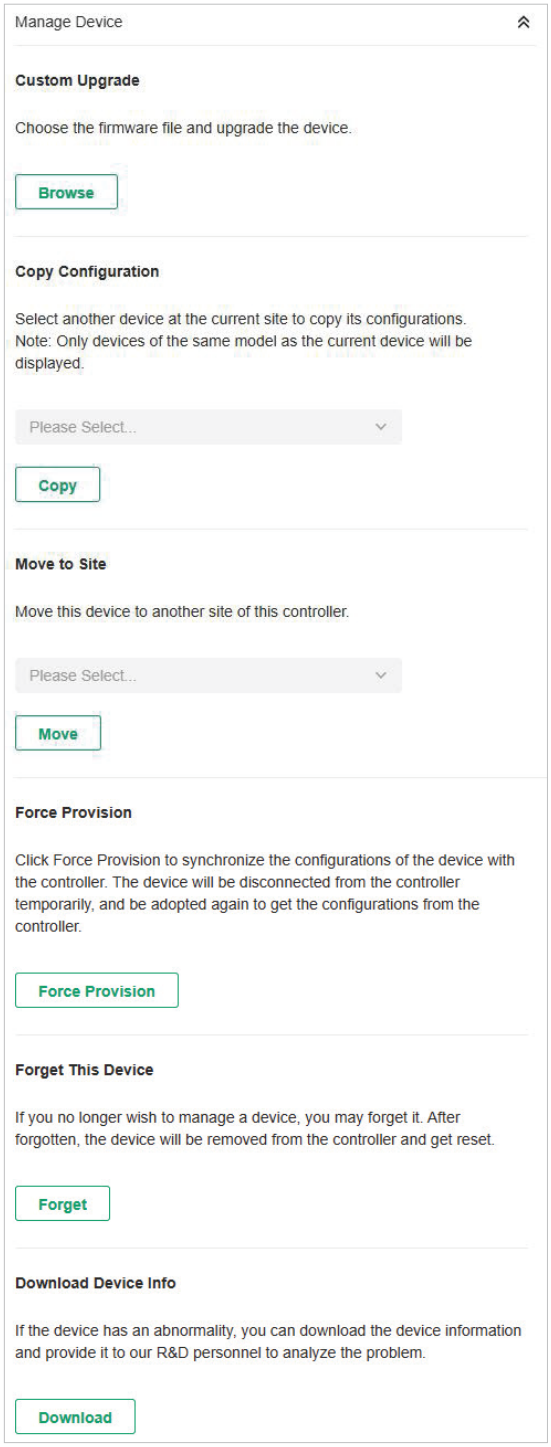


Max Associated Clients	Enable this function and specify the maximum number of connected clients. If the connected client reaches the maximum number, the AP will disconnect those with weaker signals to make room for other clients requesting connections.
RSSI Threshold	Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If the client's signal strength is weaker than the threshold, the client will lose connection with the AP.

ETH VLAN/ETH2 VLAN/ETH3 VLAN	(Only for APs with multiple LAN ports) Enable this function and add the corresponding AP's LAN port to the VLAN specified here. Then the hosts connected to this AP can only communicate with the devices in this VLAN.
ETH3 PoE Out	(Only for APs with the PoE out port) Enable this function to supply power to the connected device on this port.
Wi-Fi Multimedia (WMM)	With WMM enabled, the AP maintains the priority of audio and video packets for better media performance.
No Acknowledgment	Enable this function to specify that the APs will not acknowledge frames with QoS No Ack. Enabling No Acknowledgment can bring more efficient throughput, but it may increase error rates in a noisy Radio Frequency (RF) environment.
Unscheduled Automatic Power Save Delivery	When enabled, this function can greatly improve the energy-saving capacity of clients.
Non-PSC Channels	(Only for AP supporting 6GHz band) When enabled, the AP can use both non-PSC channels and PSC channels. Note that some clients may not discover 6GHz networks using non-PSC channels.
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.

Manage Device

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



Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. When upgrading, the device will be reboot and readopted by the controller. You can also check the box of Upgrade all devices of the same model in the site after the firmware file is uploaded.

Copy Configuration	Select another device at the current site to copy its configurations.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.
Force Provision	(Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget this AP	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.
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.

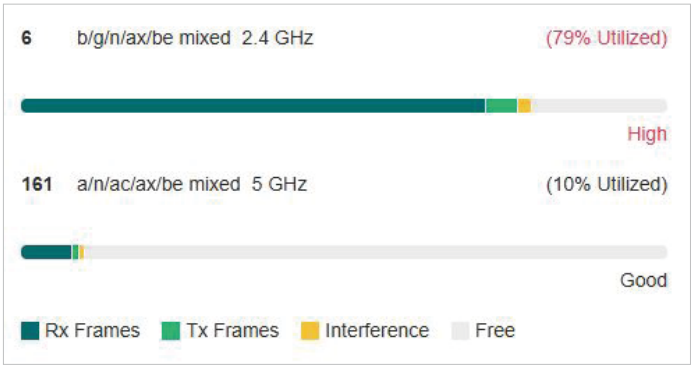
4. 5. 2 Monitor APs

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

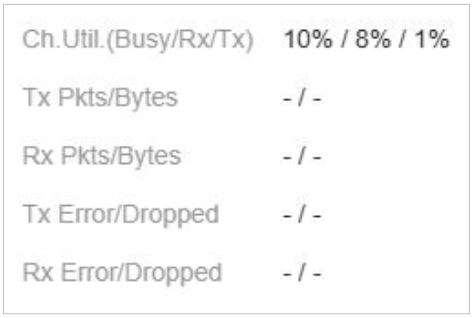
Monitor Panel

The monitor panel illustrates the active channel information on each radio band, including the AP's operation channel, radio mode and channel utilization. Four colors are used to indicate the percentage of Rx Frames (blue), Tx Frames (green), Interference (orange), and Free

bandwidth (gray).



You can hover the cursor over the channel bar for more details.



Ch.Util.(Busy/Rx/Tx)	Displays channel utilization statistics. **Busy**: Displays the sum of Tx, Rx, and also non-WiFi interference, which indicates how busy the channel is. **Rx**: Indicates how often the radio is in active receive mode. **Tx**: Indicates how often the radio is in active transmit mode.
Tx Pkts/Bytes	Displays the amount of data transmitted as packets and bytes.
Rx Pkts/Bytes	Displays the amount of data received as packets and bytes.
Tx Error/Dropped	Displays the percentage of transmit packets that have errors and the percentage of packets that were dropped.
Rx Error/Dropped	Displays the percentage of receive packets that have errors and the percentage of packets that were dropped.

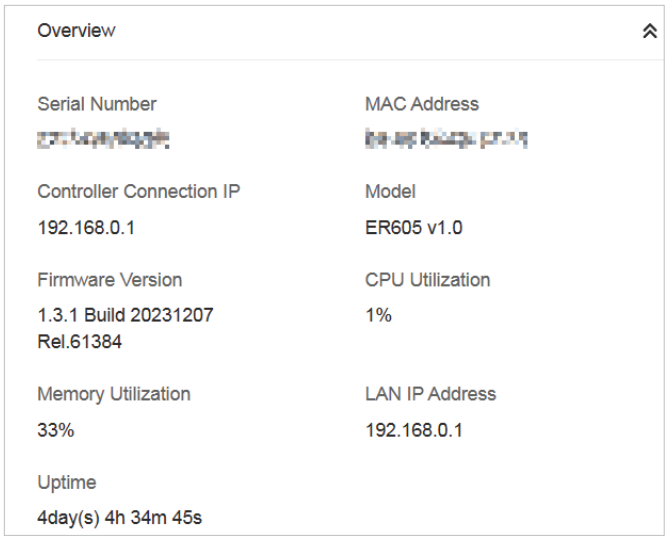
Details

In Details, you can view the basic information, traffic information, and radio information of the

device to know the device's running status.

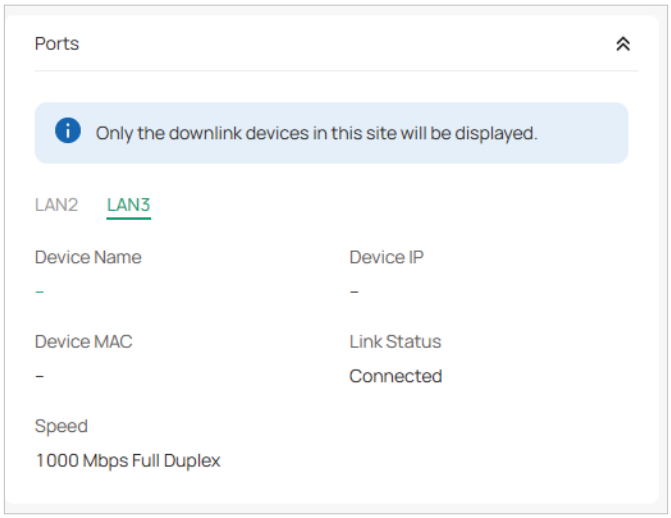
- Overview

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



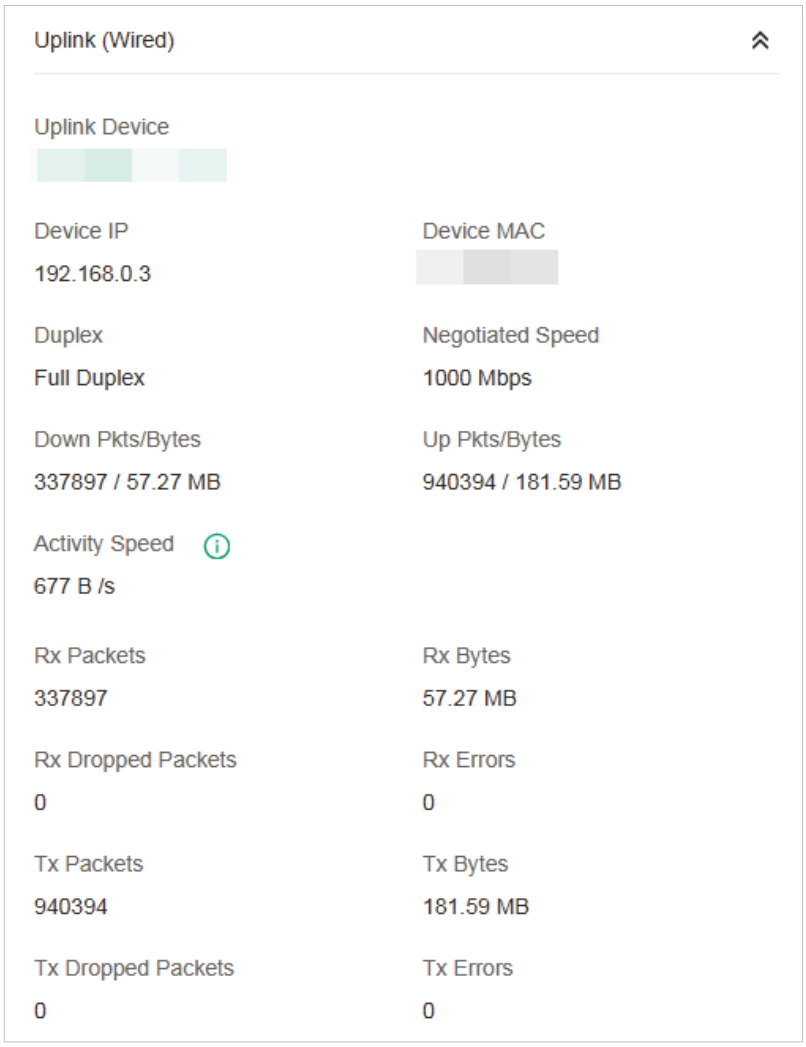
- LAN (Only for devices in the Connected status)

  Click LAN to view the traffic information of the LAN port, including the total number of packets, the total size of data, the total number of packets loss, and the total size of error data in the process of receiving and transmitting data.



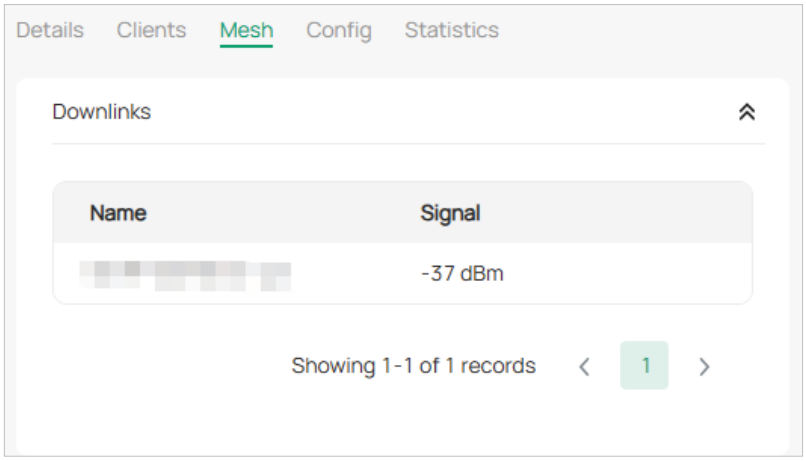
- Uplink (Only for devices in the Connected status)

  Click Uplink to view the traffic information related to the uplink device.



- Downlink (Only for devices in the Connected status)

  Click Downlink to view the information related to the downlink devices.



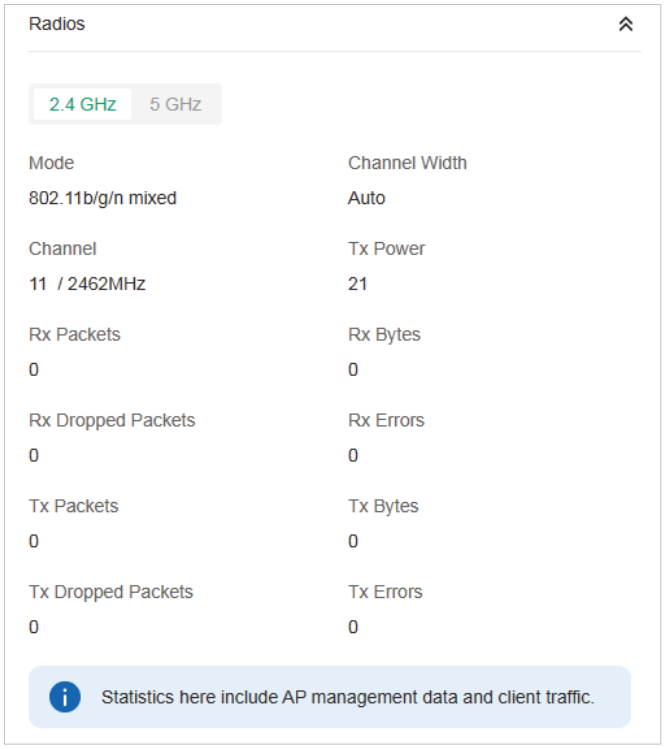
- Radios (Only for devices in the Connected status)

  Click Radio to view the radio information including the frequency band, the wireless mode, the channel width, the channel, and the transmitting power. You can also view parameters

of receiving/ transmitting data on each radio band.

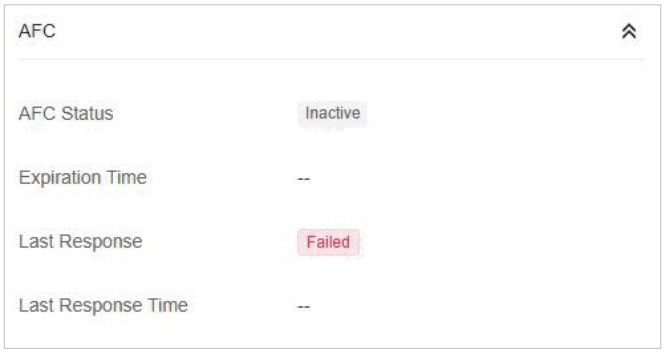
Note:

The 6 GHz band is only available for certain devices.



- AFC (Only for Wi-Fi 7 APs of US version)

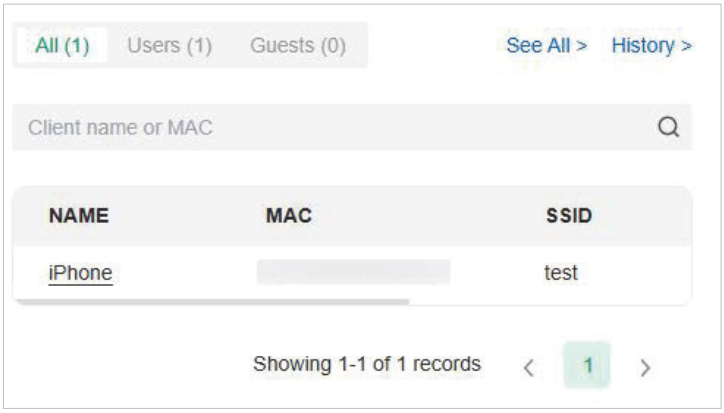
  Click AFC to view the AFC information, including the AFC status, expiration time, last response, and last response time.



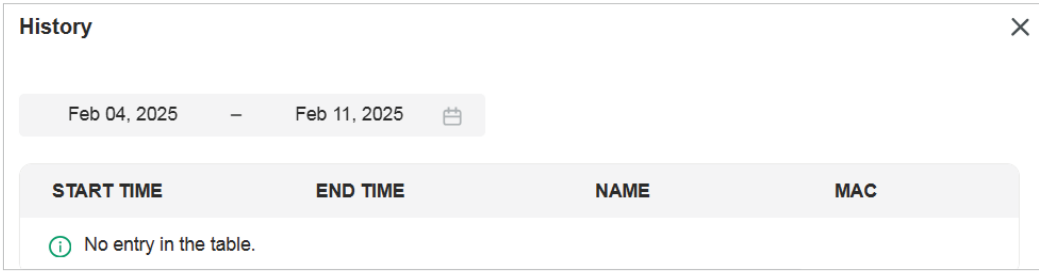
Clients

In Clients, you can view the information of users and guests connecting to the AP, including client name, MAC address and the connected SSID. Users are clients connected to the AP's SSID with Guest Network disabled, while Guests are clients connected to that with Guest

Network enabled. You can click the client name to open its Properties window.



Click History to view the client history. In the History page, you can specify the date or time period to view the clients connected during specific time, and click Export to download the list of clients.



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.

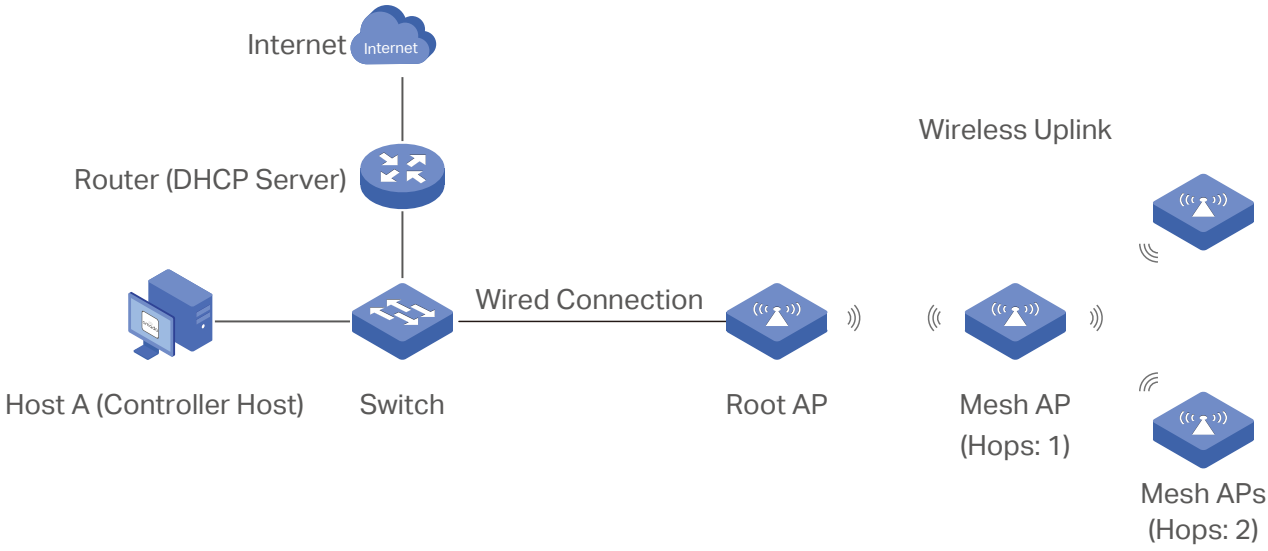
Note that only certain AP models support Mesh, and the APs should be in the same site to establish a Mesh network.

To understand how mesh can be used, the following terms used in the Controller 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.

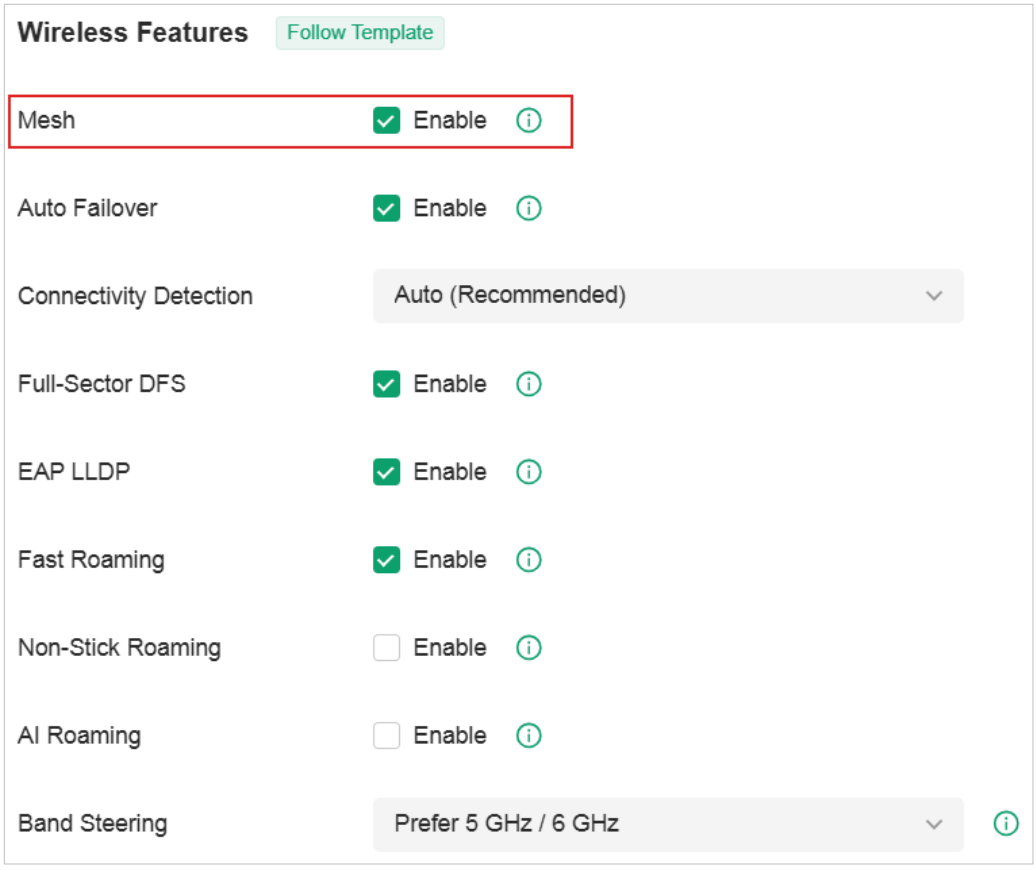
To build a mesh network, follow the steps below:

1) Enable Mesh function.

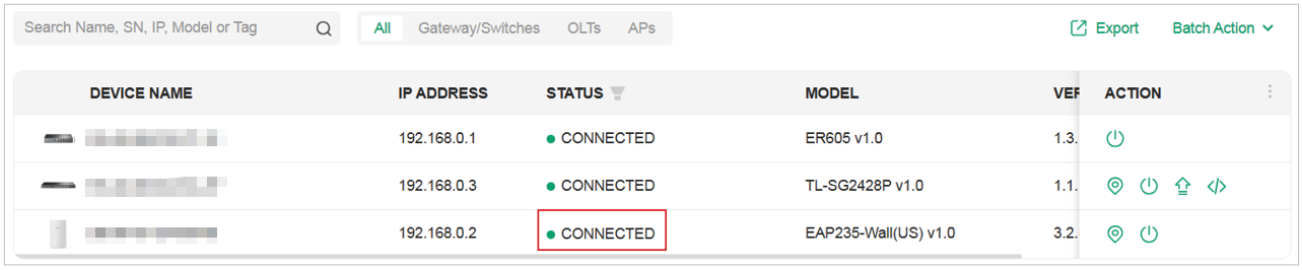
2) Adopt the Root AP.

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

1. Go to Settings > Site Settings to make sure Mesh is enabled.

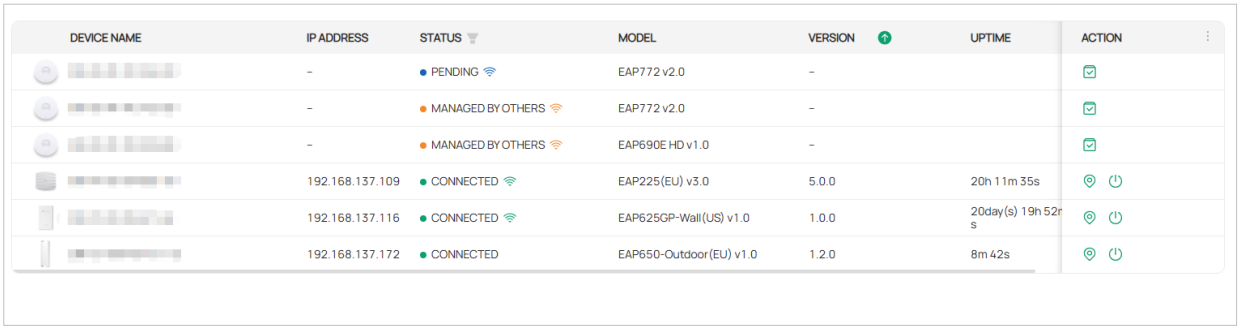


2. Go to Devices to make sure that the Root AP has been adopted by the controller. The status of the Root AP is Connected.



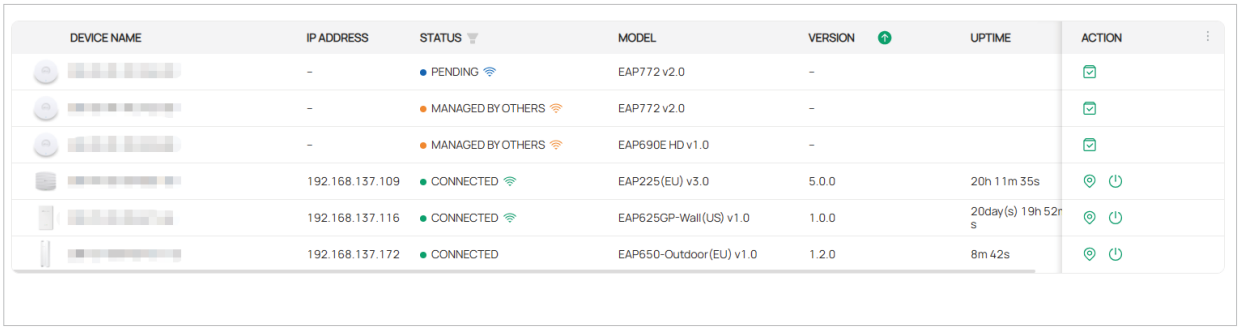
3. Install the AP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The APs that is waiting for Wireless Uplink includes two cases: factory default APs and APs that has been managed by the controller before. Go to Devices to adopt an AP in Pending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

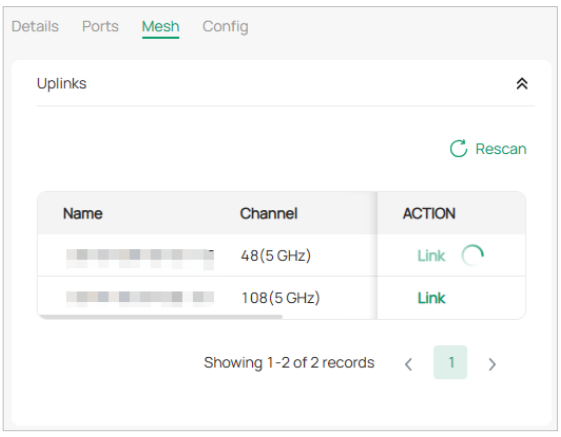


After adoption begins, the status of Pending (Wireless) AP will become Adopting (Wireless) and then Connected (Wireless). It should take roughly 2 minutes to show up Connected (Wireless) on your controller.

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.

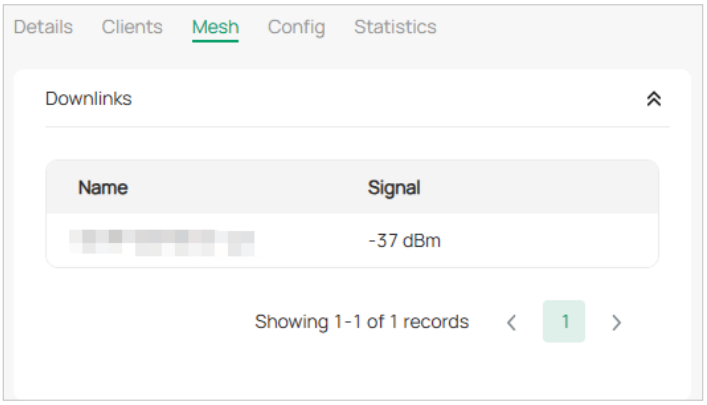


The following page will be shown as below, click Link to connect the Uplink AP.

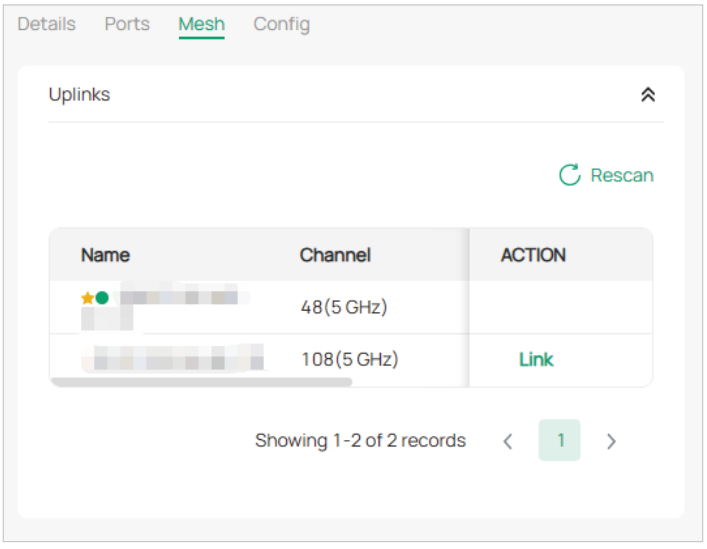


Once mesh network has been established, the AP can be managed by the controller in the same way as a wired AP. You can click the AP's name in the Devices list, and click Mesh to view and configure the mesh parameters of the AP in the Properties window.

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.



★	The icon appears before the priority uplink AP of the downlink AP. If you want to set another AP as the priority AP, click Link in Action column.
●	The icon appears before the current uplink AP of the downlink AP.

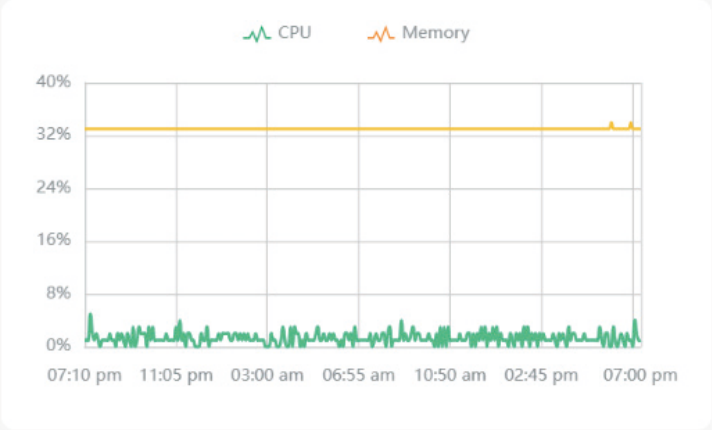
Tips:

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, 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. For more details about Mesh global configurations, refer to the Mesh feature in General Config.

Statistics

In Statistics, you can monitor the utilization of the device in last 24 hours via charts, including CPU/Memory Monitor, Channel Utilization, Dropped Packets, and Retried Packets. To view statistics of the device in certain period, click the chart to jump to View the Statistics of the Network.



4. 6 Create and Manage Bridge Groups

4. 6. 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.

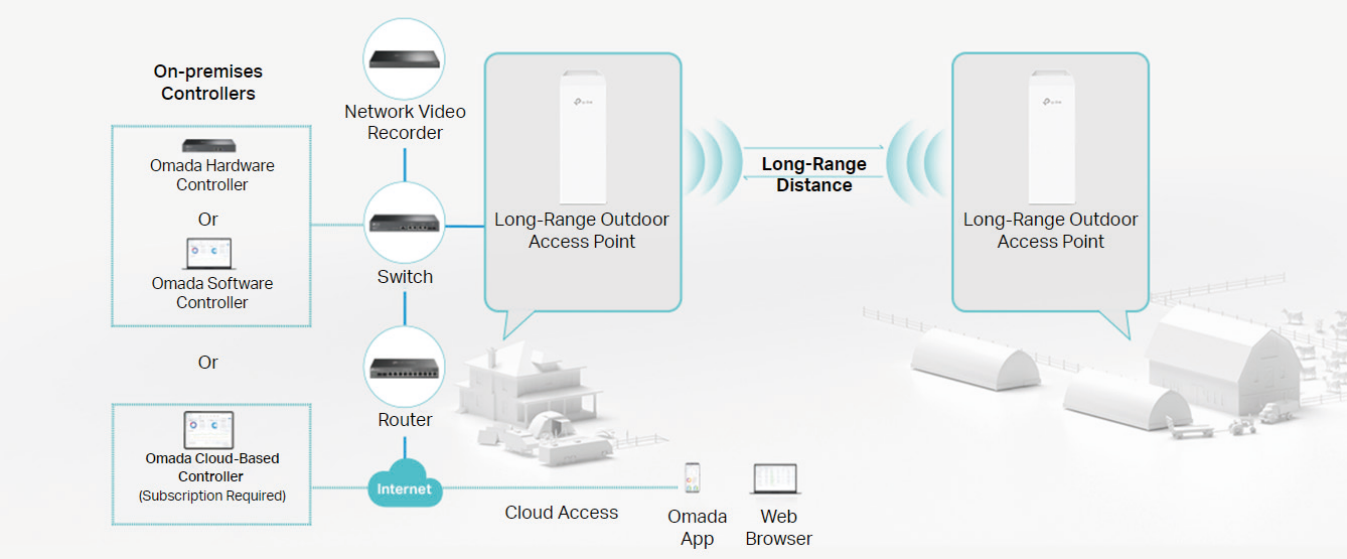
In a bridge system, the APs can be categorized mainly into two roles:

- Main AP

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

- Sub-AP

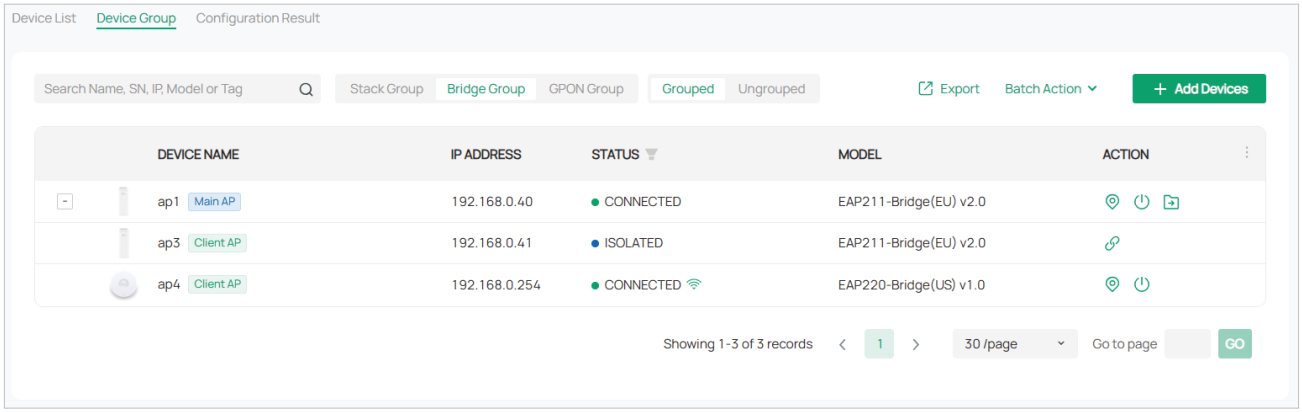
  Sub-APs connect to the Main AP via wireless bridge. A bridge system may have one or several Sub-APs.



4. 6. 2 Create a Bridge Group

1. Obtain a bridge kit product, connect an AP to your gateway/router for network access, and power on all the APs in the kit. The AP with network access will work as the Main AP, and the other AP(s) will automatically connect to the Main AP via wireless bridge.
2. Launch your controller and access a site.
3. Go to Devices > Device Group > Bridge Group. The controller will detect the bridge kit

APs and show them in the list.



4. 6. 3 Configure and Monitor the Bridge Group

You can configure and monitor bridge groups in the same way as configuring and monitoring APs. For details, refer to Configure and Monitor APs.

Chapter 5

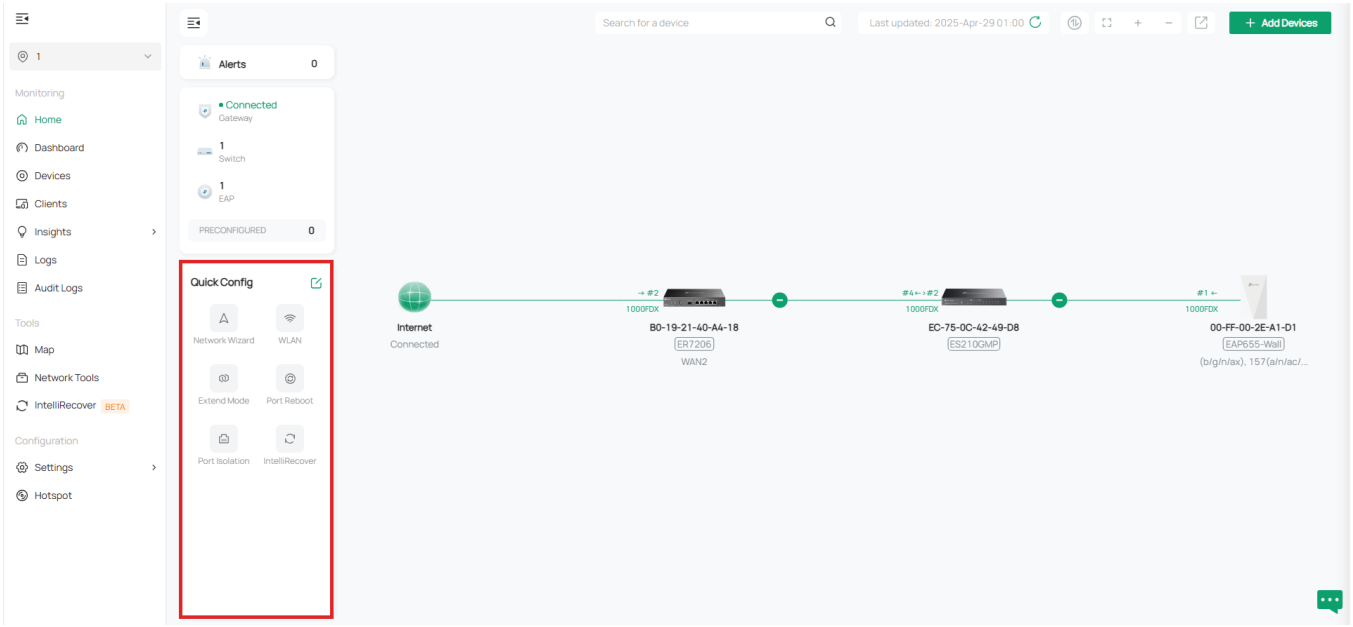
Configure the Network with Omada Central Essentials

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

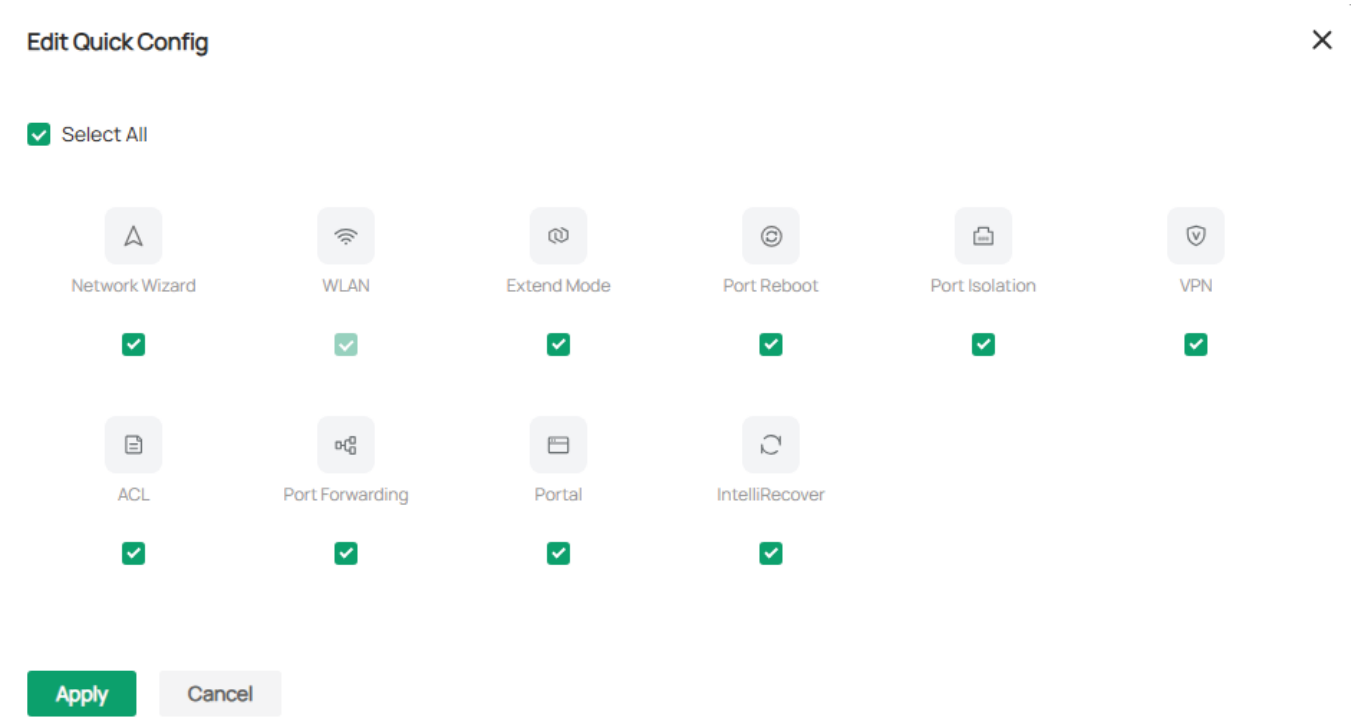
- 5.1 Quick Config in Home Page
- 5.2 Configure Wired Networks
- 5.3 Configure Wireless Networks
- 5.4 Network Security
- 5.5 Transmission
- 5.6 Configure VPN
- 5. 7 Configure VoIP
- 5.8 Services
- 5.9 Authentication
- 5.10 Create Profiles

5. 1 Quick Config in Home Page

The Home page of the Omada Central Essentials provides quick configuration for your network.

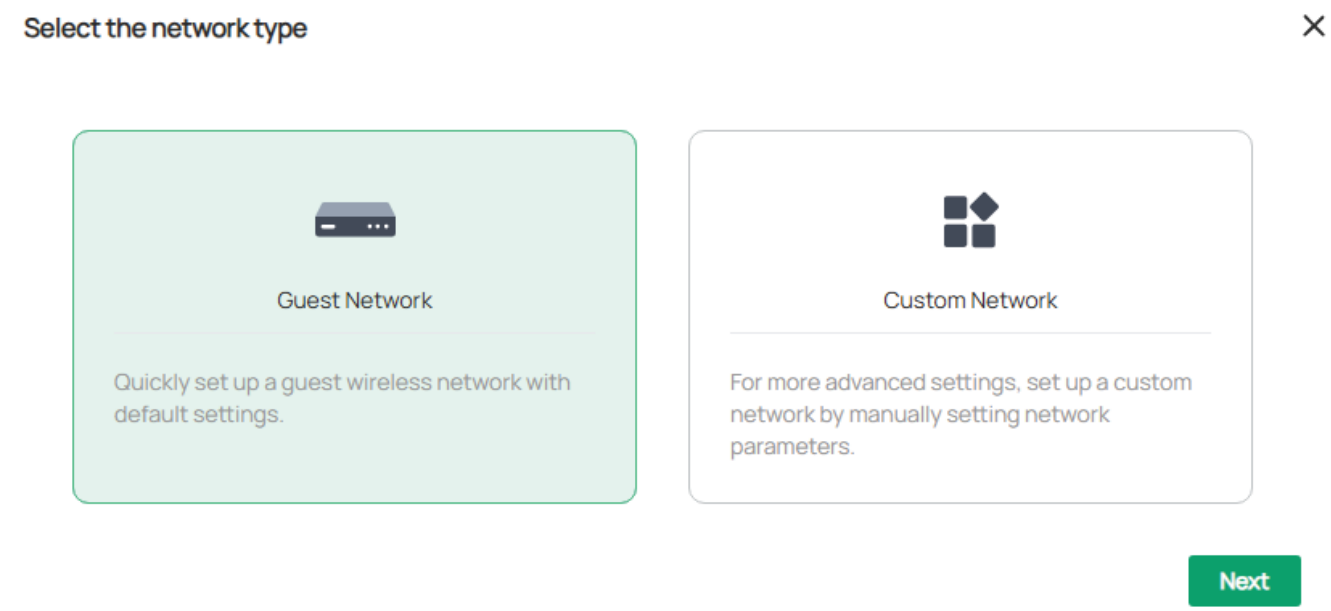


You can click the edit icon in the Quick Config section to select which to display in your Home page.



■ Network Wizard

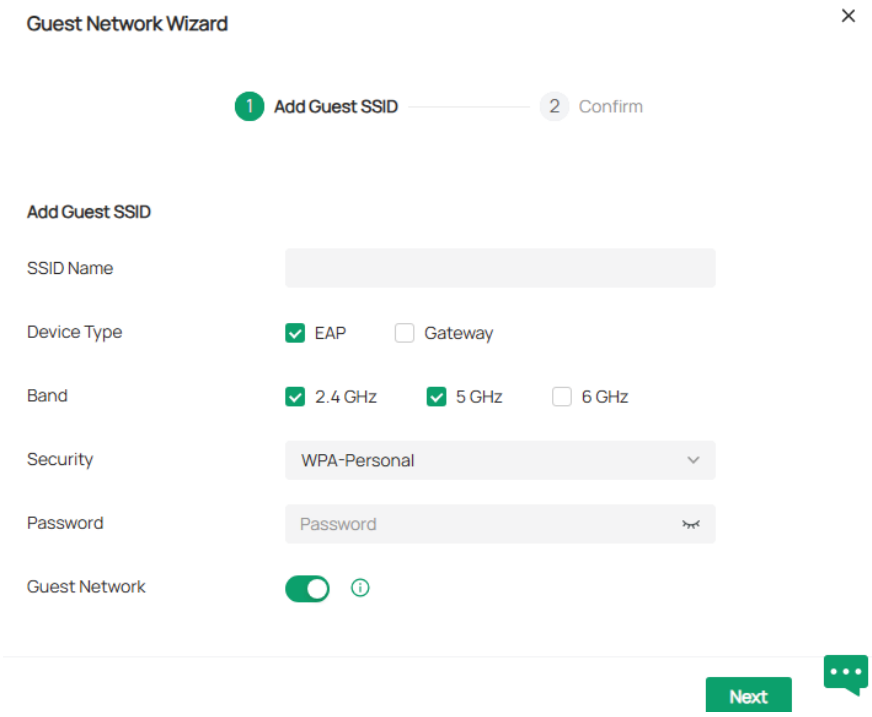
In Network Wizard, you can quickly set up a guest wireless network with default settings or a custom network by manually setting network parameters.



- Guest Network

You can quickly set up a guest wireless network with default settings.

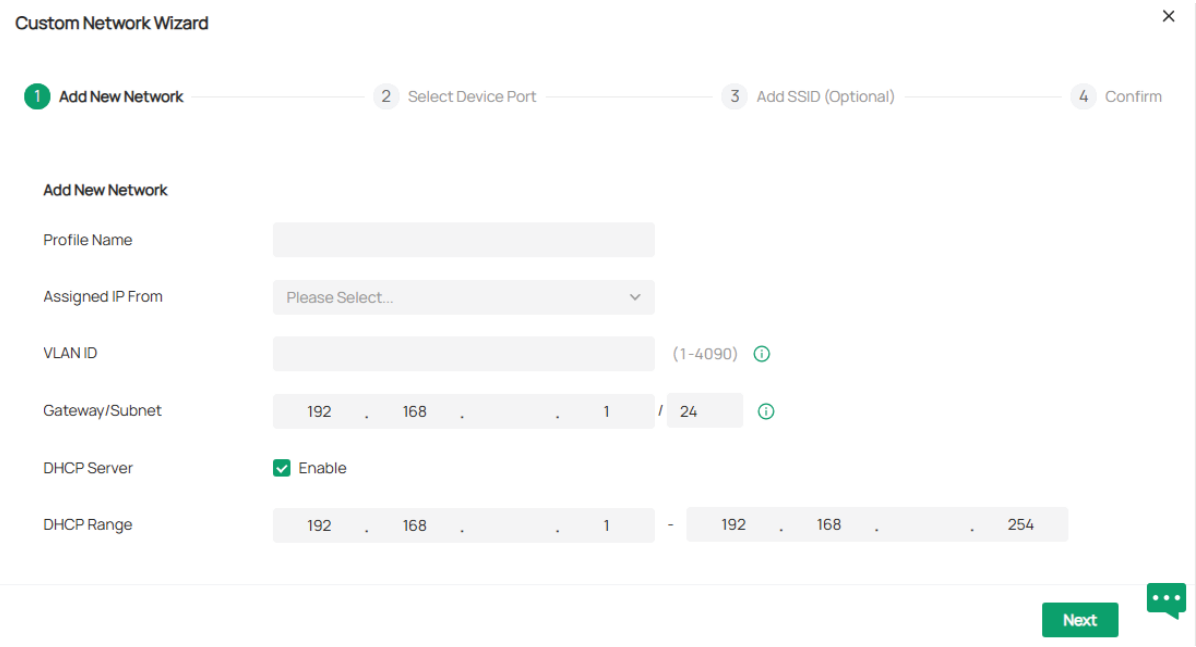
1) Configure the parameters, click Next to confirm your settings and click Apply.



- Custom Network

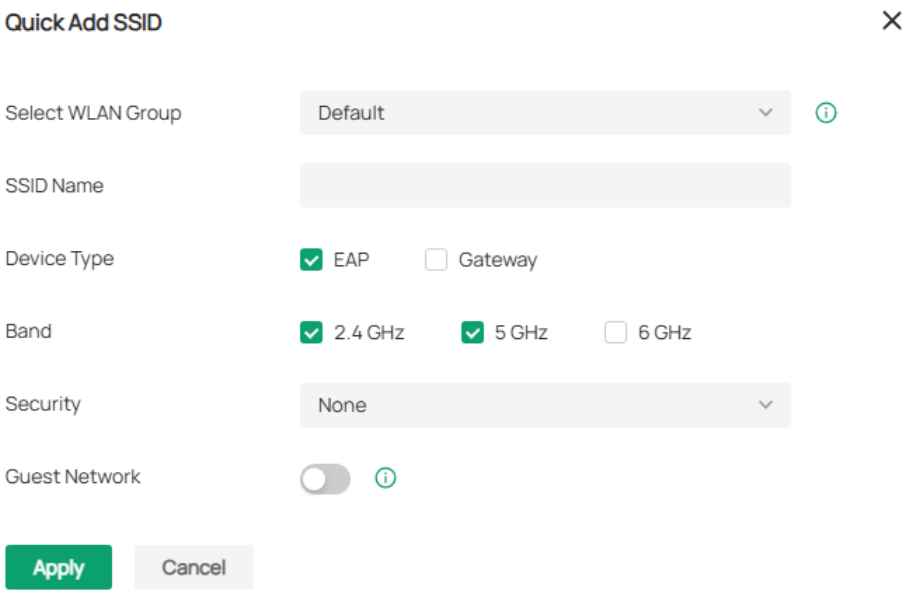
You can also set up a custom network by manually setting network parameters.

Configure the parameters, click Next to confirm your settings and click Apply.



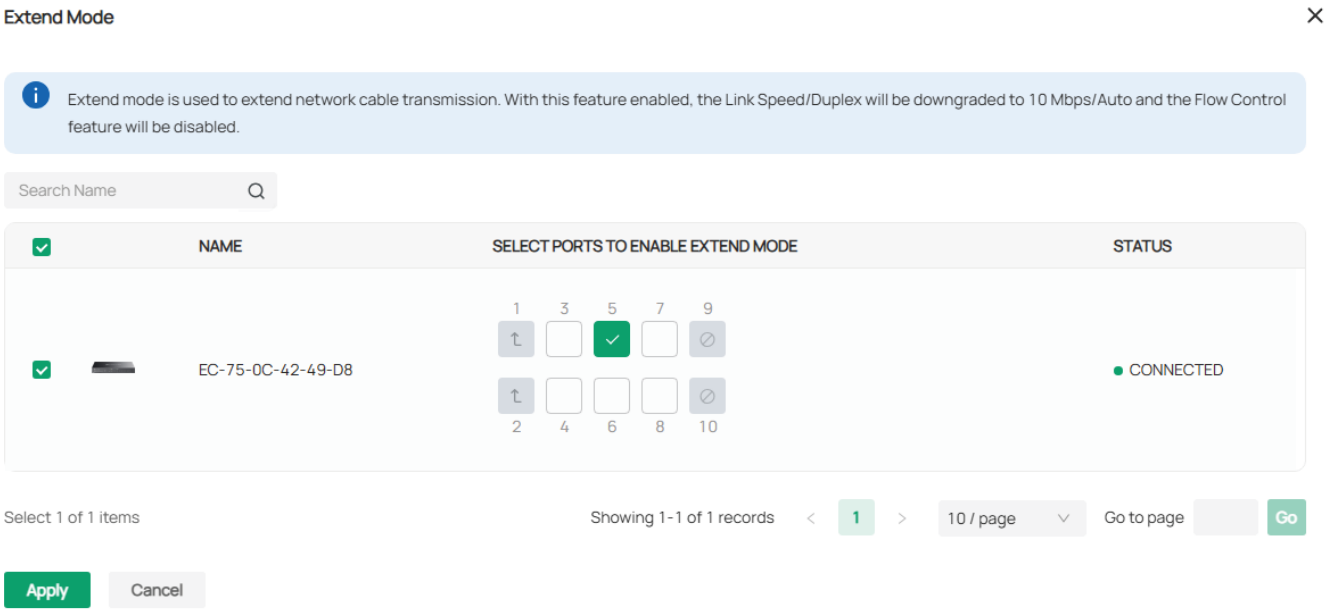
■ WLAN

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



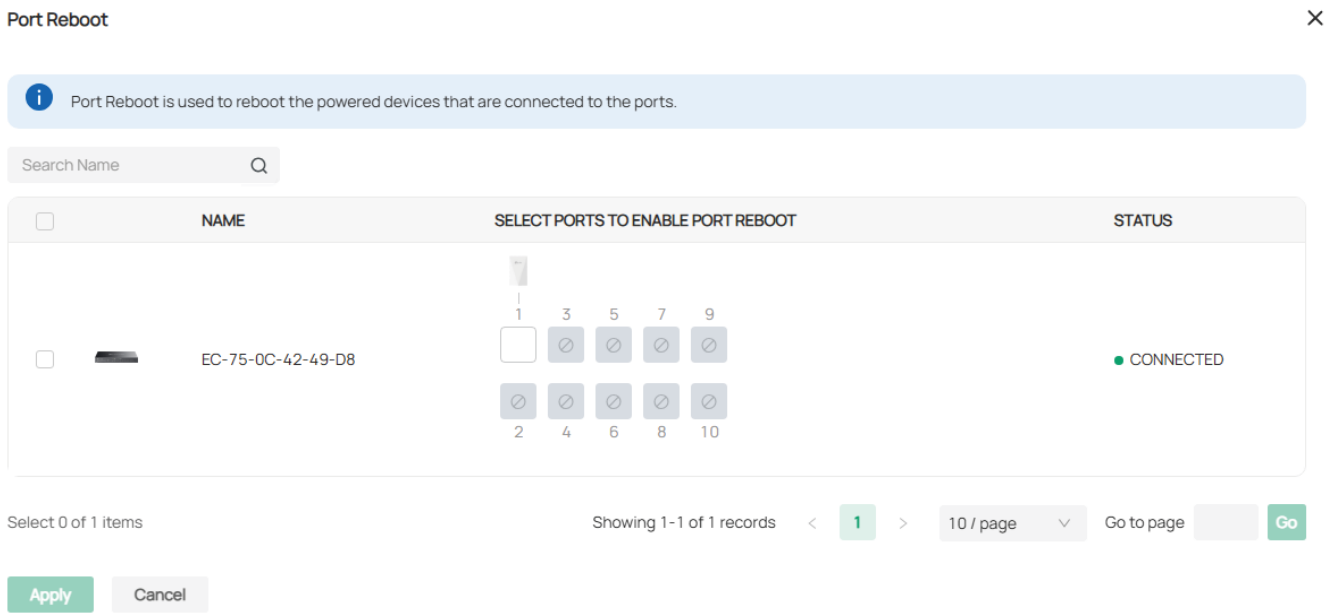
■ Extend Mode

In Extend Mode, you can quickly enable the Extend Mode for switch ports to extend network cable transmission.



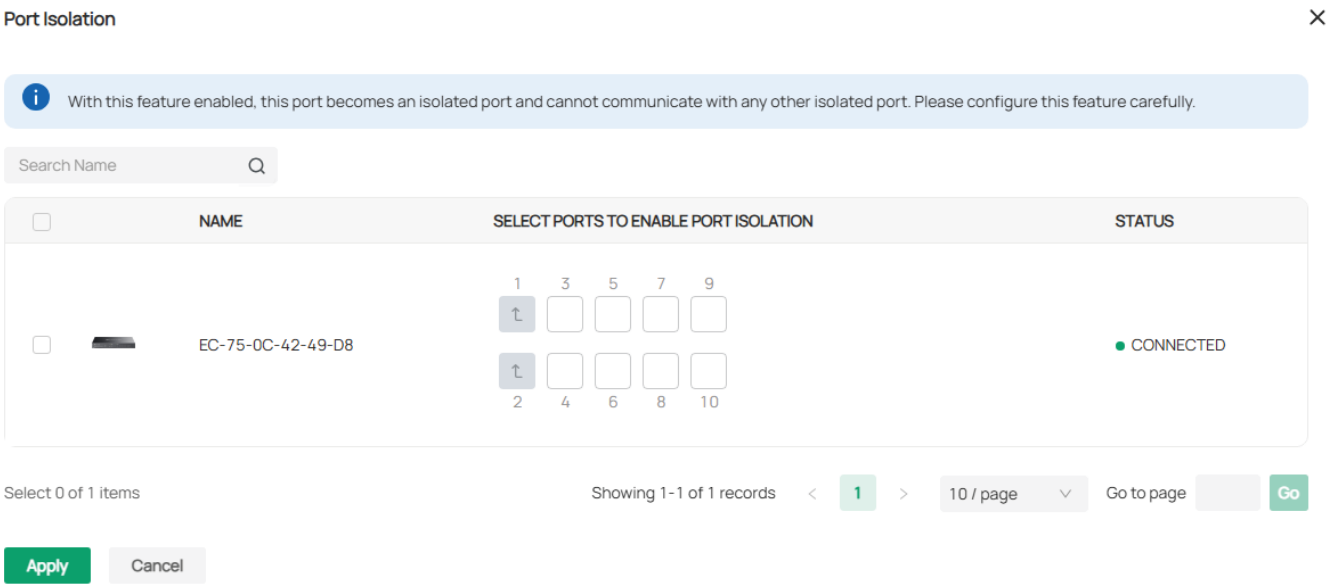
■ Port Reboot

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.



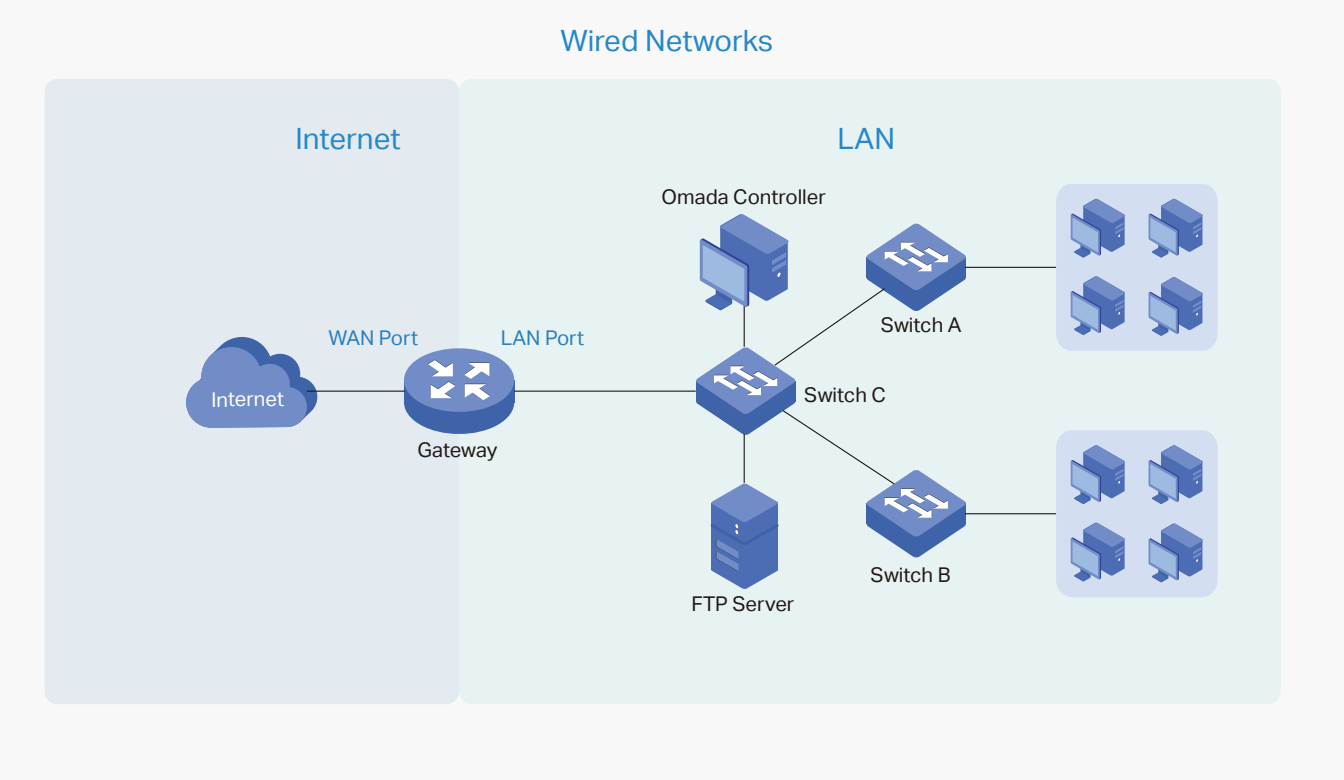
■ Other

Other Quick Config functions, including 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.

5. 2 Configure Wired Networks

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

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



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

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

5. 2. 1 Set Up an Internet Connection

Configuration

To set up an internet connection, follow these steps:

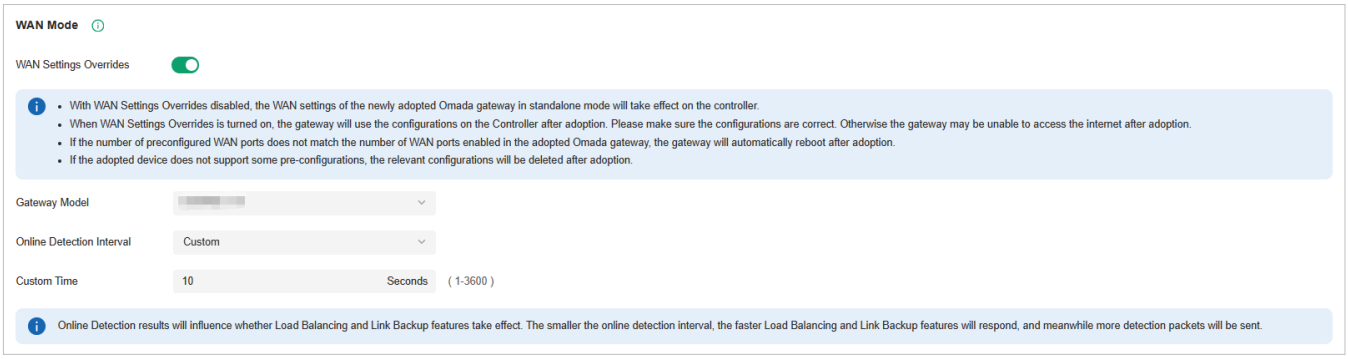
2) Configure the number of WAN ports on the gateway based on needs.

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

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

Step 1: Select WAN Mode

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet to load the following page. In the WAN Mode section, configure the number of WAN ports deployed by the gateway and other parameters. Then click Apply.



WAN Settings Overrides	With this option disabled, the WAN settings of the newly adopted Omada gateway in standalone mode will take effect on the controller. When this option is turned on, the gateway will use the configurations on the Controller after adoption. Please make sure the configurations are correct. Otherwise the gateway may be unable to access the internet after adoption. If the adopted device does not support some pre-configurations, the relevant configurations will be deleted after adoption.
Gateway Model	Specify the gateway model and version. If you change the gateway, follow the web instructions to select WAN ports and copy WAN port settings. If the number of preconfigured WAN ports does not match the number of WAN ports enabled in the adopted Omada gateway, the gateway will automatically reboot after adoption.

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.

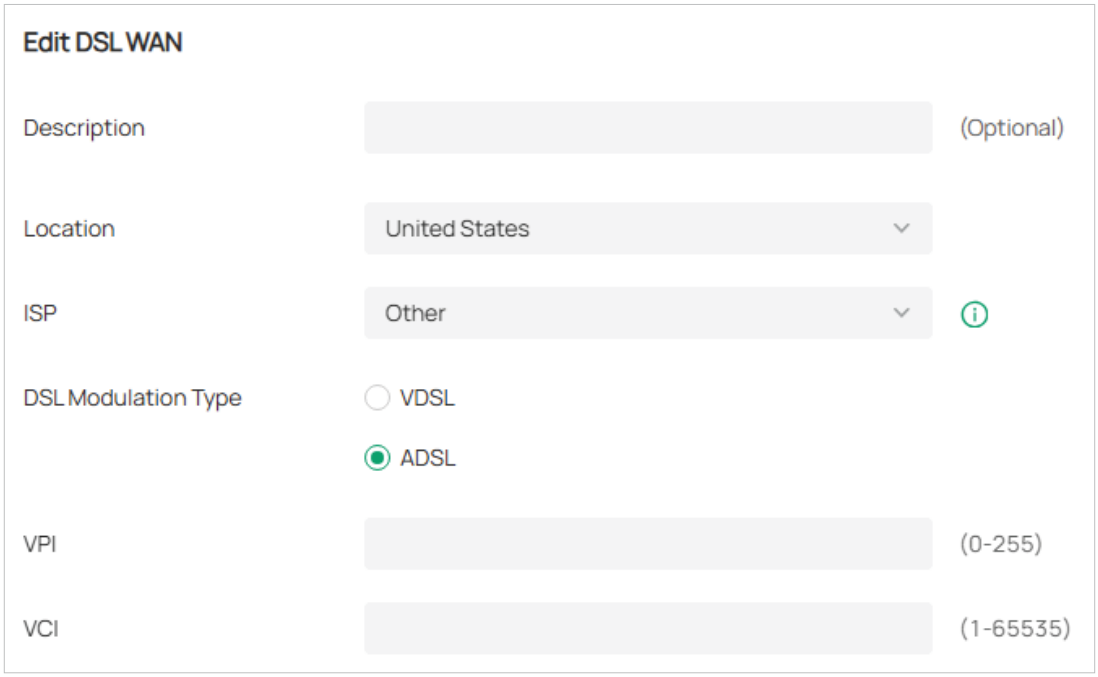
Step 2: Configure WAN Connections

Note:

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

- Set Up DSL WAN Connection

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In the WAN Ports Config section, click the edit icon of DSL WAN and configure the parameters.

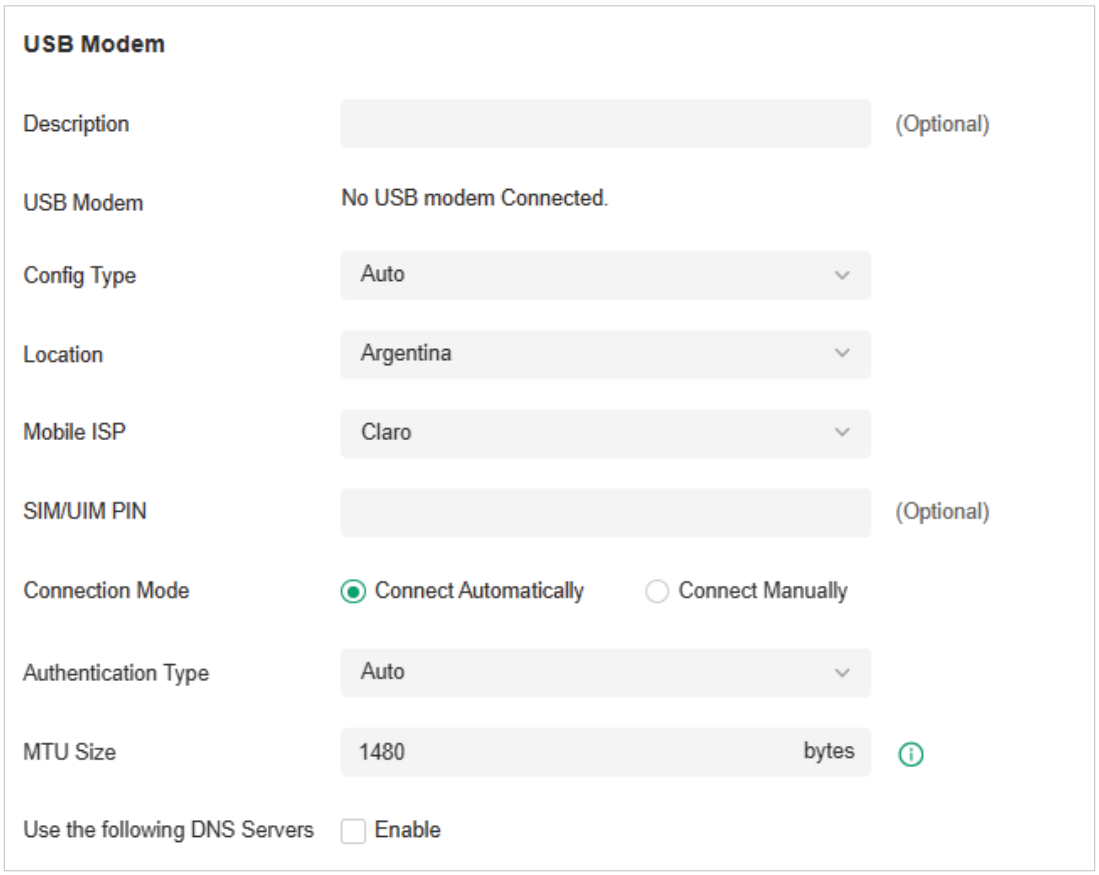


Description	Enter a description for identification.
Location	Select your location.
ISP	Select your ISP (internet service provider).

DSL Modulation Type	Select the modulation type for your DSL connection.
VPI	Enter the VPI assigned by your ISP to specify the virtual path between enpoints in an ATM network.
VCI	Enter the VCI assigned by your ISP to specify the virtual path between channels in an ATM network.

- Set Up USB Modem Connection

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In the WAN Ports Config section, click the edit icon of USB Modem and configure the parameters.



Description	Enter a description for identification.
USB Modem	Display whether a USB modem is connected to the device and the name of the connected USB modem.

Config Type	Select a configuration type for the USB modem. Auto: Use the Location and Mobile ISP information below for configuration. Manually: Enter the Dial Number, APN, Username, and password provided by your Mobile ISP.
Location	Select your location.
Mobile ISP	Select your mobile ISP.
Message	Display the current status of the SIM card.
SIM/UIM PIN	(Optional) Enter the PIN of your SIM card. The field is required when the following information appears in the Message: PIN protection is enabled and the PIN is invalid.
Connection Mode	Select the connection mode. Connect Automatically: The router will use the USB modem to connect to the internet automatically. Connect Manually: You need to turn on/off the internet manually for the gateway on the device page.
Authentication Mode	Select the Authentication mode for the USB modem. The default value is Auto, and it is recommended to keep the default value.
MTU Size	Specify the MTU (Maximum Transmission Unit) of the USB WAN port. The default value is 1480, and it is recommended to keep the default value. MTU is the maximum data unit transmitted in the physical network.
Use the following DNS Servers	Enable the feature if you want to specify the Primary and Secondary DNS servers manually.

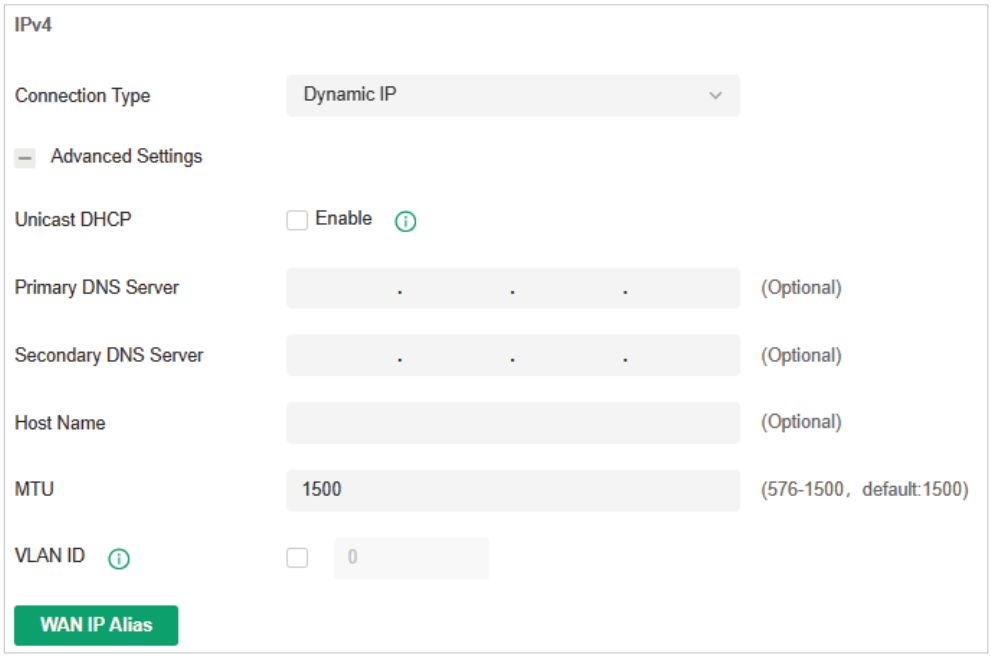
- Set Up IPv4 Connection

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In the WAN Ports 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.

■ Dynamic IP

Choose Connection Type as Dynamic IP and configure the parameters.

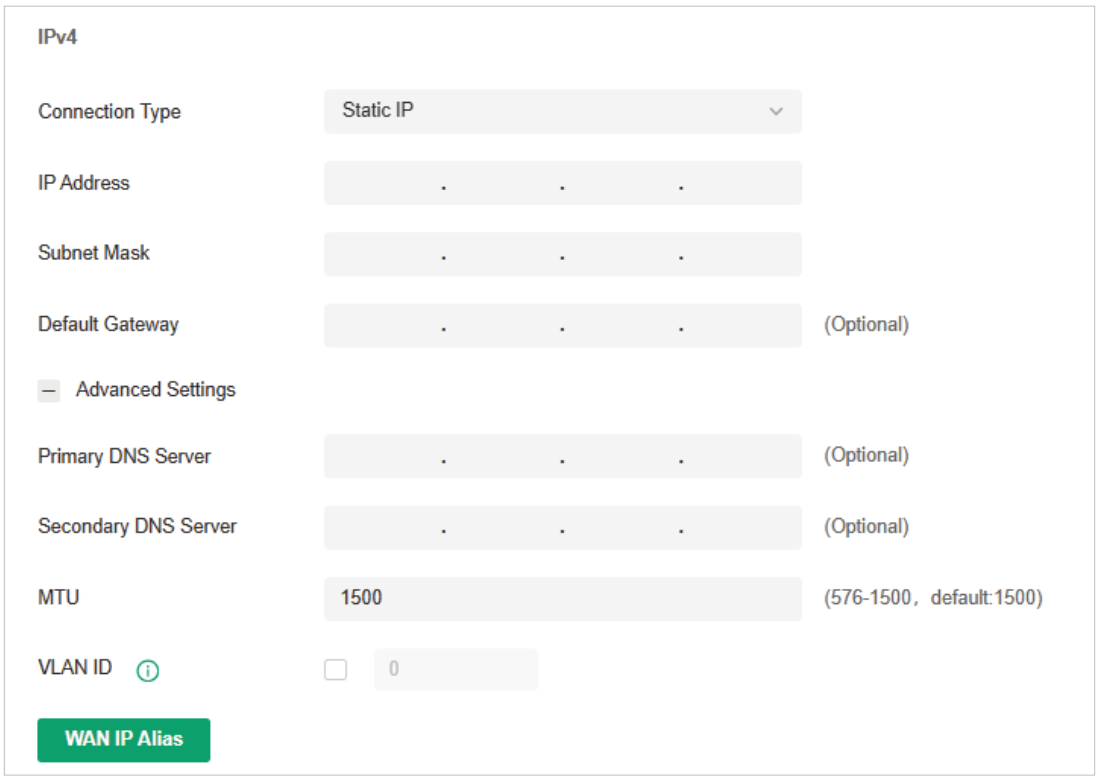


Unicast DHCP	With this option enabled, the gateway will require the DHCP server to assign the IP address by sending unicast DHCP packets. Usually you need not to enable the option.

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.

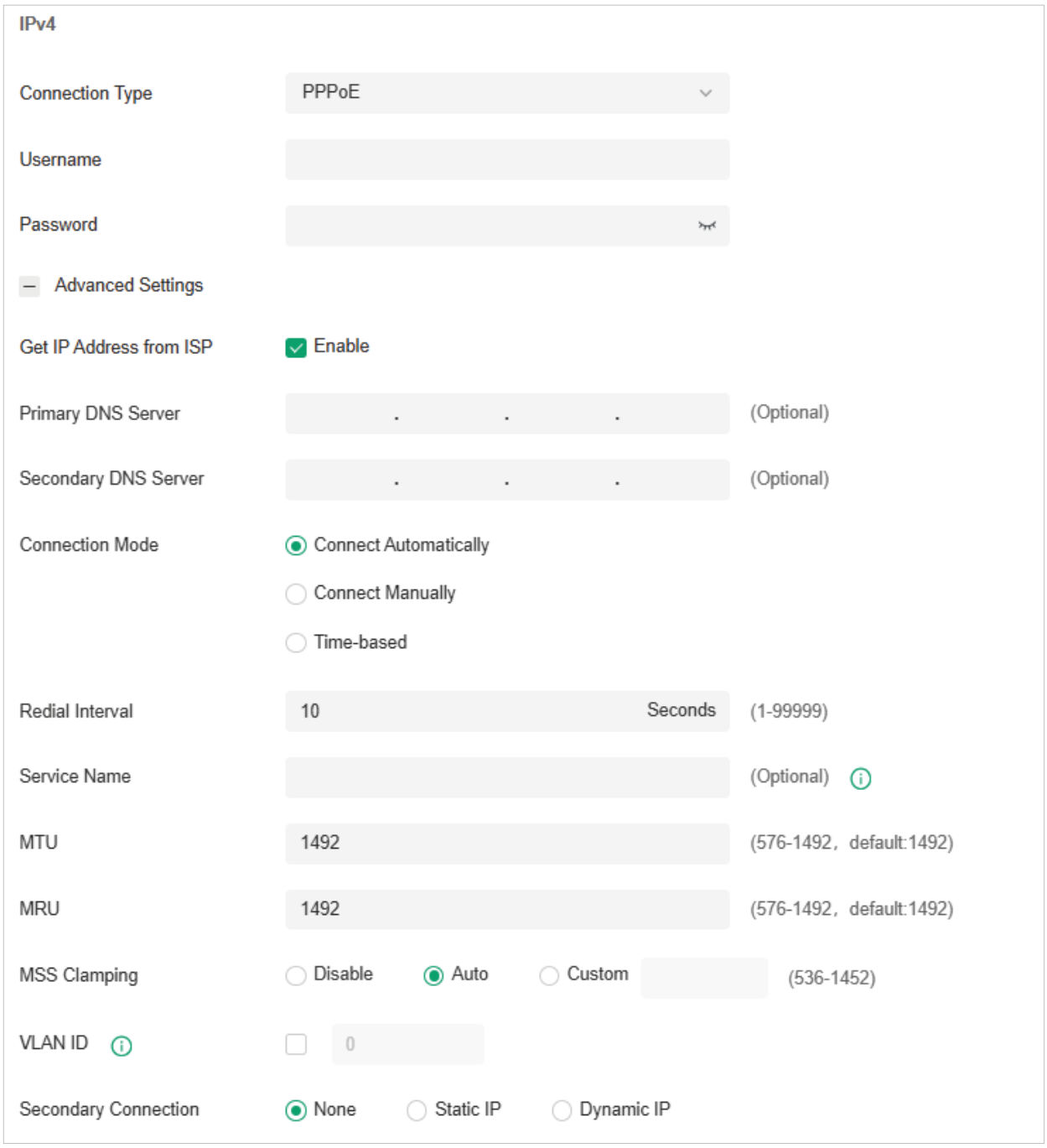


IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Default Gateway	Enter the default gateway provided by your ISP.
Primary DNS Server / Secondary DNS Server	Enter the IP address of the DNS server provided by your ISP if there is any.
MTU	Specify 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.



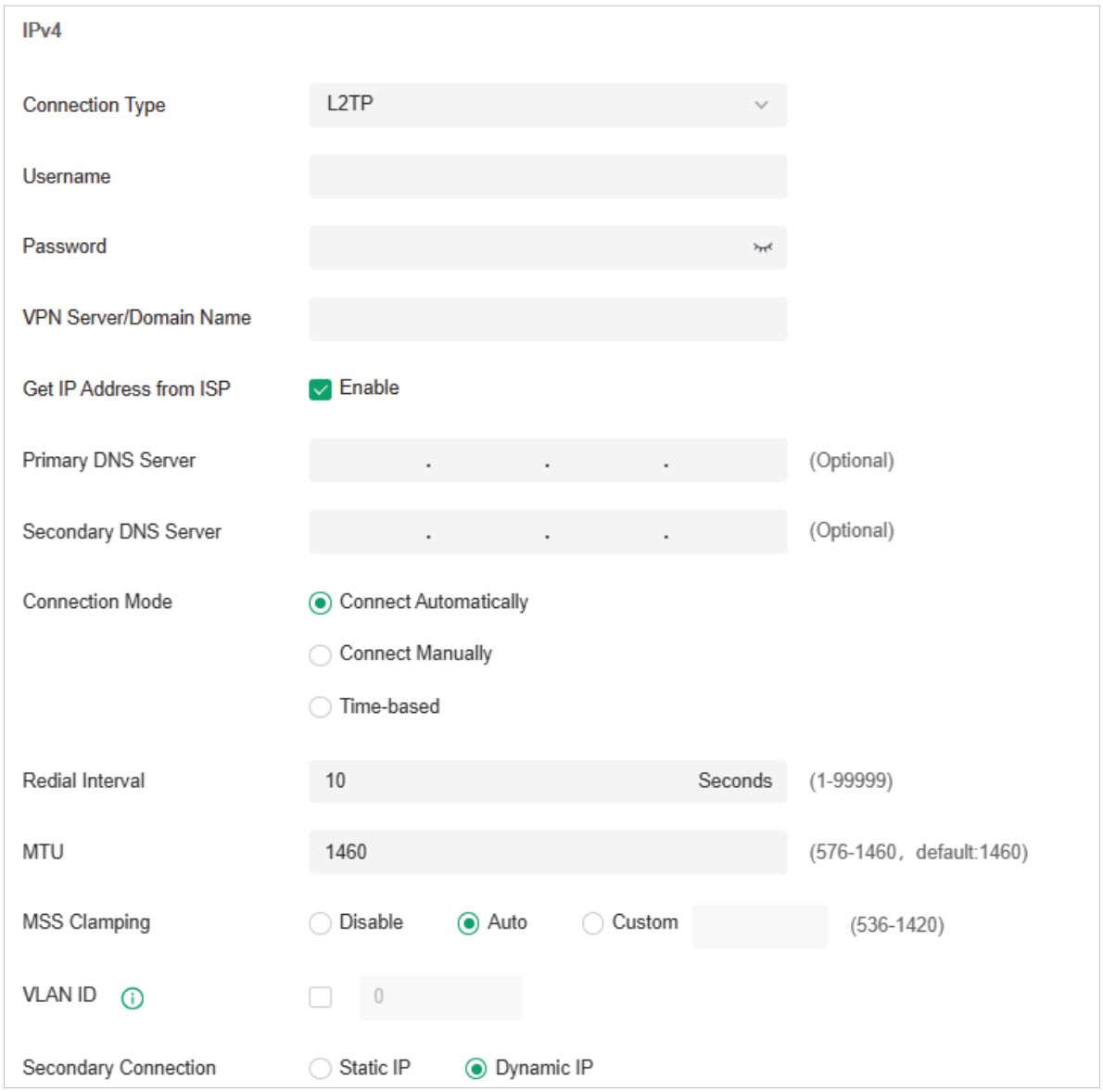
Username	Enter the PPPoE username provided by your ISP.
Password	Enter the PPPoE password provided by your ISP.

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.
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.



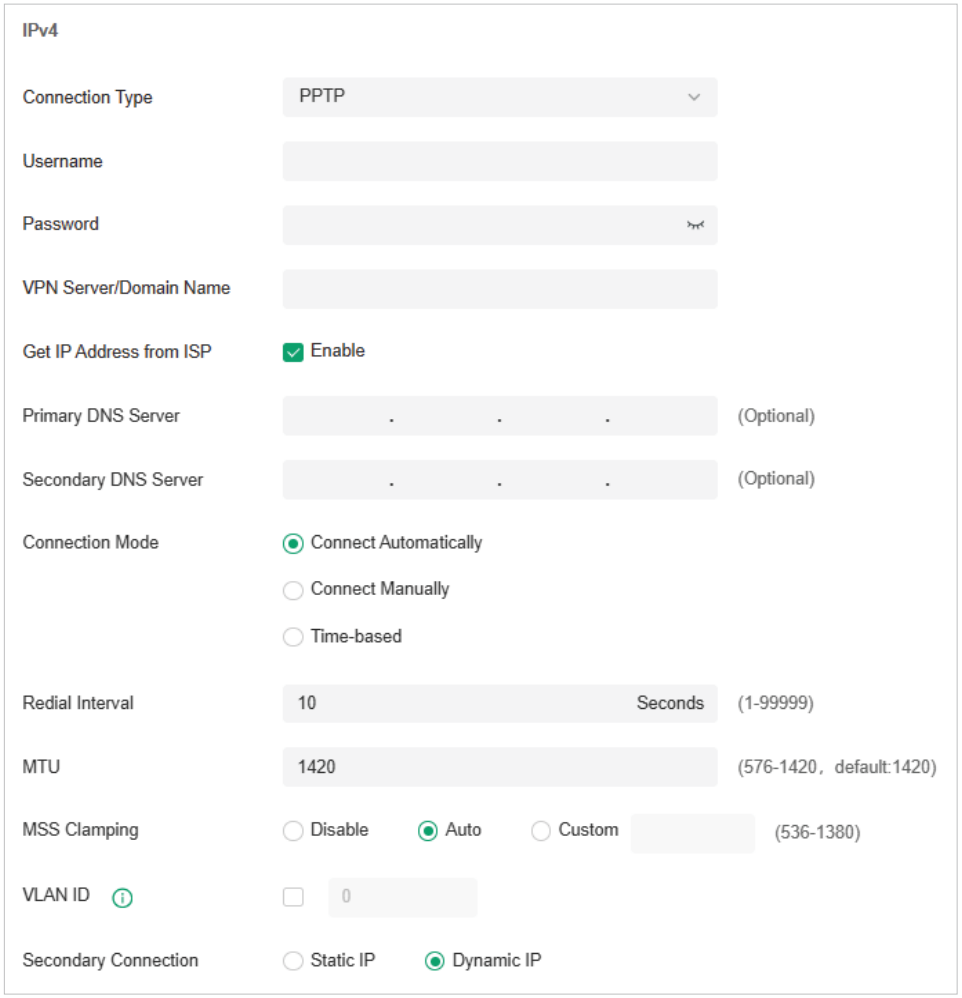
Username	Enter the L2TP username provided by your ISP.
Password	Enter the L2TP password provided by your ISP.
VPN Server / Domain Name	Enter the VPN Server/Domain Name provided by your ISP.
Get IP address from ISP	With this option enabled, the gateway gets IP address from ISP when setting up the WAN 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.
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.
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.

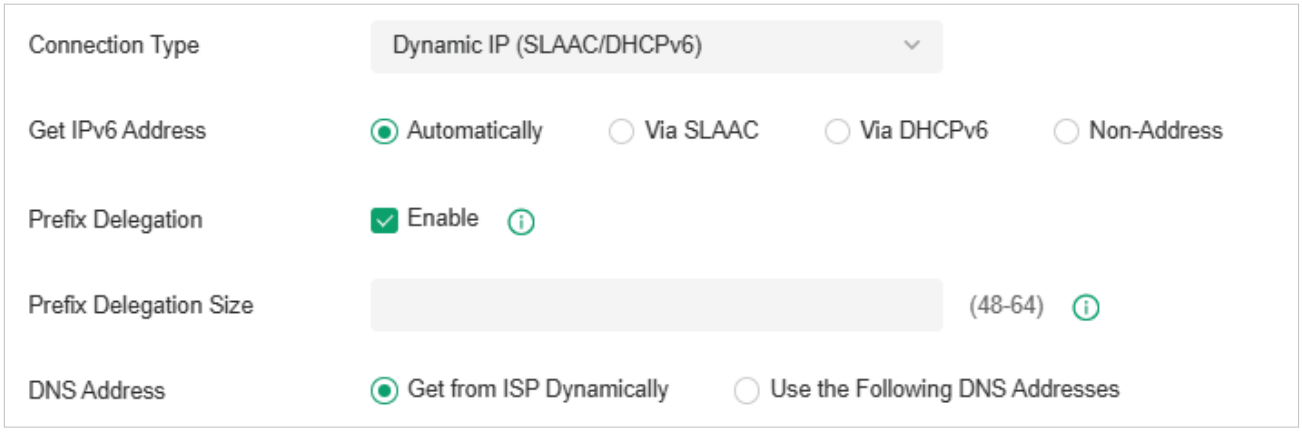
- Set Up IPv6 Connection

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

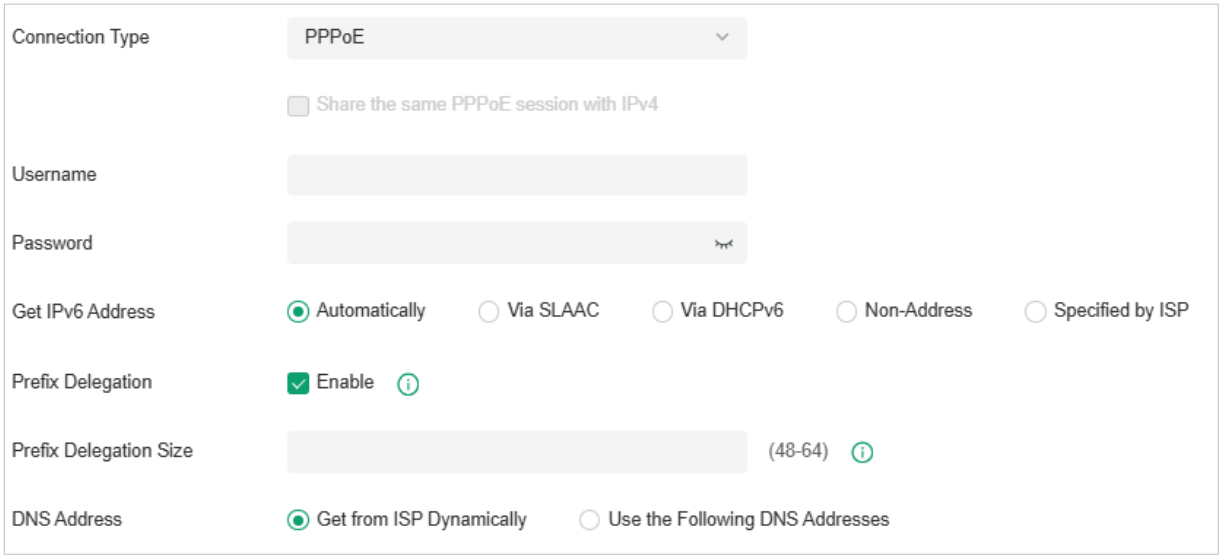
Choose Connection Type as Static IP and configure the parameters.



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.

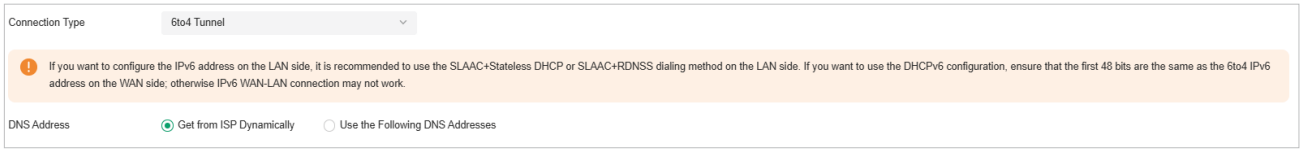


Share the same PPPoE session with IPv4	If your ISP provides only one PPPoE account for both IPv4 and IPv6 connections, and you have already established an IPv4 connection on this WAN port, you can check the box, then the WAN port will use the PPP session of IPv4 PPPoE connection to get the IPv6 address. 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

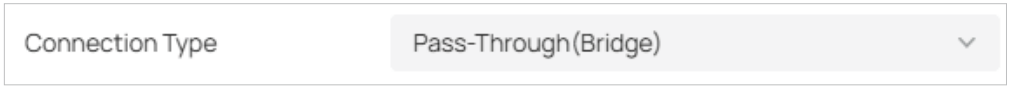
  Choose Connection Type as 6to4 Tunnel and configure the parameters.



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

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. In the WAN Ports Config section, click the edit icon of a WAN port and configure the MAC address according to actual needs.

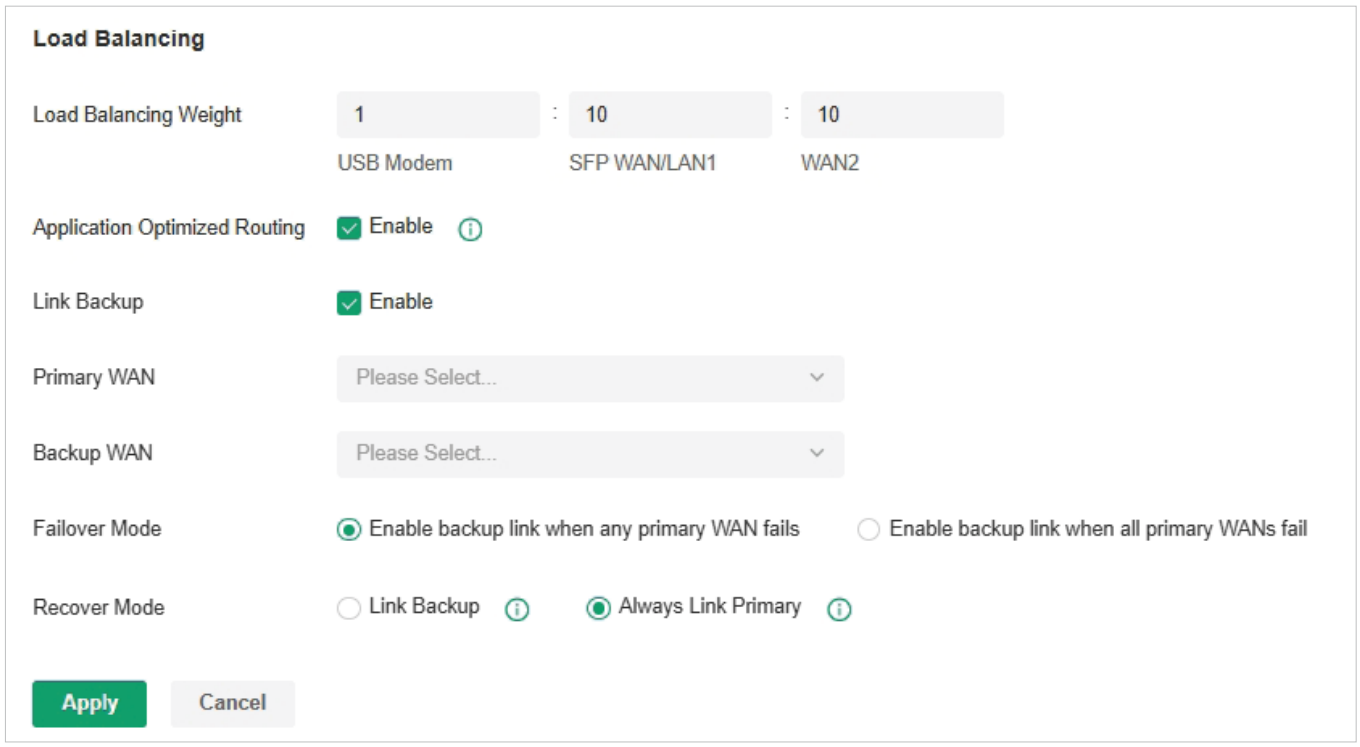
MAC Address	Use Default MAC Address: The WAN port uses the default MAC address to set up the internet connection. It's recommended to use the default MAC address unless required otherwise. Customize MAC Address: The WAN port uses a customized MAC address to set up the internet connection and you need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

Step 3: (Optional) Configure Load Balancing

Note:

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

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > Internet. 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 router will consider the source IP address and destination IP address (or destination port) of the packets as a whole and record the WAN port they pass through. Then the packets with the same source IP address and destination IP address (or destination port) will be forwarded to the recorded WAN port. This feature ensures that multi-connected applications work properly.
Link Backup	With Link Backup enabled, the router will switch all the new sessions from dropped lines automatically to another to keep an always on-line network.
Backup WAN / Primary WAN	The backup WAN port backs up the traffic for the primary WAN ports under the specified condition.
Failover Mode	Select whether to enable backup link when any primary WAN fails or all primary WANs fail.

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.

5. 2. 2 Configure LAN Networks

Overview

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

Configuration

To create a LAN, follow the guidelines:

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

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

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

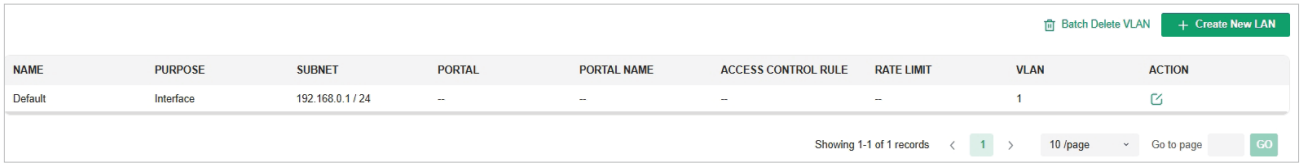
Step 1: Create a Network

Note:

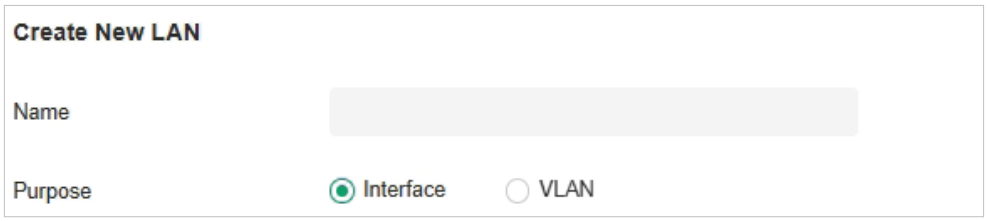
A default Network (default VLAN) named LAN is preconfigured as Interface and is associated with all LAN ports of the Gateway and all switch ports. The VLAN ID of the default Network is 1. The default Network can be edited, but not deleted.

1. Launch the controller and access a site. Go to Settings > Wired&Wireless Networks >

LAN to load the following page.



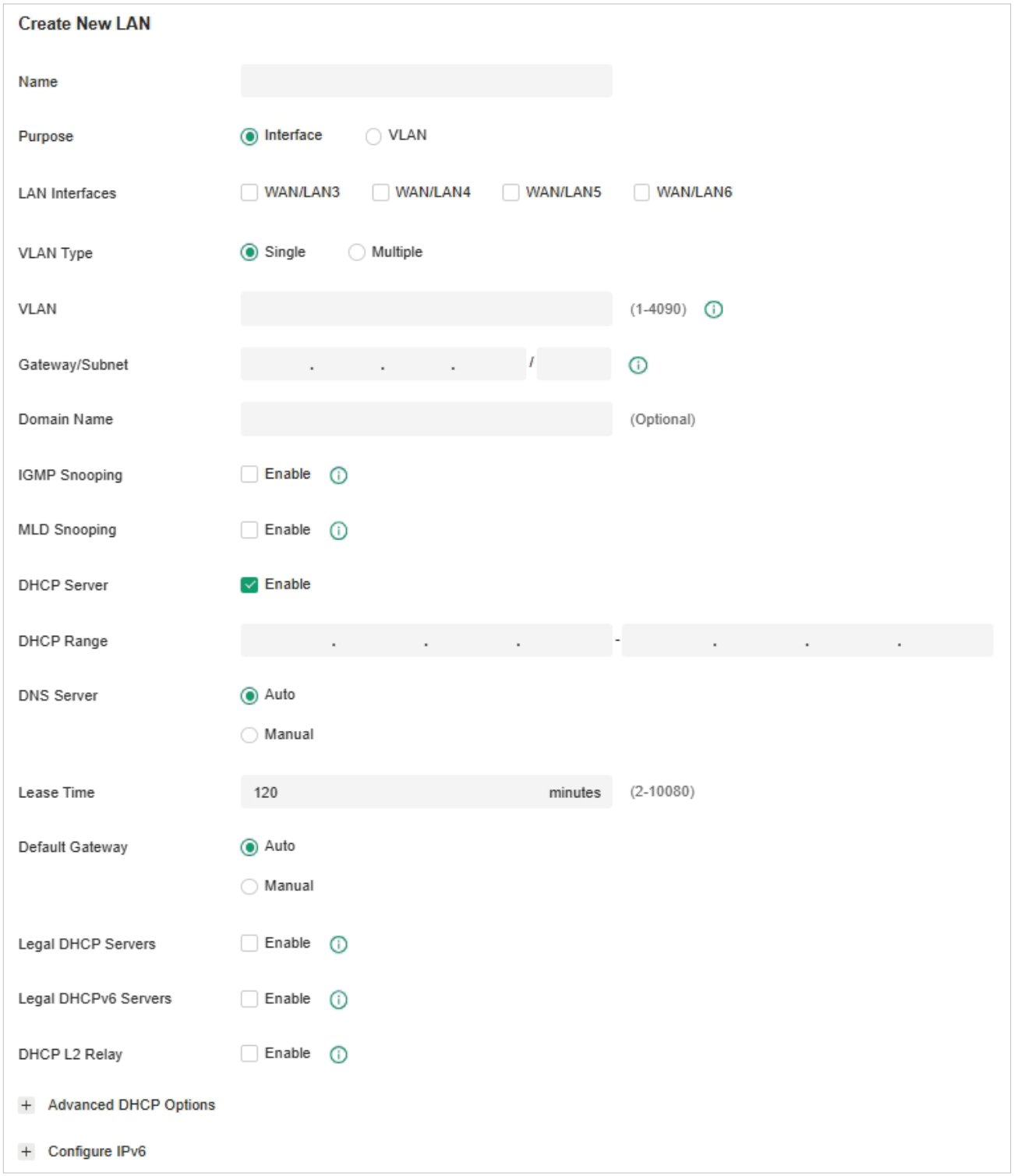
2. Click Create New LAN to load the following page, enter a name to identify the network, and select the purpose for the network.



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

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

■ Interface

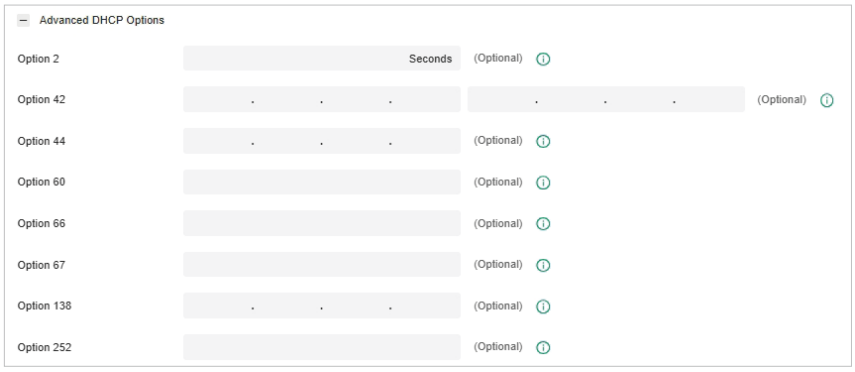


LAN Interface	Select the physical interfaces of the Gateway that this network will be associated with.

VLAN	Enter a VLAN ID with the values between 1 and 4090. Each VLAN can be uniquely identified by VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.
Gateway/Subnet	Enter the IP address and subnet mask in the CIDR format. The CIDR Notation here includes the IP address and subnet mask of the default gateway. The summary of the information that you entered will show up below in real time.
Domain Name	Enter the domain name.
IGMP Snooping	Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.
MLD Snooping	Click the checkbox to monitor MLD (Multicast Listener Discovery) traffic and thereby manage IPv6 multicast traffic.
DHCP Server	Click the checkbox to allow the Gateway to serve as the DHCP server for this network. A DHCP server assigns IP addresses, DNS server, default gateway, and other parameters to all devices in the network. Deselect the box if there is already a DHCP server in the network.
DHCP Range	Enter the starting and ending IP addresses of the DHCP address pool in the fields provided. For quick operation, click the Update DHCP Range beside the Gateway/Subnet entry to get the IP address range populated automatically, and edit the range according to your needs.
DNS Server	Select a method to configure the DNS server for the network. Auto: The DHCP server automatically assigns DNS server for devices in the network. It uses the IP address specified in the Gateway/Subnet entry as the DNS server address. Manual: Specify DNS servers manually. Enter the IP address of a server in each DNS server field.
Lease TIme	Specify how long a client can use the IP address assigned from this address pool.
Default Gateway	Enter the IP address of the default gateway. Auto: The DHCP server automatically assigns default gateway for devices in the network. It uses the IP address specified in the Gateway/Subnet entry as the default gateway address. Manual: Specify default gateway manually. Enter the IP address of the default gateway in the field.

Legal DHCP Servers	Click the checkbox to specify legal DHCP servers for the network. With legal DHCP servers configured, Gateways and Switches ensure that clients get IP addresses only from the DHCP servers specified here.
Legal DHCPv6 Servers	Click the checkbox to specify legal DHCPv6 servers for the network. With legal DHCPv6 servers configured, Gateways and Switches ensure that clients get IPv6 addresses only from the DHCPv6 servers specified here.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.

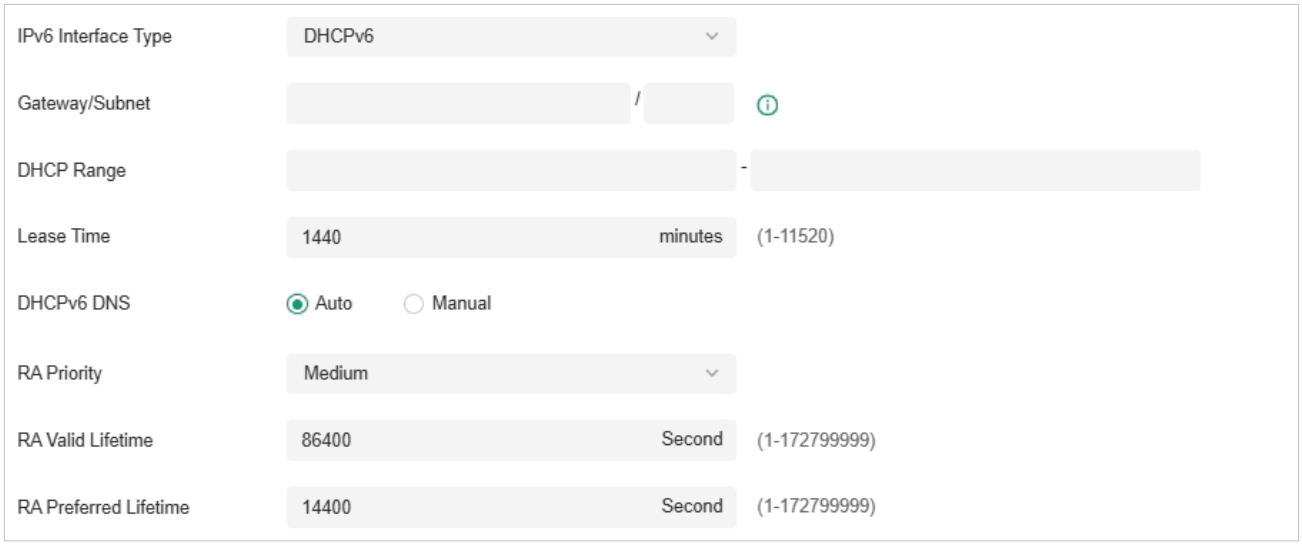
You can expand and configure Advanced DHCP Options if needed.



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.



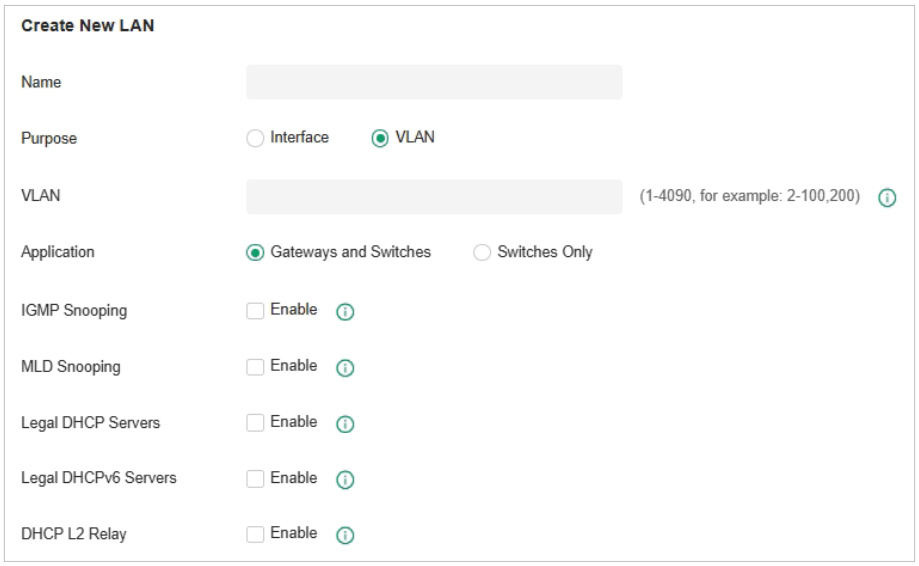
IPv6 Interface Type	Configure the type of assigning IPv6 address to the clients in the local network. None: IPv6 connection is not enabled for the clients in the local network. DHCPv6: The gateway assigns an IPv6 address and other parameters including the DNS server address to each client using DHCPv6. 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 the Update DHCP Range beside the Gateway/Subnet entry to get the IP address range populated automatically, and edit the range according to your needs.
Lease Time	This entry determines how long the assigned IPv6 address remains valid. Either keep the default 1440 minutes or change it if required by your ISP.
DHCPv6 DNS	Select a method to configure the DNS server for the network. With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. With Manual selected, enter the IP address of a server in each DNS server field.
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.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be added to the prefix to obtain a /64 subnet. The range of IPv6 Prefix ID is determined by the larger value of Prefix Delegation Size and Prefix Delegation Length (obtained from the ISP). Note that if the Prefix Delegation Length is larger than 64, the IPv6 Prefix ID cannot be obtained from Prefix Delegation, please select another method. In site view, go to Settings > Wired Network > Internet to configure Prefix Delegation Size.
DNS Server	Select a method to configure the DNS server for the network. Auto: With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. Manual: With Manual selected, enter the IP address of a server in each DNS server field.
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.

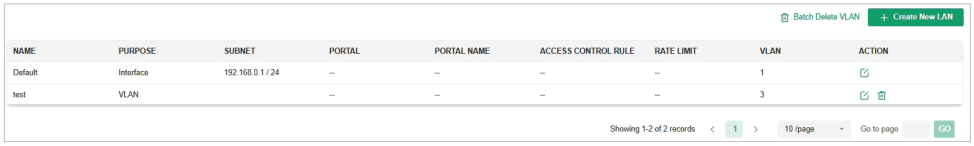
With SLAAC+RDNSS selected, configure the following parameters.

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.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be added to the prefix to obtain a /64 subnet.
DNS Server	Select a method to configure the DNS server for the network. Auto: With Auto selected, the DHCP server automatically assigns DNS server for devices in the network. Manual: With Manual selected, enter the IP address of a server in each DNS server field.
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.



VLAN	Enter a VLAN ID with the values between 1 and 4090. Each VLAN can be uniquely identified by VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.
Application	Choose the device type that this entry applies to.
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	Click the checkbox to specify legal DHCP servers for the network. With legal DHCP servers configured, Gateways and Switches ensure that clients get IP addresses only from the DHCP servers specified here.
Legal DHCPv6 Servers	Click the checkbox to specify legal DHCPv6 servers for the network. With legal DHCPv6 servers configured, Gateways and Switches ensure that clients get IPv6 addresses only from the DHCPv6 servers specified here.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.

4. Click Save. The new LAN will be added to the LAN list. In the ACTION column, you can click to edit the LAN and click the Delete icon to delete the LAN. You can click Batch Delete VLANs to delete VLANs.



Step 2: Create a Port Profile

Note:

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

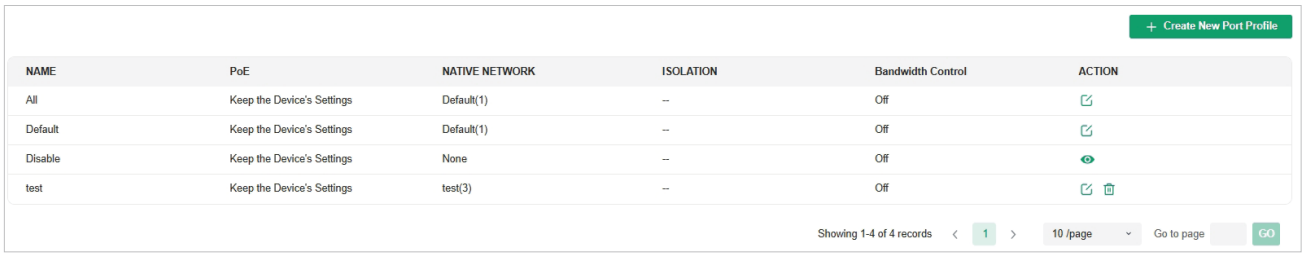
All: In the All profile, all networks except the default network (LAN) are configured as Tagged Network, and the native network is the default network (LAN). This profile is assigned to all switch ports by default.

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

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

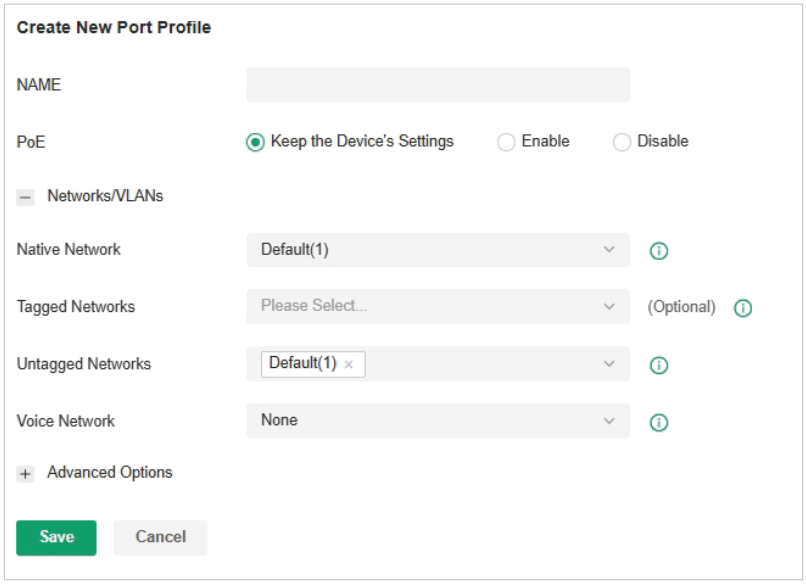
When a network is created, the system will automatically create a profile with the same name and configure the network as the native network for the profile. In this profile, the network itself is configured as the Untagged Networks, while no networks are configured as Tagged Networks. The profile can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

1. Go to Settings > Wired&Wireless Networks > LAN > Switch Profile to load the following page.



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

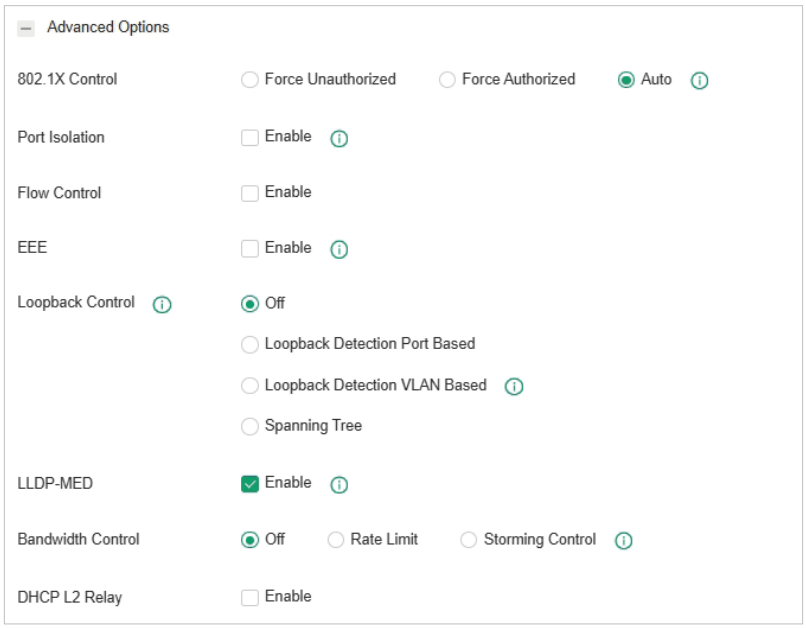
parameters.



Name	Enter a name to identify the port profile.
PoE	Select the PoE mode for the ports. Keep the Device's Settings: PoE keep enabled or disabled according to the switches' settings. By default, the switches enable PoE on all PoE ports. Enable: Enable PoE on PoE ports. Disable: Disable PoE on PoE ports.
Native Network	Select the native network from all networks. The native network determines the Port VLAN Identifier (PVID) for switch ports. When a port receives an untagged frame, the switch inserts a VLAN tag to the frame based on the PVID, and forwards the frame in the native network. Each physical switch port can have multiple networks attached, but only one of them can be native.
Tagged Networks	Select the Tagged Networks. Frames sent out of a Tagged Network are kept with VLAN tags. Usually networks that connect the switch to network devices like routers and other switches, or VoIP devices like IP phones should be configured as Tagged Networks.
Untagged Networks	Select the Untagged Networks. Frames that sent out of an Untagged Network are stripped of VLAN tags. Usually networks that connect the switch to endpoint devices like computers should be configured as Untagged Networks. Note that the native network is untagged.

Voice Network	Select the network that connects VoIP devices like IP phones as the Voice Network. Switches will prioritize the voice traffic by changing its 802.1p priority. To configure a network as Voice Network, configure it as Tagged Network first, and then enable LLDP-MED. Only tagged networks can be configured as Voice Network, and Voice Network will take effect with LLDP-MED enabled.

3. Expand and configure Advanced Options if needed.

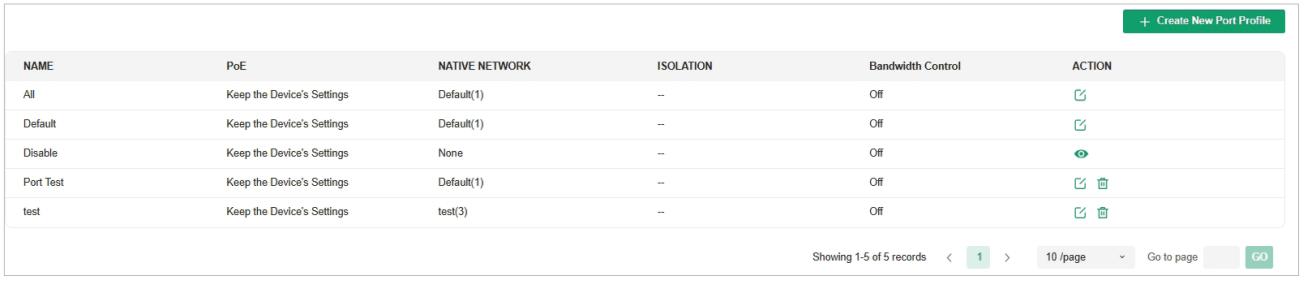


802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, enter the site view and go to **Settings** > **Authentication** > **802.1X**. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.

EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the 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. If you want to enable Spanning Tree for the switch, you also need to select the Spanning Tree protocol in the Device Config page. For details, refer to Configure and Monitor Switches.
LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP devices.
Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storm Control: Select Storm Control to allow the switch to monitor broadcast frames, multicast frames and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the frames exceeds the set rate, the frames will be automatically discarded to avoid network broadcast storm.
Ingress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.

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

4. Click Save. The new port profile is added to the profile list. You can click Edit button in the ACTION icon to edit the port profile. You can click the Delete icon in the ACTION column to delete the port profile.

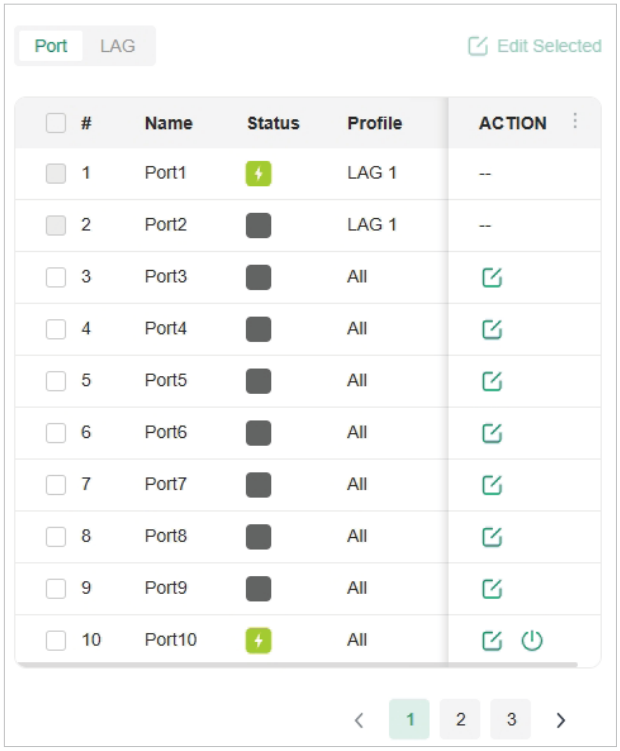


Step 3: Assign the Port Profile to the Ports

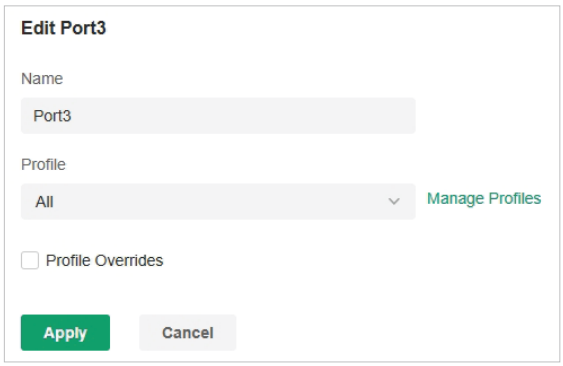
Note:

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

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

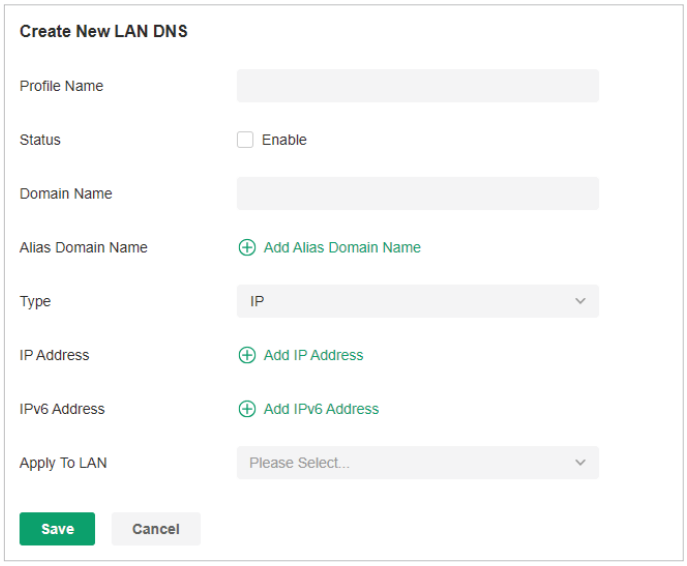


2. Select the profile from the drop-down list to assign the port profile to the desired ports of the switch. You can enable profile overrides to customize the settings for the ports, and all the configuration here overrides the port profile. For details, refer to Manage, Configure, and Monitor Devices.



5. 2. 3 Configure LAN DNS

1. Launch the controller and access a site.
2. Go to Settings > Wired&Wireless Networks > LAN > LAN DNS.
3. 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.
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.

5. 3 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.

5. 3. 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:

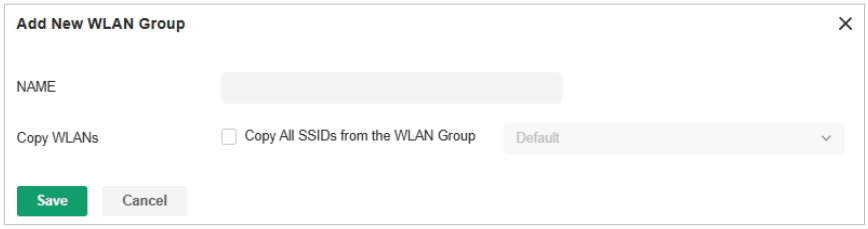
The controller provides a default WLAN group. If you simply want to configure wireless networks for the default WLAN group and apply it to all your APs, skip this step.

1. Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > WLAN to load the following page.

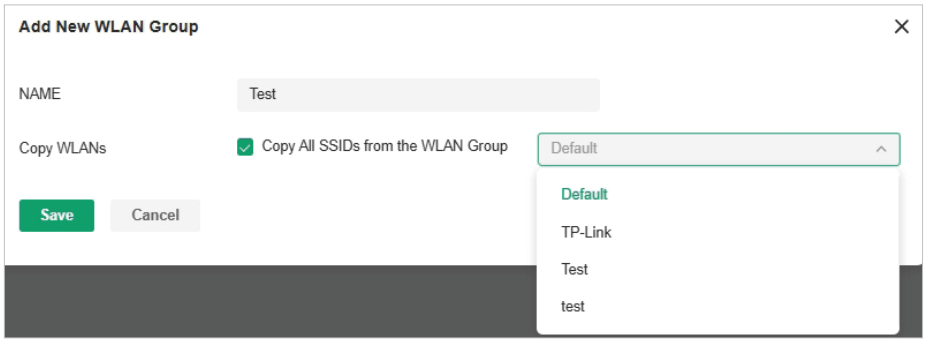


2. Select Create New Group from the drop-down list of WLAN Group to load the following

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 Networks

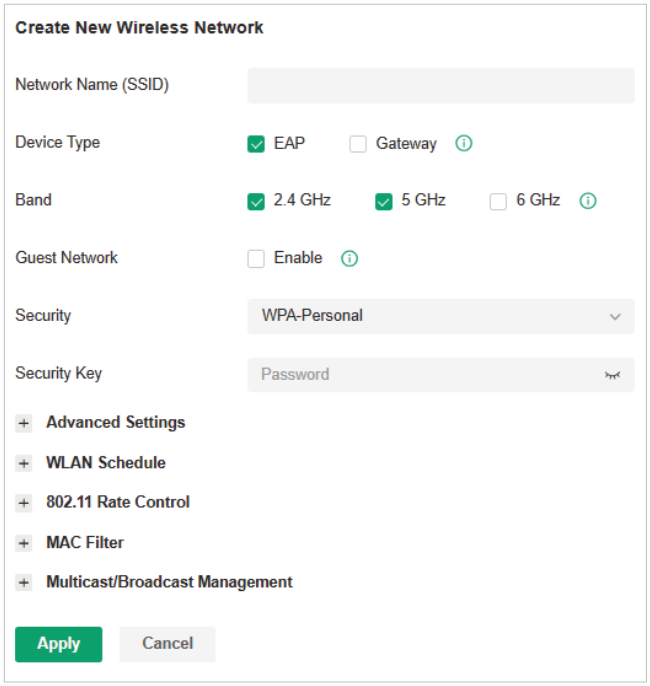
1. Select the WLAN group for which you want to configure wireless networks from the drop-down list of WLAN Group.



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.

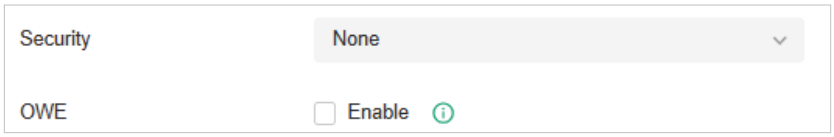


Network Name (SSID)	Enter the network name (SSID) to identify the wireless network. The users of wireless clients choose to connect to the wireless network according to the SSID, which appears on the WLAN settings page of wireless clients.
Device Type	Select the type of devices that the wireless network can apply to.
Band	Enable the radio band(s) for the wireless network.
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

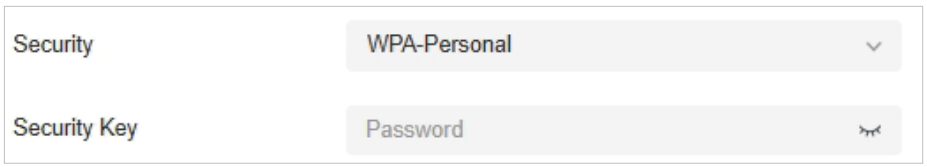
  With None selected, the hosts can access the wireless network without authentication, which is applicable to lower security requirements.



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 VAPs 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.

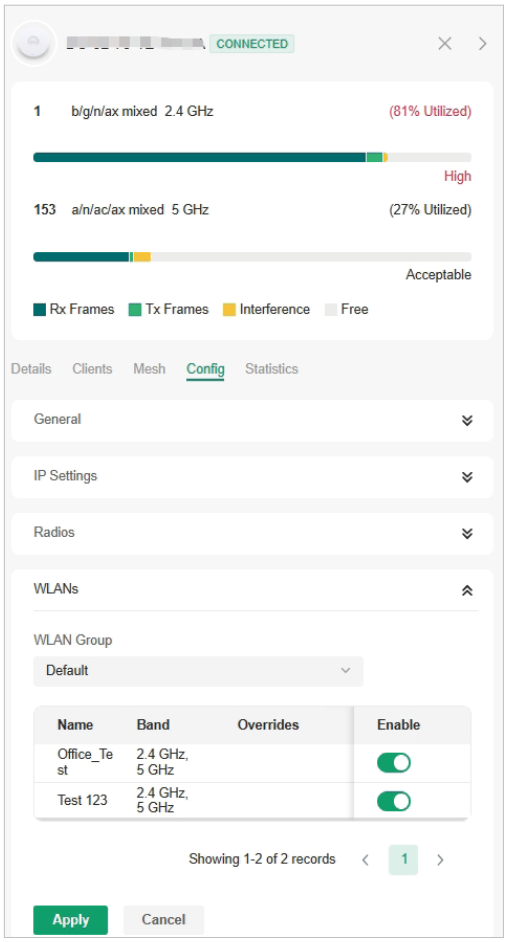
Step 3: Apply the WLAN Group

Note:

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

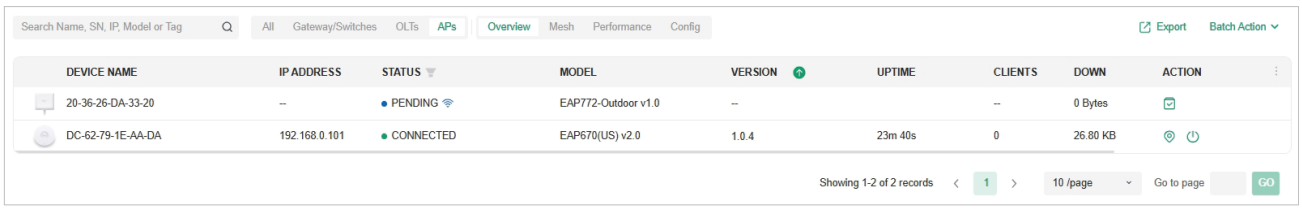
- Apply to a Single AP

  Go to Devices, select the AP. In the Properties window, go to Config > WLANs, select the WLAN group to apply.



- Apply to APs in batch

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



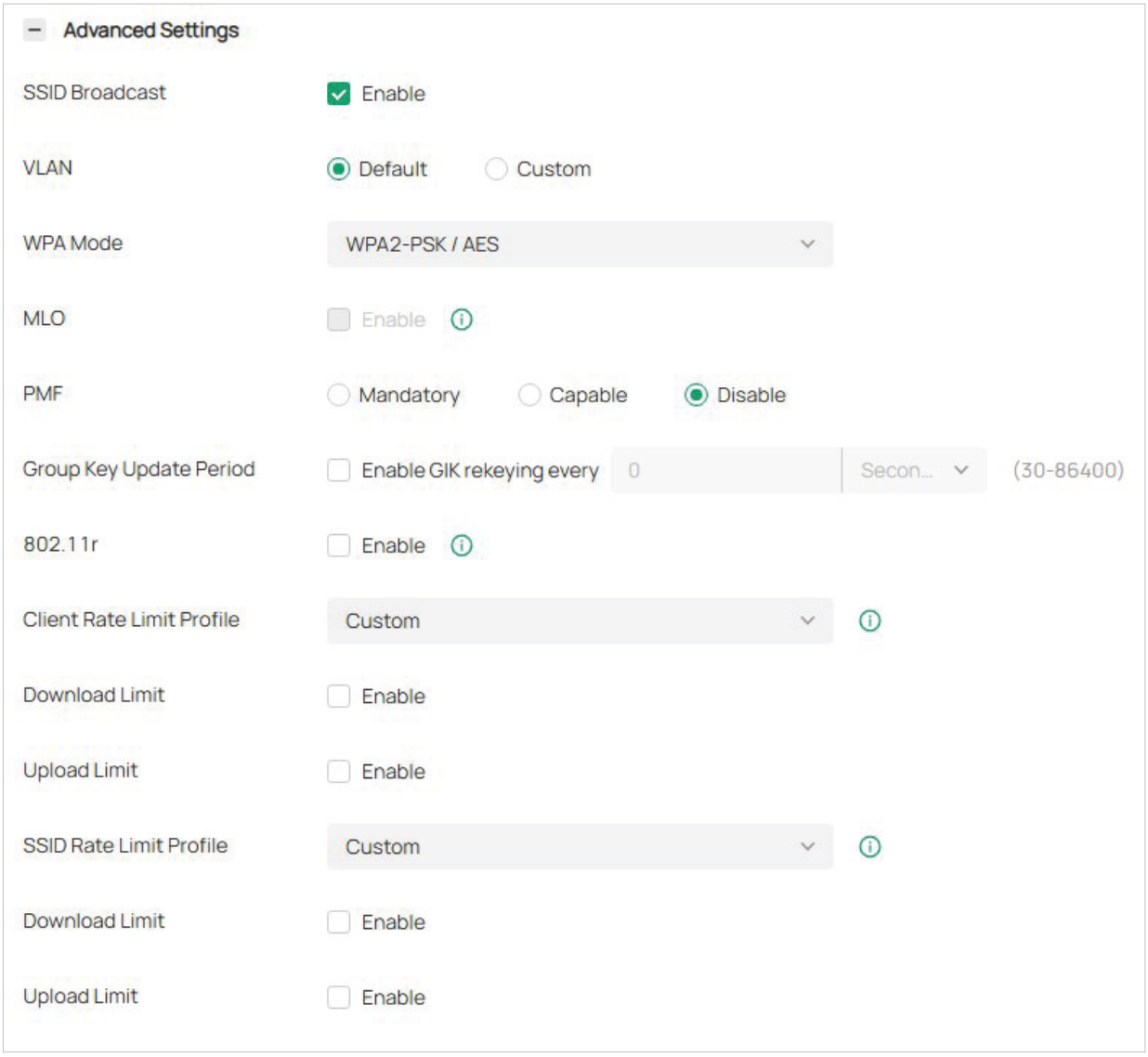
2. In the Properties window, go to Config > WLANs, select the WLAN group which you want

to apply to the AP.



5. 3. 2 Advanced Settings

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > 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.



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.
VLAN	Configure the uplink port VLAN corresponding to the SSID. Default: Using untagged transmission. Custom: Modifying the VLAN ID by binding a network or manually entering a VLAN ID. Traffic in different wireless networks will be marked with different VLAN tags accordingly. Then the APs work together with the switches which also support 802.1Q VLAN, to distribute the traffic to different VLANs according to the VLAN tags. As a result, wireless clients in different VLANs cannot directly communicate with each other.

WPA Mode	If you select WPA-Personal or WPA-Enterprise as the security strategy, you can select the WPA Mode including the version of WPA, and the encryption type. Select the version of WPA according to your needs. Select the encryption type. Some encryption type is only available under certain circumstances. AES: AES stands for Advanced Encryption Standard. Auto: 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 rekeying and specify the time period.
802.11r	Enable this feature to allow faster roaming when both the AP and client have 802.11r capabilities. Currently 802.11r does not support WPA3 encryption.
Client Rate Limit Profile	Specify the profile to limit the download and upload rates of each client to balance bandwidth usage. You can use the default profile or custom a profile.

SSID Rate Limit Profile	Specify the profile to limit the download and upload rates of each wireless band. Bandwidth is shared among all clients connected to the same wireless band of the same AP. You can use the default profile or custom a profile. **Note:** This feature requires new firmware updates for Omada APs, and the rate limit settings will only take effect on those APs running firmware that supports the feature.

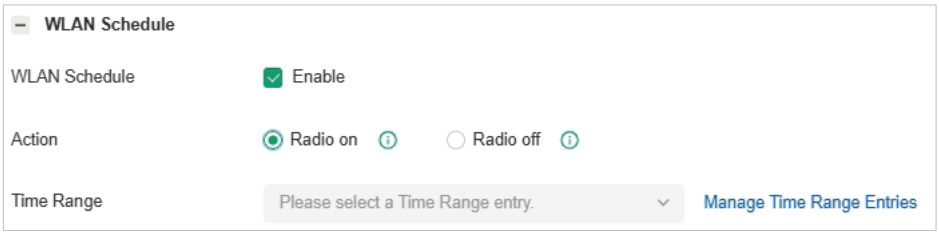
5. 3. 3 WLAN Schedule

Overview

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

Configuration

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > 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 Create Profiles.

5. 3. 4 802.11 Rate Control

Overview

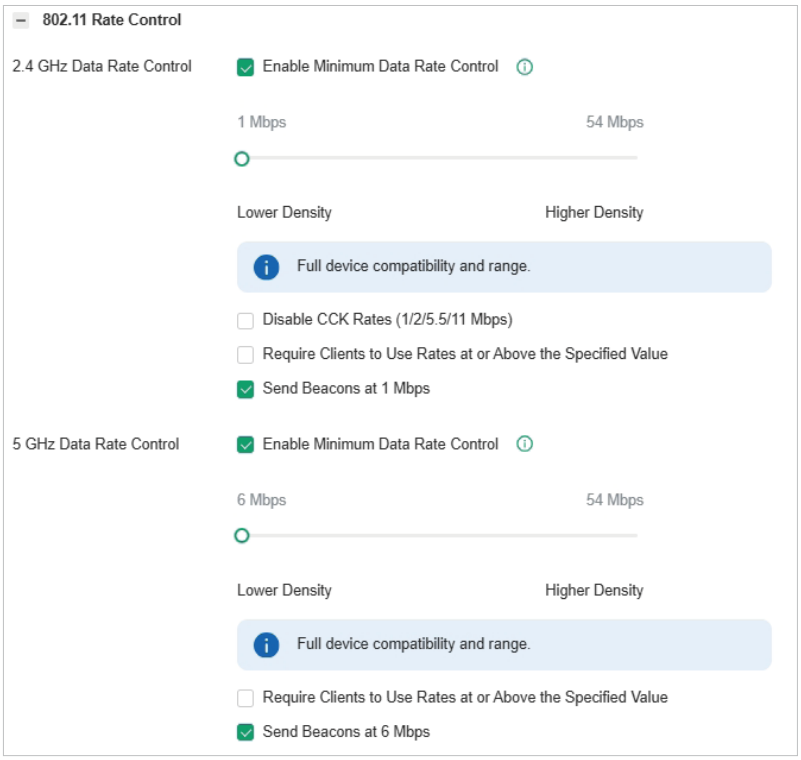
Note: 802.11 Rate Control is only available for certain devices.

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

Configuration

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > 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.



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.

5. 3. 5 Multicast/Broadcast Management

Overview

Multicast/Broadcast Management allows packet conversion and multicast filtering.

Configuration

Launch the controller and access a site. Go to Settings > Wired&Wireless Networks > 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 enabled, the controller will convert multicast packets into unicast packets when the channel utilization is below the specified threshold.
ARP-to-Unicast Conversion	When enabled, the controller will convert ARP packets into unicast packets.

IPv6-Multicast-to-Unicast Conversion	Enable this option if you have high requirements for IPv6 multicast streaming transmission, such as high-definition video on demand. When enabled, the AP maintains IPv6 multicast-to-unicast entries by listening to MLD report packets and MLD leave packets reported by clients. When the AP sends an IPv6 multicast packet to a client, it converts the packet into an IPv6 unicast packet according to the multicast-to-unicast entry, thereby improving the IPv6 transmission efficiency for better wireless experience.
Multicast Filtering	When enabled, the controller will block IPv4 multicast packets of the specified protocols. Improper settings may cause network issues.

5. 4 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.

5. 4. 1 ACL

Overview

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

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.

- **Gateway ACL**

  After Gateway ACLs are configured on the controller, they can be applied to the gateway to control traffic which is sourced from LAN ports and forwarded to the WAN ports.
  You can set the Network, IP address, port number of a packet as packet-filtering criteria in the rule.

Configuration

To complete the ACL configuration, follow these steps:

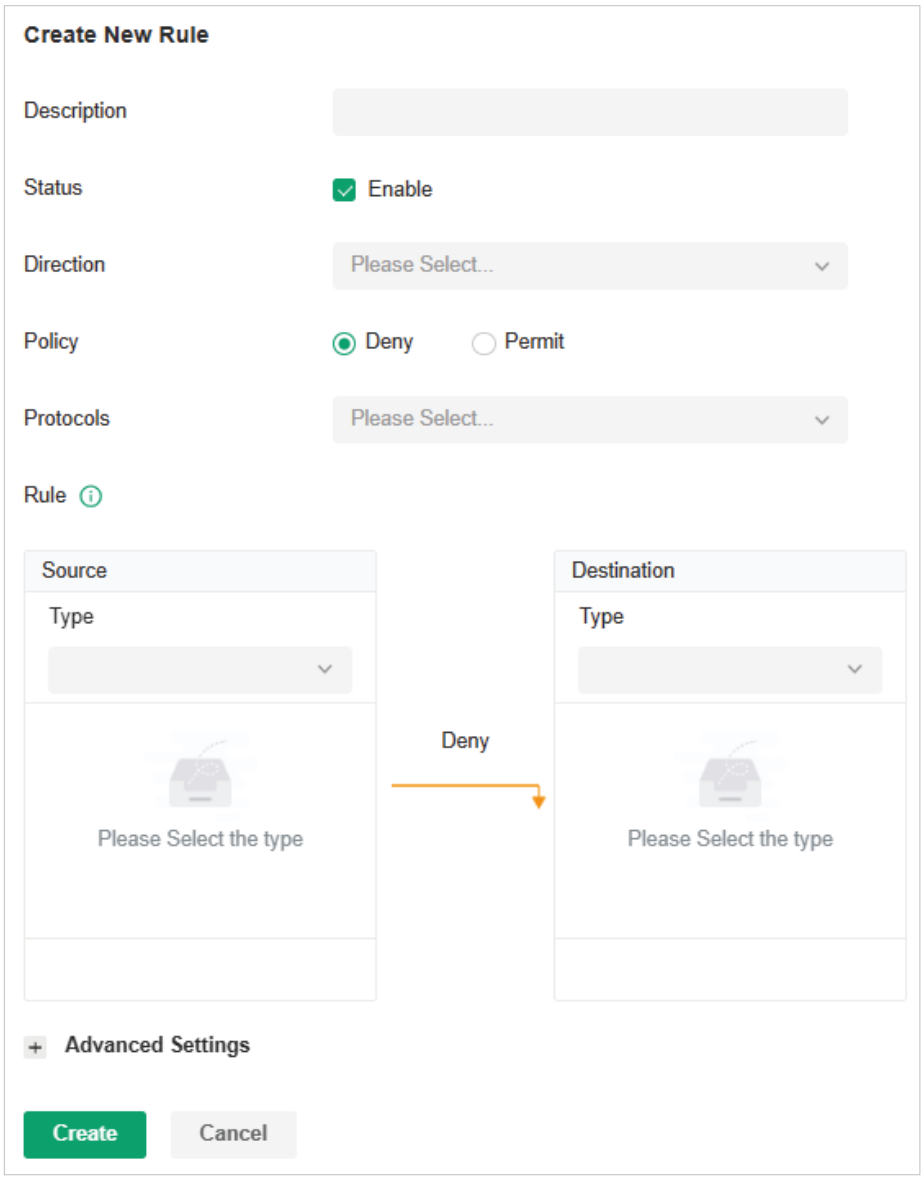
1) Create an ACL with the specified type.

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. Launch the controller and access a site. Go to Settings > Network Security > ACL. On Gateway ACL tab, click Create New Profile 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.

Description	Enter a description to identify the ACL.
Status	Click the checkbox to enable the ACL.

Direction	Select the direction of ACL application traffic. LAN->LAN: Control packet forwarding between LAN side devices. LAN->WAN: Control packet forwarding in the LAN-WAN direction.
Policy	Select the action to be taken when a packet matches the rule. Permit: Forward the matched packet. Deny: Discard the matched packet.
Protocols	Select one or more protocol types to which the rule applies from the drop-down list. The default is All, indicating that packets of all protocols will be matched. When you select one of TCP and UDP or both of them, you can set the IP address and port number of a packet as packet-filtering criteria in the rule.
Log	When enabled, the system can collect ACL entry effective log. To use this function, please configure the remote logging function first.

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

Network	Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired&Wireless Networks > LAN to create one. The gateway will examine whether the packets are sourced from the selected network.
! Network	Select a network you have created and the settings will not applied to that network.
SSID	Select the SSID you have created. If no SSIDs have been created, go to Settings > Wired&Wireless Networks > WLAN to create one. The system will examine whether the SSID of the packet is the SSID selected here.
IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the source IP address of the packet is in the IP Group.
! IP Group	Select an IP group you have created and the settings will not applied to that IP group.

IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the source IP address and port number of the packet are in the IP-Port Group.
! IP-Port Group	Select an IP-Port group you have created and the settings will not applied to that IP-Port group.
IPv6 Group	IPv6 Group:Select the IPv6 Group you have created. If no IPv6 Groups have been created, click + Create on this page or go to Settings > Profiles > Groups to create one. The system will examine whether the source IPv6 address of the packet is in the IPv6 Group.
! IPv6 Group	Select an IPv6 group you have created and the settings will not applied to that IPv6 group.
IPv6-Port Group	IPv6-Port Group:Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click + Create on this page or go to Settings > Profiles > Groups to create one. The system will examine whether the source IPv6 address and port number of the packet are in the IPv6-Port Group.
! IPv6-Port Group	Select an IPv6-Port group you have created and the settings will not applied to that IPv6-Port group.
Location	Select one or multiple locations from the list as the source address, and the system will judge whether the source IP of the data packet belongs to the selected locations.
Location Group	Select a location group you have created, and the system will judge whether the source IP of the data packet belongs to this location group. If no location group has been created, click the create button to create one, or go to Settings > Profiles > Groups to create one.

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

IP Group	Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the destination IP address of the packet is in the IP Group.
! IP Group	Select an IP group you have created and the settings will not applied to that IP group.

IP-Port Group	Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The gateway will examine whether the destination IP address and port number of the packet are in the IP-Port Group.
! IP-Port Group	Select an IP-Port group you have created and the settings will not applied to that IP-Port group.
IPv6 Group	Select the IPv6 Group you have created. If no IPv6 Groups have been created, click + Create on this page or go to Settings > Profiles > Groups to create one. The system will examine whether the destination IPv6 address of the packet is in the IPv6 Group.
! IPv6 Group	Select an IPv6 group you have created and the settings will not applied to that IPv6 group.
IPv6-Port Group	Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click + Create on this page or go to Settings > Profiles > Groups to create one. The system will examine whether the destination IPv6 address and port number of the packet are in the IPv6-Port Group.
! IPv6-Port Group	Select an IPv6-Port group you have created and the settings will not applied to that IPv6-Port group.
Location	Select one or multiple locations from the list as the destination address, and the system will judge whether the destination IP of the data packet belongs to the selected locations.
Location Group	Select a location group you have created, and the system will judge whether the destination IP of the data packet belongs to this location group. If no location group has been created, click the create button to create one, or go to Settings > Profiles > Groups to create one.
Gateway Management Page	This option will allow/block LAN network devices to access the gateway management page.

Set the advanced settings according to your needs:

Time Range	Select the checkbox to enable time-based ACL. You can create a time range or select an existing time range for the ACL rule to take effect.
Bi-Directional	When Direction is LAN->LAN, you can enable this option to configure bi-directional traffic rule.

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

5. 5 Transmission

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

5. 5. 1 Routing

Overview

- Static Route

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

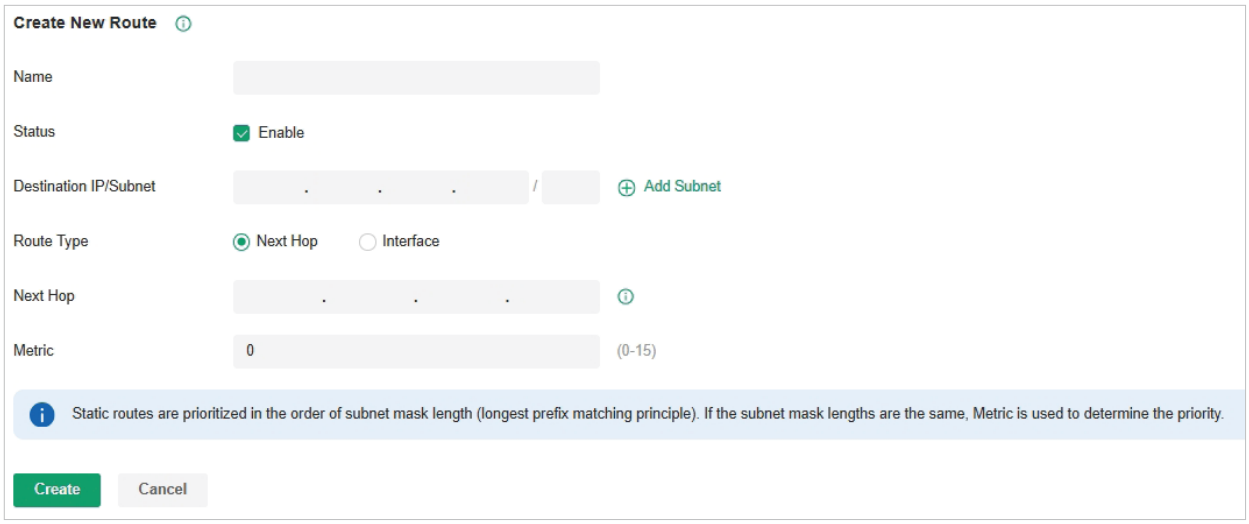
- Policy Routing

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

Configuration

- Static Route

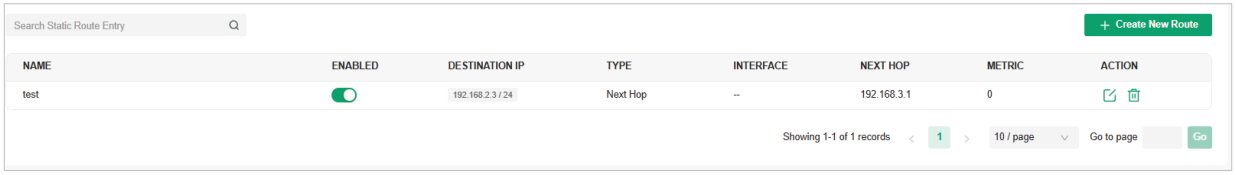
1. Go to Settings > Transmission > Routing > Static Route. Click Create New Route to load the following page and configure the parameters.



Name	Enter the name to identify the Static Route entry.

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

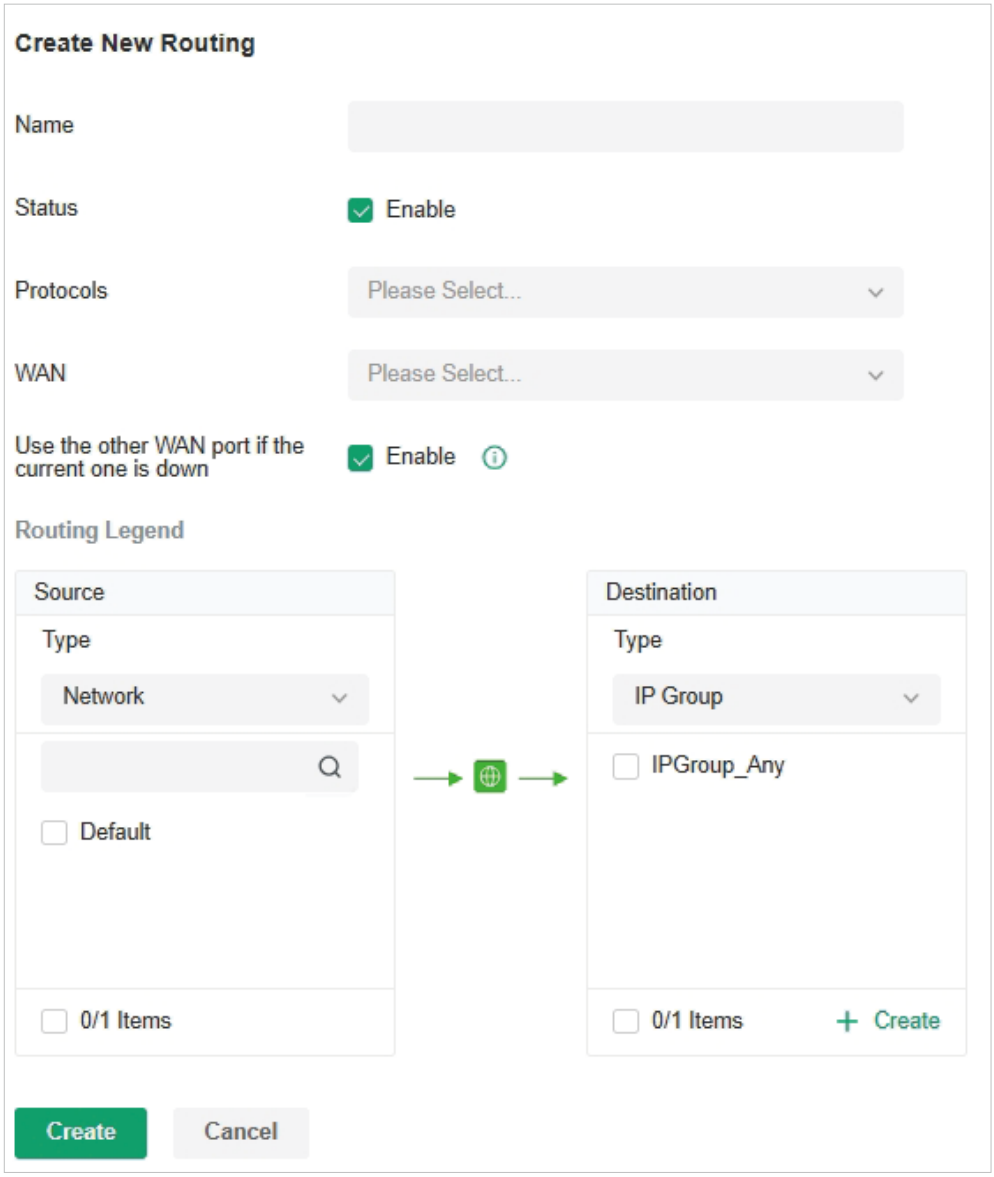
2. Click Create. The new Static Route entry is added to the table. You can click the Edit icon to edit the entry. You can click the Delete icon to delete the entry.



■ Policy Routing

1. Go to Settings > Transmission > Routing > Policy Routing. Click Create New Routing to

load the following page and configure the parameters.



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

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

2. 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.



5. 5. 2 NAT

Overview

- **Port Forwarding**

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

  Port Forwarding helps establish network connections between a host on the internet and the other in the LAN by letting the traffic pass through the specific port of the gateway.

Without Port Forwarding, hosts in the LAN are typically inaccessible from the internet for the sake of security.

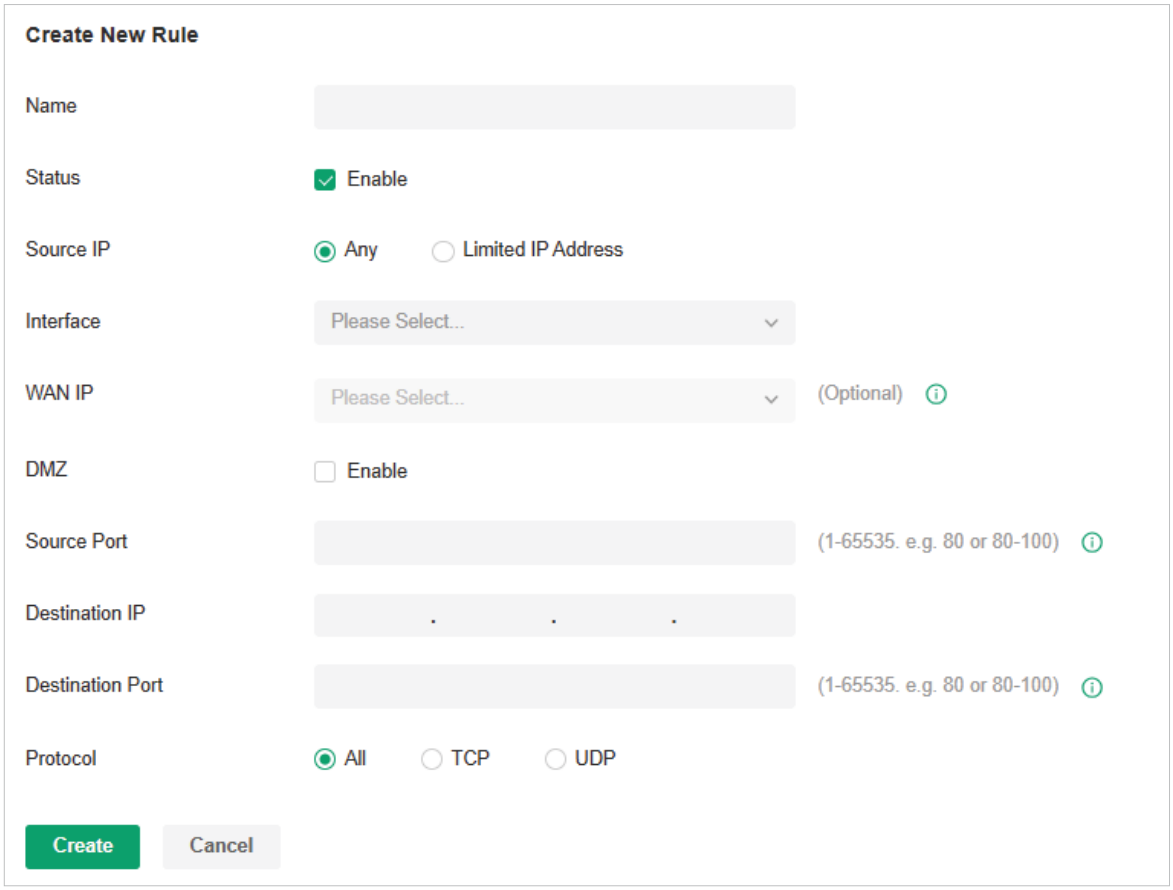
- **ALG**

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

Configuration

- Port Forwarding

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



Name	Enter the name to identify the Port Forwarding rule.
Status	Enable or disable the Port Forwarding rule.

Source IP	Any: The rule applies to traffic from any source IP address. Limited IP Address: The rule only applies to traffic from specific IP addresses. With this option selected, specify the IP addresses and subnets according to your needs.
Interface	Select the interface which the rule applies to. Traffic which is received through the interface is forwarded according to the rule.
DMZ	With DMZ enabled, all the traffic is forwarded to the Destination IP in the LAN, port to port. You need to specify the Destination IP. With DMZ disabled, only the traffic which matches the Source Port and the Protocol is forwarded. The traffic is forwarded to the Destination Port of the Destination IP in the LAN. You need to specify the Source Port, Destination IP, Destination Port, and Protocol.
Source Port	The gateway uses the Source Port to receive the traffic from the internet. Only the traffic which matches the Source Port and the Protocol is forwarded.
Destination IP	The traffic is forwarded to the host of the Destination IP in the LAN.
Destination Port	The traffic is forwarded to the Destination Port of the host in the LAN.
Protocol	Network traffic is transmitted using either TCP or UDP protocol. Only the traffic which matches the Source Port and the Protocol is forwarded. If you want both TCP traffic and UDP traffic to be forwarded, select All.

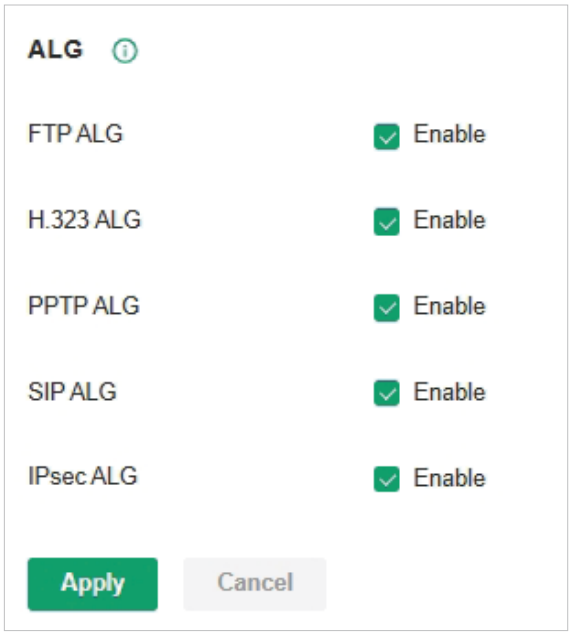
2. Click Create. The new Port Forwarding entry is added to the table. You can click the

Edit icon to edit the entry. You can click the Delete icon to delete the entry.



■ ALG

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



FTP ALG	FTP ALG allows the FTP server and client to transfer data using the FTP protocol in one of the following scenarios: The FTP server is in the LAN, while the FTP client is on the internet. The FTP server is on the internet, while the FTP client is in the LAN. The FTP server and FTP client are in different LANs.
H.323 ALG	H.323 ALG allows the IP phones and multimedia devices to set up connections using the H.323 protocol in one of the following scenarios: One of the endpoints is in the LAN, while the other is on the internet. The endpoints are in different LANs.

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

5. 5. 3 Bandwidth Control

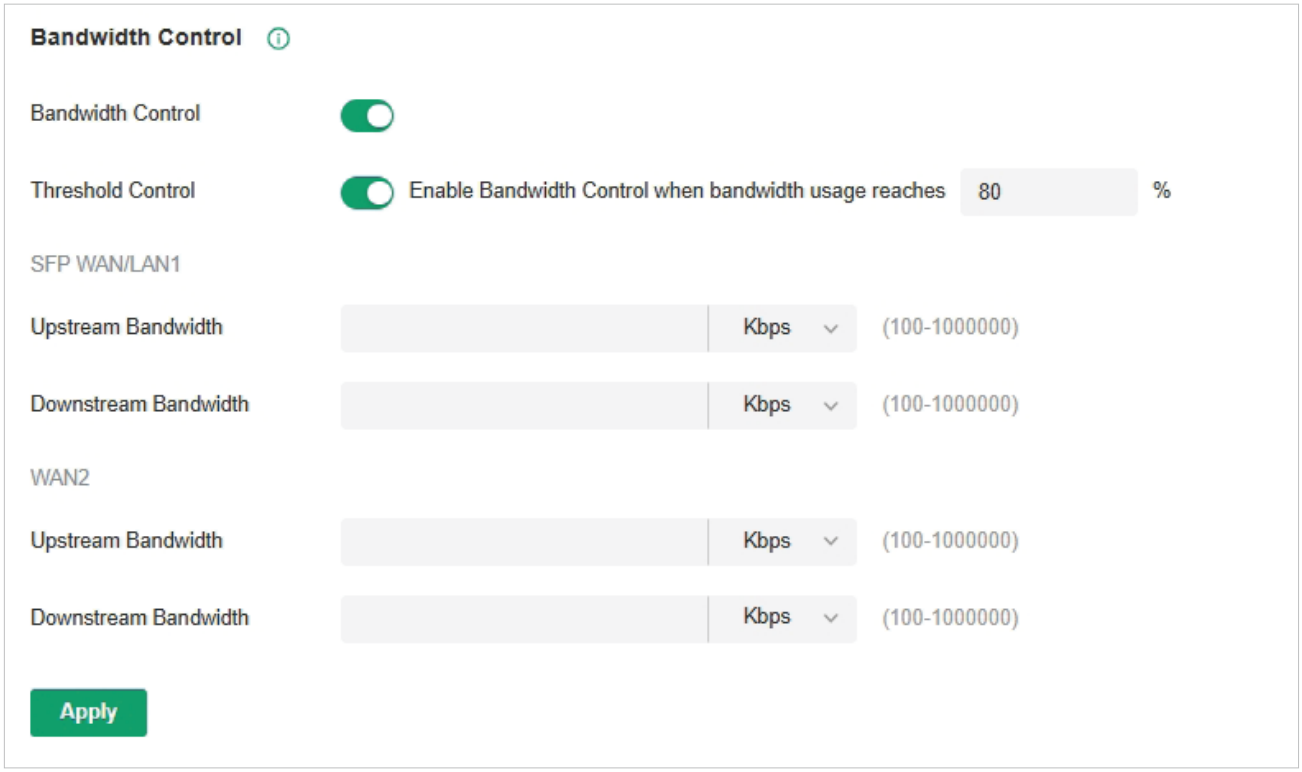
Overview

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

Configuration

1. Go to Settings > Transmission > Bandwidth Control. In Bandwidth Control, enable

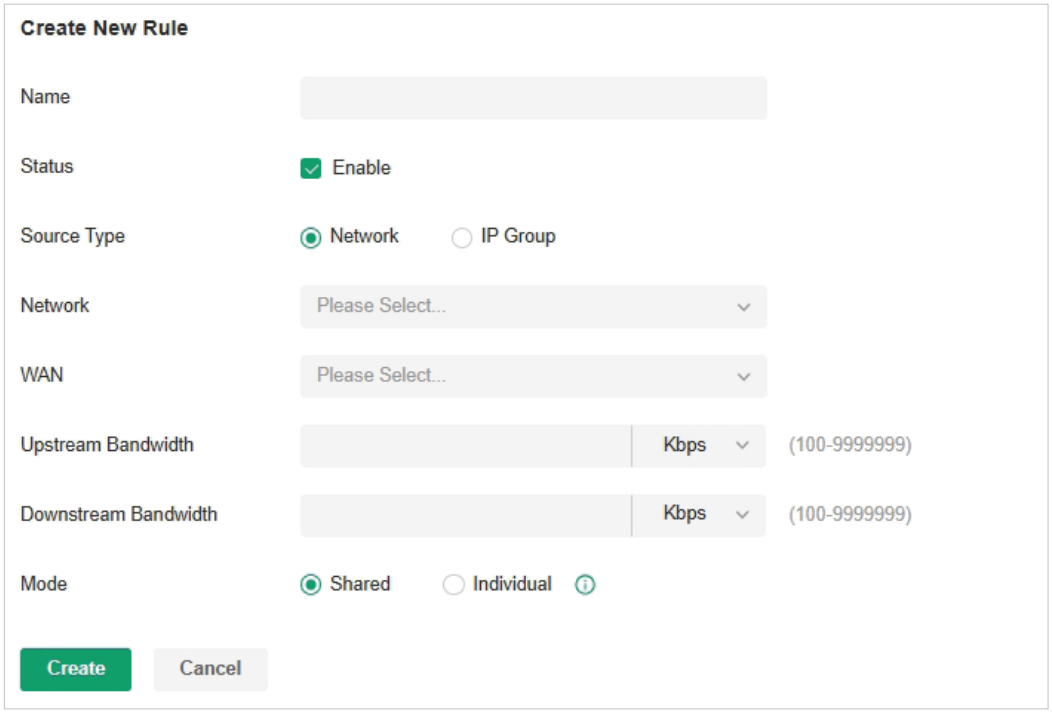
Bandwidth Control globally and configure the parameters. Then click Apply.



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

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

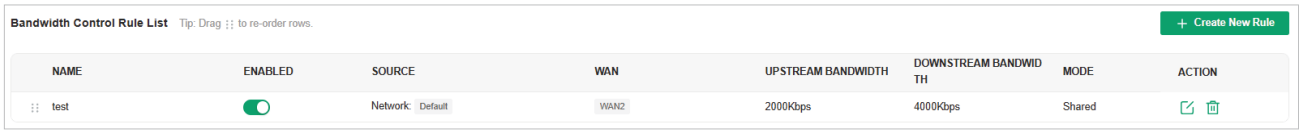
configure the parameters.



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

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

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



5. 6 Configure VPN

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

5. 6. 1 WireGuard VPN

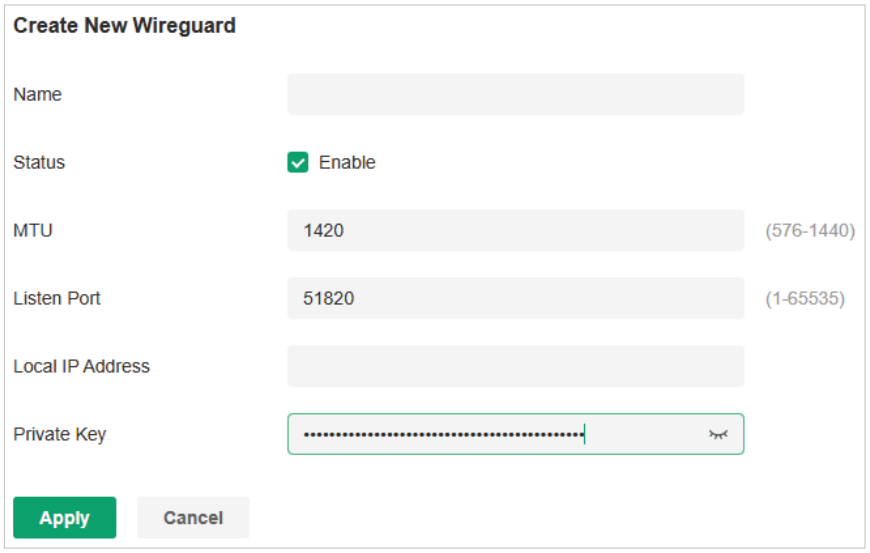
Overview

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

Configuration

■ **WireGuard**

1. Launch the controller and access a site. Go to Settings > VPN > WireGuard.
2. Click Create New WireGuard. Configure the parameters and click Apply.

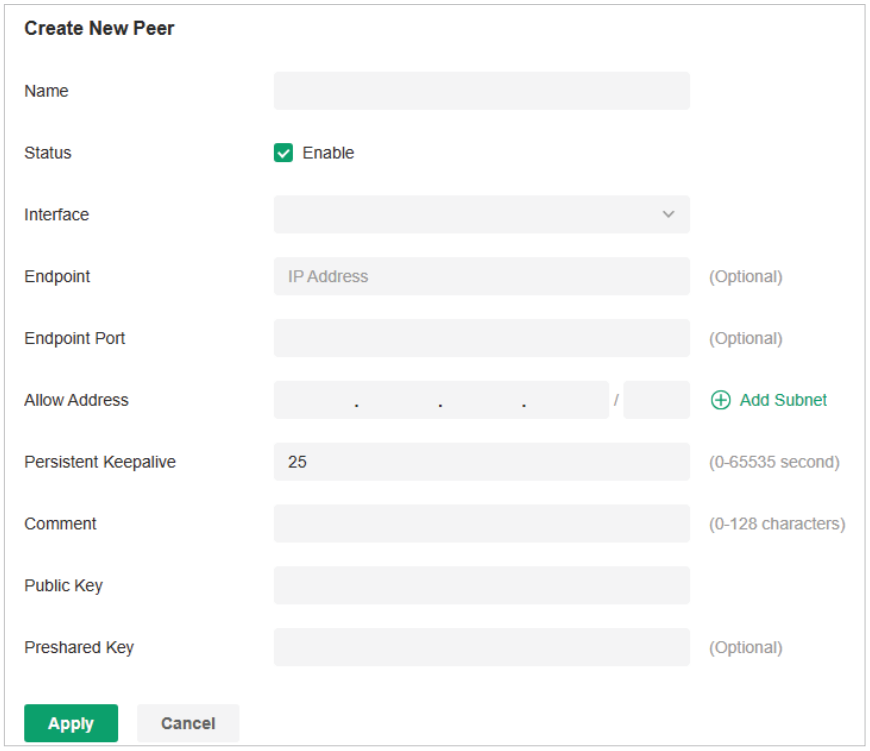


Name	Specify the name that identifies the WireGuard interface.
Status	Specify whether to enable the WireGuard interface.
MTU	Specify the MTU value of the WireGuard interface. The default value 1420 is recommended.
Listen Port	Specify the port number that the WireGuard interface listens to.

Local IP Address	Specify the IP address of the WireGuard interface.
Private Key	Specify the private key of the WireGuard interface. The value will be automatically generated on the device, and you can also modify it manually.

■ Peers

1. Launch the controller and access a site. Go to Settings > VPN > WireGuard > Peers.
2. Click Create New Peer. Configure the parameters and click Apply.



Name	Specify the name that identifies the peer.
Status	Specify whether to enable the peer.
Interface	Specify the WireGuard interface to which the peer belongs.
Endpoint	Specify the IP address of the peer. This parameters is required when the Router actively connects to other WireGurad Server.
Endpoint Port	Specify the port number of the peer. This parameters is required when the Router actively connects to other WireGurad Server.

Allowed Address	Specify the address segment that allows traffic to pass through. Generally, it is the same as the WireGuard VPN interface IP configured on the remote device.
Persistent Keepalive	Specify the tunnel keepalive packet interval.
Comment	Enter the description of the peer.
Public Key	Fill in the public key information exported from the remote device.
Preshared Key	Specify an optional shared key.

■ VPN Status

Go to Settings > VPN > WireGuard > VPN Status. The table lists information of Wireguard VPN.



Name	Display the name of the WireGuard interface.
Interface	Display the interface that the traffic goes through.
Remote IP Address	Display the remote IP address of the WireGuard interface.
Last Handshake	Display the last handshake of the WireGuard interface.
Statistics	Display the upload and download traffic of the WireGuard interface.

5. 7 Configure VoIP

VoIP (Voice over Internet Protocol) allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. You can configure the VoIP settings for your devices on Omada Central Essentials.

5. 7. 1 Call Settings

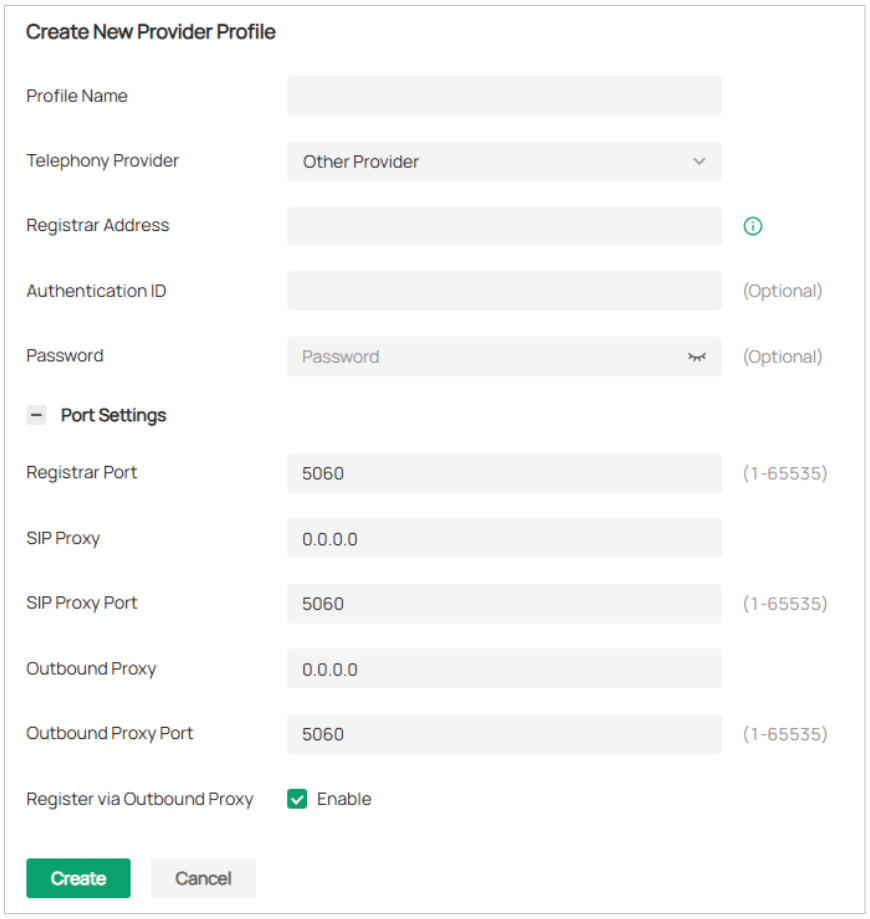
Overview

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

Configuration

- Provider

1. Launch the controller and access a site. Go to Settings > VoIP > Call Settings > Provider.
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.
Authentication ID	Specify the authentication ID specified by your provider.
Password	Specify the password specified by your provider.
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.

■ 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.

3. Launch the controller and access a site. Go to Settings > VoIP > Call Settings > Digit Map.
4. Click Create New Digit Map. Configure the parameters and click Create.



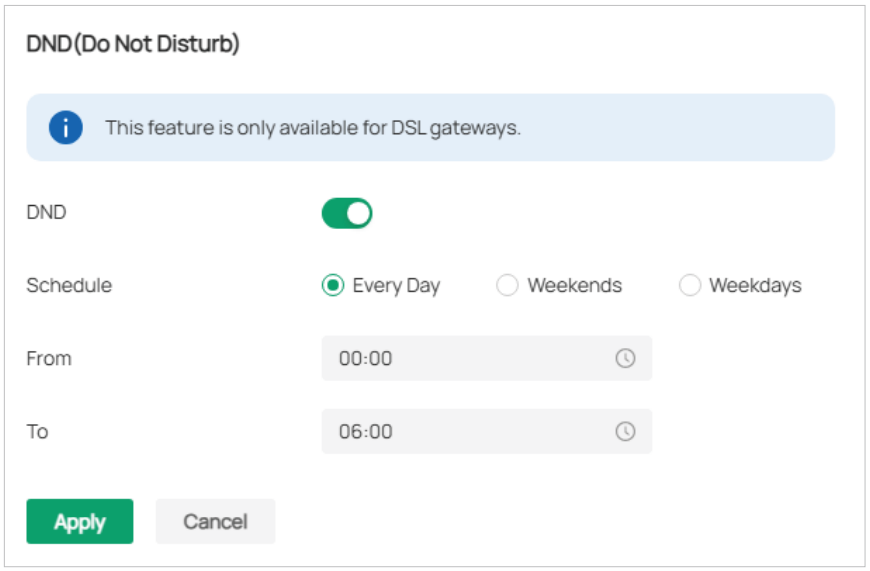
Profile Name	Enter a name to identify the profile.
Digit Map	Enter a digit map by referring to the setting examples.

■ DND & Call Blocking

- DND (Do Not Disturb)

DND (Do Not Disturb) allows you to temporarily block all incoming calls based on your specific schedule.

1. Launch the controller and access a site. Go to Settings > VoIP > Call Settings > DND&Call Blocking.
2. Enable DND. Configure the parameters and click Apply.

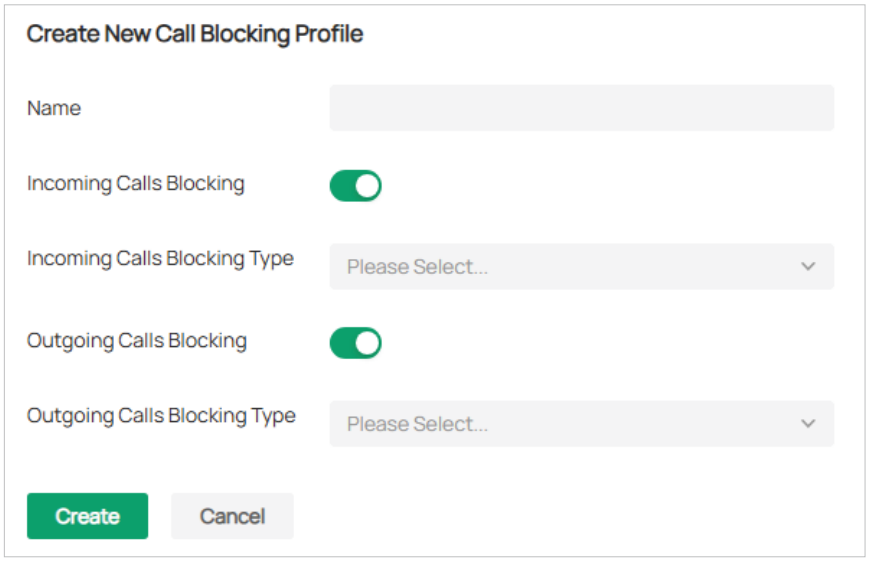


Schedule	Specify the days you want to block the incoming calls.
Time	Set the start time and end time of the DND period you want to block incoming calls.

- Call Blocking

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

1. Launch the controller and access a site. Go to Settings > VoIP > Call Settings > DND&Call Blocking.
2. Click Create New Call Blocking Profile. Configure the parameters and click Create.

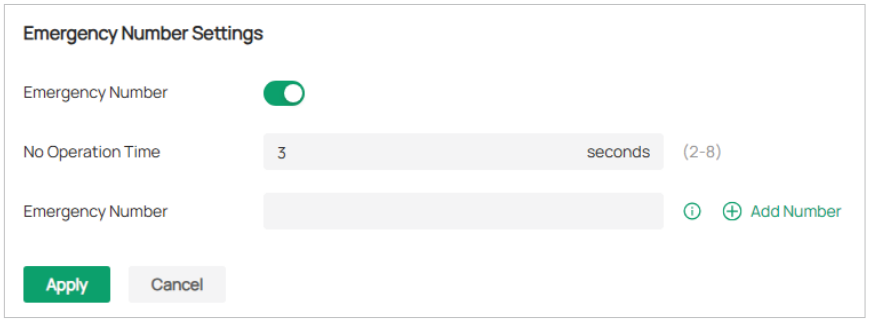


Profile Name	Enter a name to identify the profile.
Incoming Calls Blocking	Enable this option to block unwanted incoming calls.
Incoming Calls Blocking Type	Specify the types of incoming calls to block. Specific Number: Specify one or more phone numbers to block incoming calls from them. Anonymous Number: 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.

■ Emergency Number Settings

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

1. Launch the controller and access a site. Go to Settings > VoIP > Call Settings > Emergency Number Settings.
2. 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.

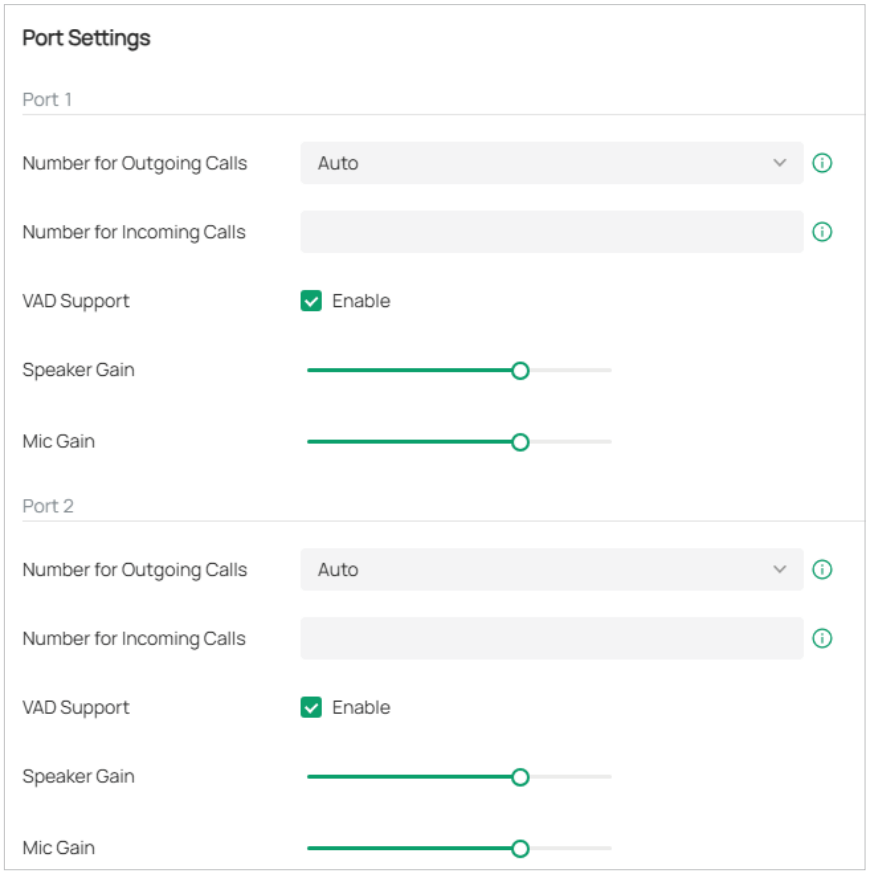
5. 7. 2 VoIP Devices

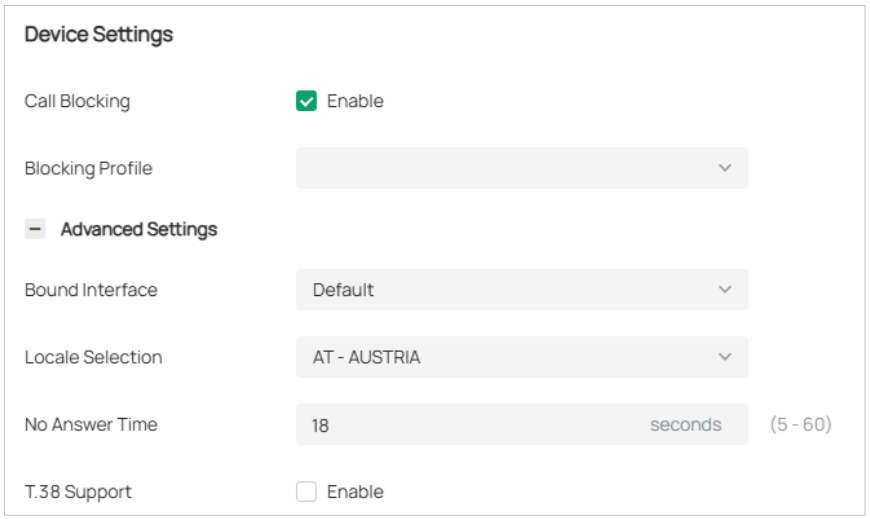
Overview

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

Configuration

1. Launch the controller and access a site. Go to 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.

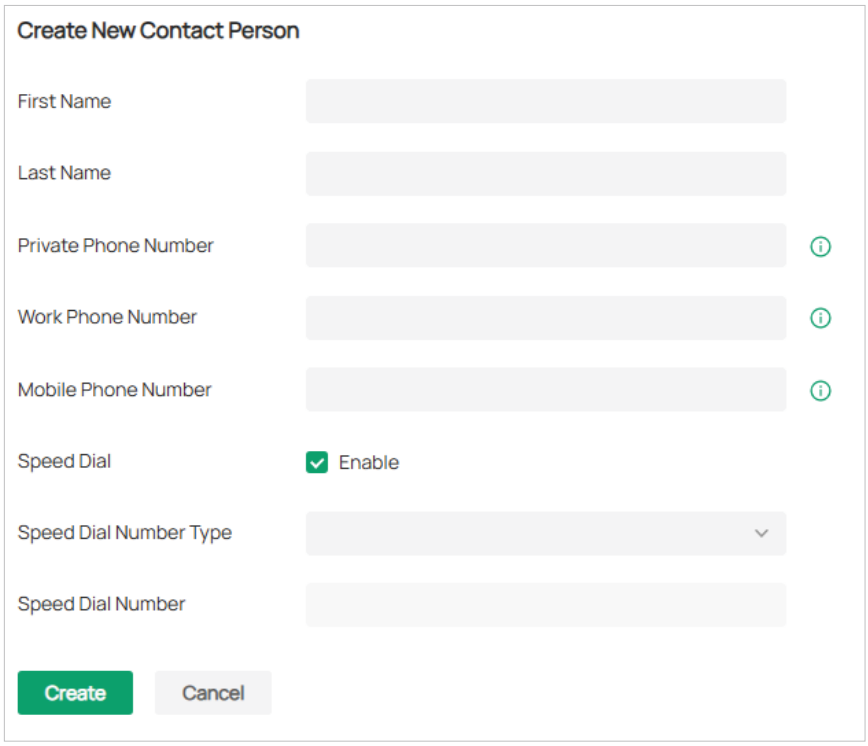
5. 7. 3 Telephone Book

Overview

In Telephone Book, you can create and manage the contact persons.

Configuration

1. Launch the controller and access a site. Go to Settings > VoIP > Telephone Book.
2. Click Create New Contact Person. Configure the parameters and click Create.



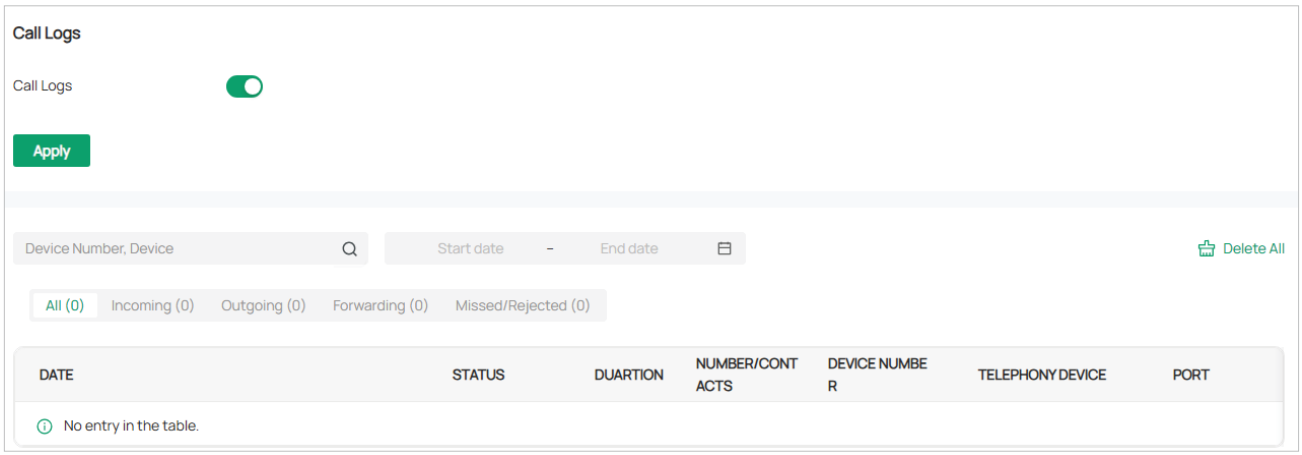
5. 7. 4 Call Logs

Overview

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

Configuration

1. Launch the controller and access a site. Go to Settings > VoIP > Call Logs.
2. Enable Call Logs and click Apply. The calls will be recorded in the table below.



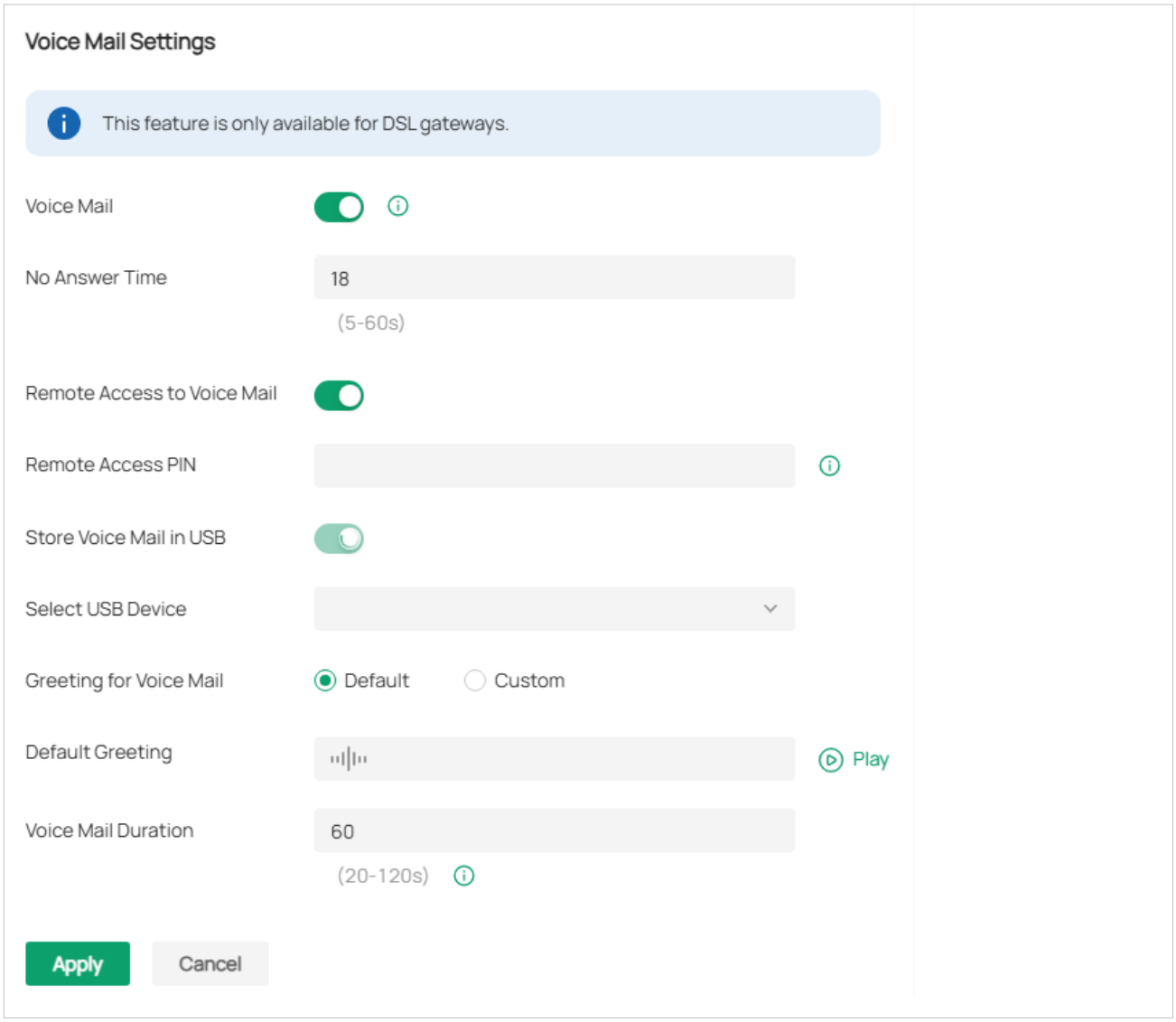
5. 7. 5 Voice Mail

Overview

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.

Configuration

1. Launch the controller and access a site. Go to Settings > VoIP > Voice Mail.
2. Enable Voice Mail. Configure the parameters and click Apply. The voice mails will be recorded in the Voice Mail List below.



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.

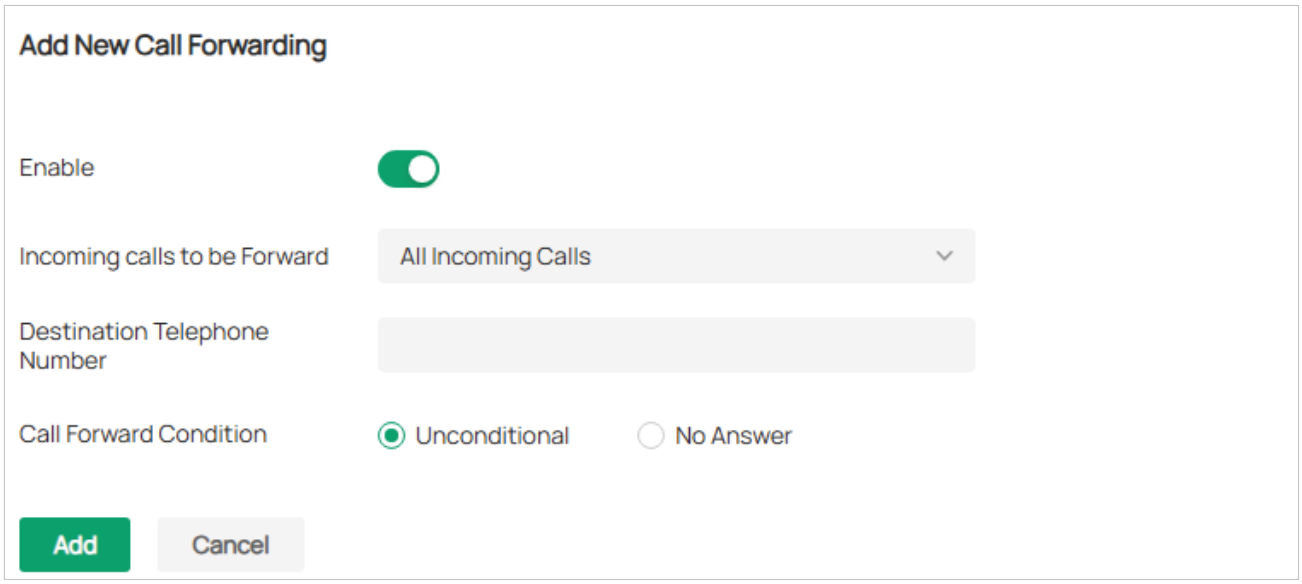
5. 7. 6 Call Forwarding

Overview

Call Forwarding allows you to redirect incoming calls to a designated phone number.

Configuration

1. Launch the controller and access a site. Go to Settings > VoIP > Call Forwarding.
2. Click Add New Call Forwarding. Configure the parameters and click Add.



Incoming calls to be Forward	Select a call type to be forwarded. All Incoming Calls: If this option is selected, all incoming calls will be forwarded. Calls to the Telephone Number: If this option is selected, select a telephone number from the list. Any incoming calls to this number will be forwarded. Calls to the Phone: If this option is selected, select a telephony device from the list. Any incoming calls to this device will be forwarded. Calls from a Person in the Telephone Book: If this option is selected, select a contact from the list. Any incoming calls from this contact will be forwarded. Calls from the Telephone Number: If this option is selected, enter a specific telephone number. Any incoming calls from this number will be forwarded.
Destination Telephone Number	Enter a Destination Telephone Number that incoming calls will be redirected to.

Call Forward Condition	Select the Call Forward Condition. Unconditional: All incoming calls will be redirected to the designated telephone number whether the receiver is busy or not. No Answer: Incoming calls that are not answered for the specified time period will be redirected to the designated telephone number.

5. 8 Services

Services provide convenient network services and facilitate network management. You can set fixed IP address for certain device in DHCP Reservation and configure servers or terminals in DDNS and SSH.

5. 8. 1 DHCP Reservation

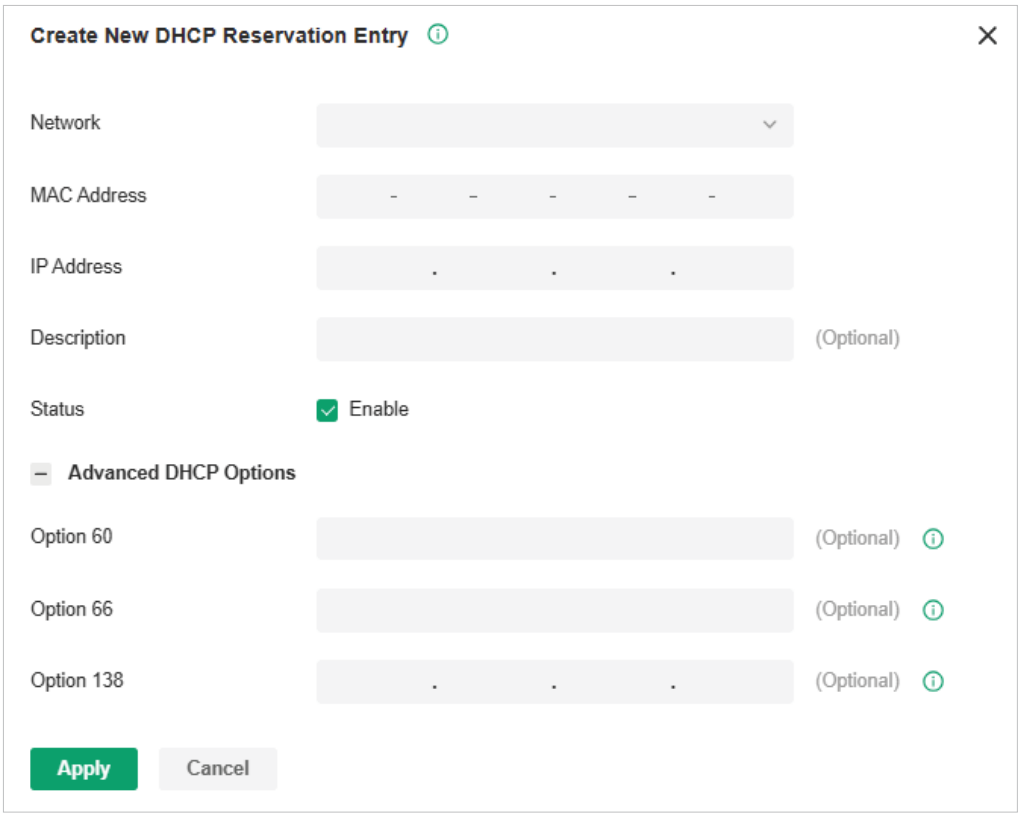
Overview

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

Configuration

- To manually add DHCP Reservation entries:

1. Launch the controller and access a site. Go to Settings > Services > DHCP Reservation.
2. Click Create New DHCP Reservation Entry and configure the parameters. Then click Apply.

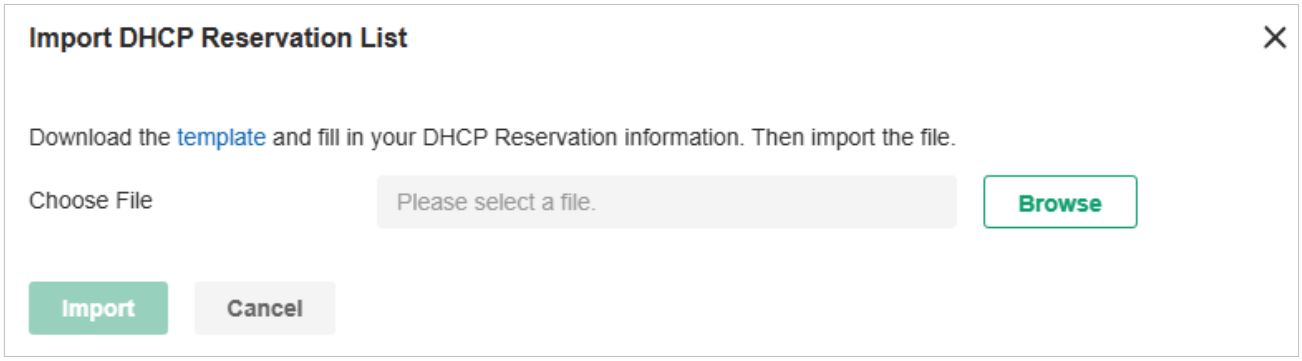


Network	Select the network the DHCP reservation entry is used for.
MAC Address	Specify the MAC address of the device for which you want to reserve an IP address.
IP Address	Specify the fixed IP address for the device.
Description	Enter description for the entry for identification.
Status	Enable or disable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

Advanced DHCP Options	Configure the advanced DHCP options if needed. Option 60: Enter the value for DHCP Option 60. DHCP clients use this field to optionally identify the vendor type and configuration of a DHCP client. Mostly it is used in the scenario where the APs apply for different IP addresses from different servers according to the needs. Option 66: Enter the value for DHCP Option 66. It specifies the TFTP server information and supports a single TFTP server IP address. Option 138: Enter the value for DHCP Option 138. It is used in discovering the devices by the system.

- To import DHCP Reservation entries in batch:

1. Launch the controller and access a site. Go to Settings > Services > DHCP Reservation.
2. Click Export to export the template in csv format. Based on this template, you can add custom address reservation entries that need to be imported.
3. Click Import and import the customized template. You can download the template, then edit and upload it for batch import.



5. 8. 2 Dynamic DNS

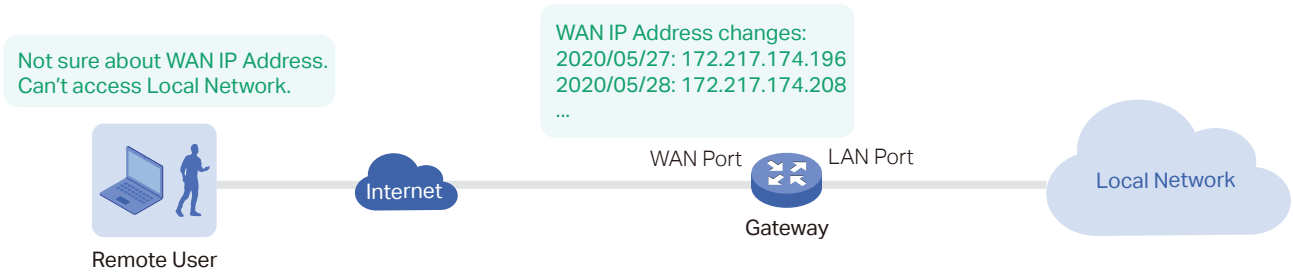
Overview

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

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

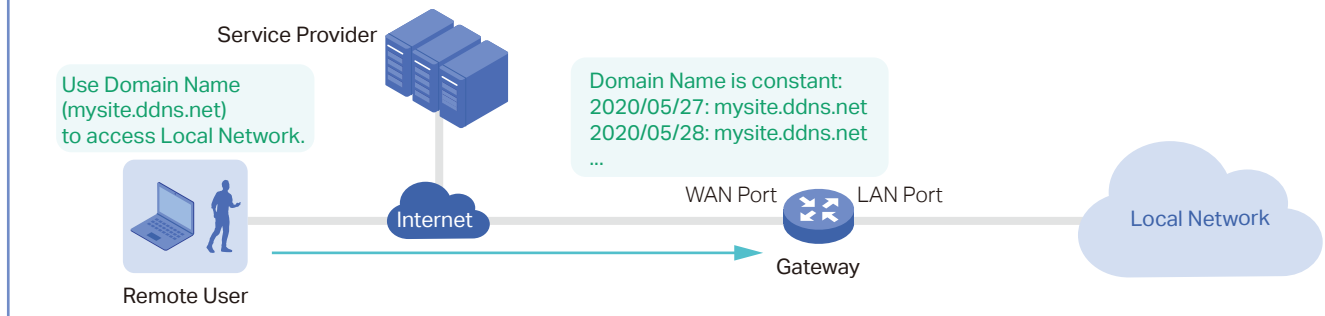
Before:

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



After:

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

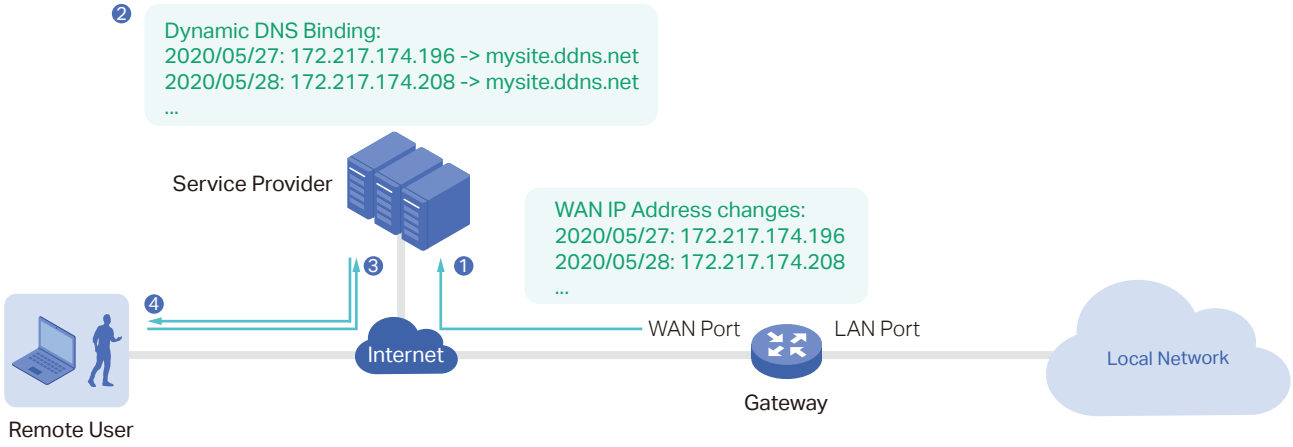


Prerequisite:

- 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.

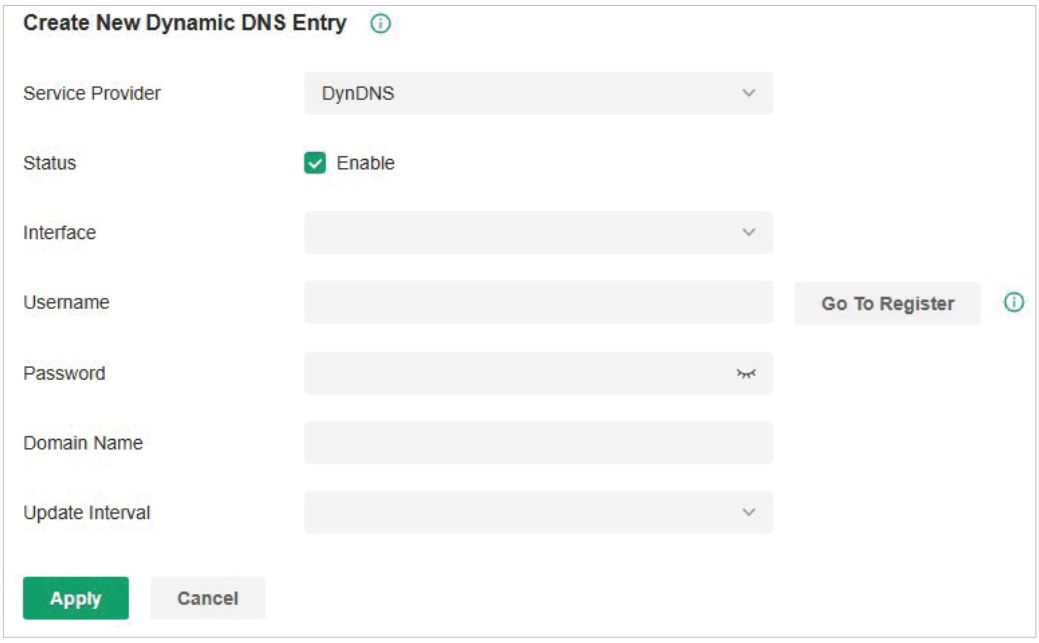
How Dynamic DNS works:

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

Launch the controller and access a site. Go to Settings > Services > Dynamic DNS. Click Create New Dynamic DNS Entry, to load the following page. Configure the parameters and click Create.



Service Provider	Select your service provider which Dynamic DNS works with.
Status	Enable or disable the Dynamic DNS entry.
Interface	Select the WAN Port which the Dynamic DNS entry applies to.
Username	Enter your username for the service provider. If you haven't registered at the service provider, click Go To Register.
Password	Enter your password for the service provider.
Domain Name	Enter the Domain Name which is provided by your service provider. Remote users can use the Domain Name to access your local network through WAN port.
Interval Mode	Choose to use fixed or custom interval.
Update Interval	Specify the update interval to report the changes of the WAN IP address for the DDNS service.

5. 8. 3 SSH

Overview

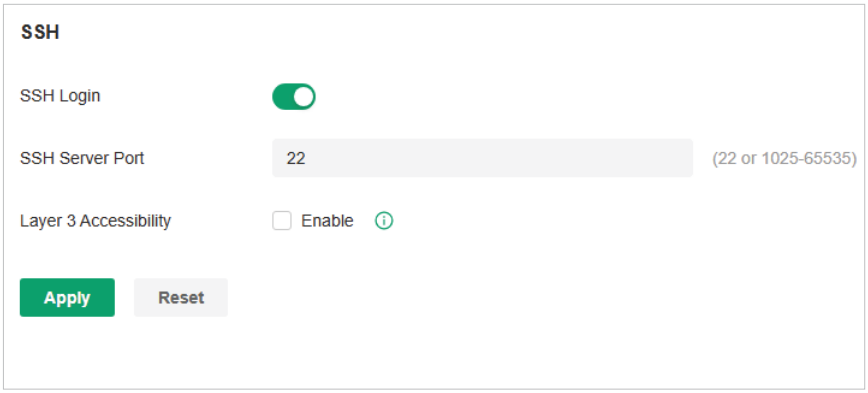
SSH (Secure Shell) provides a method for you to securely configure and monitor network devices via a command-line user interface on your SSH terminal.

Note:

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

Configuration

Launch the controller and access a site. Go to Settings > Services > SSH. Enable SSH Login globally and configure the parameters. Then click Apply.



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

5. 9 Authentication

Authentication is a portfolio of features designed to authorize network access to clients, which enhances the network security.

5. 9. 1 Portal

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

The controller provides several types of Portal authentication:

- **Simple Password**

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

- **Hotspot**

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

  - **Voucher**

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

- **Form Auth**

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

- **External 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 Controller.

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**

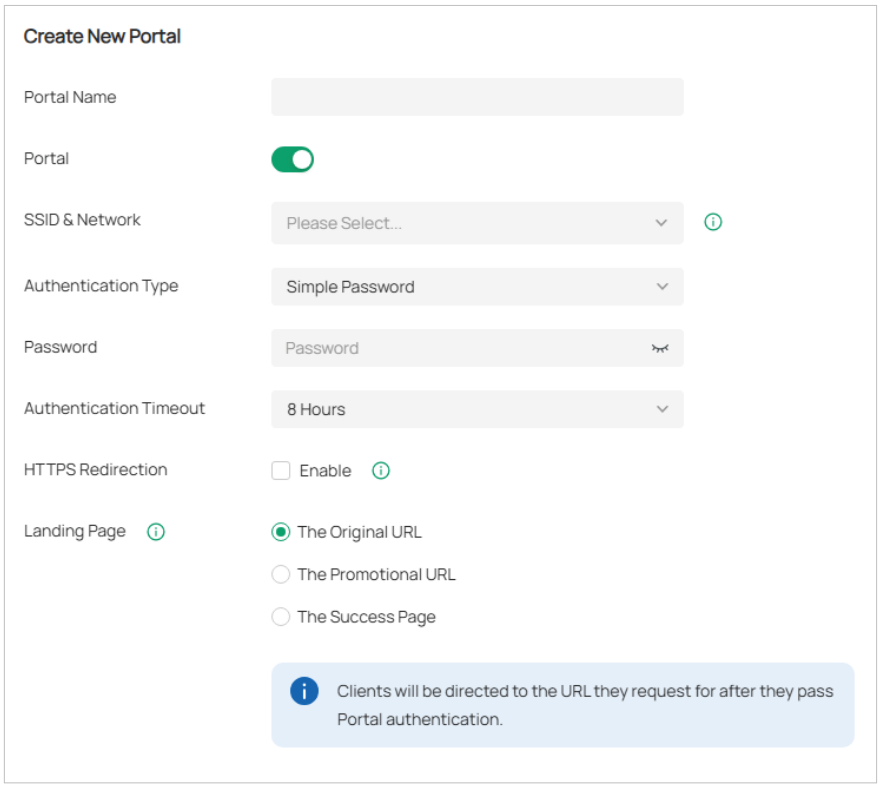
  Pre-Authentication Access allows unauthenticated clients to access the specific network resources.

- Authentication-Free Client

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

Create New Portal

1. Launch the controller and access a site. Go to Settings > Authentication > Portal.
2. On Portal tab, click Create New Portal. Specify the portal name and enable Portal.



3. 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. Select the Authentication Type and configure authentication settings.

- **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 Vouchers for detailed information about how to create vouchers.

- **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.

■ **External Portal Server**

Custom Portal Server	Specify the IP address or URL that redirect to an external portal server.

5. Configure redirection and landing settings.

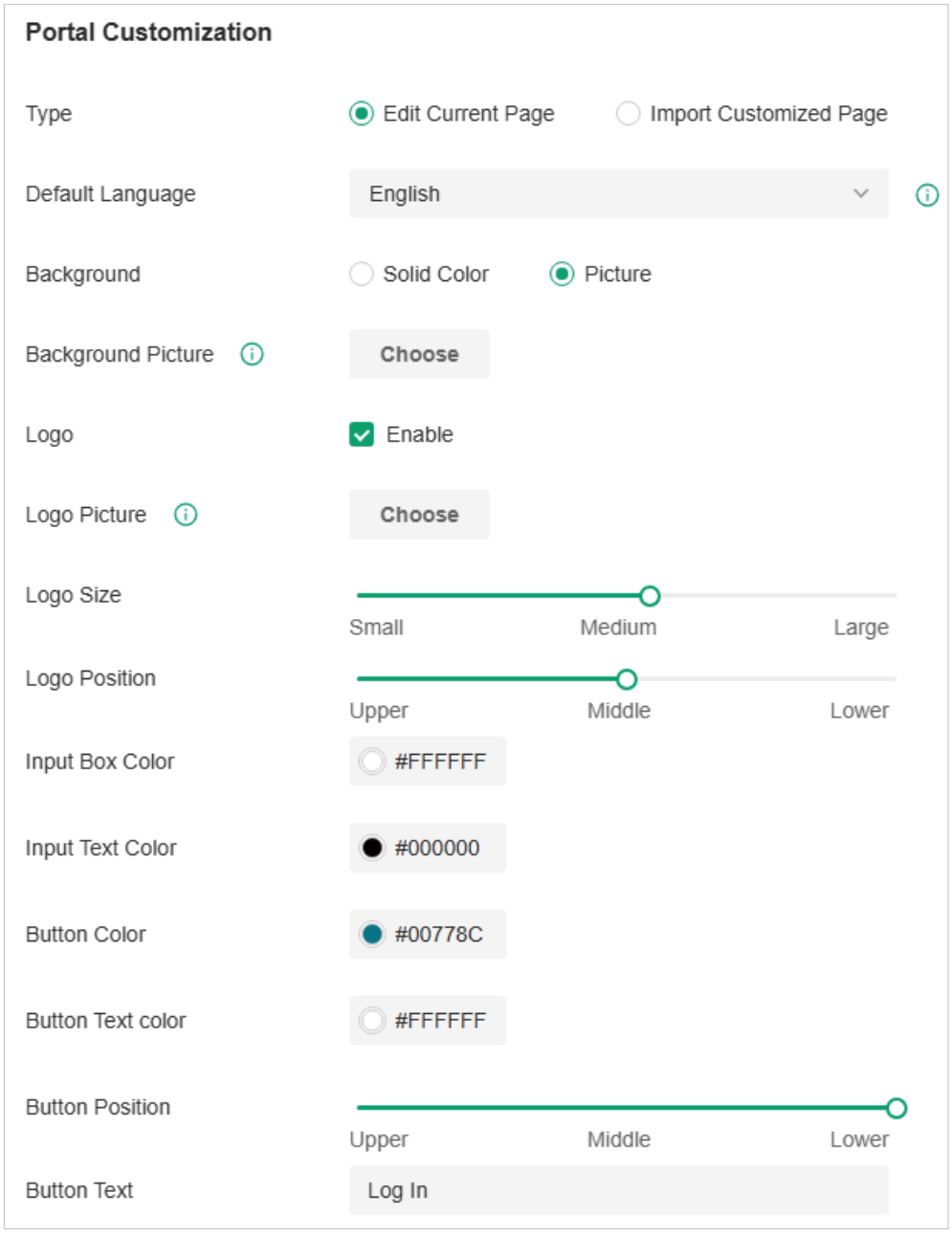
HTTPS Redirection	Click the checkbox to enable HTTPS Redirection. With this feature enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this feature disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected 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.

(Optional) Portal Customization

When creating or editing a portal entry, you can customize the Portal page in the Portal Customization section.

Note:

Portal Customization is not available when you configure external authentication types.

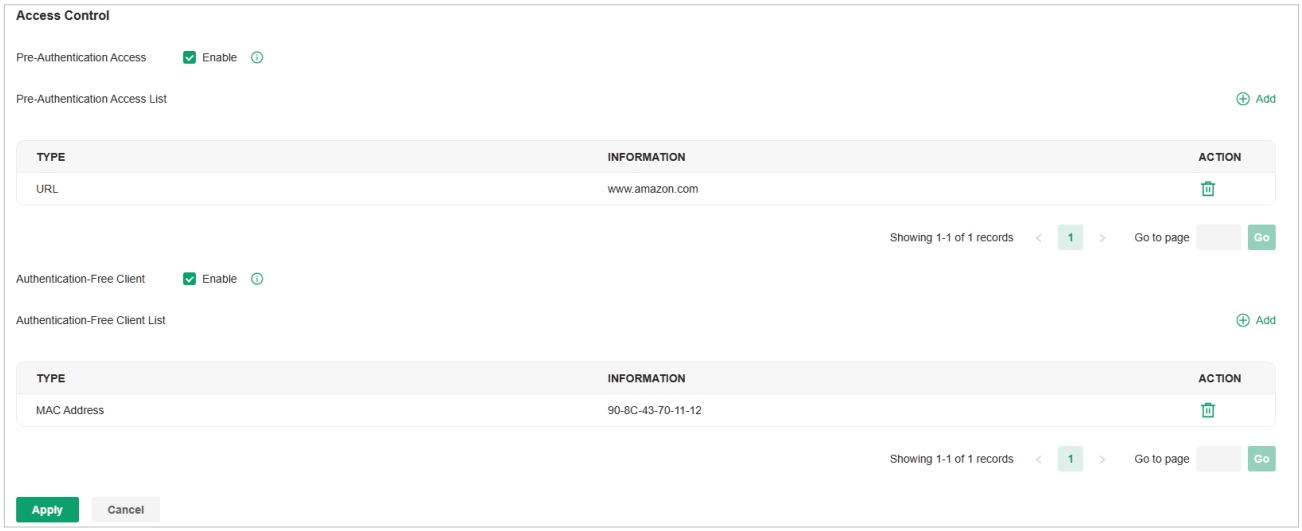


Type	Select the type of the Portal page. Edit Current Page: Edit the related parameters to customize the Portal page based on the provided page. Import Customized Page: Click Import to import your unique Portal page for branding it as per your business.
Default Language	Select the default language displayed on the Portal page. The controller automatically adjusts the language displayed on the Portal page according to the system language of the clients. If the language is not supported, the controller will use the default language specified here.
Background	Select the background type. Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker. Picture: Click Choose and select a picture from your PC as the background.
Logo	Click to show the logo on the portal page.
Logo Picture	Click Choose and select a picture from your PC as the logo.
Logo Size/ Logo Position	Adjust the logo size and position on the Portal Page.
Input Box Color/ Input Text Color	(For cetain anthentication types) Configure your desired background and text color for the input box by entering the hexadecimal HTML color code manually or through the color picker.
Button Color/ Button Text Color	Configure your desired background and text color for the button by entering the hexadecimal HTML color code manually or through the color picker.
Button Position	Select the button position on the Portal Page.
Button Text	Enter the text for the button.
Welcome Information	Click the checkbox and enter text as the welcome information. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.

Terms of Service	Click the checkbox and enter text as the terms of service in the following box. Click Add Terms to enter the name and context of the terms which will appear after a client clicks the link in Terms of Service.
Copyright	Click the checkbox and enter text as the copyright in the following box. You can specify the desired text font size and configure the text color by entering the hexadecimal HTML color code manually or through the color picker.
Show Redirection Countdown After Authorized	When enabled, the system will show the portal's redirection countdown.

(Optional) Access Control

On Access Control tab, you can configure access control rules if needed.



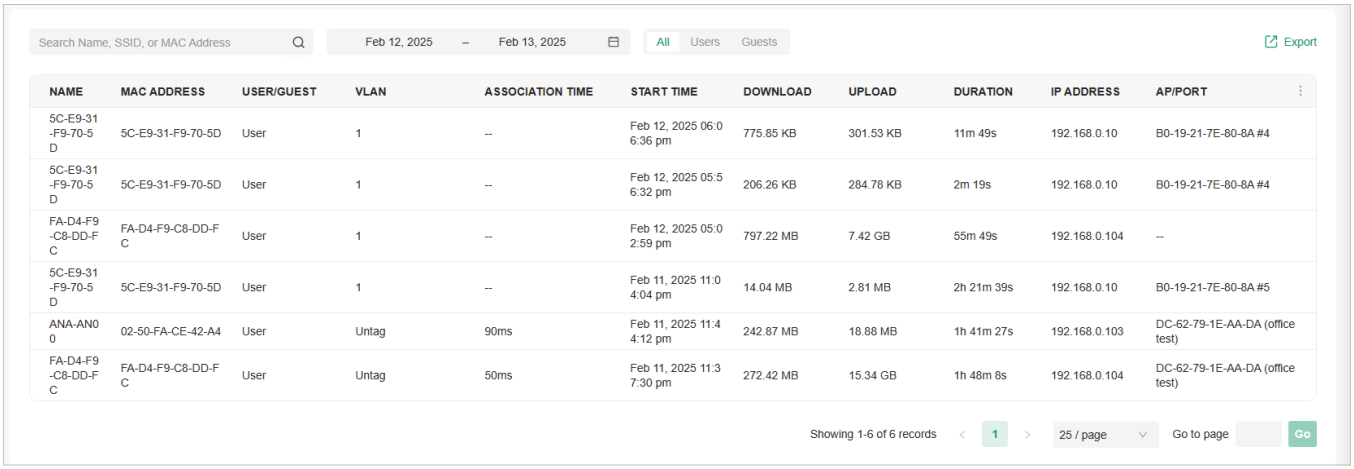
Pre-Authentication Access	Click the checkbox to enable Pre-Authentication Access. With this feature enabled, unauthenticated clients are allowed to access the subnets and web resources specified in the Pre-Authentication Access List below.
Pre-Authentication Access List	Click Add to configure the IP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

Authentication-Free Client List	Click Add and enter the IP address or MAC address of Authentication-Free clients.

5. 9. 2 Past Portal Authorizations

In Past Portal Authorization, a table lists all clients that passed the portal authorization before.

In the table, you can view the client's name, MAC address, authorization credential, uplink and downlink traffics, authorization time and duration, IP address, and the network/port it connected to. For detailed monitoring and management, refer to Manage Client Authentication in Hotspot.



A search bar and a time selector are above the table for searching and filtering.

	Enter the client name, MAC address, Authorized By, or SSID/Network to search the clients.
	Filter the clients based on Start Time. Click the selector to open the calendar. Click a specific date twice in the calendar to display the clients authorized on the day. To display the clients authorized during a time range, click the start date and end date in the calendar.

5. 10 Create Profiles

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

5. 10. 1 Groups

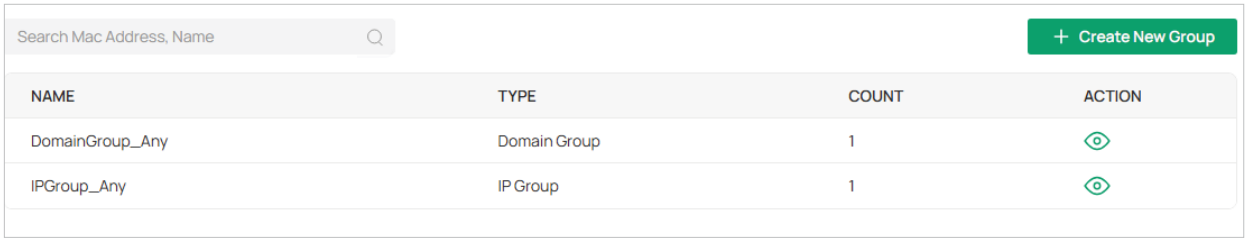
Overview

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

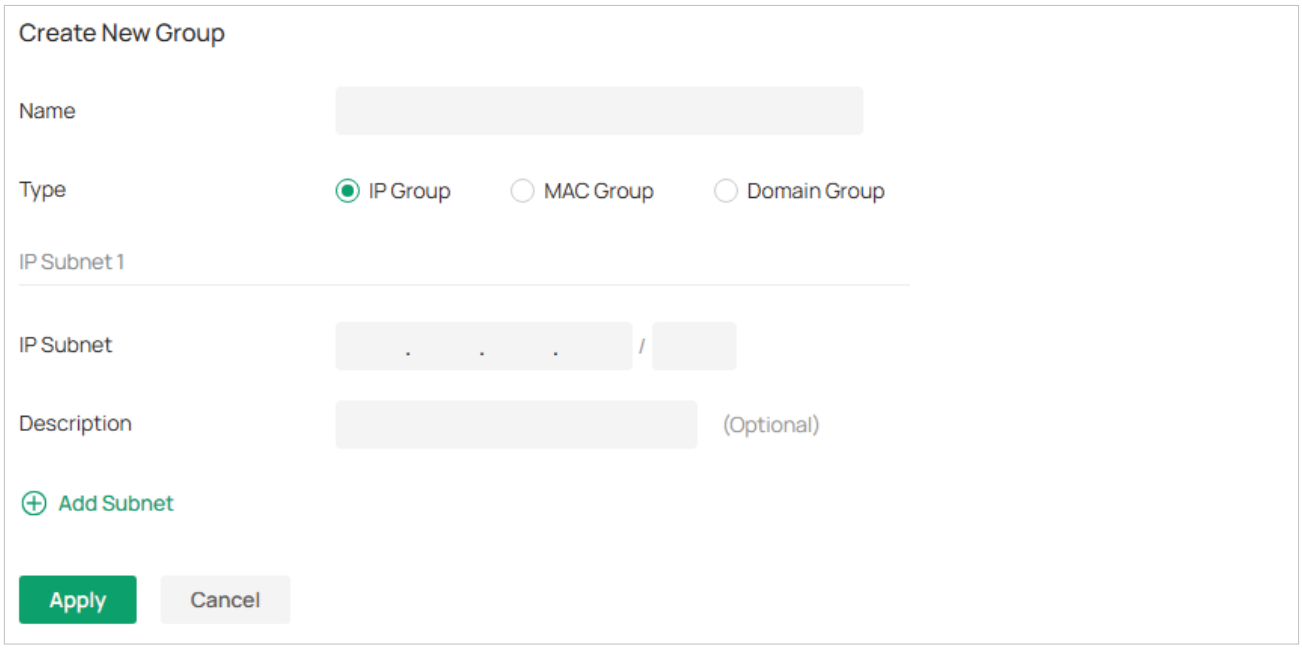
Configuration

To configure the group profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Profile > Groups. Click Create New Group to add a new group profile.



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



- To create an IP group profile:

  Choose the IP Group type and specify IP subnets.

- To configure a MAC group profile:

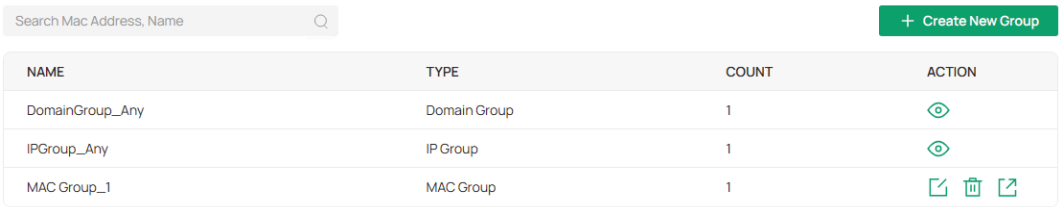
  Choose the MAC Group type and add MAC addresses in the MAC Addresses List.

- To configure a domain group profile:

  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.

3. Click Apply to save the entry.

   You can view and edit the group list, and export the MAC group if needed. You can apply the customized profiles during site configuration.



5. 10. 2 Time Range

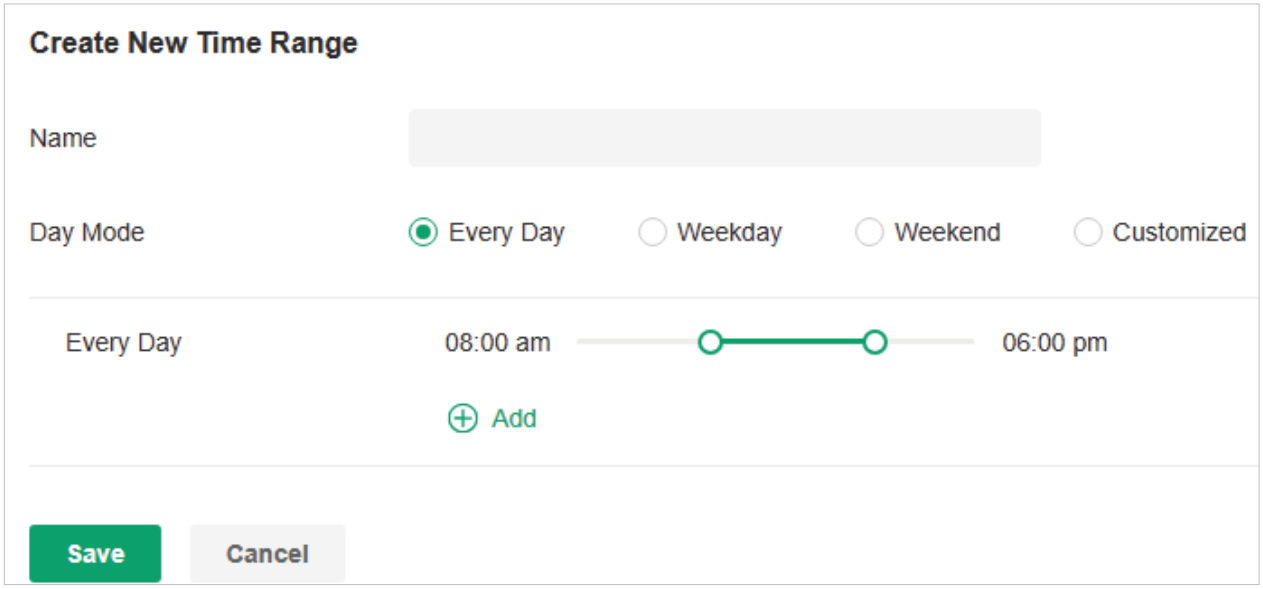
Overview

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

Configuration

To configure the time range profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Profile >Time Range. Click Create New Time Range to add a new time range entry. By default, there is no entry in the list.

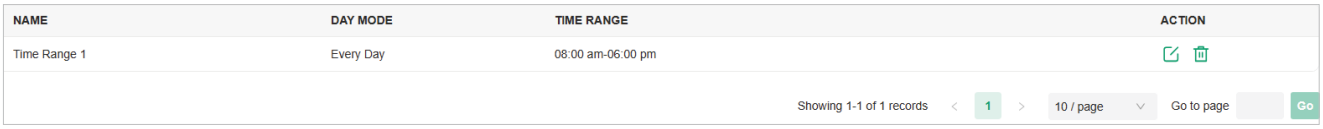


2. Enter a Name for the new entry, select the Day Mode, and specify the time range. Click +Add to add a new time period, click Save to save the entry. After saving the newly added entry, you can apply them to site configuration.

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

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

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



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

5. 10. 3 Rate Limit

Overview

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

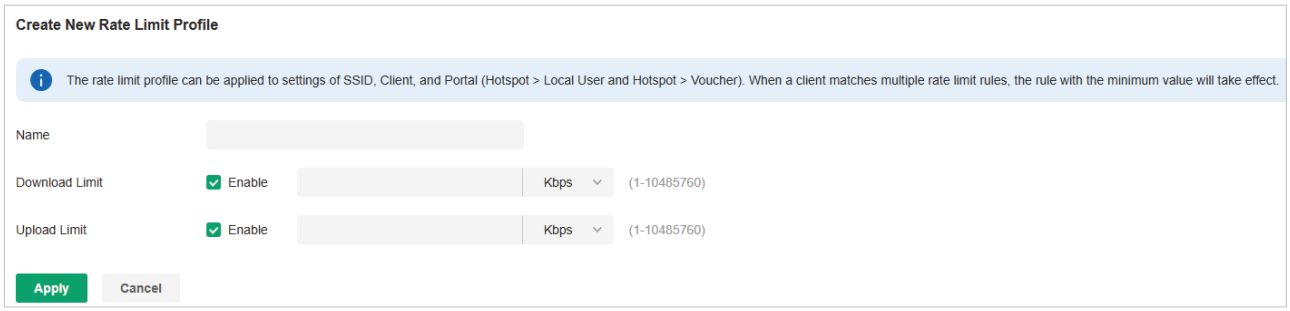
Configuration

To configure the rate limit profiles, follow these steps:

1. Launch the controller and access a site. Go to Settings > Profile > Rate Limit. By default, there is an entry with no limits, and it can not be deleted. Click Create New Rate Limit Profile to add a new group entry.



2. Enter a name and specify the download/upload rate limit for the new entry. After saving the newly added entry, you can apply them to other configurations 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.

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

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

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

5. 10. 4 APN Profile

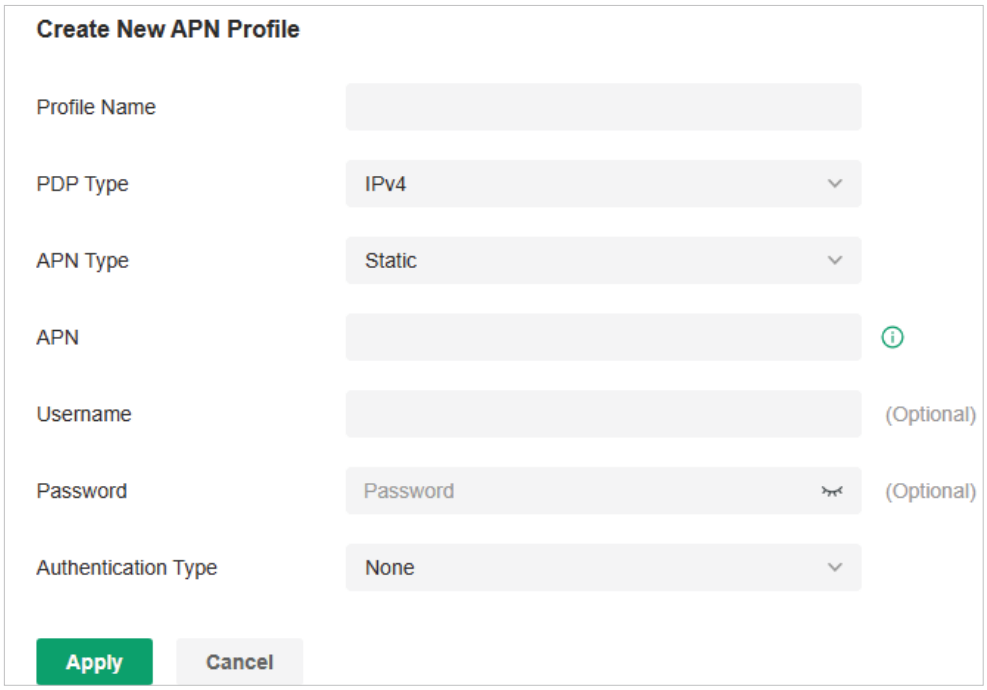
Overview

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. Launch the controller and access a site. Go to Settings > Network Profile > APN Profile. Click Create New APN Profile to add a new profile .



2. 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.
Apply to SIM	(For models with dual SIM cards) Select the SIM card to which the APN profile will be applied.

3. Click Apply to save the profile. Now you can select the predefined entry of APN profile when configuring rules of related modules.

Chapter 6

Monitor the Network

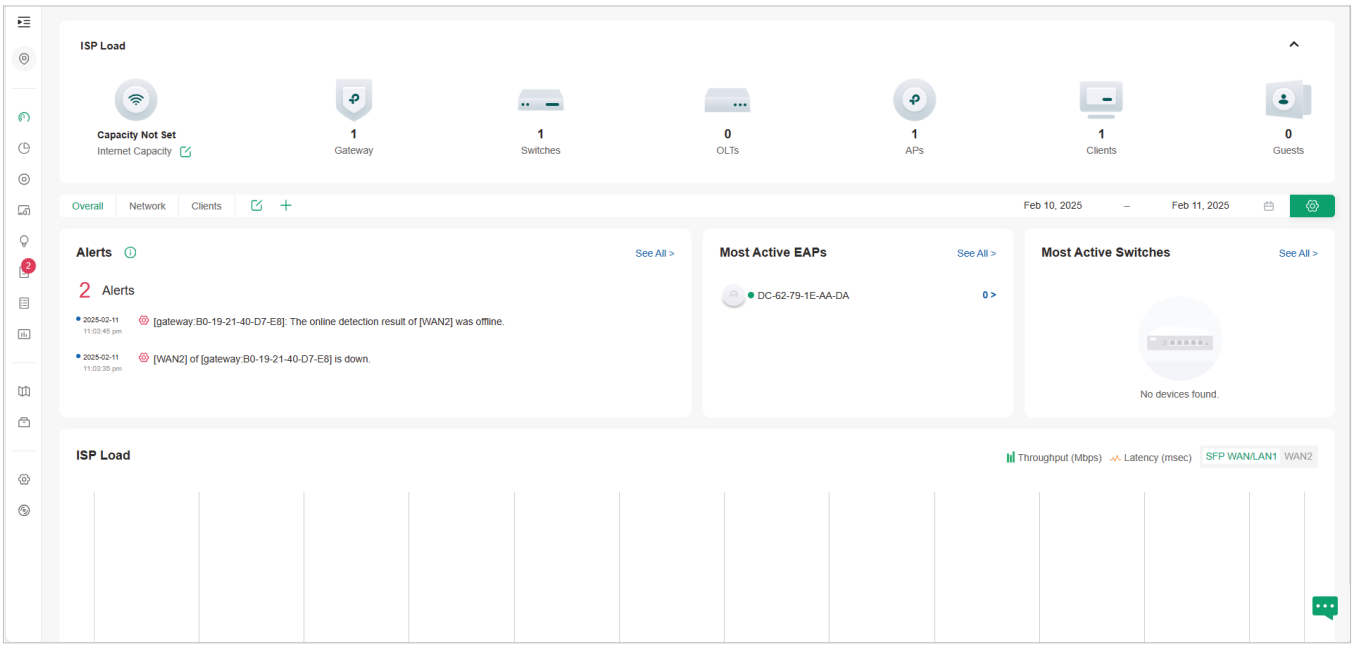
This chapter guides you on how to monitor the network devices, clients, and their statistics. Through visual and real-time presentations, the Omada Central Essentials keeps you informed about the accurate status of the managed network. This chapter includes the following sections:

- 6.1 View the Status of Network with Dashboard
- 6.2 Monitor the Network with Map
- 6.3 View Statistics During Specified Period with Insight
- 6.4 View and Manage Logs
- 6.5 Audit Logs
- 6.6 Monitor the Network with Tools
- 6.7 IntelliRecover

6. 1 View the Status of Network with Dashboard

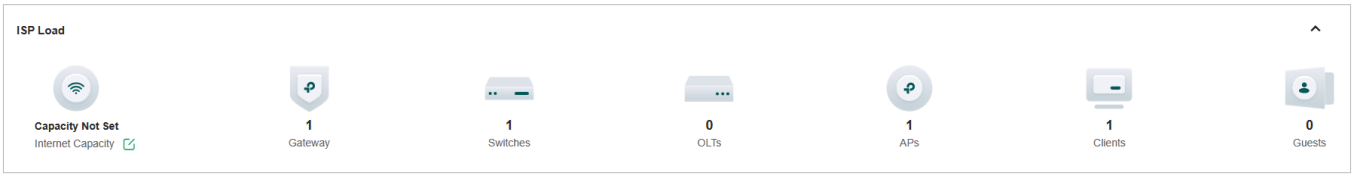
6. 1. 1 Page Layout of Dashboard

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



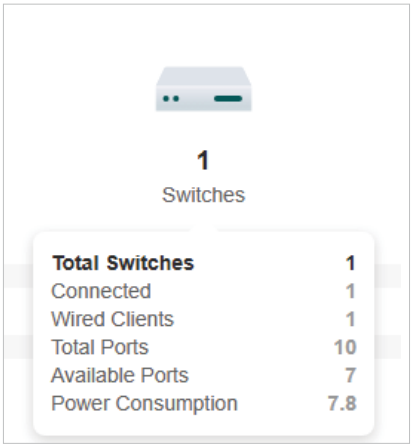
Topology Overview

Topology Overview on the top shows the status of ISP Load and numbers of devices, clients and guests.



You can hover the cursor over the gateway, switch, AP, client or guest icons to check their

status. For detailed information, click the icon here to jump to the Devices or Clients section.



Tab Bar

You can customize the widgets displayed on the tab for Dashboard page. Three tabs are created by default and cannot be deleted.



Overall	Displays the network overview information.
Network	Displays network information such as Alerts, Wi-Fi Traffic Distribution, and more.
Clients	Displays client information such as Most Active Clients, Clients Freq Distribution, and more.

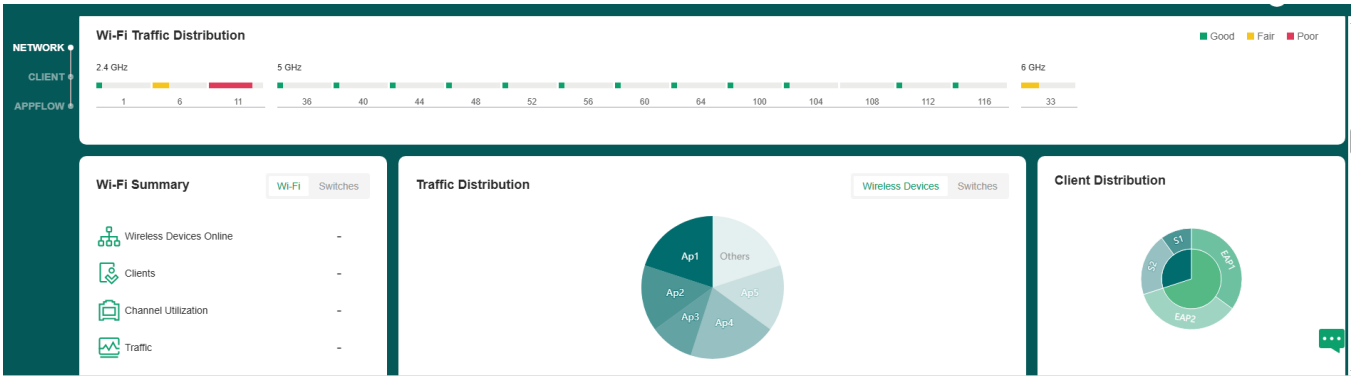
In the tab bar, you can take the following action to edit the tabs and customize the widget to be displayed.

	Click the icon to edit the tabs. For the default tabs, you can reset them to the default settings. For a created tab, you can edit its name or delete it.
+	Click the icon and enter the name in the pop-up window to create a new tab.

	Click the date to display a calendar. To quickly display the statistics of today, yesterday, last 24 hours, or last several days, click the default date/period at the right side in the calendar. To display the statistics of a specific date, click the date twice in the calendar. To display the statistics of a specific time range, click the start date and end date in the calendar.
	Click a tab and then click a widget in the pop-up page to add it to this tab or remove it.

6. 1. 2 Explanation of Widgets

The widgets are divided into different categories. You can click the setting icon to add or remove the widgets.



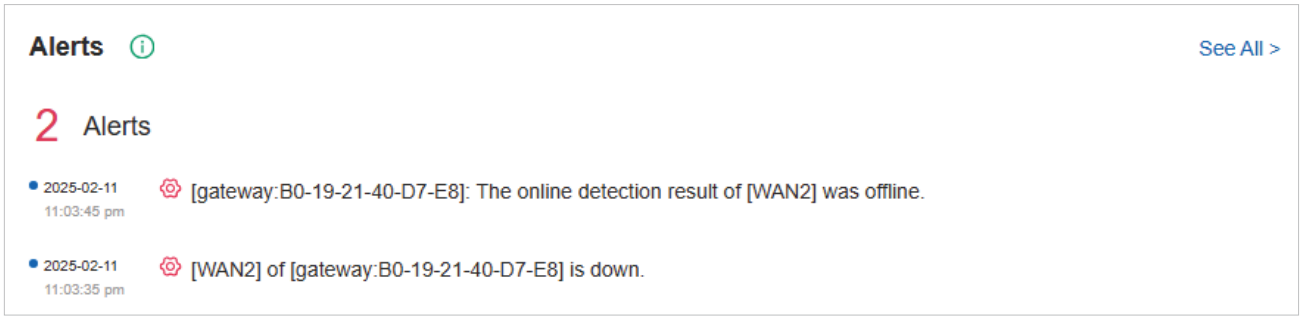
Network

Network widgets use lists and charts to illustrate the traffic status of wired and wireless networks in the site.

- Alerts

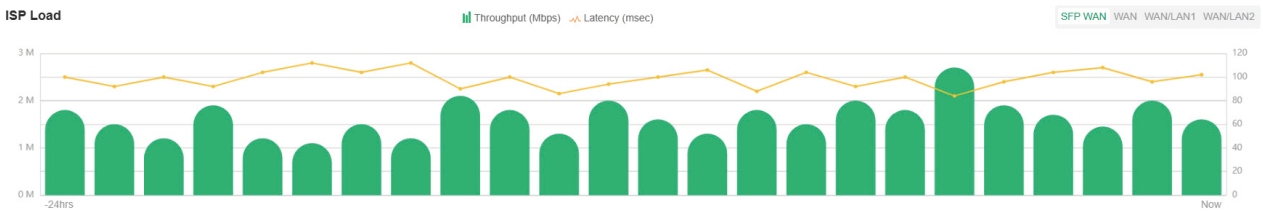
  The Alerts widget displays the total number of unarchived alerts happened in the site and details of the latest alerts. To view all the alerts and archive them, click See All to jump to

Log > Alerts. To specify events appeared in Alerts, go to Log > Notifications and configure the events as the Alert level. For details, refer to View and Manage Logs.



- ISP Load

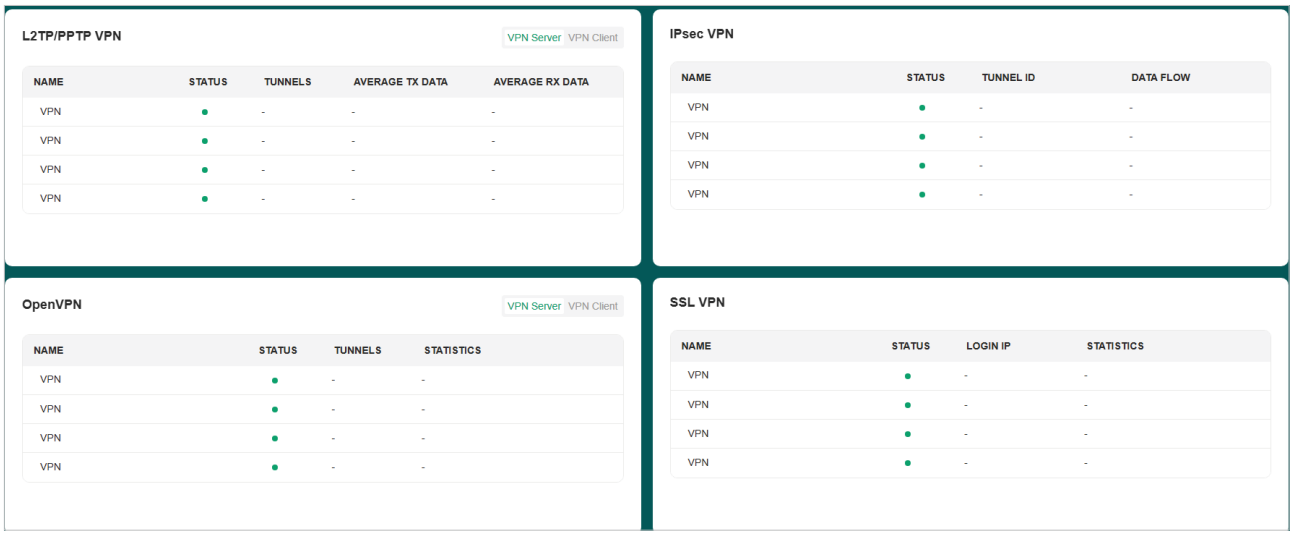
ISP Load use a line chart to display the throughput and latency of gateway's WAN port within the time range. Click the tab on the right to view the statistics of each WAN port and move the cursor on the line chart to view specific values of throughput and latency. For detailed statistics of certain gateway's WAN port within a time range, refer to View the Statistics of the Network.



To test the current download and unload speed and the latency of WAN port, click Test Speed on the widget to display the speed test result.

- VPNs

VPN widgets display the information of VPN servers and VPN clients. Click the corresponding tab to display the statistics.

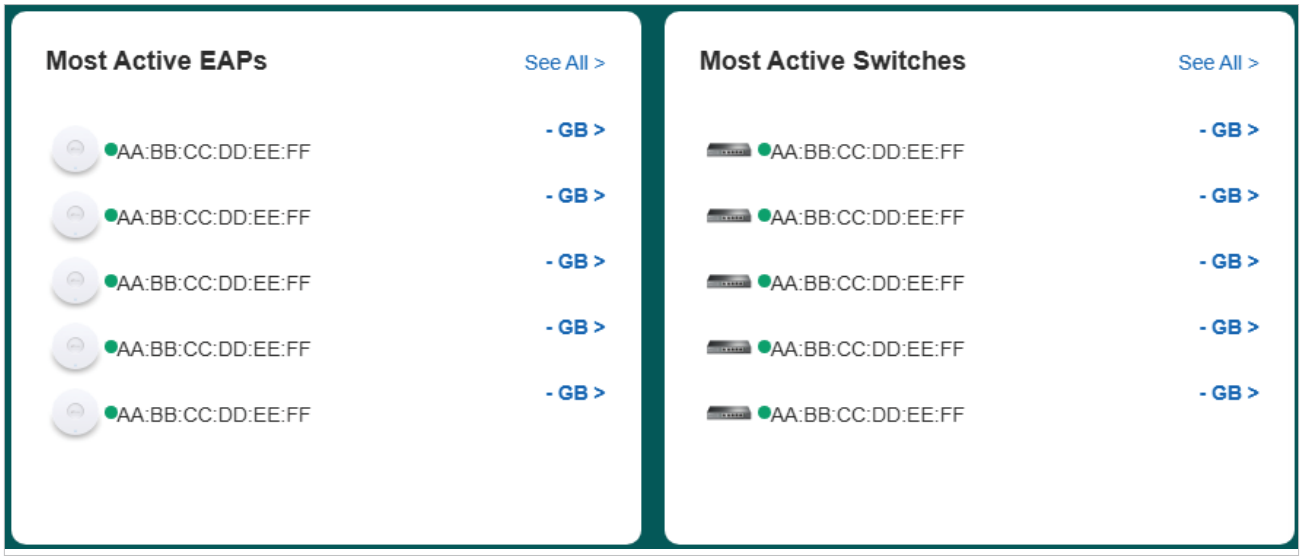


- Most Active EAPs/Most Active Switches

These two widgets can display most active EAPs and switches in the site based on the total number of traffic within the time range. Only the devices that has been adopted by the controller will be displayed.

To view all the devices discovered by the controller, click See All to jump to the Devices section. You can also click the traffic number in the widget to open the device's Properties

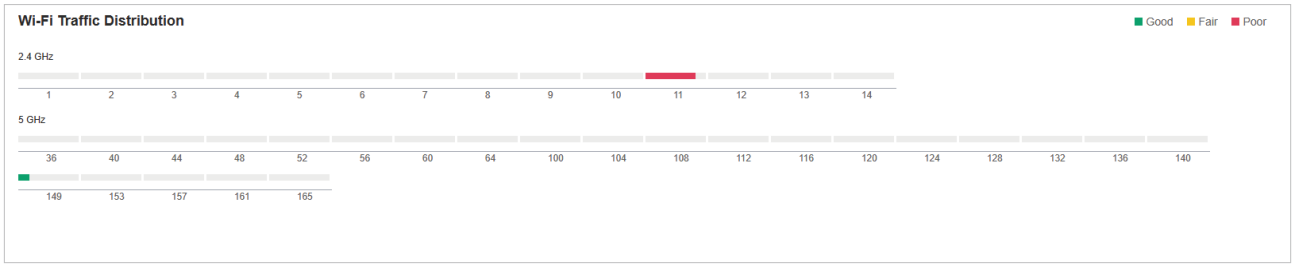
window for further configurations and monitoring. For details, refer to Configure and Monitor Controller-Managed Devices.



- Wi-Fi Traffic Distribution

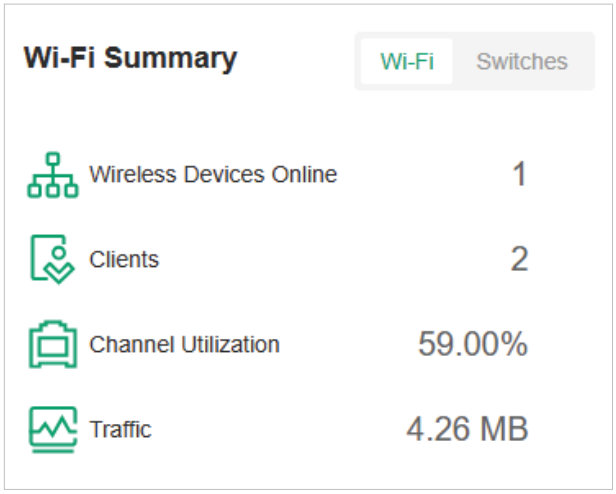
The Wi-Fi Traffic Distribution widget displays channel distribution of all connected EAPs in the site. Good, Fair, and Poor are used to describe channel status which indicates channel

interference from low to high. You can hover your cursor over the band to view the number of EAPs and clients on the channel.



- Wi-Fi Summary

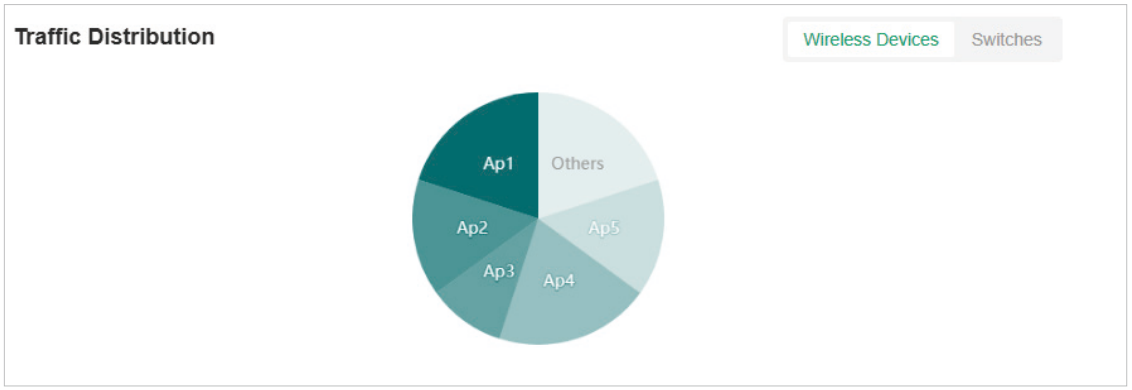
The Wi-Fi Summary widget summarizes the real-time status of wireless networks in the site, including the number of connected EAPs and clients, the channel utilization, and the total number of traffic within the time range.



- Traffic Distribution

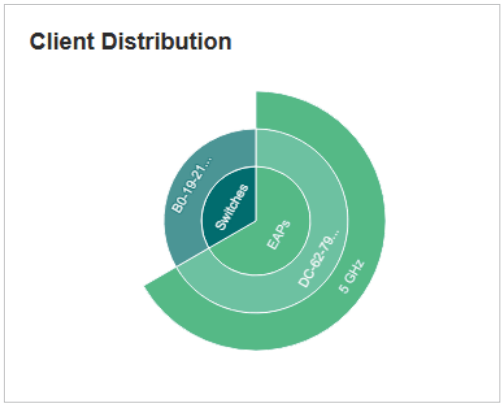
The Traffic Distribution widget uses a pie chart to display the traffic distribution on EAPs and switches in the site within the time range. Click the tab to display the statistic of EAPs

or switches, and click the slice to view the total number of traffic, its proportion, and the device name.



- Client Distribution

The Client Distribution widget uses a sunburst chart to display the real-time distribution of connected clients in the site. The chart has up to three levels. The inner circle is divided by the device category the clients connected to, the middle is by the device name, and the outer is by the frequency band. You can hover the cursor over the slice to view specific values.



- Traffic Activities

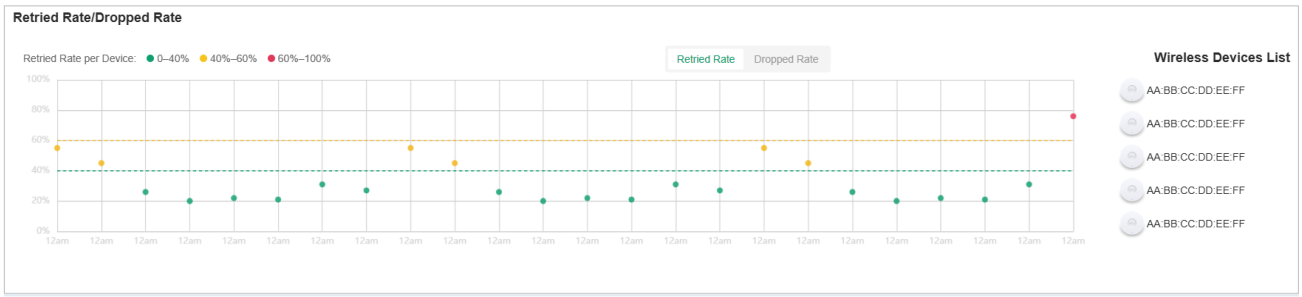
The Traffic Activities widget displays the Tx and Rx data of EAPs and switches within the time range. Only activities of the devices in the connected status currently will be counted.

Click the tab to display the statistic of EAPs or switches, and move the cursor on the line chart to view specific values of traffic. For detailed statistics of certain devices within a time range, refer to View the Statistics of the Network.



- Retried Rate/Dropped Rate

The Retried Rate/Dropped Rate widget displays the rate of retried and dropped packets of the connected EAPs within the time range. Select an AP from the list and click the tab to display the chart of retried rate or dropped rate. You can move the cursor on the point to view specific values.

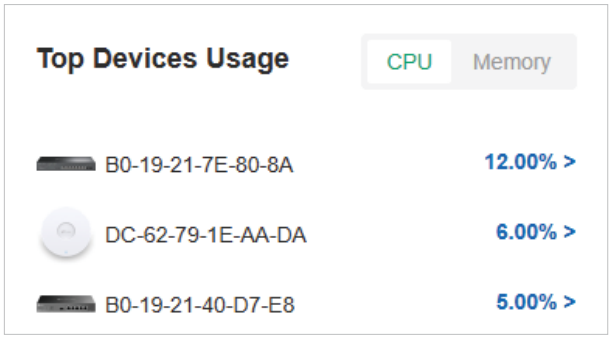


Retried Rate	Displays the percentage of packets that needed to be re-sent because they were corrupted upon arriving at the proper destination.
Dropped Rate	Displays the percentage of packets that were dropped before reaching their intended destination.

- Top Devices Usage

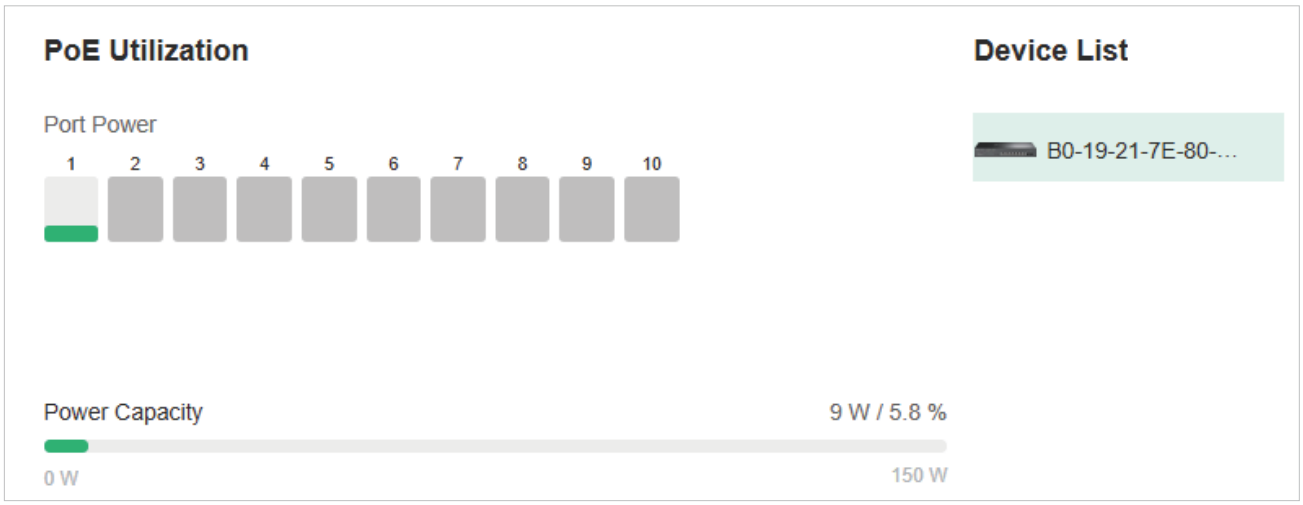
The Top Devices Usage widget displays the CPU utilization and memory utilization of devices within the time range. Click the tab to select the CPU or memory for display. Click the traffic

number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to Configure and Monitor Controller-Managed Devices.



- PoE Utilization

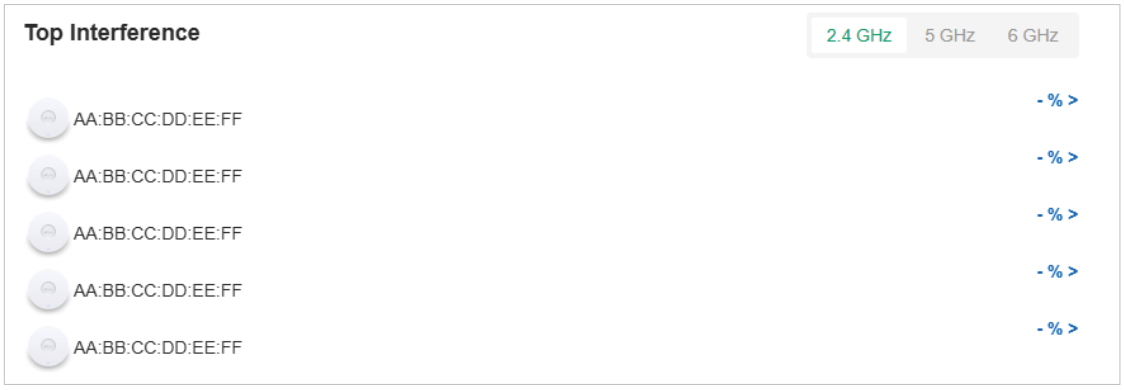
The PoE Utilization widgets describes the PoE utilization of a switch. Select a switch from the switch list to display the ports connected to PoE devices. You can hover the cursor over a certain port to view specific values. The bar below displays the current power capacity provided by PoE and its proportion of the PoE budget.



- Top Interference

The Top Interference widget displays the environment interference of wireless products. Click the tab to select the band. Click the traffic number in the widget to open the device's

Properties window for further configurations and monitoring. For details, refer to Configure and Monitor Controller-Managed Devices.



Client

Client widgets use lists and charts to illustrate the traffic status of wired and wireless clients in the site.

- Most Active Clients

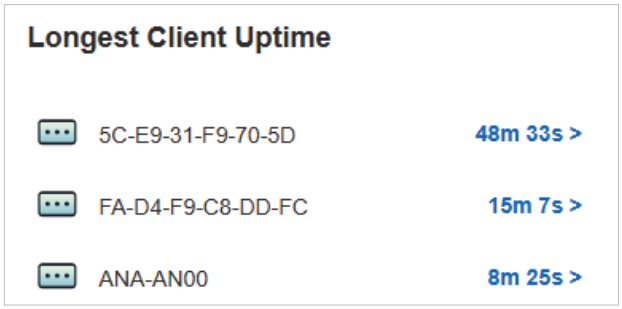
  The Most Active Clients widget can display most active clients. Only the clients in the connected status currently will be displayed.
  To view all the clients connected to the network, click See All to jump to the Clients section. You can also click the traffic number in the widget to open the client's Properties window for further configurations and monitoring. For details, refer to Manage Wired and Wireless Clients in Clients Page.



- Longest Client Uptime

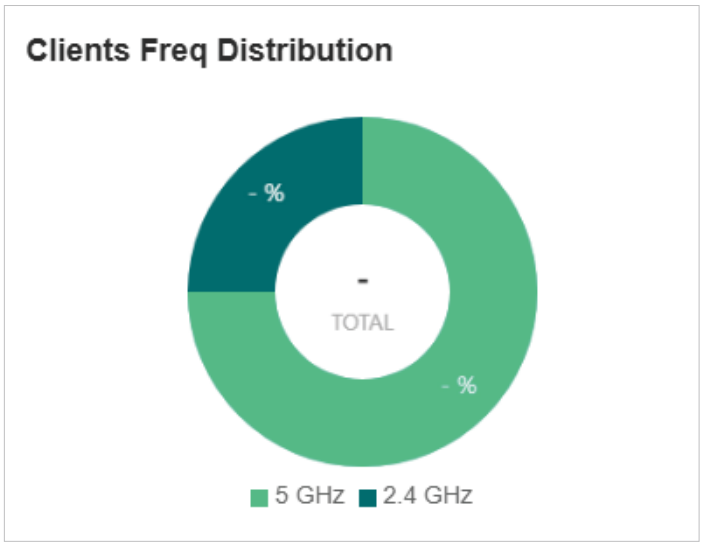
  The Longest Client Uptime widget can display top clients sorted by the uptime. Only the clients in the connected status currently will be displayed. You can also click the uptime in

the widget to open the client's Properties window for further configurations and monitoring. For details, refer to 7.1 Manage Wired and Wireless Clients in Clients Page.



- Clients Freq Distribution

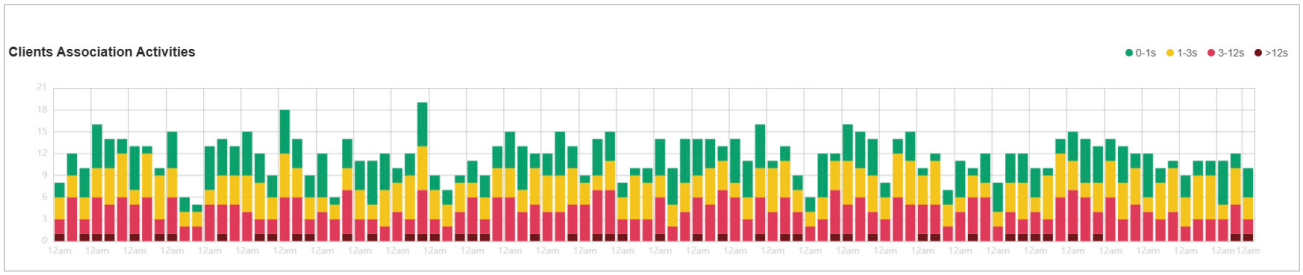
The Clients Freq Distribution widget uses a donut chart to display the distribution of wireless clients connected to the bands in the site. The chart has two levels. The inner circle shows the total number of wireless clients, and the outer displays the proportion of clients that connect to the two bands. You can hover the cursor over the slice to view the number of clients in a band.



- Clients Association Activities

The Clients Association Activities widget displays how the number of client connected to EAPs changes over time and the duration during which the clients communicate with the EAPs. In the stacked chart, you can easily compare the total number of clients and analyze the variation of each time period.

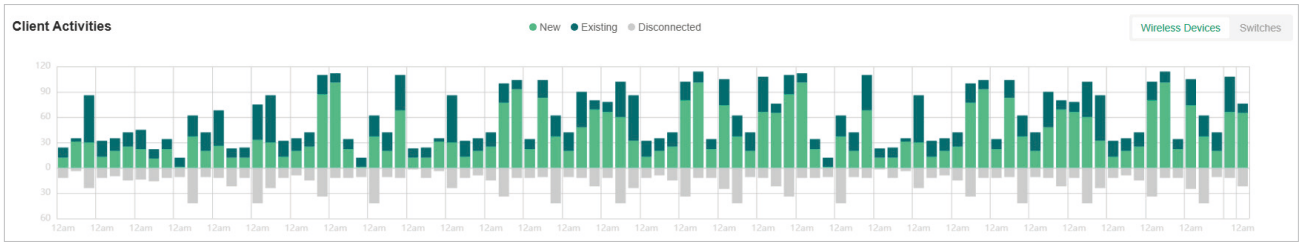
The total value of a column shows the total number of clients connected to EAPs in this time period, and the segments in four colors represents the client number of different durations in specific time.



- Client Activities

The Client Activities widget displays how the number of connected client changes over time within the time range. In the stacked chart, you can easily compare the total number of clients and analyze the variation of each time period.

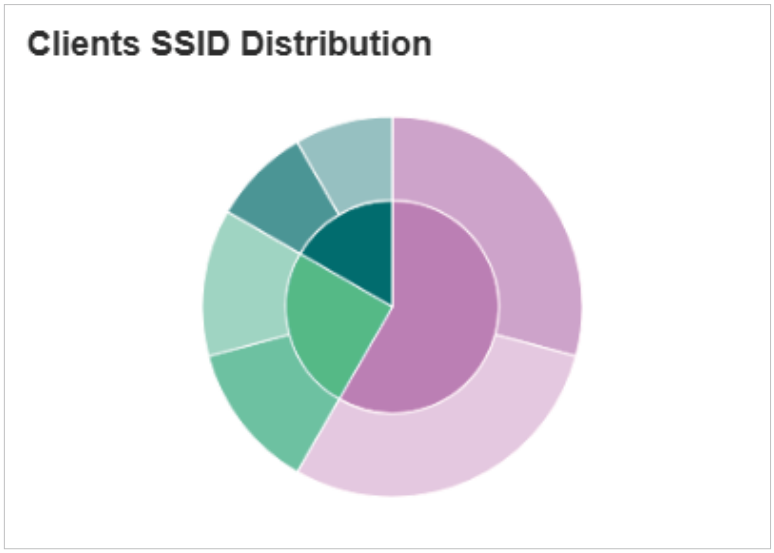
The total value of a column shows the total number of connected clients in this time period, and the segments in three colors shows the change of client number compared with the last time period. Blue represents the newly connected clients, orange is the clients have been connected in the last period, and gray is the newly disconnected clients.



- Clients SSID Distribution

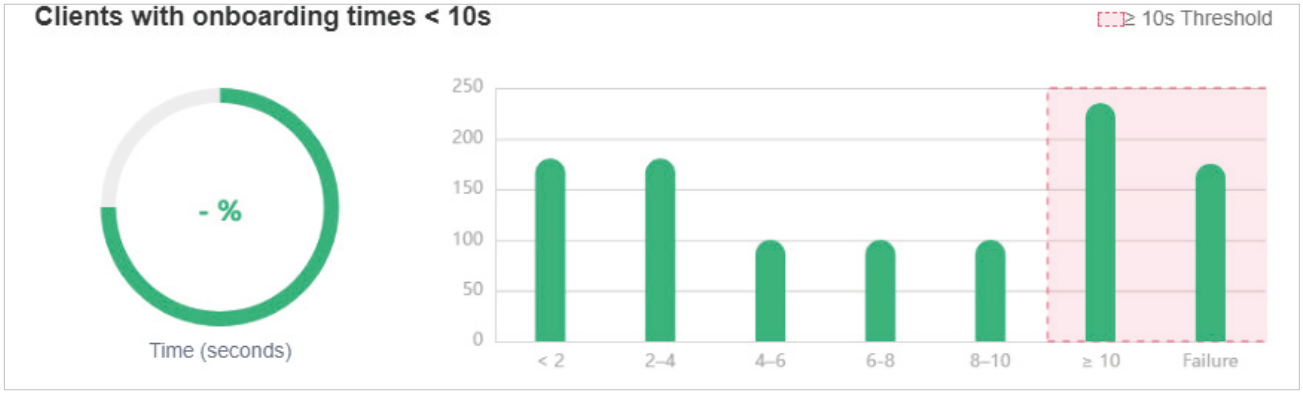
The SSID Distribution widget uses a sunburst chart to display the distribution of wireless clients connected to the different SSIDs in the site. The chart has two levels. The inner circle is divided by the EAP's SSID that the clients connected to, and the outer is by the frequency band. You can hover the cursor over the slice to view the number of clients

connected to the SSID in a band. Click a certain SSID to further display the statistics of its band frequency distribution.



- Clients with Onboarding Times

The Clients with Onboarding Times widget describes the time wireless clients uses when connecting to a certain SSID. The donut chart on the left shows the proportion of clients that uses less than 10 seconds to connect to the devices. The line graph on the right displays the number of clients according to the different time that the clients takes to connect to the SSIDs.



- Clients with RSSI

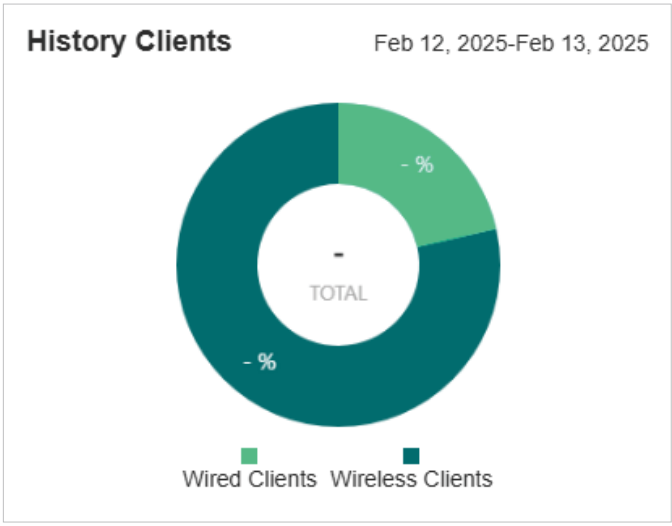
The Clients with RSSI widget describes the RSSI (Received Signal Strength Indication) that wireless clients experience in the environment. RSSI is a negative value measuring the power level being received after any possible loss at the antenna and cable level. The higher the RSSI value, the stronger the signal. The donut chart on the left shows the proportion of

clients whose RSSI value is bigger than -72 dBm. The line graph on the right displays the number of clients according to the different range values of RSSI.



- History Clients

  This widget uses a donut chart to display the distribution of wired and wireless clients in the site. The chart has two levels. The inner circle shows the total number of clients, and the outer displays the proportion of each client type. You can hover the cursor over the slice to view the number of a client type.



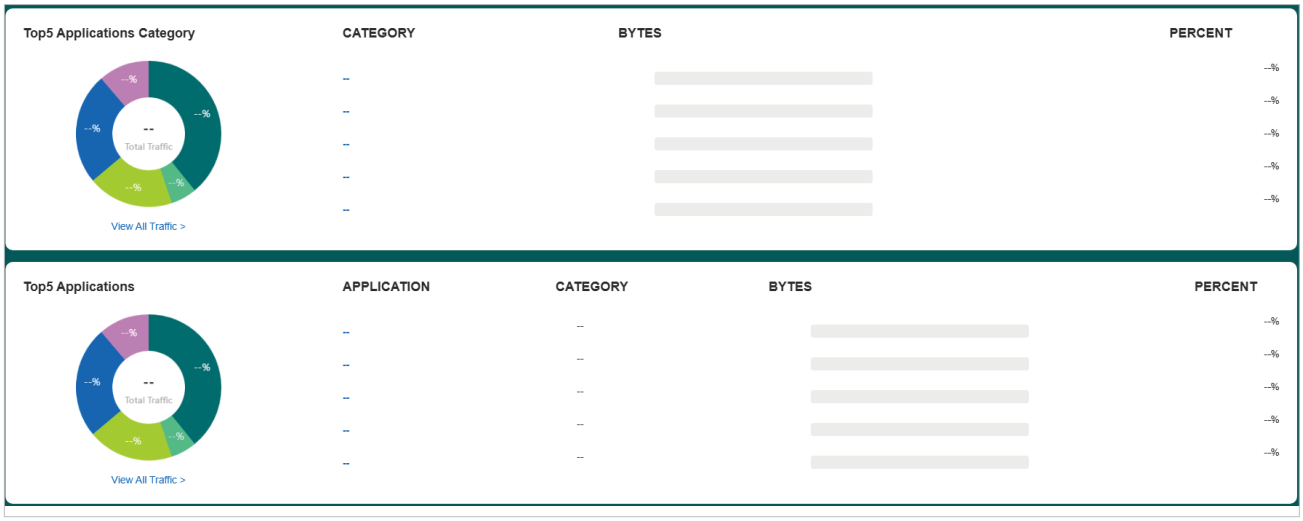
AppFlow

AppFlow widgets use lists and charts to illustrate the application information in the site.

- Top Application Categories / Top Applications

  These two widgets display top application categories and top applications in the site.

To view detailed traffic information, click View All Traffic to go to the Application Analytics page. A DPI-supported gateway is required for detailed traffic information.

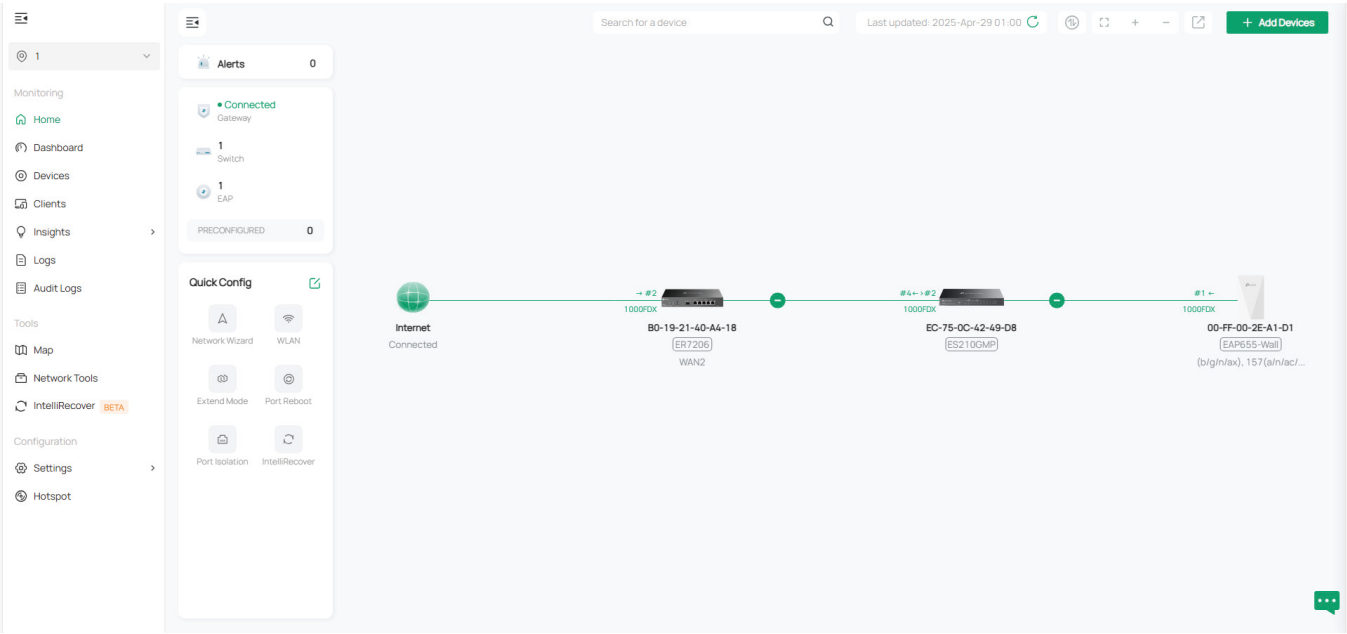


6. 2 Monitor the Network with Map

With the Map function, you can look over the topology and device provisioning of network in Topology, and customizes a visual representation of your network in Heat Map.

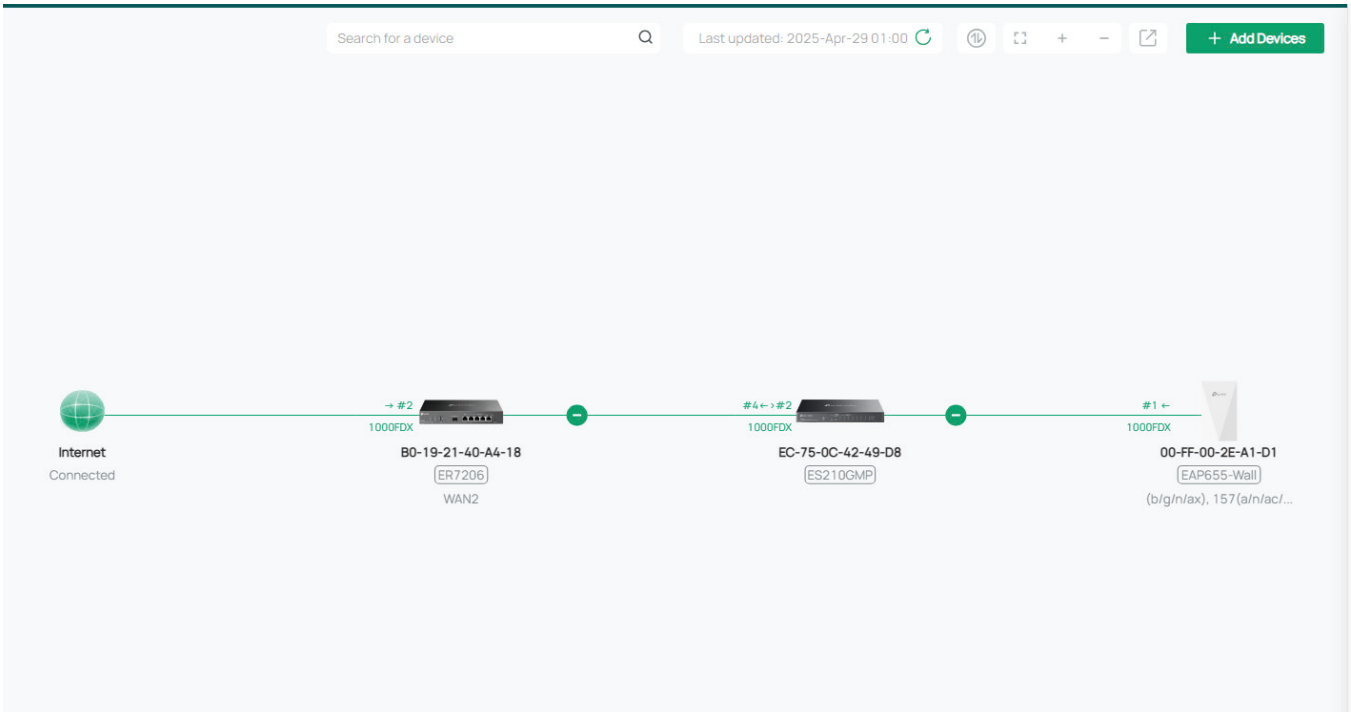
6. 2. 1 Topology

Go to Home, and you can view the topology generated by the controller automatically. You can click the icon of devices to open the Properties window. For detailed configuration and monitoring in the Properties window, refer to Manage, Configure, and Monitor Controller-Managed Devices.



For a better overview of the network topology, you can control the display of branches, the

size of the diagram, and the link labels.



- Display of Branches

  The default view shows the all devices connected by solid and dotted lines. Click the icon of the client group to view clients connected to the same device. Click the nods ⊕ to unfold or ⊖ to fold the branches.

- Diagram Size

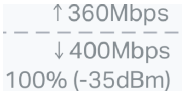
  Click the icons at the right corner to adjust the size of the topology and view the legends.

⛶	Click to fit the topology to the web page.
+	Click to zoom in the topology.
—	Click to zoom out the topology.

ⓘ	Click to view the meaning of lines in the topology. Solid and dotted lines are used to indicate wired and wireless connections, respectively, and four colors are used to indicate the link speed.

- Link Labels

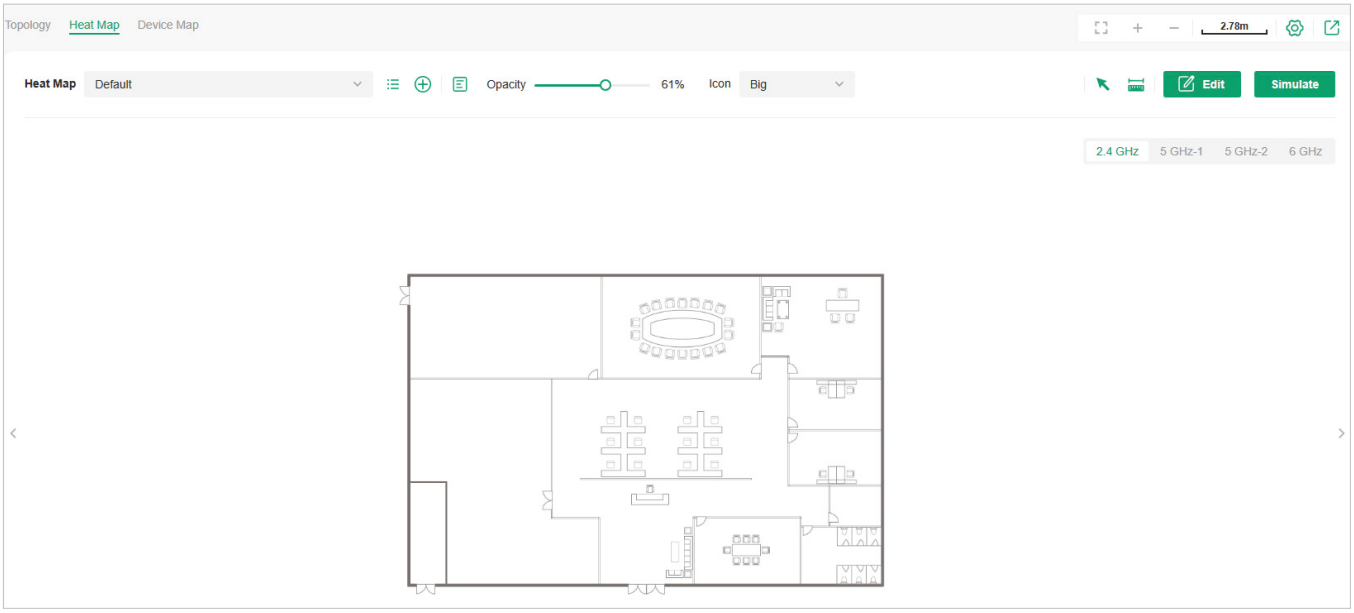
Click Link Labels at the left corner, and labels will appear to display the link status. Information on the labels varies due to the link connections.

	(For the WAN port of the gateway connected to the internet) Displays the port name, link speed and duplex type.
	(For simple wired connections) Displays the connected port number, link speed, and duplex type. Note that only the switch's port number can be displayed in the label.
	(For Link Aggregation) Displays the LAG ID, port number of LAG members, LAG speed, and duplex type.
	(For wireless connections between APs) Displays the negotiation rate of uplink and downlink and the RSSI (displayed in percentage and dBm).
	(For wireless connections between clients) Displays the connected SSID, wireless channel of AP, and its signal strength.

6. 2. 2 Heat Map

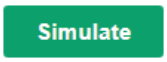
Go to Map > Heat Map, and a default map is shown as below. You can upload your local map images and add devices and different types of walls to customize a visual representation of

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 61%	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.

	Click to edit the elements including walls and devices on the map.
	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.
	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:

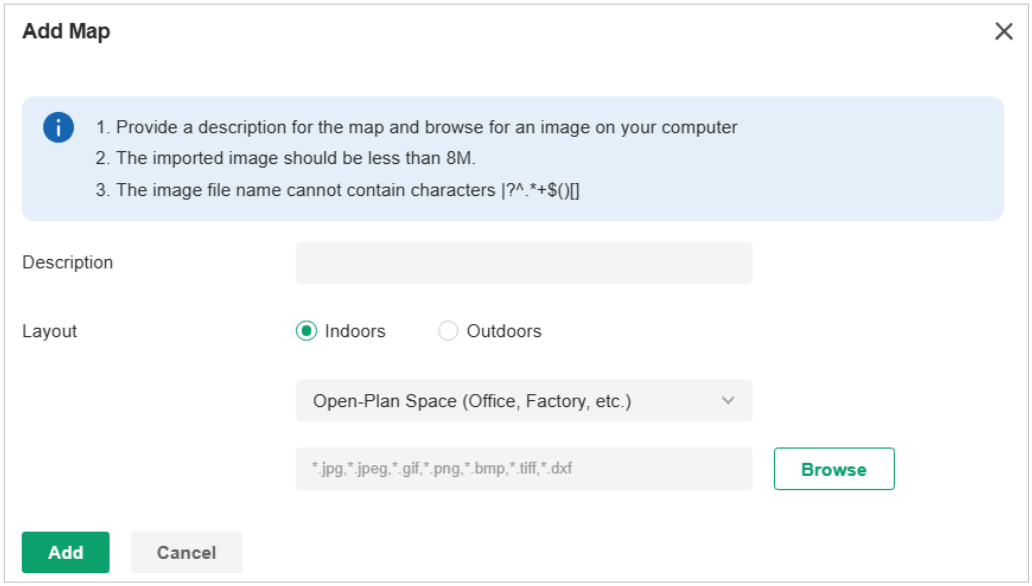
1) Add a map and configure the general parameters for the map.

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

3) View simulation results.

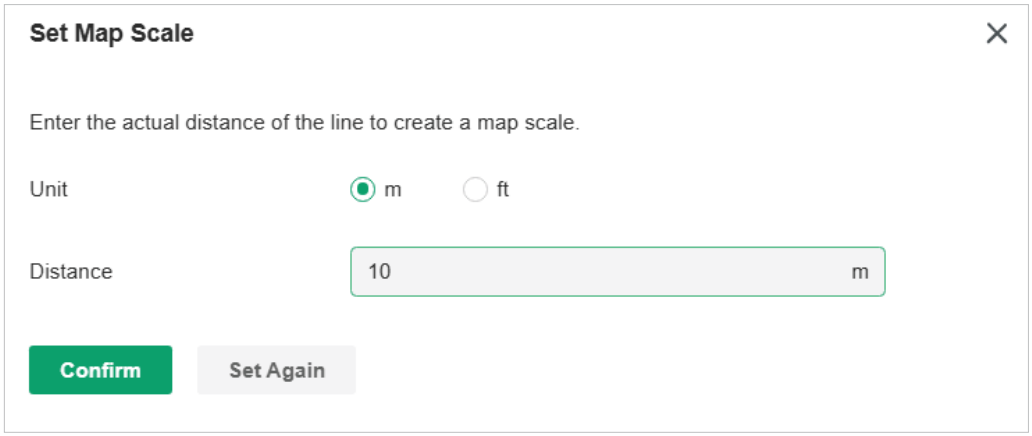
Step 1: Add Map

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



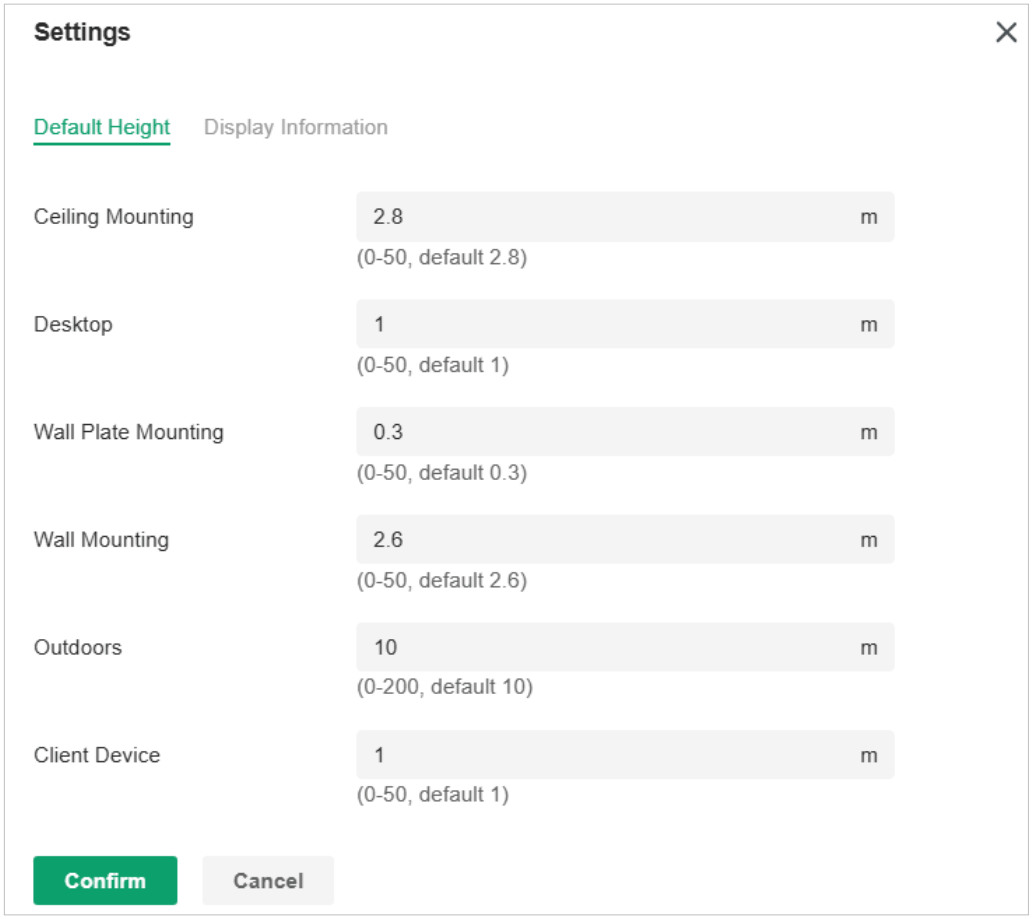
Description	Enter a description for the map.
Layout	Select the general layout of the map, which will make the simulation more accurate and the upload the map in the .jpg, .jpeg, .gif, .png, .bmp, .tiff, .dxf format. **Tip:** You can upload a CAD (.dxf) file, and the controller will automatically identify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

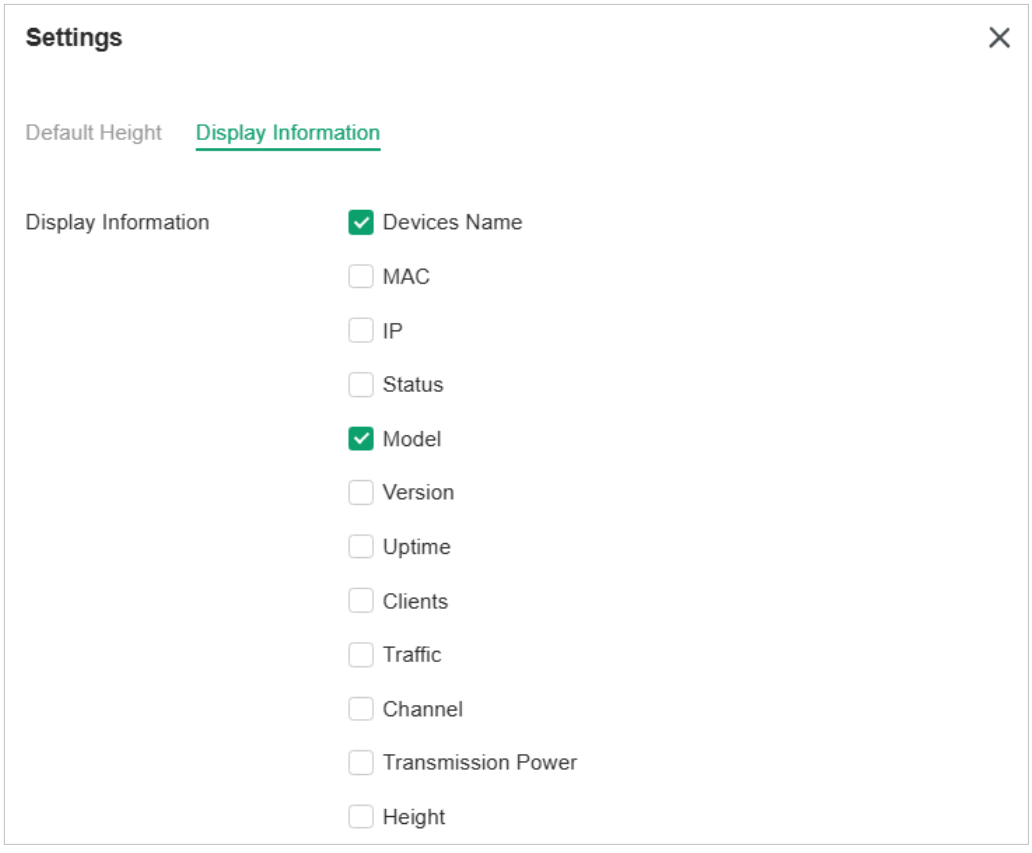
2. Click the scale icon on the upper right to set a map scale. Draw a line on the map by clicking and dragging, and then define the distance of the line.



3. Click the settings icon to set the default height of the added devices and the information

displayed on the map. Then click Confirm.

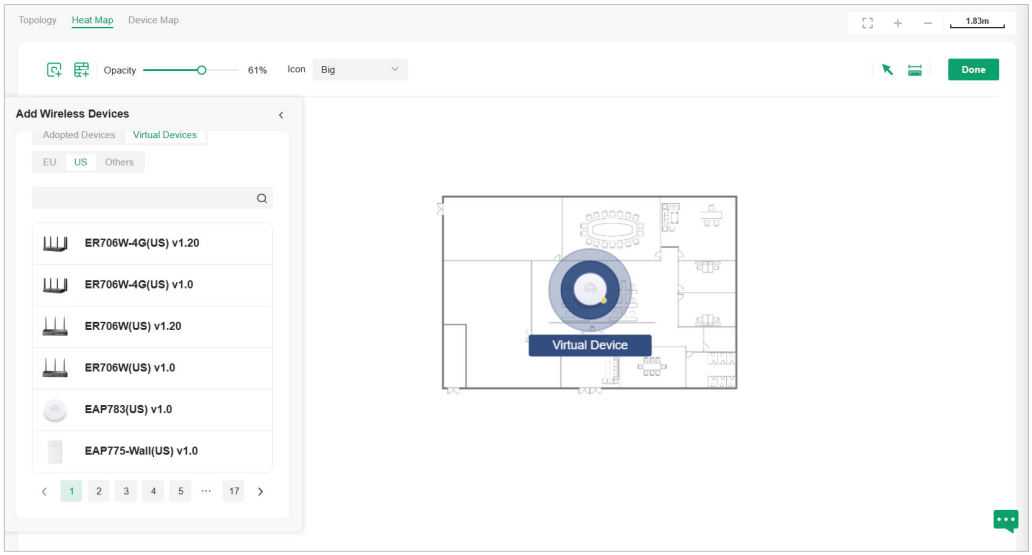




Default Height	Specify the default height for devices. You can change the height for individual device later.
Display Information	Select the information you want to see on the map.

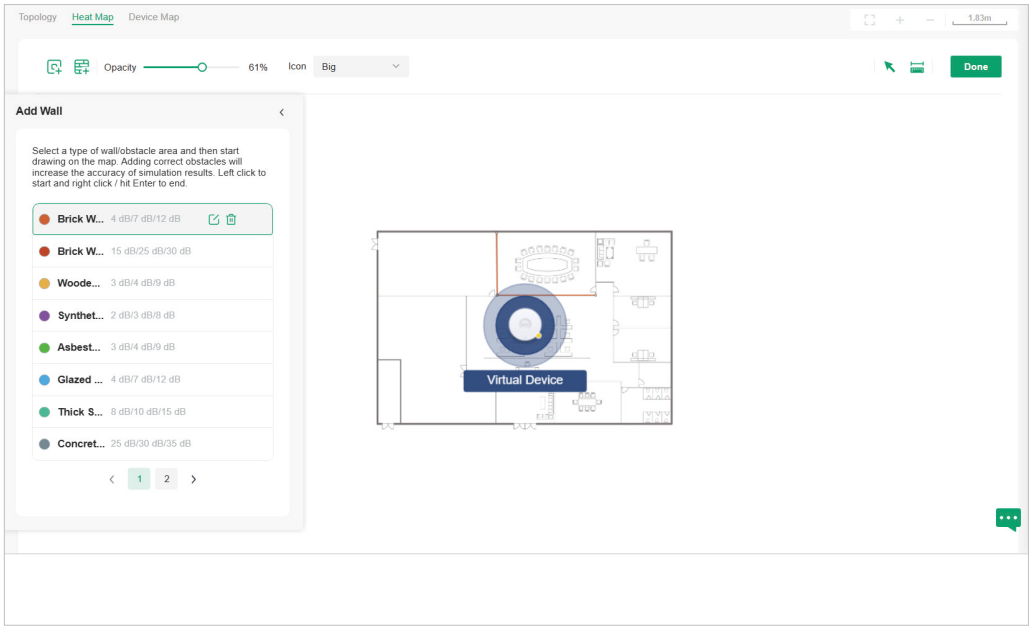
Step 2: Add Devices and Walls

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.

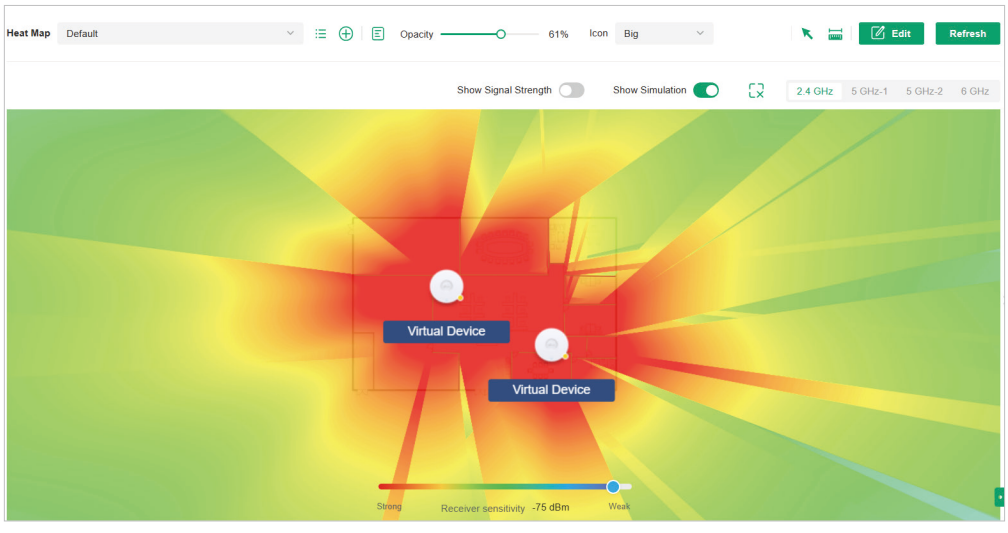


4. Click the Done icon to exit the editing status of the map.

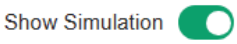
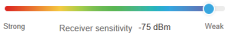
Step 3: View and Export Results

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.

	Enable or disable the display of simulation results on the map.
	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.
	Adjust the receiver sensitivity, and the new settings will take effect after refreshing the simulation.

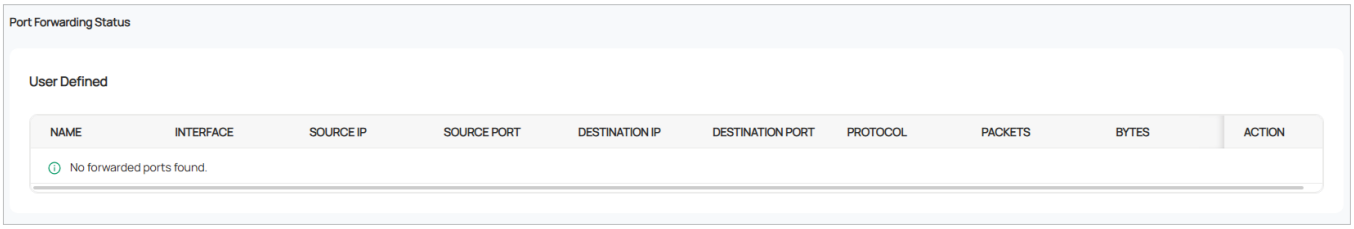
2. (Optional) If you want to export a network coverage report, click the Export icon on the upper right to export a report in .docx format.

6. 3 View Statistics During Specified Period with Insight

In the Insight page, you can monitor the port forwarding status and the uses of the dynamic DNS services.

6. 3. 1 Port Forwarding Status

In Port Forwarding Status, a table displays information about the port forwarding entries used by the gateway managed by the controller.



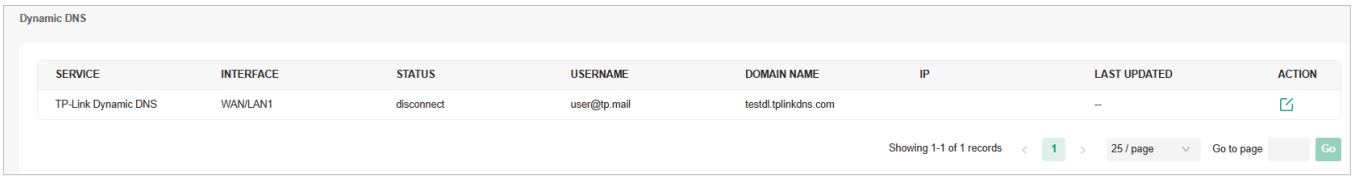
The listed information is explained as follows.

Name	Display the name of the port forwarding entry.
Interface	Display the WANs used by the port forwarding entry.
Source IP	(Only for user-defined entries) Display the source IP address. A specific IP address/Mask: The specified source IP address. 0.0.0.0/0: All IP addresses are set as the source IP address.
Source Port	The traffic through the source port, also known as internal port, will be forwarded to the LAN.
Destination IP	Display the destination IP address, and it will receive the forwarded port traffic.
Destination Port	Display the destination port, also known as internal port, that will receive the forwarded traffic.
Protocol	Display the protocol that will be forwarded.
Packets	Display the number of transferred packets.
Bytes	Display the number of transferred bytes.

6. 3. 2 Dynamic DNS

In Dynamic DNS, a table displays information about the uses of the dynamic DNS services.

You can click the Edit icon in the Action column to edit the entry.



Service	Display the name of the DDNS service.
Interface	Display the WANs used by the DDNS entry.
Status	Display the status of the latest DDNS update.
Username	Display the username of the DDNS account.
Domain Name	Display domain name registered with the DDNS service.
IP	Display the IP address of the domain name.
Last Updated	Display the time when the IP address of the domain name was last updated.

6. 4 View and Manage Logs

The controller uses logs to record the activities of the system, devices, users and administrators, which provides powerful supports to monitor operations and diagnose anomalies. In the Logs page, you can conveniently monitor the logs in Alerts and Events, and configure their notification levels in Notifications.

All logs can be classified from the following four aspects.

- Occurred Hierarchies

  Two categories in occurred hierarchies are Controller and Site, which indicate the log activities happened, respectively, at the controller level and in the certain site. Only Main Administrators can view the logs happened at the controller level.

- Notifications

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

- Severities

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

- Contents

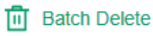
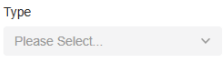
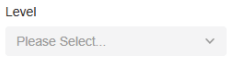
  Four types in contents are Operation, System, Device, and Client, which indicate the log contents relating to.

6. 4. 1 Alerts

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

for you to search, filter, and archive.

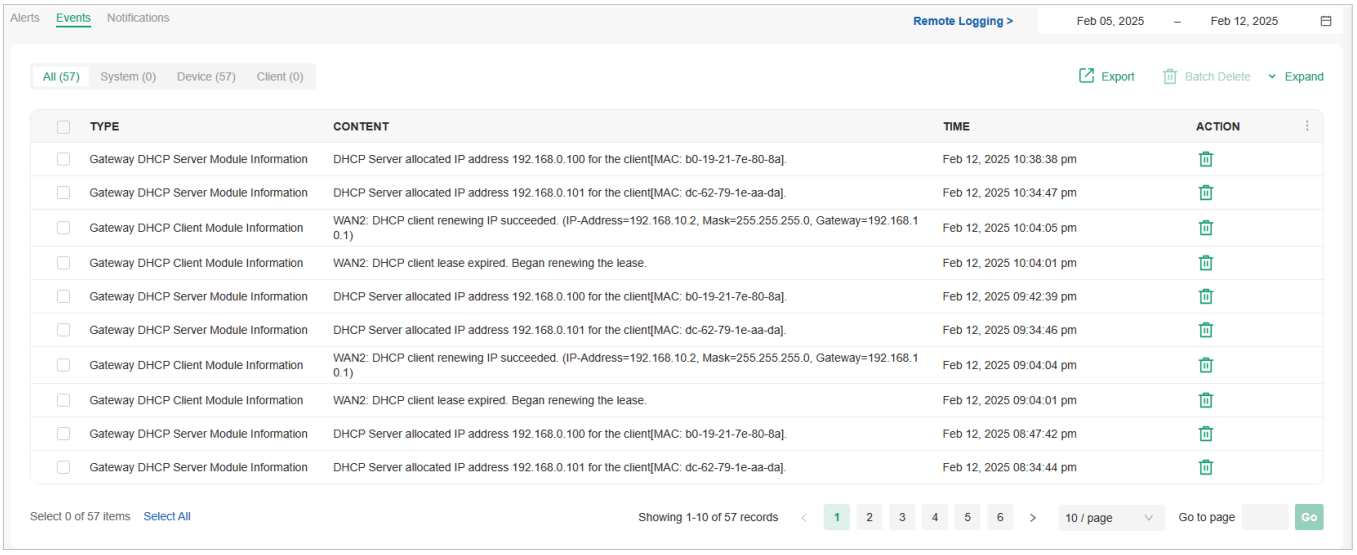


 	Click to change the view mode for a better overview. : Displays the logs in a table. : Displays the logs in graphs.
	Click the tab to filter the unresolved and resolved logs. You can click the Resolved icon or Batch Resolved to resolve a single log and all, respectively.
	Click All to display all types of logs. Click System or Deviceto display the corresponding type of logs only.
	Click to export the logs in .CSV or .XLSX format.
	Click to resolve the logs in batches.
	Click to delete the logs in batches.
 	Expand: Click to display more filters. Collapse: Click to display less filters.
	Select the content type to filter the logs.
	Select the severity levels to filter the logs.
	Enter the key words to search the logs.
Content	Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.

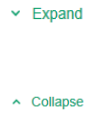
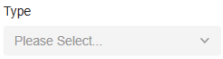
Time	Displays when the activity happened.
	Click to resolve the log entry.
	Click to delete the log entry. Once deleted the logs cannot be recovered.

6. 4. 2 Events

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

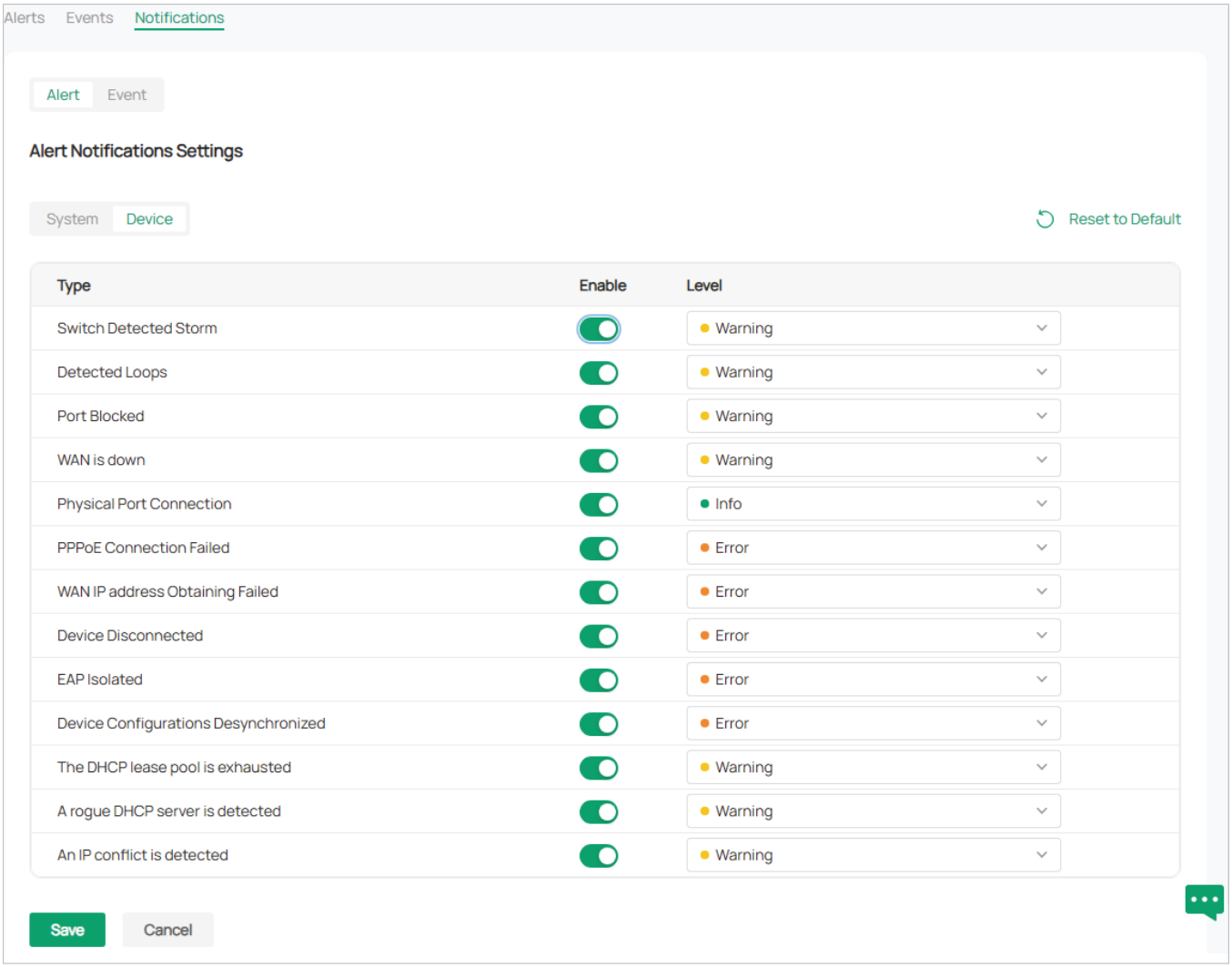


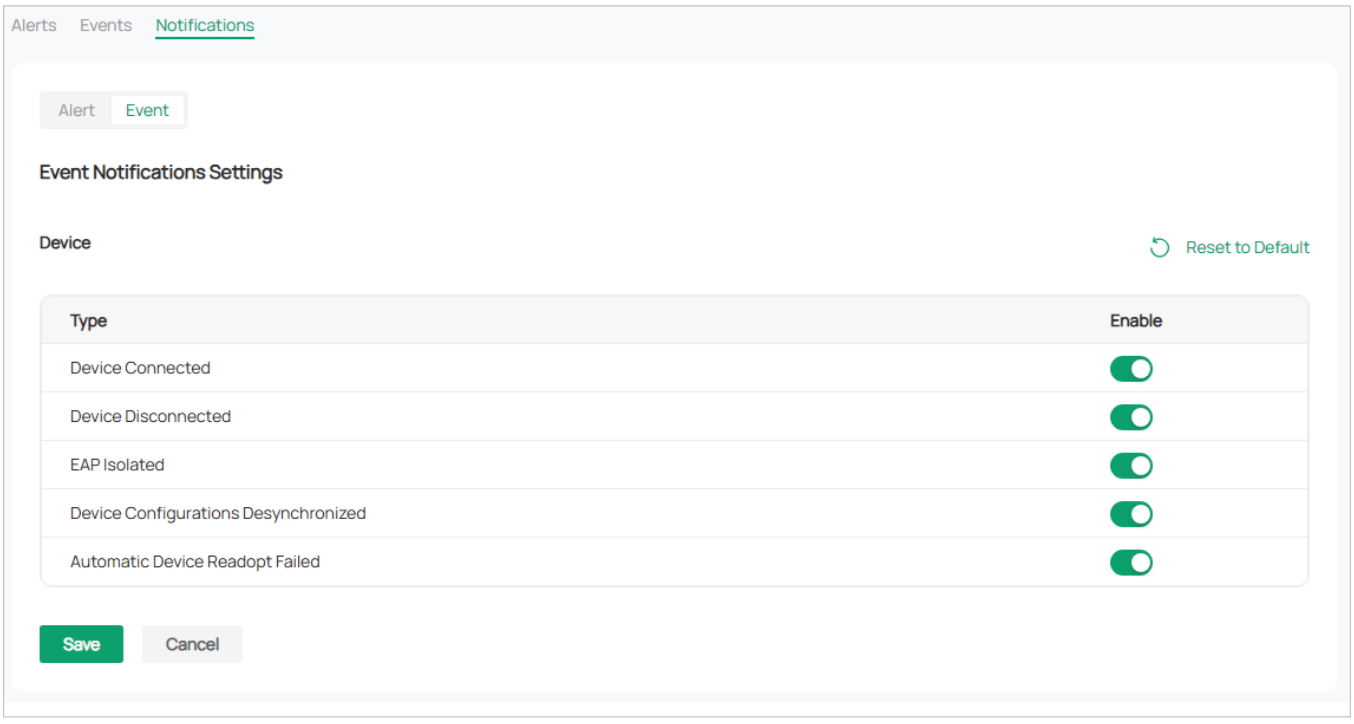
Feb 05, 2025 – Feb 12, 2025	Filter the logs based on Start Time. Click the selector to open the calendar. Click a specific date twice in the calendar to display the logs on the day. To display the logs during a time range, click the start date and end date in the calendar.
All (59) System (0) Device (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.
Batch Delete	Click to delete the logs in batches.

	Expand: Click to display more filters. Collapse: Click to display less filters.
	Select the content type to filter the logs.
	Enter the key words to search the logs.
Content	Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.
Time	Displays when the activity happened.
	Click to delete the corresponding event logs.

6. 4. 3 Notifications

In Notifications, you can find all kinds of activity logs classified by the content and specify their notification categories as Event and Alert for the current site.


Alerts
Events
Notifications
Alert
Event
Alert Notifications Settings
System
Device
Reset to Default
Type
Enable
Level
Switch Detected Storm
Warning
Detected Loops
Warning
Port Blocked
Warning
WAN is down
Warning
Physical Port Connection
Info
PPPoE Connection Failed
Error
WAN IP address Obtaining Failed
Error
Device Disconnected
Error
EAP Isolated
Error
Device Configurations Desynchronized
Error
The DHCP lease pool is exhausted
Warning
A rogue DHCP server is detected
Warning
An IP conflict is detected
Warning
Save
Cancel


Alerts
Events
Notifications
Alert
Event
Event Notifications Settings
Device
Reset to Default
Type
Enable
Device Connected
Device Disconnected
EAP Isolated
Device Configurations Desynchronized
Automatic Device Readopt Failed
Save
Cancel

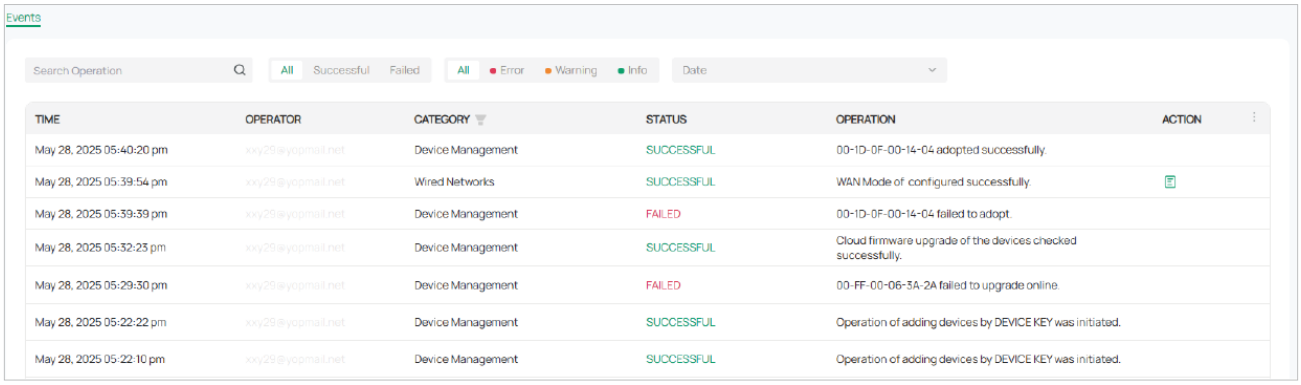
To specify the logs as Alert/Event, enable the corresponding type and click Save. The following icons and tab are provided as auxiliaries.

Reset to Default	Click to reset all notification configurations in the current site to the default.
	Click the tabs to select the activity logs, and then the enabled logs will be displayed under the Events/Alerts tab.
	Click the tabs to display the configurations of corresponding log types.

6. 5 Audit Logs

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

1. Launch your controller.
2. In the Global View or Site View, go to the Audit Logs page.
3. On the Events page, check and manage the audit logs.



6. 6 Monitor the Network with Tools

The controller provides many tools for you to analyze your network:

- Network Check

  Test the device connectivity via ping, traceroute, or DNSLookup.

- Terminal

  Open Terminal to execute CLI or Shell commands.

- Cable Test

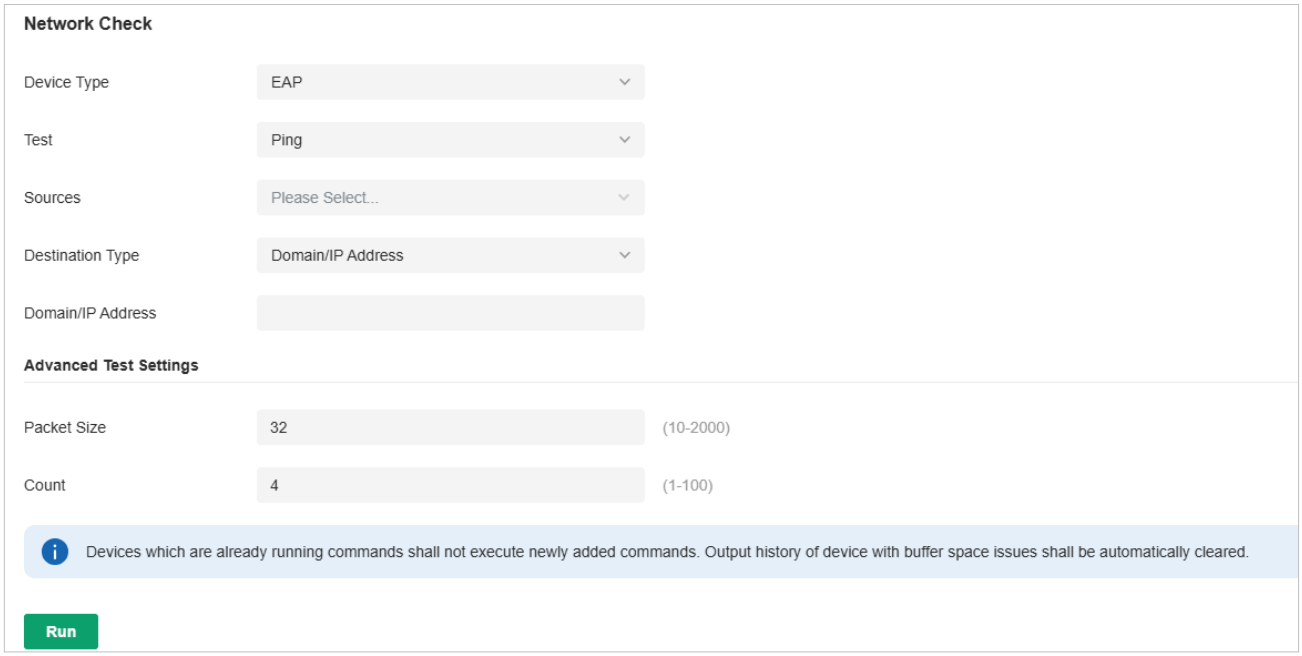
  Perform cable test to check the cable issues.

Note:

Firmware updates are required for earlier devices to support these tools.

6. 6. 1 Network Check

1. Launch the controller and access a site.
2. Go to Network Tools > Network Check.
3. Configure the test parameters.



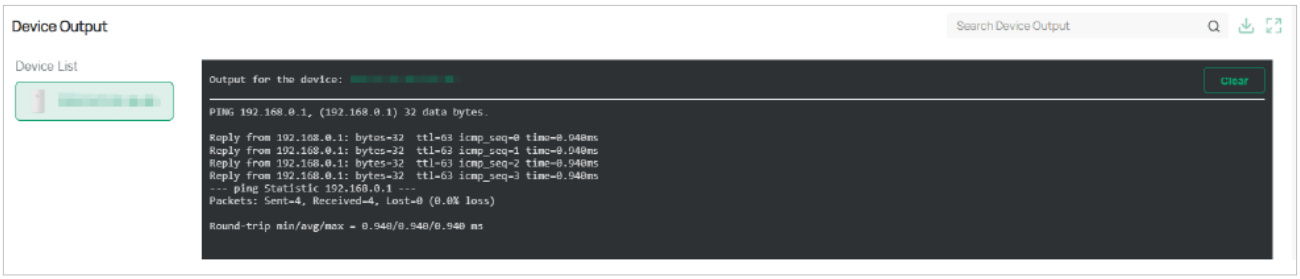
Device Type	Select the device type to perform a test.

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. DNSLookup: 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. Client is available only when an AP device performs the ping test. 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.

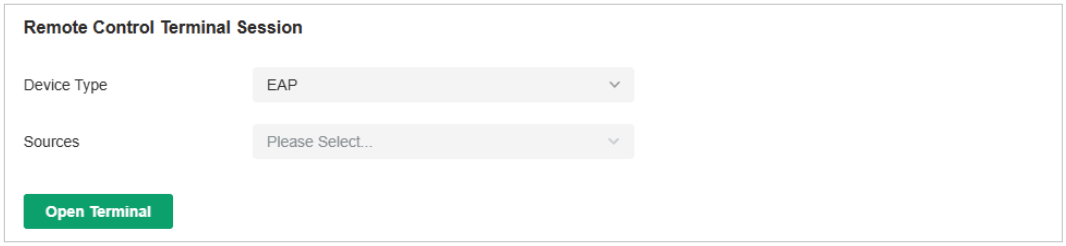
4. Click Run to perform the test. You can view the test result in the Device Output section.



You can click the Download/Zoom icons above the test result field to download the test logs locally, or zoom in/out the display area.

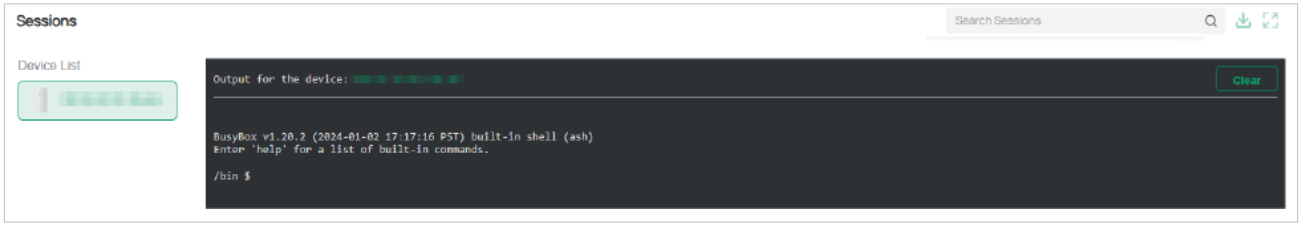
6. 6. 2 Terminal

1. Launch the controller and access a site.
2. Go to Network Tools > Terminal.
3. Configure the parameters.



Device Type	Select the device type to run CLI or Shell commands.
Sources	Select one or multiple devices to test.

4. Click Open Terminal. Now you can run CLI or Shell commands.

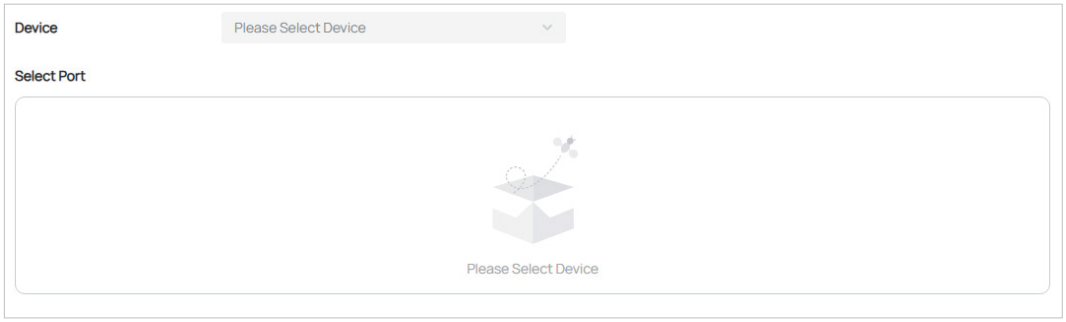


You can click the Download/Zoom icons above the test result field to download the test logs locally, or zoom in/out the display area.

6. 6. 3 Cable Test

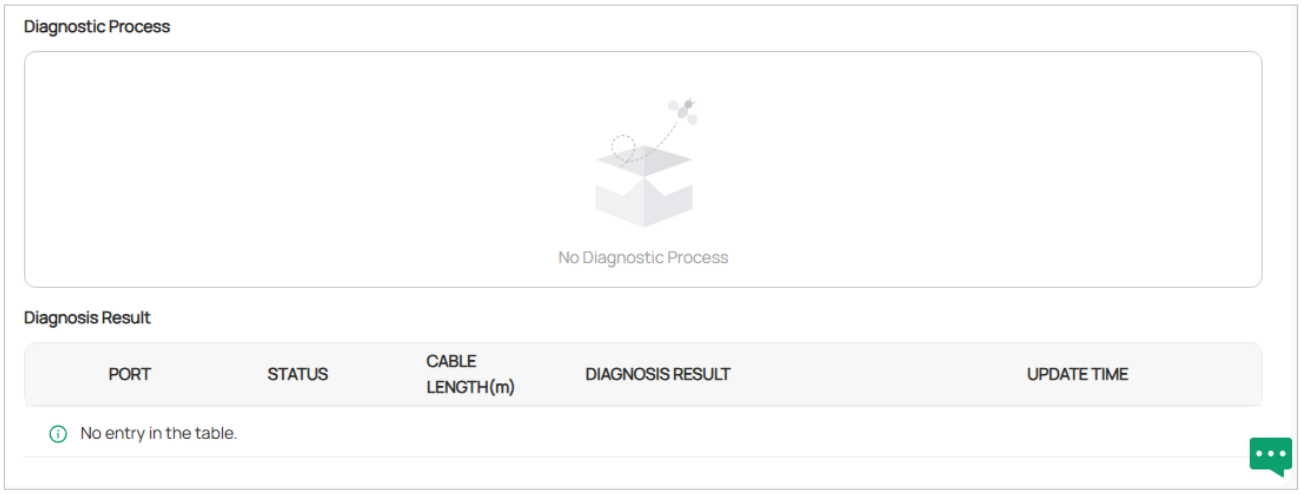
1. Launch the controller and access a site.
2. Go to Network Tools > Cable Test.

3. Configure the parameters.



Device	Select the device in the pop-up window to run the cable test.
Sources	Select the ports of the device to run the cable test.

4. After running the cable test, you can check the diagnostic process and results below.



6. 7 IntelliRecover

Overview

IntelliRecover can help you monitor the status of PoE devices, automatically repairing abnormal devices.

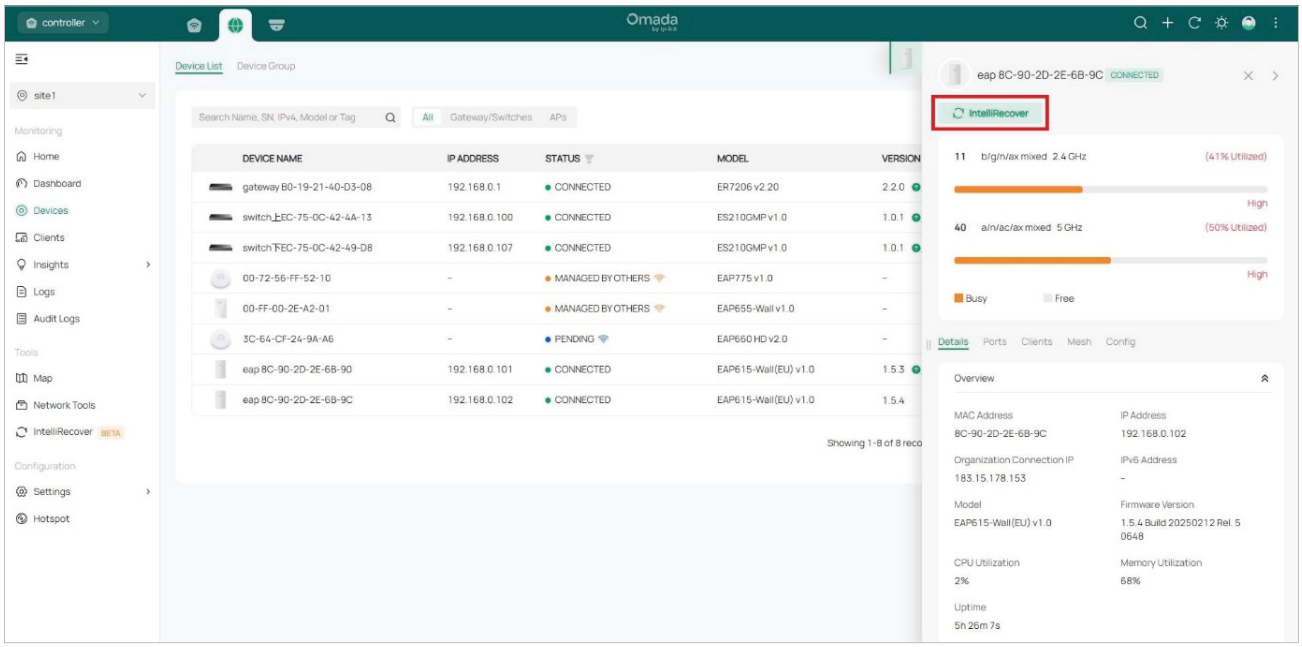
Network Preparation:

- A PoE Switch that can be managed by Omada Controller;
- EAPs, security devices, or clients powered by the PoE switch.

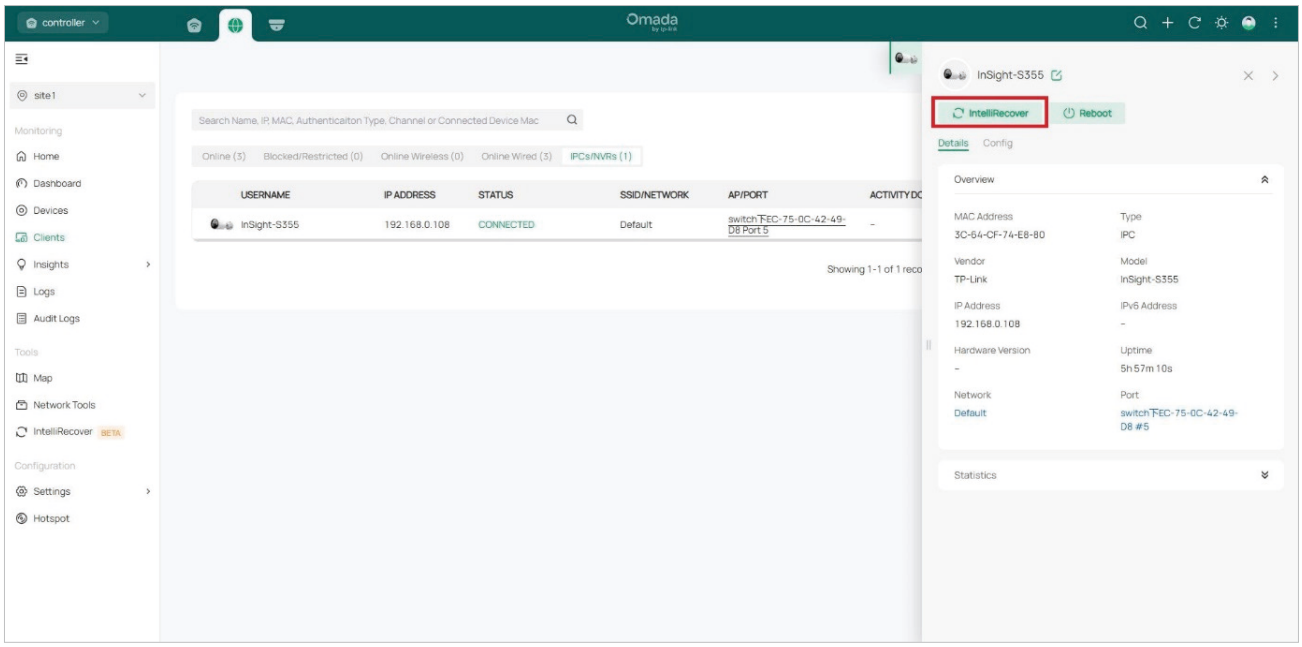
Configuration

To configure IntelliRecover, follow these steps:

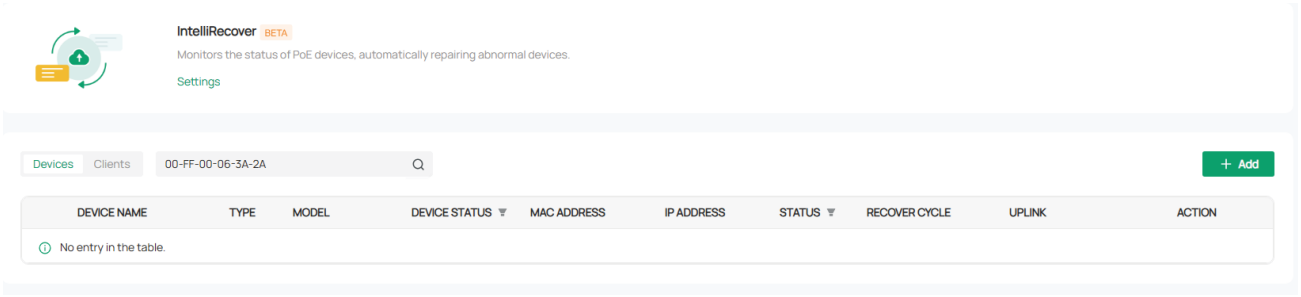
1. Launch the controller and access a site. Go to Devices. After adopting the PoE switch, and the EAP or security device directly connected to the PoE switch, click the EAP or security device to open its Properties window. Click IntelliRecover to enable the function for the device so that it can be added to the monitoring list.



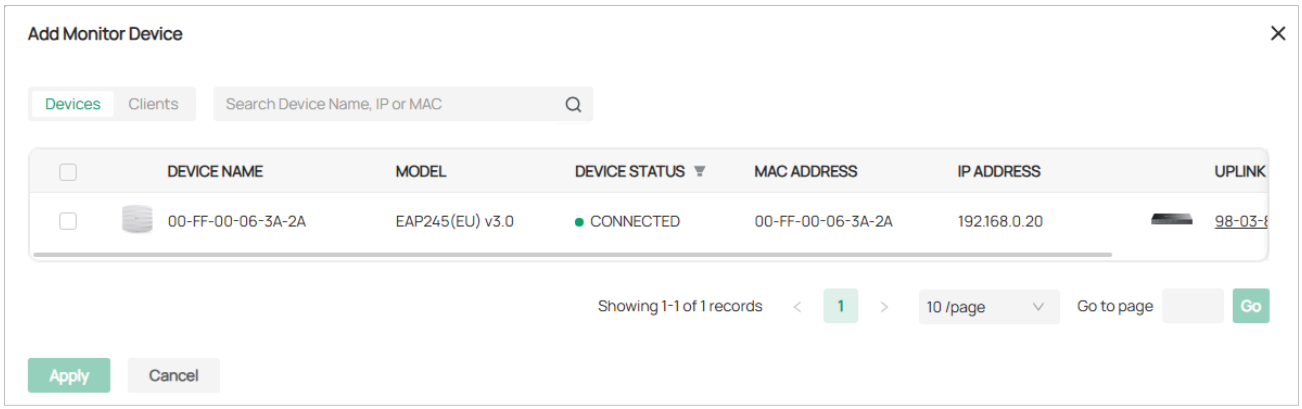
2. Go to Clients. Click the client device to open its Properties window. Click IntelliRecover to enable the function for the client so that it can be added to the monitoring list.



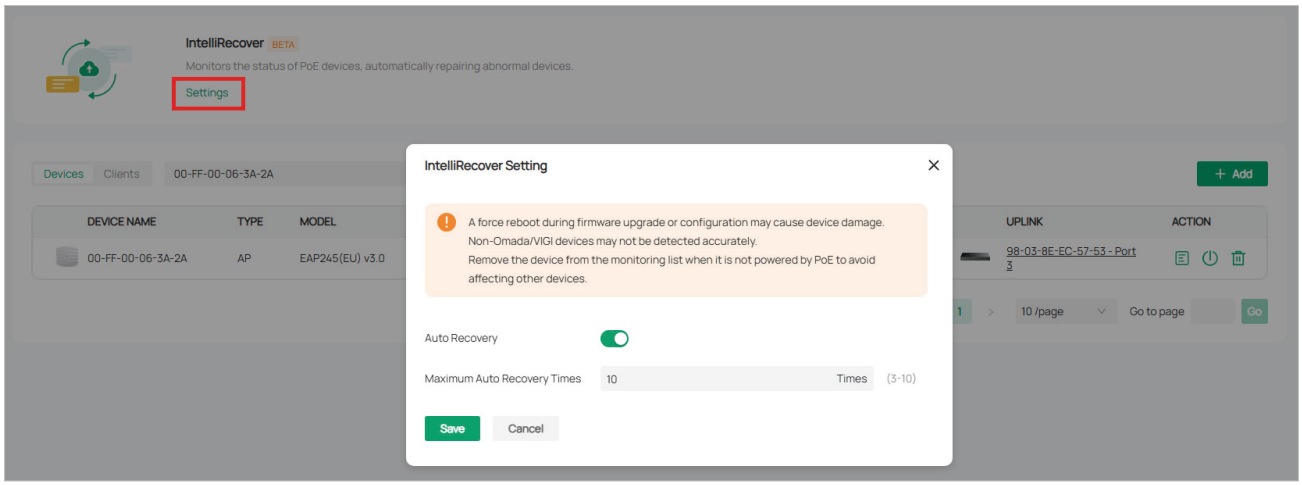
3. Go to the IntelliRecover page. Click Add to add the devices or clients to the monitoring list.



4. Select the devices or clients to be monitored and click Apply.



5. Click Settings on the IntelliRecover page and configure the parameters.



Auto Recovery	Click to enable or disable the Auto Recovery funtion.
Maximum Auto Recovery Times	Specify the maximum auto recovery times for the monitored devices. When the limit has been reached, the monitered devices will not be automatically rebooted.

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.



Chapter 7

Monitor and Manage the Clients

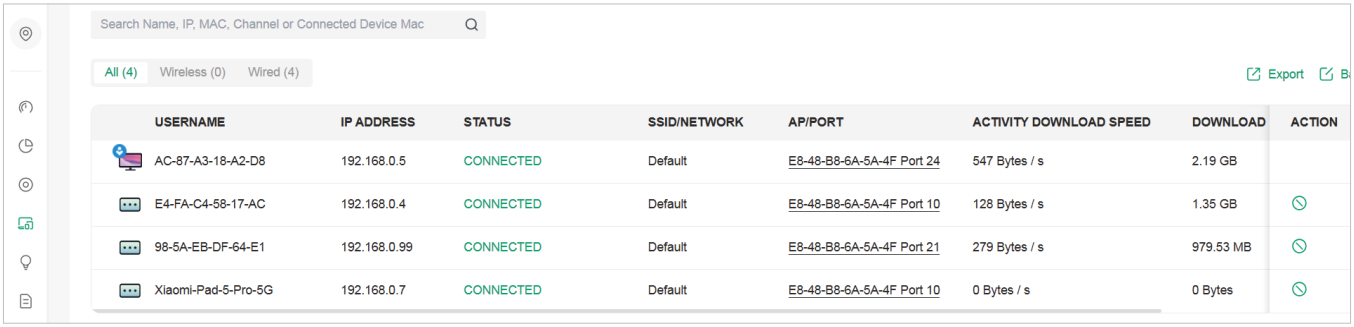
This chapter guides you on how to monitor and manage the clients through the Clients page using the clients table and the properties window and the Hotspot system. To view clients that have connected to the network in the past, refer to View the Statistics During the Specified Period with Insight. This chapter includes the following sections:

- 7.1 Manage Wired and Wireless Clients in Clients Page
- 7.2 Manage Client Authentication in Hotspot

7. 1 Manage Wired and Wireless Clients in Clients Page

7. 1. 1 Introduction to Clients Page

The Clients page offers a straight-forward way to manage and monitor clients. It displays all connected wired and wireless clients in the chosen site and their general information. You can also open the Properties window for detailed information and configurations.



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

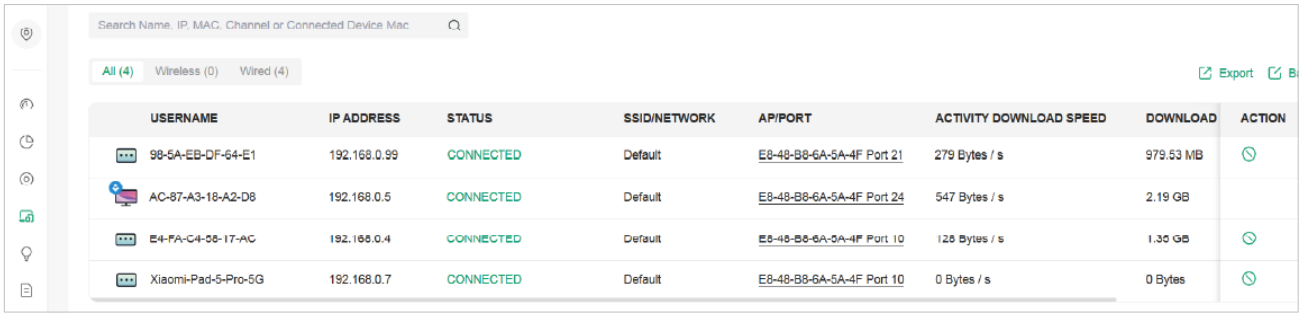
7. 1. 2 Using the Clients Table to Monitor and Manage the Clients

To quickly monitor and manage the clients, you can customize the columns and filter the clients for a better overview of their information. Also, quick operations and batch configuration are available.

- Customize the Information Columns

  Click the ellipse icon next to the Action column and you have three choices: Default Columns, All Columns, and Customize Columns. To customize the information shown in the table, click the checkboxes of information type.

To change the list order, click the column head and the ascending and descending icon appears for you to choose the display order.



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

- Filter the Clients

To search specific client(s), use the search box above the table. To filter the clients by their connection type, use the tab bars above the table. For wireless clients, you can further filter them by the frequency band and the type of connected wireless network.

Search Name, IP, MAC, Channel or Connected Device Mac	Filter clients using the search box based on username, IP address, MAC address or channel.
All (4) Wireless (0) Wired (4)	Filter clients based on their connection type.
All (0) 2.4 GHz (0) 5 GHz (0) 6 GHz (0)	(For wireless clients) Filter wireless clients based on the frequency band they are using.
All (0) Users (0) Guests (0)	(For wireless clients) Filter wireless clients based on the type of connected wireless network. Guests are clients connected to the guest network, which you can set during the Quick Setup, creating wireless networks, etc.

- Quick Operations

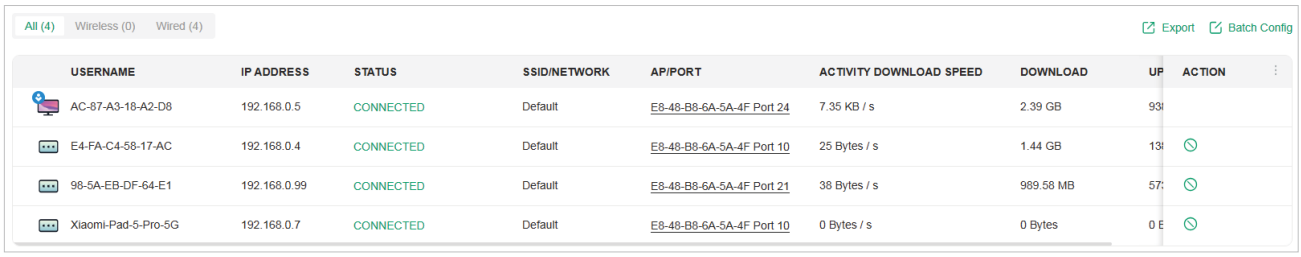
For quick operations on a single client, click the icons in the Action column. The available icons vary according to the client status and connection type.

	Click to block the client in the chosen site. You can view blocked clients in Known Clients.
	(With portal authentication enabled) Click to manually authorize the client that has not passed the portal authentication.

	(With portal authentication enabled) Click to unauthorize the client that has passed the portal authentication.
	(For wireless clients) Click to reconnect the wireless client to the wireless network.

- Multiple Select for Batch Configuration

To select multiple clients and add them to the Properties window, click Batch Config on the upper-right and then check the boxes. When you finish choosing the clients, click Done and the chosen client(s) will be added to the Properties window for batch client configuration.



7. 1. 3 Using the Properties Window to Monitor and Manage the Clients

In Properties window, you can view more detailed information about the connected client(s) and manage them. To open the Properties window, click the entry of a single client, or click the edit icon to select multiple clients for batch configuration. Use the following icons for the Properties window.

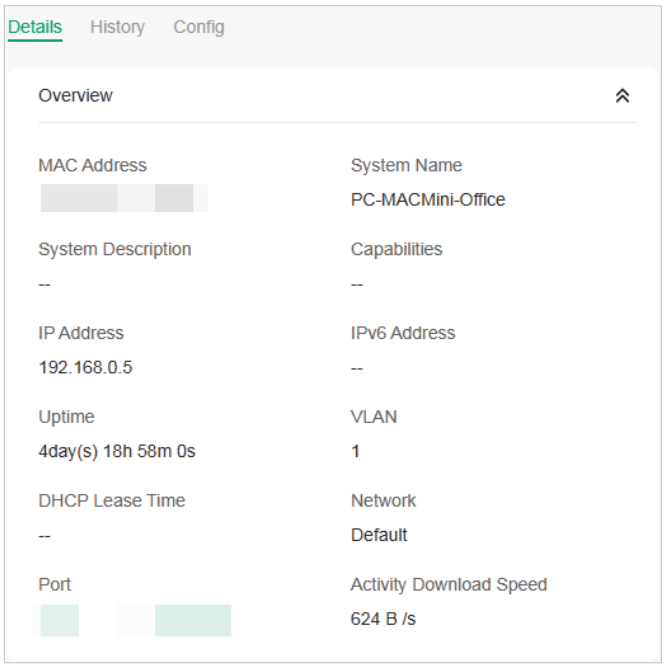
	Click to select multiple clients and add them to the Properties window for batch monitoring and management.
	Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click .
	Click to maximize the Properties window. You can also use the icon on pages other than the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

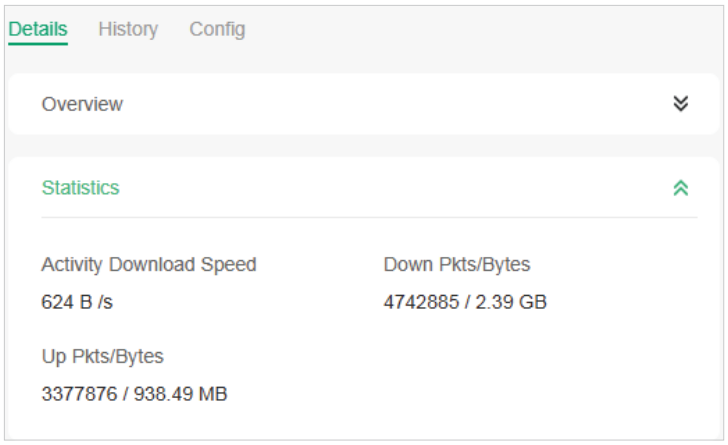
Monitor and Manage a Single Client

- Monitor a Single Client

After opening the Properties window of a single client, you can view the basic information, traffic statistics, and connection history under the Details and History tabs.

Under the Details tab, Overview and Statistics displays the basic information and traffic statistics of the client, respectively. The listed information varies due to the client's status and connection type.



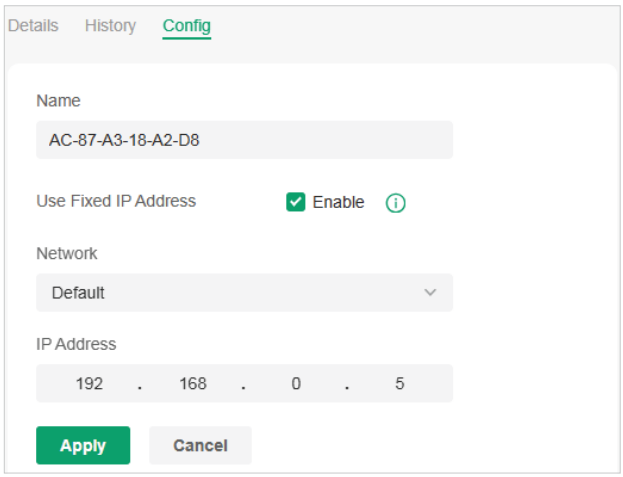


Under the History tab, you can view the connection history of the client.



■ Manage a Single Client

In Config, you can configure the following parameters:

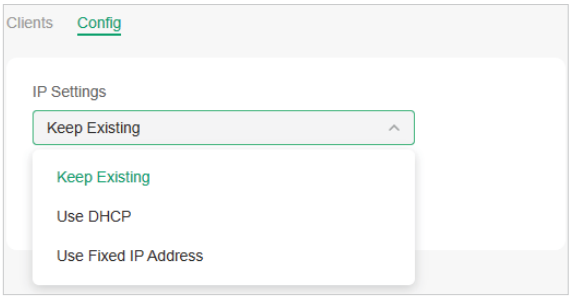


Name	Specify the client's name to better identify different clients, and the name is used as the client's username in the table on the Clients page.

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. To view and configure networks, refer to Configure Wired Networks. Note: A gateway is required for this function. Otherwise, you cannot set a fixed IP address for the client.

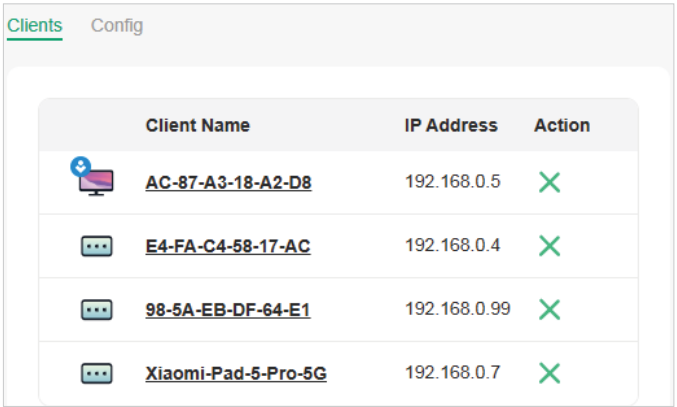
- Monitor and Manage Multiple Clients

To manage multiple clients at the same time, click the edit button, select multiple clients, and click Done. Then you can configure the following parameters under the Config tab.



IP Setting	Keeping Existing: The IP setting of the chosen clients remains their current settings. Use DHCP: The IP addresses of the clients is automatically assigned by the DHCP server, such as the Layer 3 switch and the gateway. Use Fixed IP Address: Select a network and assign fixed IP addresses to the chosen clients manually. To view and configure networks, refer to Configure Wired Networks. Note that a gateway is required for this function. Otherwise, you cannot set fixed IP addresses for the chosen clients.

You can view their names and IP addresses in the Clients tab and remove client(s) from Batch Client Configuration by clicking the block icon in the Action column.



7. 2 Manage Client Authentication in Hotspot

Hotspot is a portal management system for centrally monitoring and managing the clients authorized by portal authentication. The following four tabs are provided in the system for a easy and direct management.

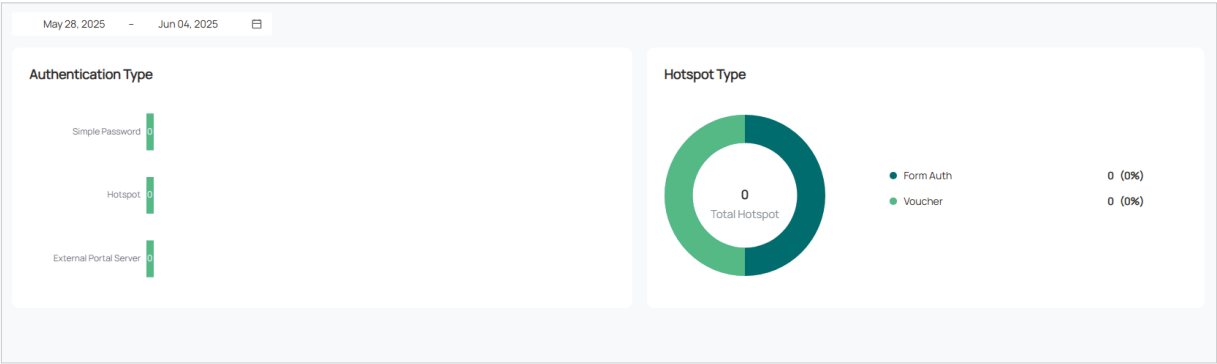
Dashboard	Monitor portal authorizations at a glance through different visualizations.
Authorized Clients	View the records of the connected and expired portal clients.
Voucher Groups	Create vouchers for Portal authentication, and view and manage the related information.
Form Auth Data	Customize your survey contents and publish it to collect data.
Operators	Create operator accounts for Hotspot management, view their information, and manage them.

To access the system, click Hotspot in the sidebar of the Site interface.

7. 2. 1 Dashboard

In the dashboard, you can monitor portal authorizations at a glance through different visualizations.

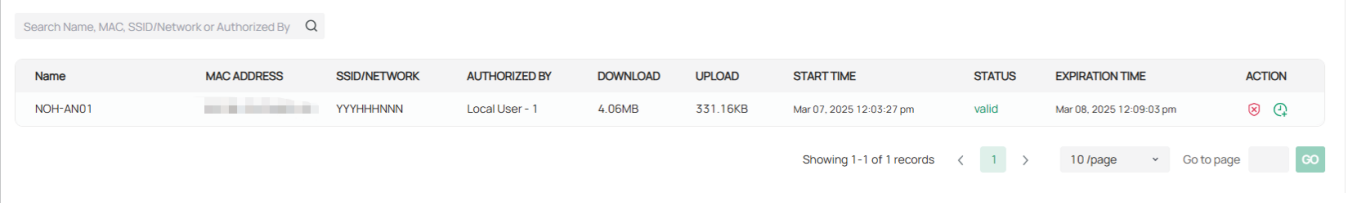
To open the dashboard, click Hotspot in the sidebar of the Site interface and click Dashboard. Specify the time period to view portal authorization histories.



7. 2. 2 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 of the Site interface and 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.

7. 2. 3 Voucher Groups

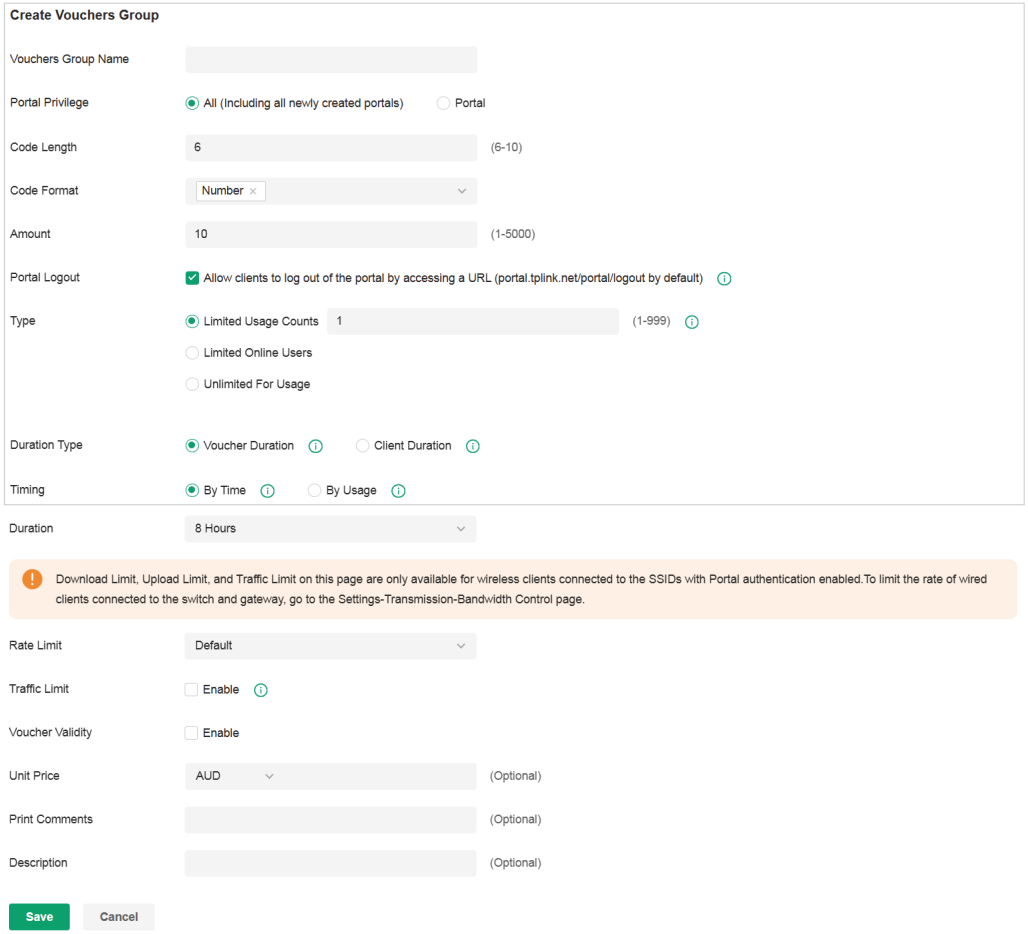
The Voucher Groups tab is used to create vouchers and manage unused voucher codes. With voucher configured and codes created, you can distribute the voucher codes generated by the controller to clients for them to access the network via portal authentication. For detailed configurations, refer to Portal.

Create vouchers

Follow the steps below to create vouchers for authentication:

1. Click Hotspot in the sidebar of the Site interface and click Voucher Groups.
2. Click +Create Vouchers Group on the upper-right, and the following window pops up.

Configure the following parameters and click Save.

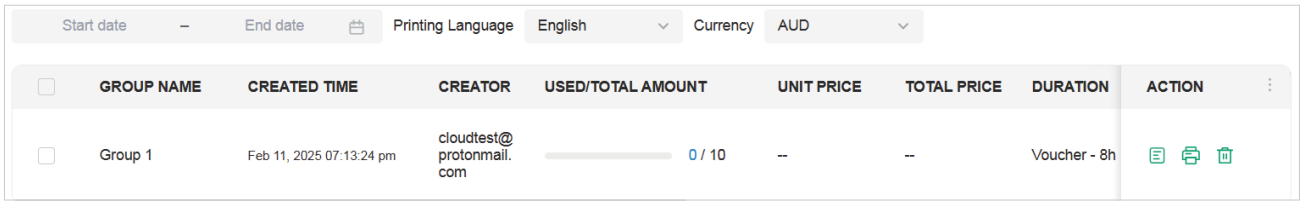


Vouchers Group Name	Enter a name to identify the group.
Portal Privilege	All: The vouchers will take effect for all voucher type portals, including newly created ones. Portal: Select the portal for which the vouchers will take effect.
Code Length	Specify the length of the code(s) from 6 to 10 digits.
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 guests 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 omada.properties file. **Note:** Some devices may require firmware update to support Portal Logout.
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.
Duration Type	Specify whether to limit the voucher duration or client duration.
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: Download/Upload Limit on this page are only available for wireless clients connected to the SSIDs with Portal authentication enabled. To limit the rate of wired clients connected to the switch and gateway, go to the Settings >Transmission > Bandwidth Control.

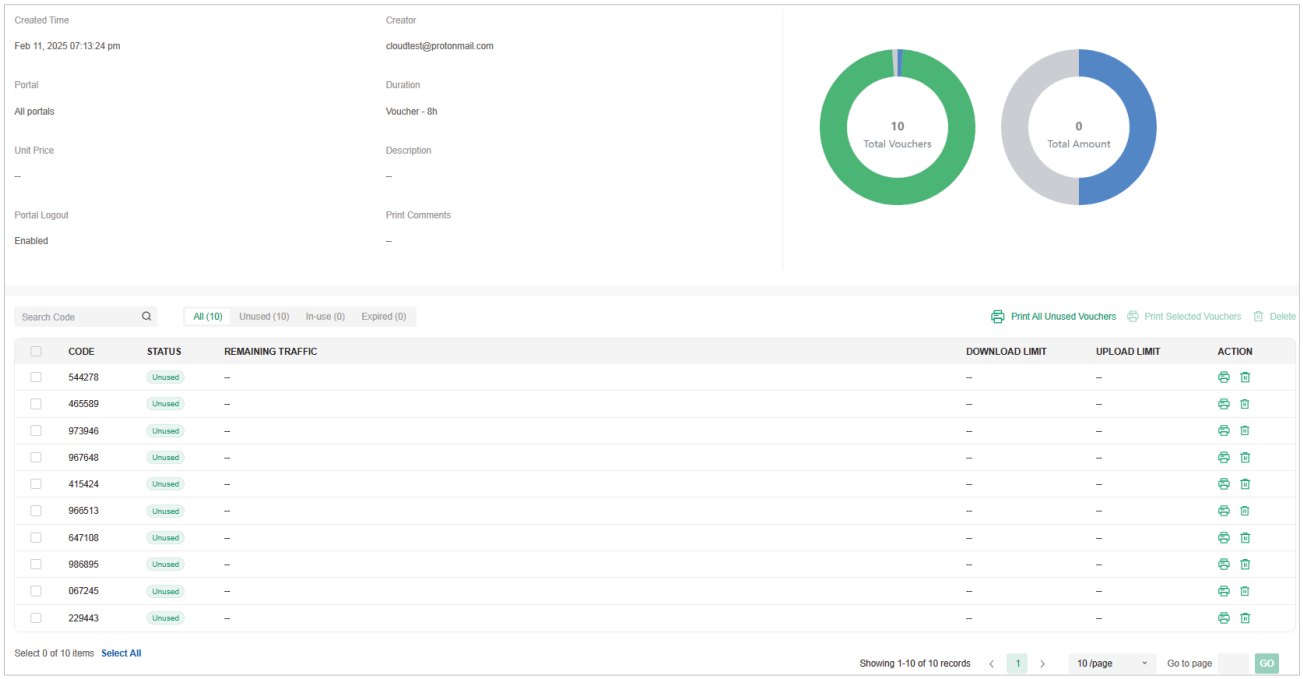
Traffic Limit	Click the checkbox and specify the daily/weekly/monthly/total traffic limit for the voucher, and the value of the traffic limit can be set in MB or GB. Once the limited is reached, the client(s) can no longer access the network using the voucher. Note: Traffic Limit on this page are only 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 the Settings > Transmission > Bandwidth Control.
Voucher Validity	Enable this option and configure the start time and expiration time of the voucher. The voucher can no longer be used no matter whether it runs out of available time or reaches the expiration time
Unit Price (optional)	Set the amount and currency type for the voucher (for statistical purposes only).
Print Comments	Enter print comments if needed and the comments will be printed when you print the created voucher codes.
Description (optional)	Enter notes for the created voucher code(s), and the input description is displayed in the voucher list under the voucher tab.

3. The voucher group is generated.

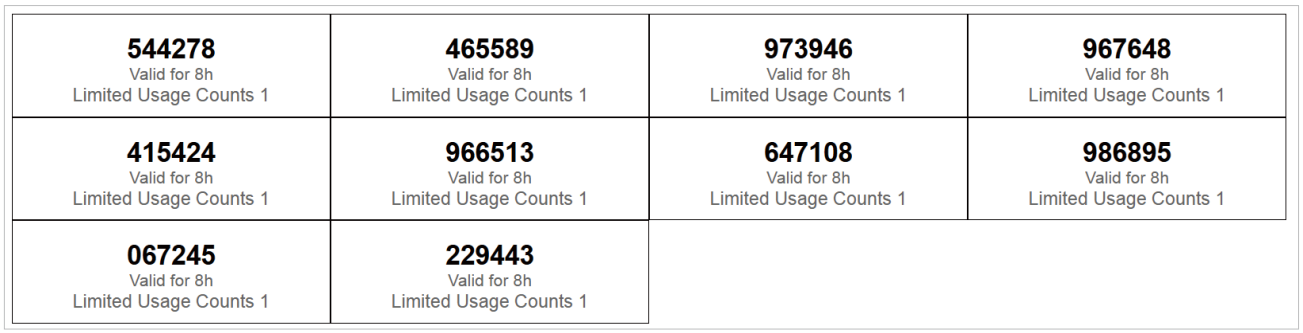


2	The voucher code can be used for an unlimited number of times within its valid period, but only a limited number of wireless clients can access the internet with this voucher code at the same time. The number on the right shows the limited number of users.
2	The voucher code can only be used for a limited number of times within its valid period. The number on the right shows the limited number of authentication times.

You can click the Details icon in the Action column to view the voucher codes.



4. Print the vouchers. Click to print a single voucher, or click checkboxes of vouchers and click Print Selected Vouchers to print the selected vouchers. And you can click Print All Unused Vouchers to print all unused vouchers.



5. Distribute the vouchers to clients, and then they can use the codes to pass authentication. If a voucher code expires, it will be automatically removed from the list.

6. To delete certain vouchers manually, click the trash bin icon to delete a single voucher, or Delete to delete multiple voucher codes at a time.

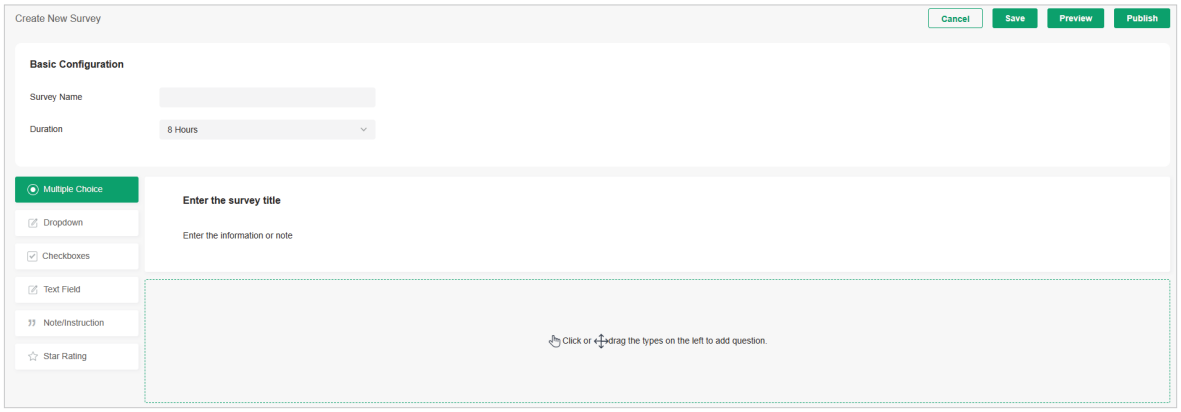
7. 2. 4 Form Auth Data

The Form Auth Data tab is used to create and manage surveys. You can customize your survey contents and publish it to collect data.

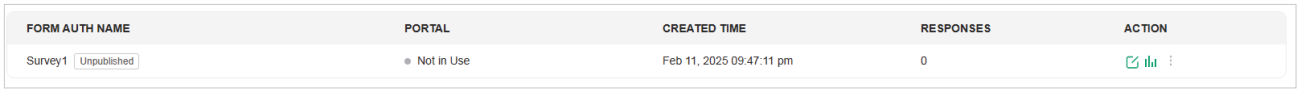
Create Surveys

To create surveys, follow the steps below.

1. Click Hotspot in the sidebar of the Site interface and click Form Auth Data.
2. **Click** Create New Survey and the following window pops up.



3. Specify the survey name and duration, then customize the contents.
4. Preview and save the settings or publish the survey.
5. The surveys are created and displayed in the table. You can use icons for management and click the ellipse icon for more management options.



7. 2. 5 Operators

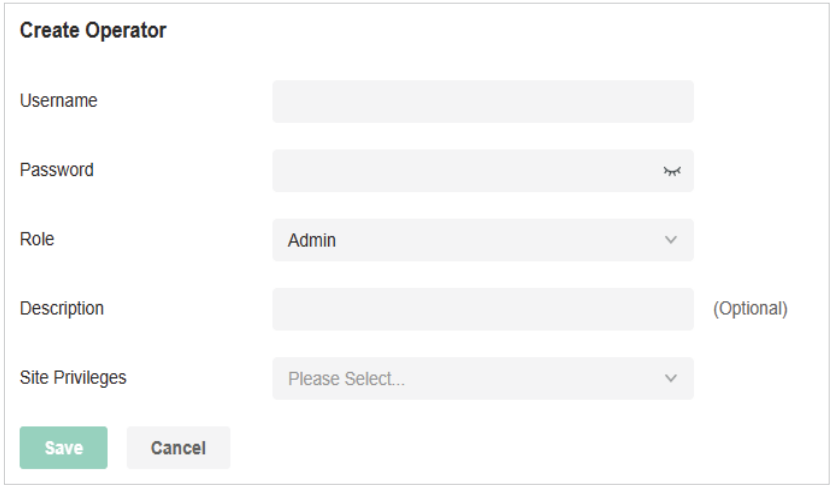
The Operators tab is used to manage and create operator accounts that can only be used to remotely log in to the Hotspot system and manage vouchers and local users for specified sites. The operators have no privileges to create operator accounts, which offers convenience and ensures security for client authentication.

Create Operators

To create operator accounts, follow the steps below.

1. Click Hotspot in the sidebar of the Site interface and 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. Select sites from the drop-down list of Site Privileges. Click Save.

6. 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.



7. Then you can use an operator account to log in to the Hotspot system:

- For software controller

  Visit the URL https://Controller Host's IP Address:8043/ControllerID/login/#hotspot (for example: https://192.168.0.174:8043/4d4ede7983bb983545d017c628feaa3d/login/#hotspot), and use the operator account to enter the Hotspot system.

- For hardware controller

  Visit the URL https://Controller Host's IP Address:443/ControllerID/login/#hotspot (for example: https://192.168.0.174:443/4d4ede7983bb983545d017c628feaa3d/login/#hotspot), and use the operator account to enter the Hotspot system.

- For cloud-based controller

  Visit the URL https://URL of the controller/ControllerID/login/#hotspot, and use the operator account to enter the Hotspot system.