



User Guide

Omada SDN Controller

About this Guide

This User Guide provides information for centrally managing TP-Link devices via Omada SDN Controller. Please read this guide carefully before operation.

Intended Readers



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

Conventions

When using this guide, notice that:

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

In this guide, the following conventions are used:

| | |
|--|---|
| Controller | Stands for the Omada SDN Controller. |
| 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 tips for you to learn about the feature and its configurations. |

More Information

- For technical support, the latest version of the User Guide and other information, please visit <https://www.tp-link.com/support>.
- To ask questions, find answers, and communicate with TP-Link users or engineers, please visit <https://community.tp-link.com> to join TP-Link Community.

CONTENTS

About this Guide

1.Omada SDN Controller Solution Overview

| | | |
|-----|-----------------------|---|
| 1.1 | Overview..... | 2 |
| 1.2 | Core Components | 3 |

2.Get Started with Omada SDN Controller

| | | |
|-------|---|----|
| 2.1 | Set Up Your Software Controller..... | 7 |
| 2.1.1 | Determine the Network Topology..... | 7 |
| 2.1.2 | Install the Software Controller | 8 |
| 2.1.3 | Start and Log In to the Software Controller | 10 |
| 2.2 | Set Up Your Hardware Controller..... | 15 |
| 2.2.1 | Determine the Network Topology..... | 15 |
| 2.2.2 | Deploy the Hardware Controller..... | 15 |
| 2.2.3 | Start and Log in to the Controller | 16 |
| 2.3 | Set Up Your Cloud-Based Controller..... | 20 |

3.Manage Omada Managed Devices and Sites

| | | |
|-------|---|----|
| 3.1 | Create Sites..... | 22 |
| 3.2 | Adopt Devices..... | 26 |
| 3.2.1 | For Software Controller / Hardware Controller | 26 |
| 3.2.2 | For Cloud-Based Controller..... | 37 |

4.Configure the Network with the SDN Controller

| | | |
|-------|--|----|
| 4.1 | Navigate the UI..... | 42 |
| 4.2 | Modify the Current Site Configuration..... | 47 |
| 4.2.1 | Site Configuration..... | 47 |
| 4.2.2 | Services..... | 48 |
| 4.2.3 | Advanced Features | 50 |
| 4.2.4 | Device Account | 53 |
| 4.3 | Configure Wired Networks..... | 54 |
| 4.3.1 | Set Up an Internet Connection | 54 |
| 4.3.2 | Configure LAN Networks..... | 74 |
| 4.4 | Configure Wireless Networks..... | 87 |

| | | |
|------------|--------------------------------------|------------|
| 4.4.1 | Set Up Basic Wireless Networks..... | 87 |
| 4.4.2 | Advanced Settings | 93 |
| 4.4.3 | WLAN Schedule..... | 94 |
| 4.4.4 | 802.11 Rate Control..... | 95 |
| 4.4.5 | MAC Filter..... | 96 |
| 4.4.6 | Multicast/Broadcast Management | 97 |
| 4.4.7 | AI WLAN Optimization..... | 98 |
| 4.5 | Network Security..... | 102 |
| 4.5.1 | ACL | 102 |
| 4.5.2 | URL Filtering..... | 112 |
| 4.5.3 | MAC Filtering..... | 115 |
| 4.5.4 | Attack Defense | 116 |
| 4.5.5 | Firewall | 120 |
| 4.5.6 | IP-MAC Binding..... | 122 |
| 4.5.7 | IDS/IPS..... | 124 |
| 4.6 | Transmission..... | 127 |
| 4.6.1 | Routing..... | 127 |
| 4.6.2 | NAT | 130 |
| 4.6.3 | Session Limit..... | 135 |
| 4.6.4 | Bandwidth Control..... | 136 |
| 4.6.5 | Gateway QoS | 138 |
| 4.7 | Configure VPN..... | 143 |
| 4.7.1 | VPN..... | 143 |
| 4.7.2 | VPN User..... | 169 |
| 4.7.3 | IPsec Failover | 171 |
| 4.7.4 | SSL VPN..... | 172 |
| 4.7.5 | WireGuard VPN | 179 |
| 4.8 | Create Profiles..... | 182 |
| 4.8.1 | Time Range | 182 |
| 4.8.2 | Groups | 184 |
| 4.8.3 | Rate Limit..... | 186 |
| 4.8.4 | PPSK | 188 |
| 4.8.5 | Gateway QoS Service | 191 |
| 4.8.6 | Bonjour Service..... | 192 |
| 4.8.7 | RADIUS Profile..... | 192 |
| 4.8.8 | LDAP Profiles | 195 |
| 4.9 | Authentication..... | 197 |
| 4.9.1 | Portal..... | 197 |
| 4.9.2 | 802.1X..... | 206 |

| | | |
|--------------|-------------------------------|------------|
| 4. 9. 3 | MAC-Based Authentication..... | 209 |
| 4. 10 | Services..... | 212 |
| 4. 10. 1 | DHCP Reservation..... | 212 |
| 4. 10. 2 | Dynamic DNS..... | 213 |
| 4. 10. 3 | mDNS..... | 215 |
| 4. 10. 4 | SNMP..... | 217 |
| 4. 10. 5 | UPnP..... | 218 |
| 4. 10. 6 | SSH..... | 218 |
| 4. 10. 7 | Reboot Schedule..... | 219 |
| 4. 10. 8 | Port Schedule..... | 220 |
| 4. 10. 9 | IPTV..... | 221 |
| 4. 10. 10 | Upgrade Schedule..... | 223 |
| 4. 10. 11 | DNS Proxy..... | 224 |
| 4. 10. 12 | DNS Cache..... | 225 |
| 4. 10. 13 | Export Data..... | 226 |
| 4. 11 | CLI Configuration..... | 229 |
| 4. 11. 1 | Site CLI..... | 231 |
| 4. 11. 2 | Device CLI..... | 232 |

5.Configure the SDN Controller

| | | |
|-------------|--|------------|
| 5. 1 | Manage the Controller..... | 236 |
| 5. 1. 1 | General Settings..... | 236 |
| 5. 1. 2 | Mail Server..... | 238 |
| 5. 1. 3 | History Data Retention..... | 240 |
| 5. 1. 4 | Customer Experience Improvement Program..... | 241 |
| 5. 1. 5 | HTTPS Certificate..... | 241 |
| 5. 1. 6 | Access Config..... | 243 |
| 5. 2 | Manage Your Controller Remotely via Cloud Access..... | 245 |
| 5. 3 | Maintenance..... | 247 |
| 5. 3. 1 | Controller Status..... | 247 |
| 5. 3. 2 | User Interface..... | 247 |
| 5. 3. 3 | Backup & Restore..... | 249 |
| 5. 4 | Migration..... | 252 |
| 5. 4. 1 | Site Migration..... | 252 |
| 5. 4. 2 | Controller Migration..... | 257 |
| 5. 5 | Auto Backup..... | 265 |

6.Configure and Monitor Controller-Managed Devices

| | | |
|-------------|--|------------|
| 6. 1 | Introduction to the Devices Page..... | 269 |
|-------------|--|------------|

| | | |
|------------|--|------------|
| 6.2 | Configure and Monitor the Gateway | 273 |
| 6.2.1 | Configure the Gateway..... | 273 |
| 6.2.2 | Monitor the Gateway..... | 286 |
| 6.3 | Configure and Monitor Switches | 287 |
| 6.3.1 | Configure Switches..... | 287 |
| 6.3.2 | Monitor Switches..... | 313 |
| 6.4 | Configure and Monitor APs | 318 |
| 6.4.1 | Configure APs..... | 318 |
| 6.4.2 | Monitor APs..... | 330 |

7. Monitor and Manage the Clients

| | | |
|------------|--|------------|
| 7.1 | Manage Wired and Wireless Clients in Clients Page | 344 |
| 7.1.1 | Introduction to Clients Page..... | 344 |
| 7.1.2 | Using the Clients Table to Monitor and Manage the Clients..... | 344 |
| 7.1.3 | Using the Properties Window to Monitor and Manage the Clients..... | 346 |
| 7.2 | Manage Client Authentication in Hotspot Manager | 351 |
| 7.2.1 | Dashboard..... | 351 |
| 7.2.2 | Authorized Clients..... | 352 |
| 7.2.3 | Vouchers..... | 352 |
| 7.2.4 | Local Users..... | 355 |
| 7.2.5 | Form Auth Data..... | 359 |
| 7.2.6 | Operators..... | 359 |

8. Monitor the Network

| | | |
|------------|---|------------|
| 8.1 | View the Status of Network with Dashboard | 363 |
| 8.1.1 | Page Layout of Dashboard..... | 363 |
| 8.1.2 | Explanation of Widgets..... | 365 |
| 8.2 | View the Statistics of the Network | 378 |
| 8.2.1 | Performance..... | 378 |
| 8.2.2 | Switch Statistics..... | 381 |
| 8.3 | Monitor the Network with Map | 384 |
| 8.3.1 | Topology..... | 384 |
| 8.3.2 | Heat Map..... | 386 |
| 8.3.3 | Device Map..... | 391 |
| 8.3.4 | Site Map..... | 394 |
| 8.4 | Monitor the Network with Reports | 397 |
| 8.5 | View the Statistics During Specified Period with Insight | 399 |
| 8.5.1 | Known Clients..... | 399 |
| 8.5.2 | Past Connections..... | 400 |

| | | |
|-------------|---|------------|
| 8. 5. 3 | Past Portal Authorizations | 401 |
| 8. 5. 4 | Switch Status | 402 |
| 8. 5. 5 | Port Forwarding Status..... | 406 |
| 8. 5. 6 | VPN Status..... | 407 |
| 8. 5. 7 | Routing Table | 410 |
| 8. 5. 8 | Dynamic DNS..... | 411 |
| 8. 5. 9 | Rogue APs | 411 |
| 8. 6 | View and Manage Logs | 414 |
| 8. 6. 1 | Alerts..... | 415 |
| 8. 6. 2 | Events..... | 416 |
| 8. 6. 3 | Notifications..... | 417 |
| 8. 7 | Monitor the Network with Tools | 423 |
| 8. 7. 1 | Network Check..... | 423 |
| 8. 7. 2 | Packet Capture | 424 |
| 8. 7. 3 | Terminal..... | 425 |

9.Manage Accounts of the SDN Controller

| | | |
|---------|--|-----|
| 9. 1 | Introduction to User Accounts..... | 428 |
| 9. 2 | Create and Manage Custom Account Roles | 428 |
| 9. 3 | Manage and Create Local User Accounts | 430 |
| 9. 3. 1 | Edit the Main Administrator Account..... | 430 |
| 9. 3. 2 | Create and Manage Other Local Accounts | 430 |
| 9. 4 | Manage and Create Cloud User Accounts | 433 |
| 9. 4. 1 | Set Up the Cloud Main Administrator..... | 433 |
| 9. 4. 2 | Create and Manage Other Cloud Accounts..... | 433 |

10.Manage Customer Networks in MSP Mode

| | | |
|----------|--|-----|
| 10. 1 | Quick Start..... | 437 |
| 10. 1. 1 | Enable the MSP Mode..... | 437 |
| 10. 1. 2 | Add and Manage Customers | 438 |
| 10. 1. 3 | Assign and Manage Licenses..... | 439 |
| 10. 1. 4 | Add Sites and Devices..... | 440 |
| 10. 2 | Add and Manage Accounts | 441 |
| 10. 2. 1 | Configure Role Settings..... | 441 |
| 10. 2. 2 | Manage the Main Administrator Account..... | 443 |
| 10. 2. 3 | Add New MSP User Accounts..... | 444 |
| 10. 3 | Manage System Settings | 447 |
| 10. 3. 1 | Configure MSP Settings | 447 |

| | | |
|--------|-------------------------|-----|
| 10.3.2 | Export for Support..... | 452 |
| 10.3.3 | Export Data..... | 452 |

Appendix 1: Omada APP

| | | |
|-----|---|-----|
| 1 | Install Omada App on the Mobile Device | 455 |
| 2 | Manage Your Network in Standalone Mode | 455 |
| 3 | Manage Your Network in Controller Mode | 458 |
| 3.1 | Locally Manage Your Devices Using the Omada App..... | 458 |
| 3.2 | Remotely Manage Your Devices Using the Omada App..... | 461 |



Omada SDN Controller Solution Overview

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

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

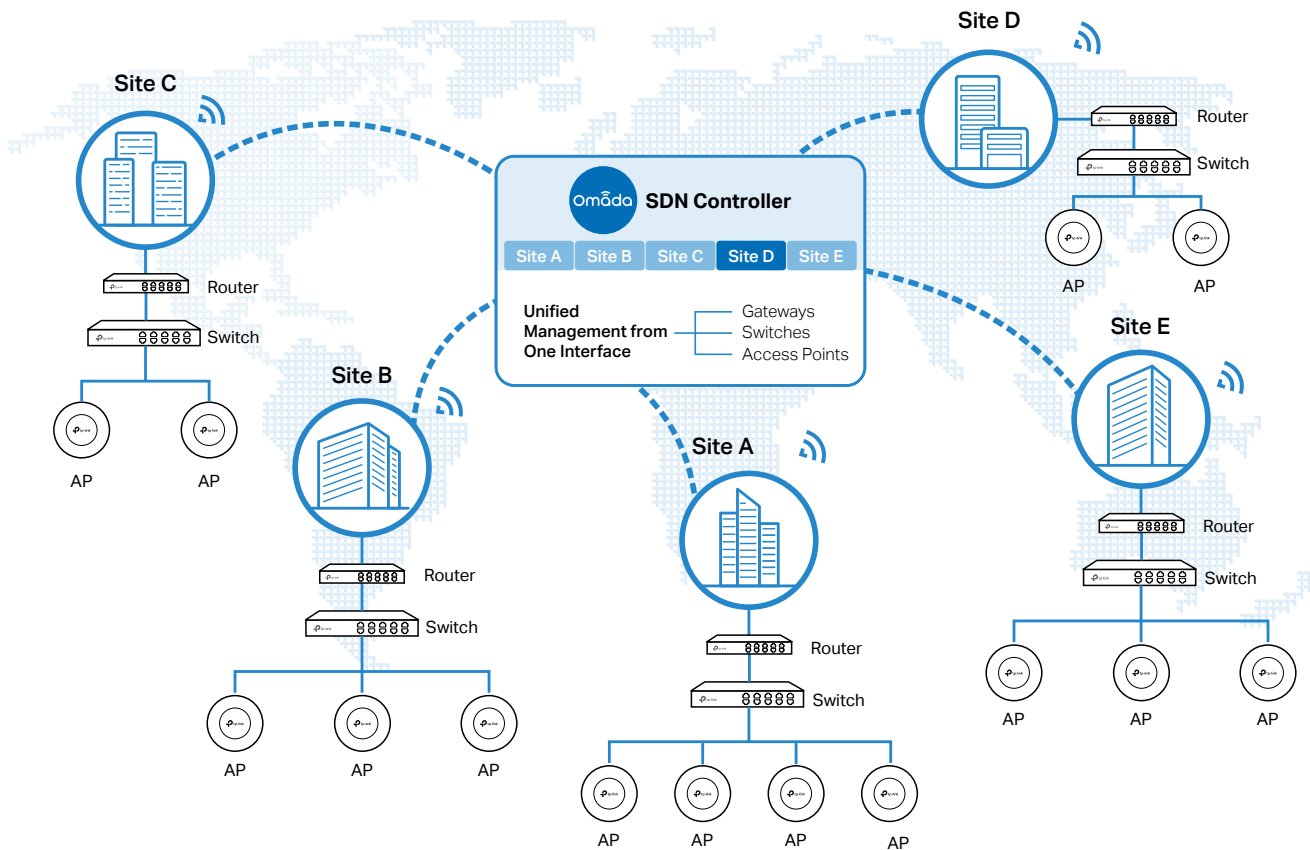
The chapter includes the following sections:

- [1.1 Overview](#)
- [1.2 Core Components](#)

♥ 1.1 Overview

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

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



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

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

♥ 1.2 Core Components

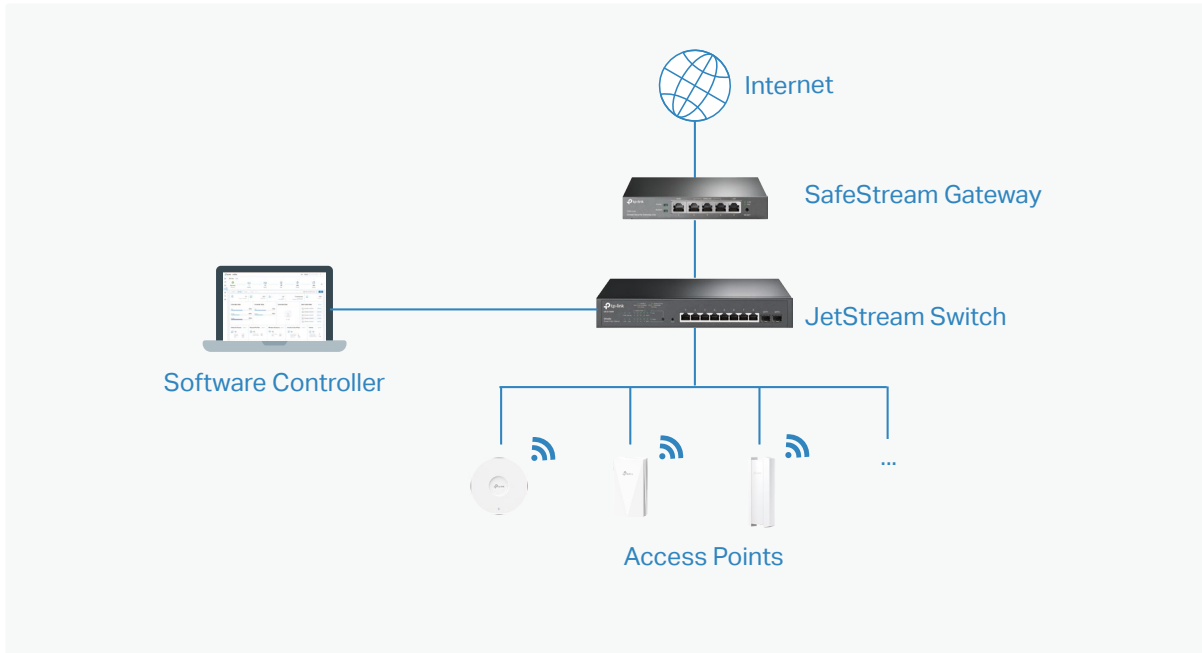
An Omada SDN network consists of the following core components:

- **SDN Controller** — 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.

SDN Controller

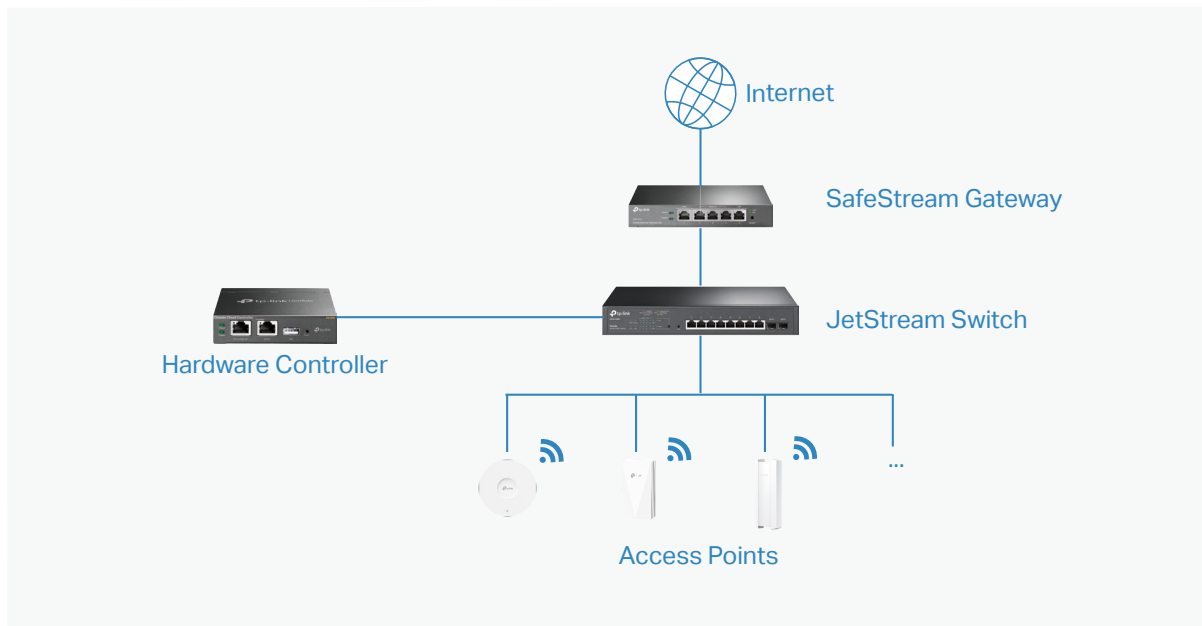
Tailored to different needs and budgets, Omada SDN Controller offers diverse deployment solutions. Omada Software Controller, Hardware Controller, and Cloud-Based Controller each has their own set of advantages and applications.

- **Omada Software Controller**
Omada Software Controller can be hosted on any computers with Windows or Linux systems on your network.



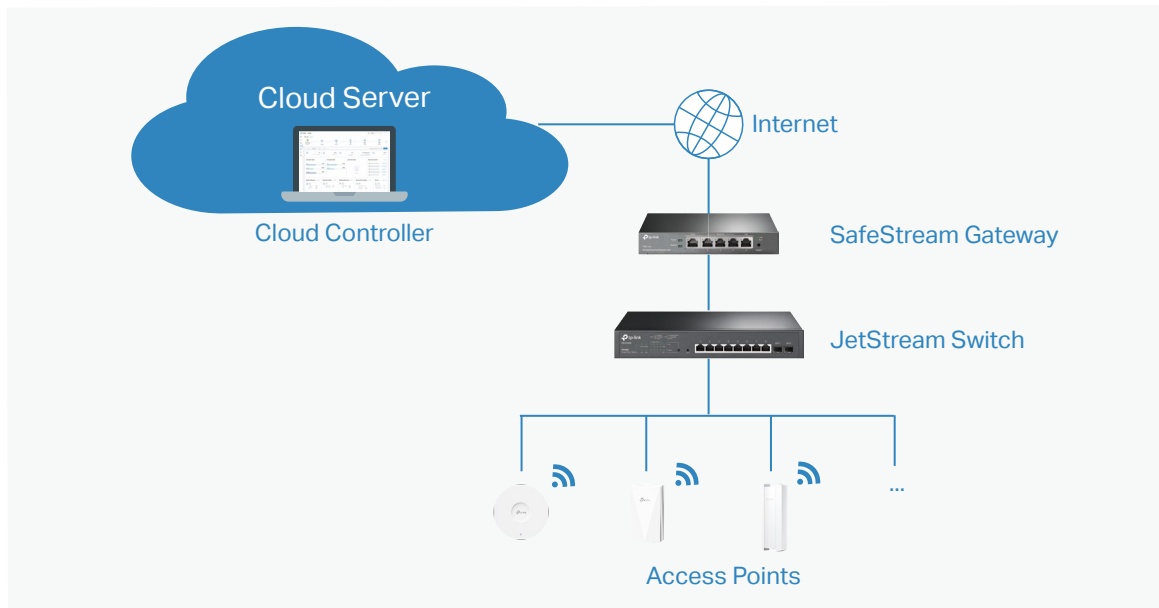
■ Omada Hardware Controller

Omada Hardware Controller is the management device which is pre-installed with Omada Software Controller. You just need to purchase the device, then the built-in software controller is ready to use. About the size of a mobile phone, the device is easy to deploy and install on your network.



■ Omada Cloud-Based Controller

Omada Cloud controller is deployed on the Omada Cloud server, providing paid license service with tiered pricing. With paid licenses bound to the devices on the controller, 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.



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

Gateways

TP-Link's Omada Router supports Gigabit Ethernet connections on both WAN and LAN ports which keep the data moving at top speed. Including all the routing and network segmentation functions that a business router must have, SafeStream VPN Router will be the backbone of the 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 SDN Controller is available on certain models only. Please check the [Omada Cloud SDN Platform Compatibility List](#) for more information.

Switches

TP-Link's JetStream 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 SDN Controller is available on certain models only. Please check the [Omada Cloud SDN Platform Compatibility List](#) for more information.

Access Points

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

Managing the access points centrally through Omada SDN Controller is available on certain models only. Please check the [Omada Cloud SDN Platform Compatibility List](#) for more information.

2

Get Started with Omada SDN Controller

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

- [2.1 Set Up Your Software Controller](#)
- [2.2 Set Up Your Hardware Controller](#)
- [2.3 Set Up Your Cloud-Based Controller](#)

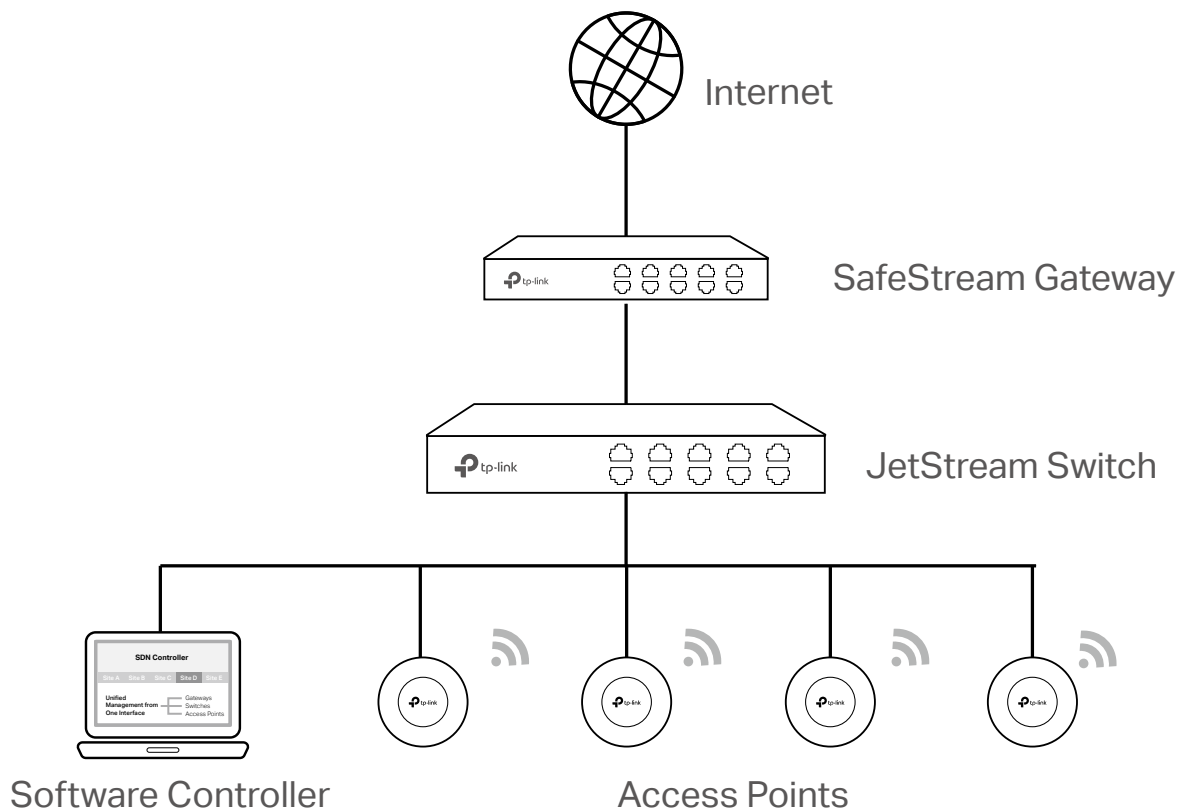
♥ 2.1 Set Up Your Software Controller

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

- 1) Determine the network topology.
- 2) Install the Software Controller.
- 3) Start and log in to the controller.

2.1.1 Determine the Network Topology

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



! Note:

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

2.1.2 Install the Software Controller

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

Installation on Windows Host

Omada Software Controller can be hosted on any computers with Windows systems on your network. Make sure your PC's hardware and system meet the following requirements, then properly install the Software Controller.

■ Hardware Requirements

To guarantee operational stability, we recommend that you use the hardware which meets or exceeds the following specifications:

CPU: Intel Core i3-8100, i5-6500, or i7-4700 with 2 or more cores and 4 or more threads.


Memory: 16 GB RAM or more.

■ System Requirements

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

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

■ Install the Software Controller

Download the installation file of Software Controller from the <https://www.tp-link.com/support/download/omada-software-controller>. Then follow the instructions to install the controller. After a successful installation, a shortcut icon  of the controller will be created on your desktop.

Installation on Linux Host

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

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

■ Hardware Requirements

To guarantee operational stability, we recommend that you use the hardware which meets or exceeds the following specifications:

CPU: Intel Core i3-8100, i5-6500, or i7-4700 with 2 or more cores and 4 or more threads.

Memory: 16 GB RAM or more.

■ System Requirements

Operating System: 64-bit Linux operating system, including Ubuntu 14.04/16.04/17.04/18.04, CentOS 6.x/7.x, Fedora 20 (or above), and Debian 9.8.

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

■ Install the Software Controller

Download the installation file of Software Controller from the <https://www.tp-link.com/support/download/omada-software-controller>. Check the prerequisites and follow the steps based on your file version to install the controller.

- Prerequisites for installing

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

- Ensure that the Java Runtime Environment (JRE) has been installed in your system. The controller requires that the system has Java 8 installed. Download the file according to your operating system from https://www.java.com/download/linux_manual.jsp and follow the instructions to install the JRE.

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

- Ensure that MongoDB has been installed in your system. The controller works when the system runs MongoDB 3.0.15–3.6.18. Download the file according to your operating system from the <https://www.mongodb.com/try/download> and follow the instructions to install the MongoDB.
- Ensure that you have **jsvc** and **curl** installed in your system before installation, which is vital to the smooth running of the system. If your system does not have **jsvc** or **curl** installed, you can install it manually with the command: **apt-get install** or **yum install**. For example, you can use the command: **apt-get install jsvc** or **yum install jsvc** to get **jsvc** installed. And if dependencies are missing, you can use the command: **apt-get -f install** to fix the problem.

- Install the .tar.gz file

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

sudo

- Extract the tar.gz file using the command:

tar zxvf Omada_Controller_vx.x.x_linux_x64_targz.tar.gz

- Install the Controller using the command:

sudo bash ./install.sh

- Install the .deb file

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

sudo

- Install the .deb file using the command:

dpkg -i Omada_Controller_vx.x.x_linux_x64.deb

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

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

- a. **tpeap start** — Start the controller, use the command.
- b. **tpeap stop** — Stop running the Controller.
- c. **tpeap status** — Show the status of Controller.

For more detailed information about the installation on Linux hosts, refer to the [Installation Instructions](#).


ⓘ **Note:**

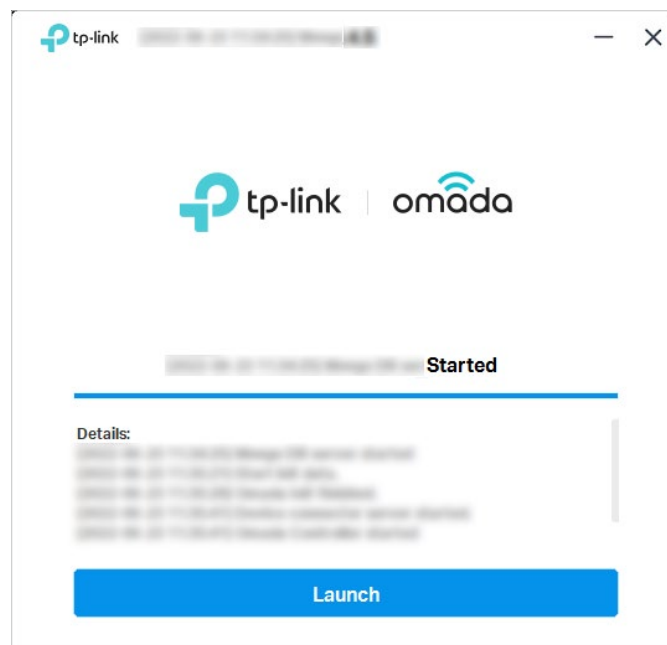
- For installing the .tar.gz, if you want the Controller to run as a user (it runs as root by default) you should modify OMADA_USER value in bin/control.sh.
- To uninstall the Controller, go to the installation path: /opt/tplink/EAPController, and run the command: sudo bash ./uninstall.sh.
- During uninstallation,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

2.1.3 Start and Log In to the Software Controller

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

Launch the Software Controller

Double-click the icon  and the following window will pop up. After a while, your web browser will automatically open.



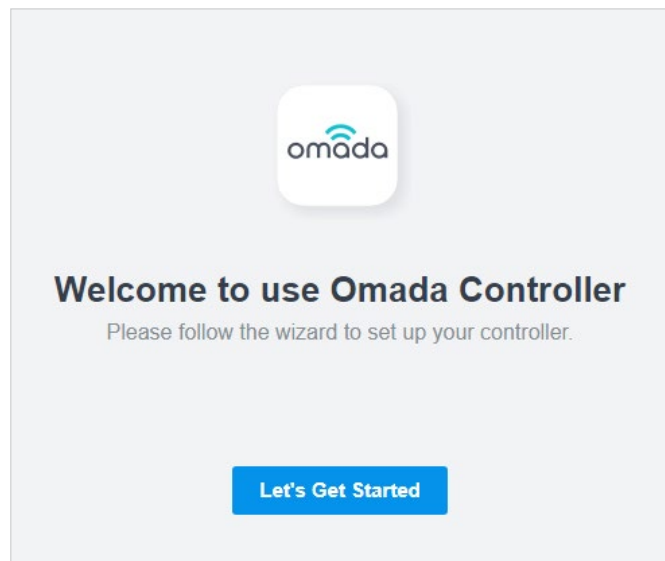
Note:

- If your browser does not open automatically, click [Launch](#). You can also launch a web browser and enter <http://127.0.0.1:8088> in the address bar.
- If your web browser opens but prompts a problem with the website's security certificate, click Continue.

Complete Basic Configurations

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

1. Click [Let's Get Started](#).



2. Set up controller access settings.

Controller Access

Create an administrator name and password for local login to Omada Controller.

Controller Main Administrator

Administrator Name: Enter the username with letters (case-sensitive), numbers, underscores, or hyphens.

Email: ⓘ

Password:

Confirm Password:

To enjoy Omada Cloud Service, you can log in and bind your TP-Link ID to your controller.

Cloud Access:

TP-Link ID:

Password:

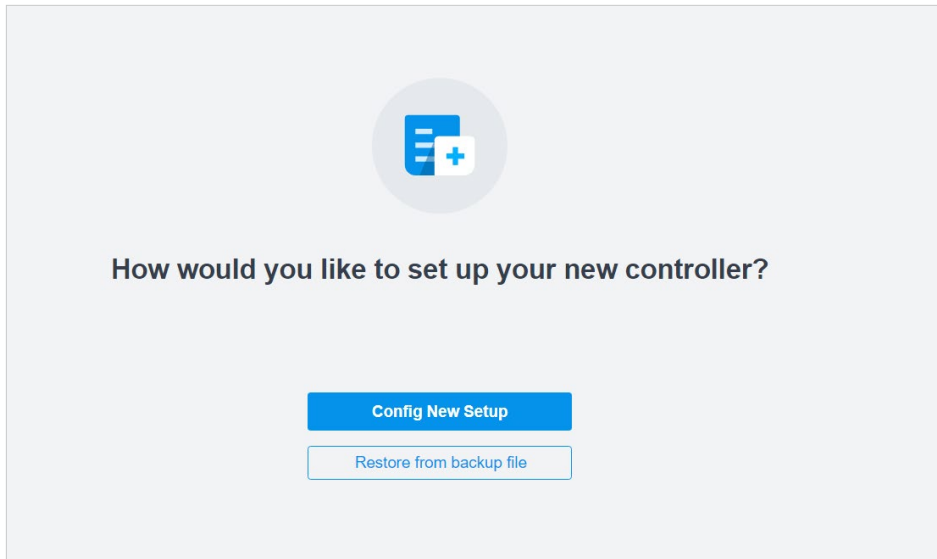
[Log in and bind](#) No TP-Link ID? [Register now.](#)

Terms

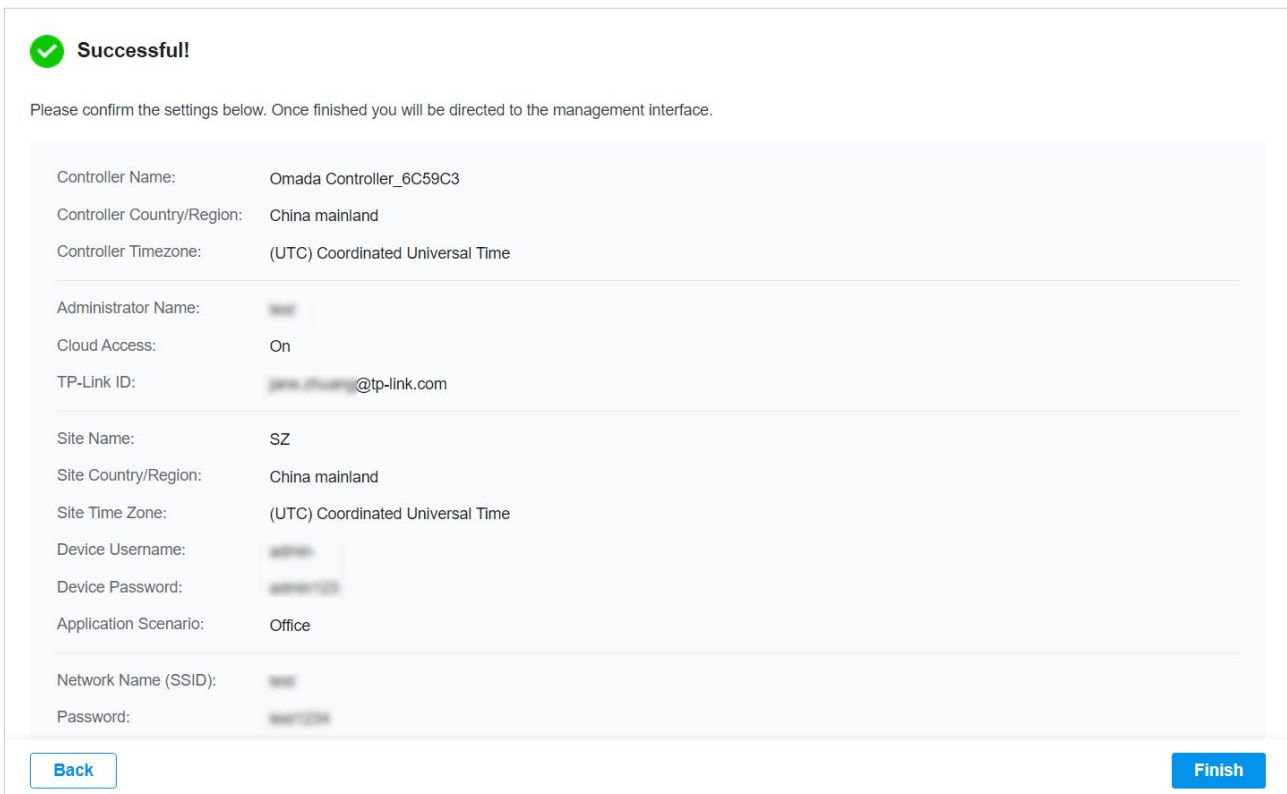
I accept the [Terms of Use](#) and confirm that I have fully read and understood the [Privacy Policy](#).

- Create an Administrator username and password for login to the controller. Specify the email address for resetting your password in case that you forget the password. After logging into the Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to [8. 6. 3 Notifications](#).
- If you want to access the controller to manage networks remotely, enable [Cloud Access](#), and bind your TP-Link ID to your Controller. For more details about cloud access, please refer to [5. 2 Manage Your Controller Remotely via Cloud Access](#).
- Read and agree to TP-Link's Terms of Use.
- Click [Next](#).

- 3. Choose how would you like to set up your new controller. You can configure a new setup or restore from backup file.

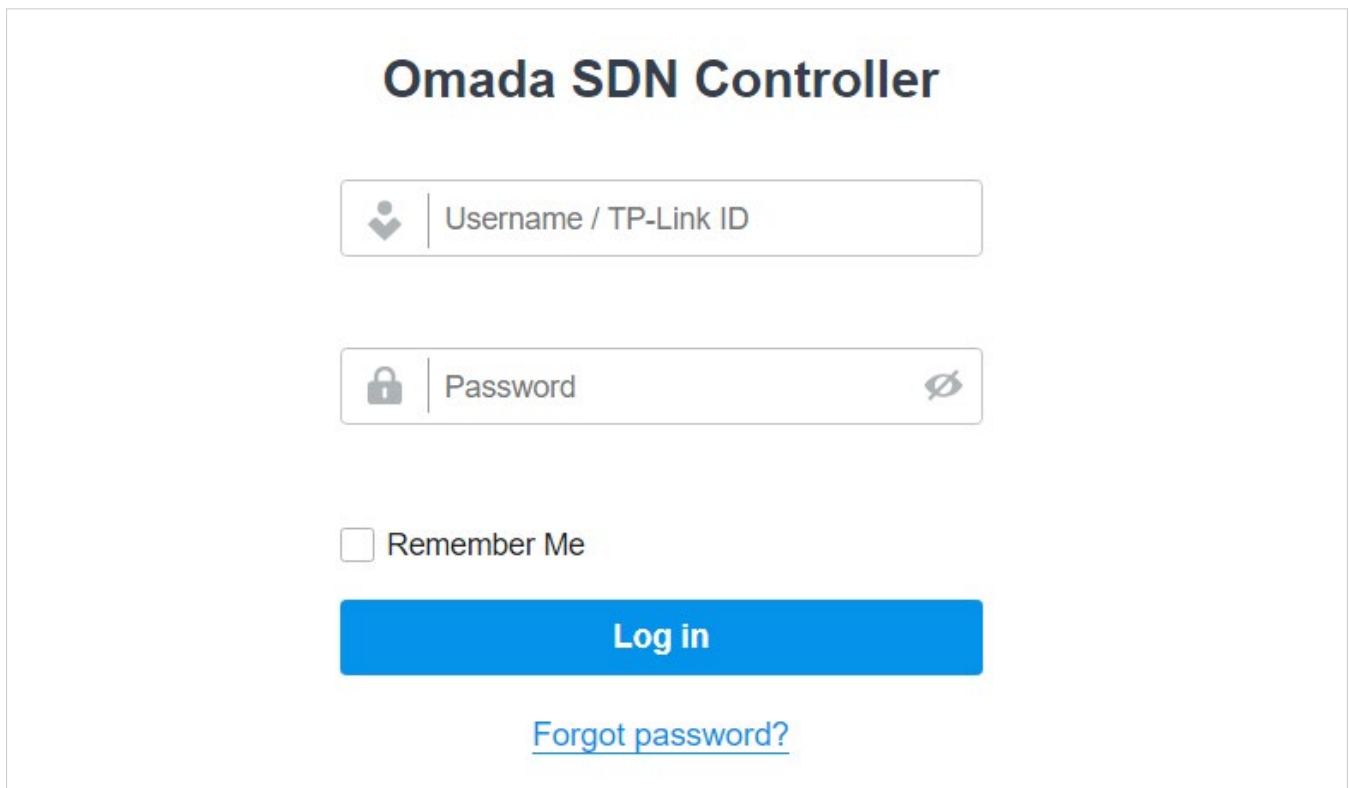


- 4. Follow the setup wizard to set up the controller.



Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page. Log in to the management interface using the username and password you have set in the basic configurations.



The image shows the login page for the Omada SDN Controller. At the top, the title "Omada SDN Controller" is displayed in a large, bold, black font. Below the title, there are two input fields. The first field is for the "Username / TP-Link ID" and contains a user icon on the left. The second field is for the "Password" and contains a lock icon on the left and a "show/hide" icon (an eye with a slash) on the right. Below the password field, there is a checkbox labeled "Remember Me". At the bottom of the form, there is a prominent blue button with the text "Log in" in white. Below the button, there is a blue, underlined link that says "Forgot password?".

ⓘ Note:

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

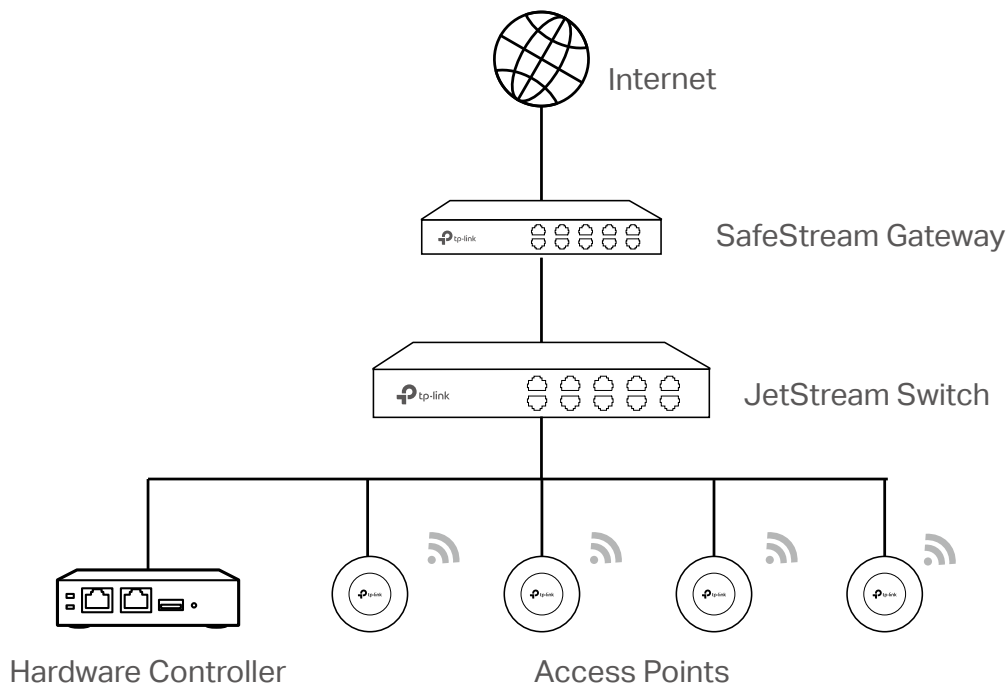
♥ 2.2 Set Up Your Hardware Controller

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

- 1) Determine the network topology.
- 2) Deploy the Hardware Controller.
- 3) Start and log in to the controller.

2.2.1 Determine the Network Topology

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



! Note:

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

2.2.2 Deploy the Hardware Controller

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

2.2.3 Start and Log in to the Controller

Log In to the Management Interface

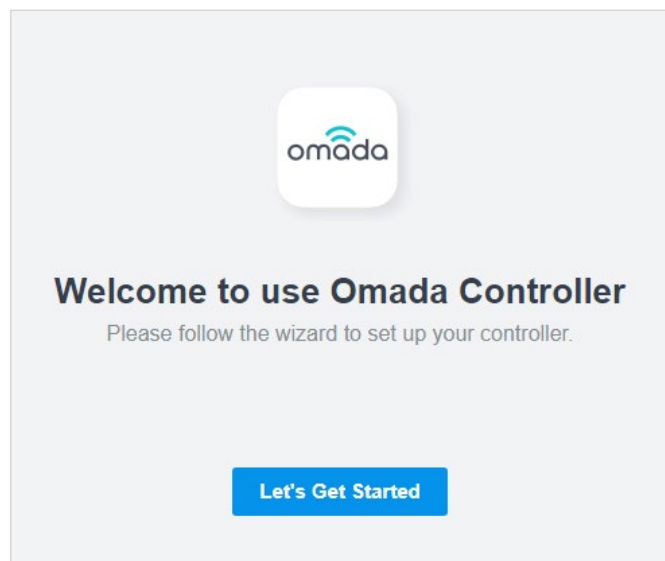
Follow the steps below to enter the management interface of the Hardware Controller:

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

Complete Basic Configurations

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

1. Click [Let's Get Started](#).



2. Set up controller access settings.

Controller Access

Create an administrator name and password for local login to Omada Controller.

Controller Main Administrator

Administrator Name: Enter the username with letters (case-sensitive), numbers, underscores, or hyphens.

Email: ⓘ

Password:

Confirm Password:

To enjoy Omada Cloud Service, you can log in and bind your TP-Link ID to your controller.

Cloud Access:

TP-Link ID:

Password:

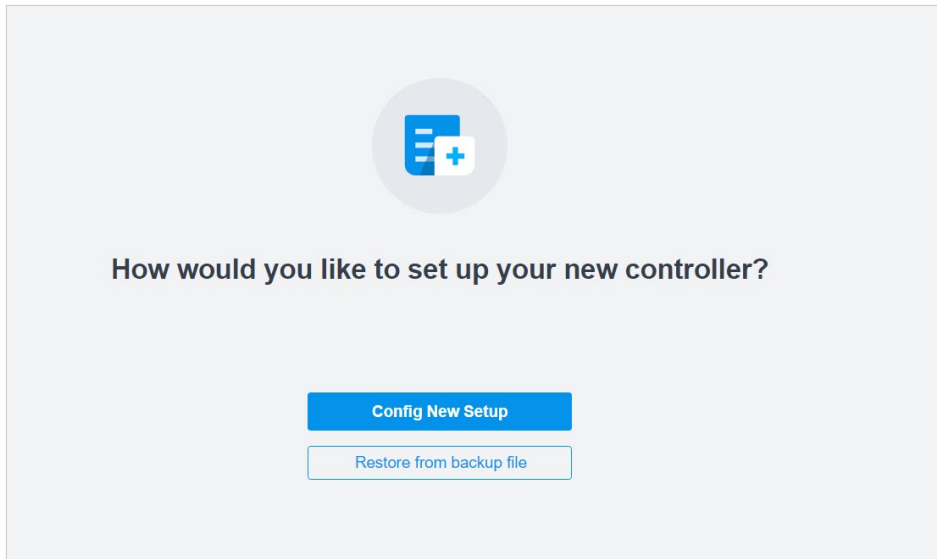
[Log in and bind](#) No TP-Link ID? [Register now.](#)

Terms

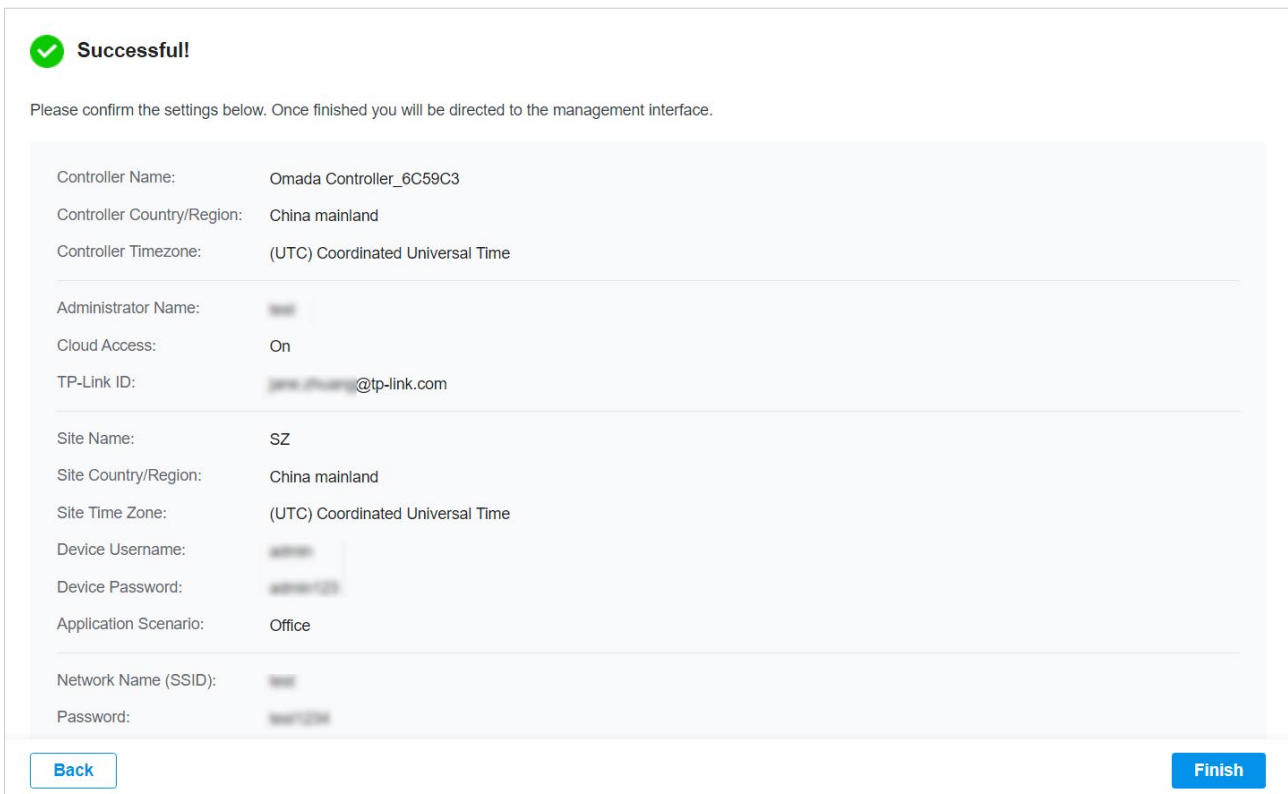
I accept the [Terms of Use](#) and confirm that I have fully read and understood the [Privacy Policy](#).

- a. Create an Administrator username and password for login to the controller. Specify the email address for resetting your password in case that you forget the password. After logging into the Controller, set a mail server so that you can receive emails and reset your password. For how to set a mail server, refer to [8. 6. 3 Notifications](#).
- b. If you want to access the controller to manage networks remotely, enable [Cloud Access](#), and bind your TP-Link ID to your Controller. For more details about cloud access, please refer to [5. 2 Manage Your Controller Remotely via Cloud Access](#).
- c. Read and agree to TP-Link's Terms of Use.
- d. Click [Next](#).

- 3. Choose how would you like to set up your new controller. You can configure a new setup or restore from backup file.

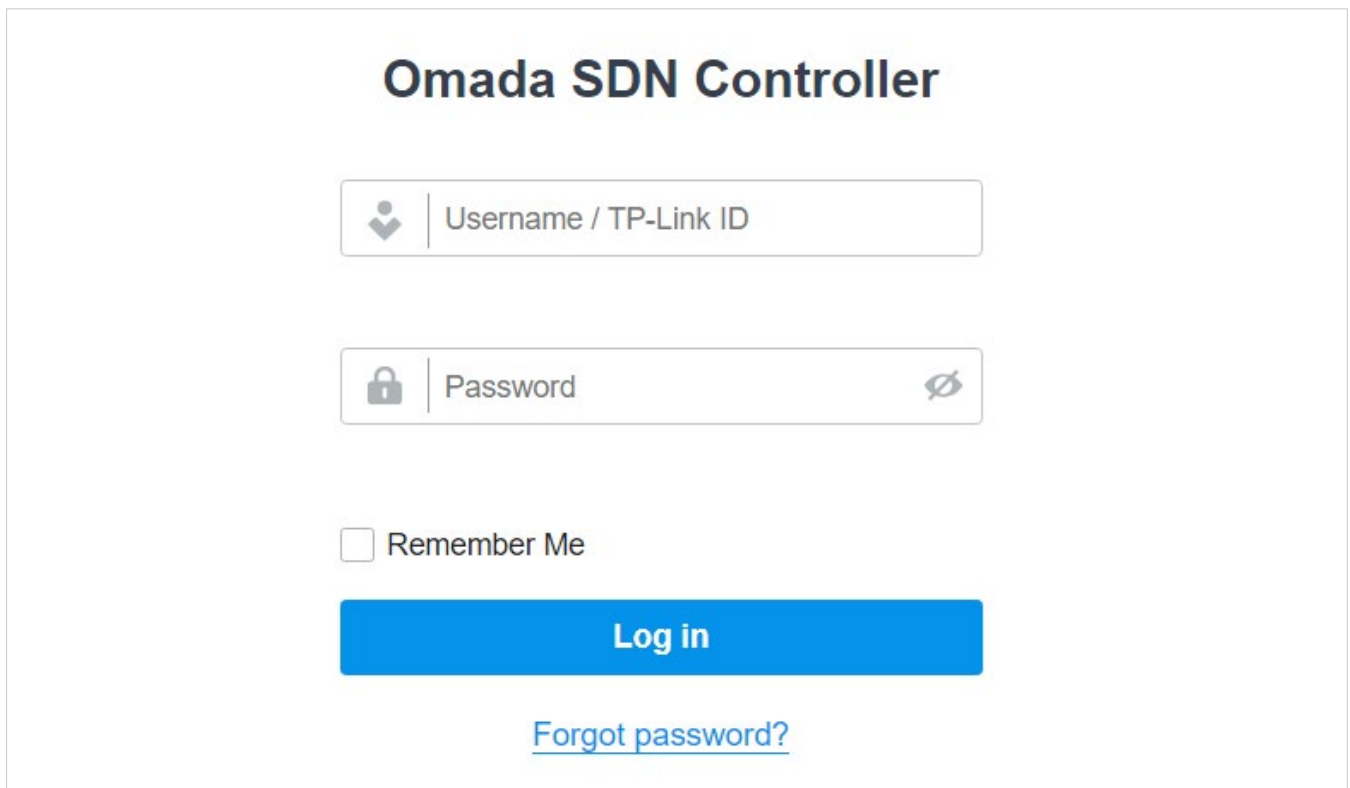


- 4. Follow the setup wizard to set up the controller.



Log In to the Management Interface

Once the basic configurations are finished, the browser will be redirected to the following page. Log in to the management interface using the username and password you have set in the basic configurations.



The image shows the login page for the Omada SDN Controller. At the top, the title "Omada SDN Controller" is displayed in a large, bold, black font. Below the title, there are two input fields. The first field is for the "Username / TP-Link ID" and contains a user icon on the left. The second field is for the "Password" and contains a lock icon on the left and a "show/hide" eye icon on the right. Below these fields is a checkbox labeled "Remember Me". At the bottom of the form is a prominent blue button with the text "Log in" in white. Below the button is a blue, underlined link that says "Forgot password?".

ⓘ Note:

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

♥ 2.3 Set Up Your Cloud-Based Controller

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

1. Contact the sales staff to grant the Omada Cloud-Based Controller permission.
2. 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.
3. Click [Add Controller](#) and register for an Omada Cloud-Based Controller. Follow the instructions to complete the setup process.
4. Add devices with the serial number, make sure the devices are online and in factory default.
5. Assign appropriate licenses in order to manage and configure the devices on the cloud-based controller. Then wait until your controller is deployed

For detailed information about device-based licensing, refer to <https://www.tp-link.com/omada-sdn/license/>.

ⓘ Note:

Only when you have available licenses can you register for the Cloud-Based Controller and manage the devices. To successfully register for a Cloud-Based Controller, purchase appropriate licenses.

3

Manage Omada Managed Devices and Sites

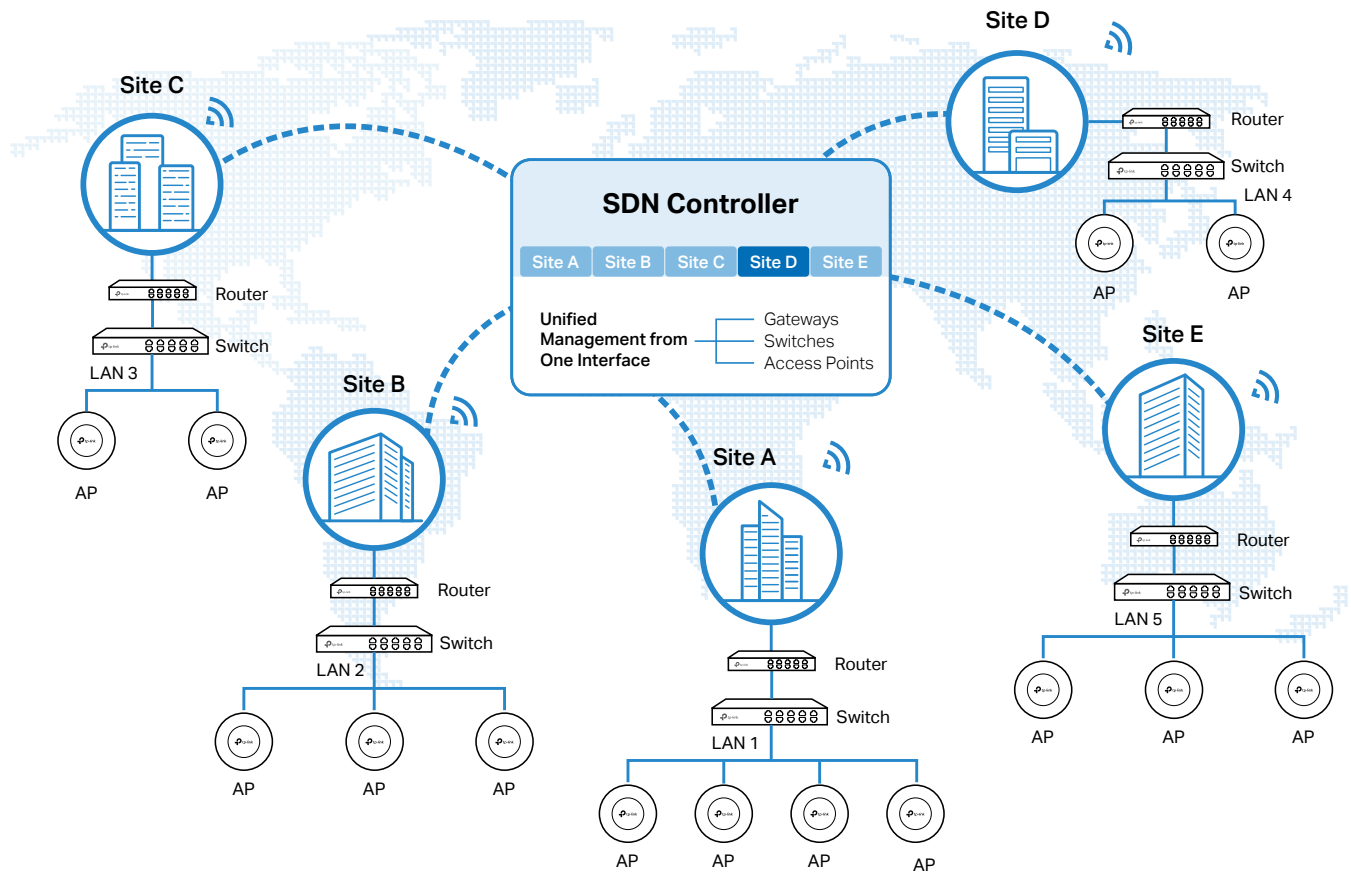
Start managing your network by creating sites and adopting devices so that you can configure and monitor your devices centrally while keeping things organized. The chapter includes the following sections:

- [3.1 Create Sites](#)
- [3.2 Adopt Devices](#)

♥ 3.1 Create Sites

Overview

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



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

Configuration

To create and manage a site, follow these steps:

- 1) Create a site.
- 2) View and edit the site.
- 3) Go into the site.

[Create a Site](#)[View and Edit the Site](#)[Go Into the Site](#)

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

■ Create a site from scratch

1. In Global view, click [Add New Site](#) in the [Site List](#) section.
2. Enter a [Site Name](#) to identify the site, and configure other parameters according to where the site is located. Create a username and password for login to newly adopted devices. Then click [Apply](#). The new site will be added to the [Site List](#) and the drop-down list of [Organization](#).

Add New Site ✕

Site Configuration

Name:

Country/Region:

Time Zone:

Application Scenario:

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

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

Address: (Optional) [Refresh](#)

Device Account ⓘ

Username:

Password:

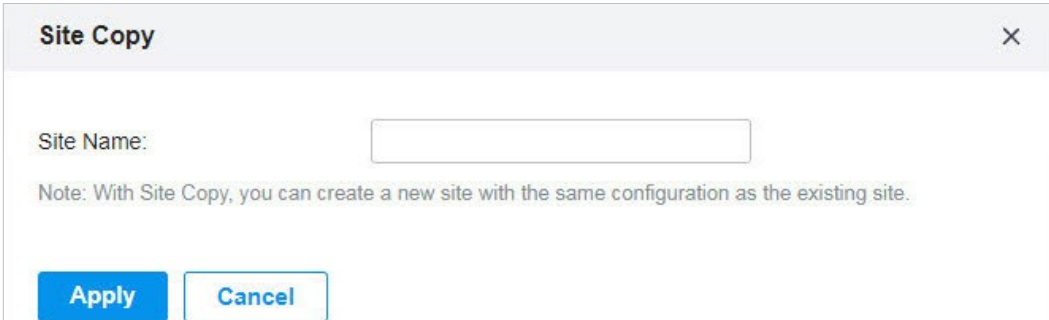
[Apply](#) [Cancel](#)

■ 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  in the ACTION column of the site which you want to copy.

2. Enter a [Site Name](#) to identify the new site. Click [Apply](#). The new site will be added to the [Site List](#) and the drop-down list of [Organization](#).



Site Copy [X]

Site Name:

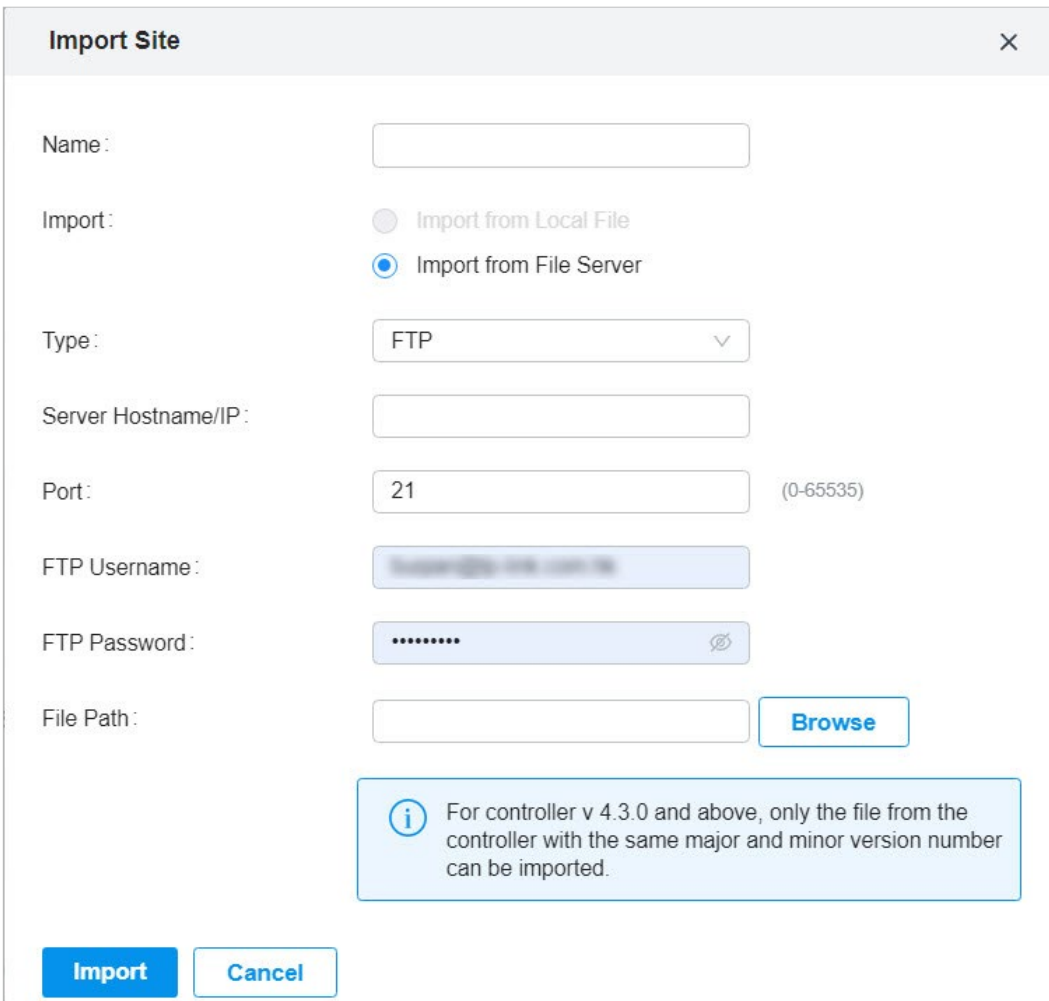
Note: With Site Copy, you can create a new site with the same configuration as the existing site.

[Apply](#) [Cancel](#)

■ Import a site from another controller

If you want to migrate seamlessly from an old controller to a new one, import the site configuration file of the old controller into the new one. Before that, you need to export the site configuration file from the old controller, which is covered in [5. 4. 1 Site Migration](#).

1. Click [Import Site](#) in the [Site List](#) section.
2. Enter a [Site Name](#) to identify the site, and configure other parameters according to actual site needs. Browse your file explorer and choose a site configuration file. Click [Import](#). The new site will be added to the [Site List](#) and the drop-down list of [Organization](#).



Import Site [X]

Name:

Import: Import from Local File
 Import from File Server

Type: [v]

Server Hostname/IP:

Port: (0-65535)

FTP Username:

FTP Password: [eye icon]

File Path: [Browse](#)

Import [Cancel](#)

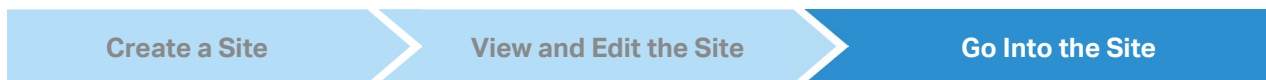
i For controller v 4.3.0 and above, only the file from the controller with the same major and minor version number can be imported.



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.

| NAME | COUNTRY/REGION | ALERTS | UPGRADE | GATEWAY | SWITCHES | EAPS | CLIENTS | ACTION |
|---------|----------------|--------|---------|---------|----------|-------------|---------|--------|
| Default | Netherlands | | | | 0 / 1 | 0 / 2 / 0 | | |
| Younity | United States | | | | 0 / 8 | 0 / 285 / 0 | | |

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



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

Click the icon of the site in the Site List to go into the site. Alternatively, select the site from the drop-down list of [Organization](#).

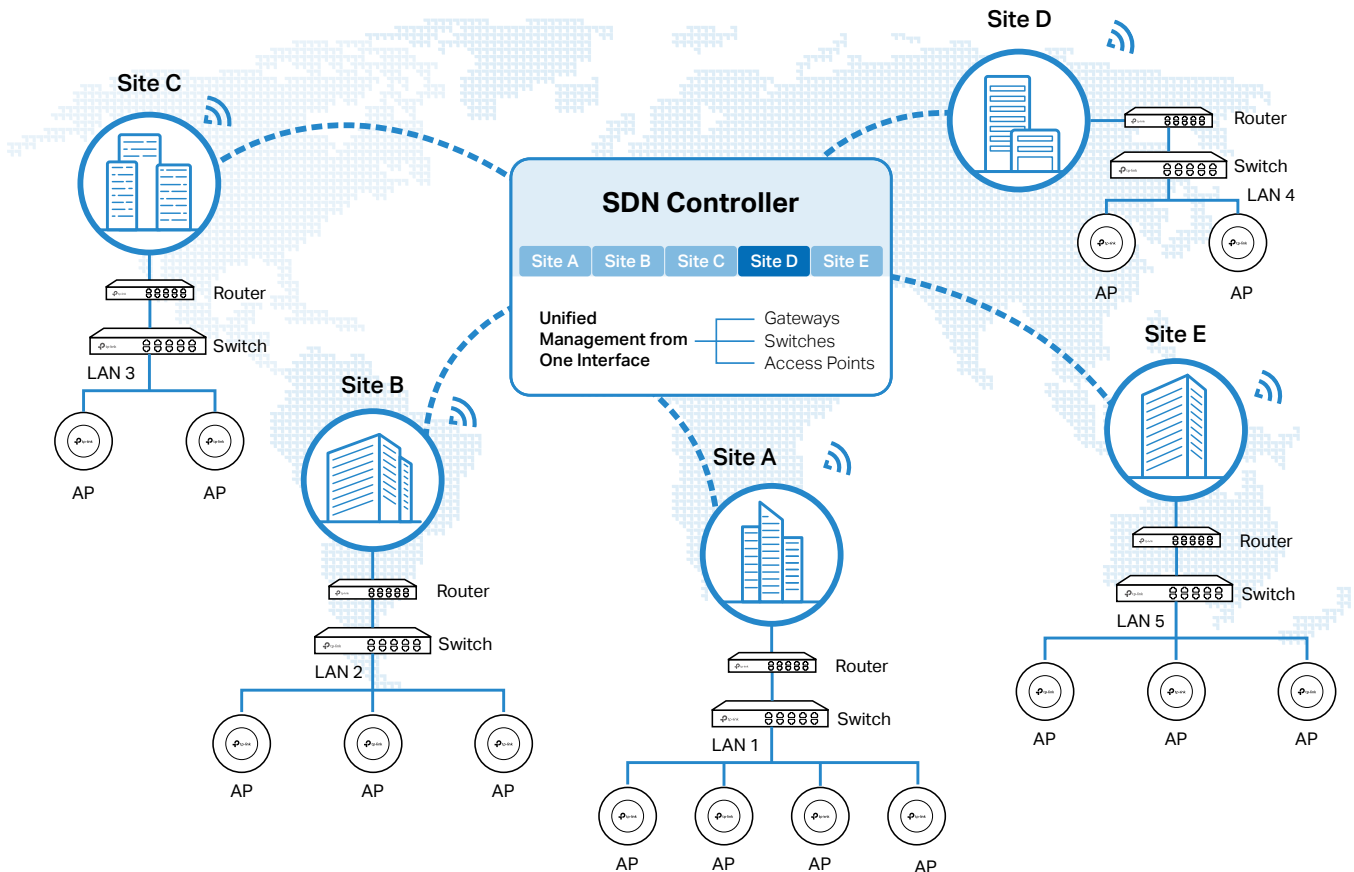
The screenshot shows the Omada Controller interface. At the top, there's a navigation bar with 'tp-link | omada | Omada Controller' and a 'DST' indicator. Below that is the 'Controller Overview' section with various metrics: 2 Sites, 0 Gateways, 9 Switches, 287 APs, and 0 Clients. A table below shows '2 Sites in 2 Countries' with columns for Connected/Disconnected status for Gateways, Switches, and APs, as well as Wired/Wireless Users and Guests. The 'Site List' section is visible at the bottom, showing a table with columns for Name, Country/Region, Alerts, Upgrade, Gateway, Switches, EAPS, Clients, and Action. The 'Organization' dropdown menu is open, showing 'Global View', 'Default', and 'Younity' options.

The [Organization](#) field indicates the site which you are currently in. Some configuration items in the menu are applied to the site which you are currently in, whereas others are applied to the whole controller.

♥ 3.2 Adopt Devices

Overview

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



Configuration

Choose a procedure according to the type of your controller:

- [3.2.1 For Software Controller / Hardware Controller](#)
- [3.2.2 For Cloud-Based Controller](#)

3.2.1 For Software Controller / Hardware Controller

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

- 1) Prepare for communication between the controller and devices.
- 2) Prepare for device discovery.
- 3) Adopt the devices.

**Prepare for Communication****Prepare for Device Discovery****Adopt the Devices****ⓘ Note:**

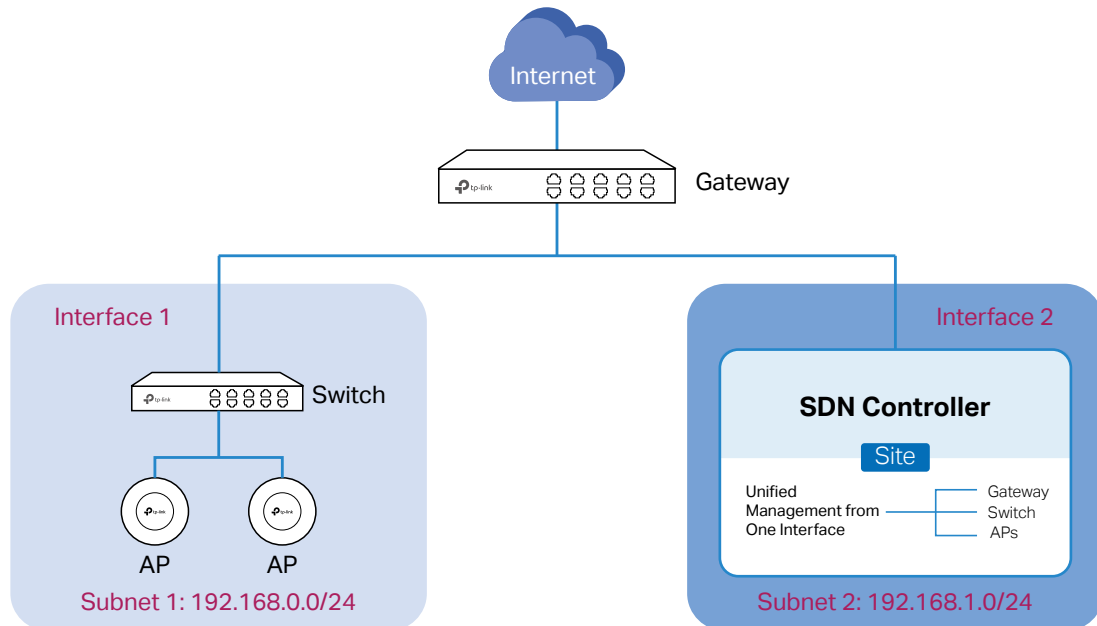
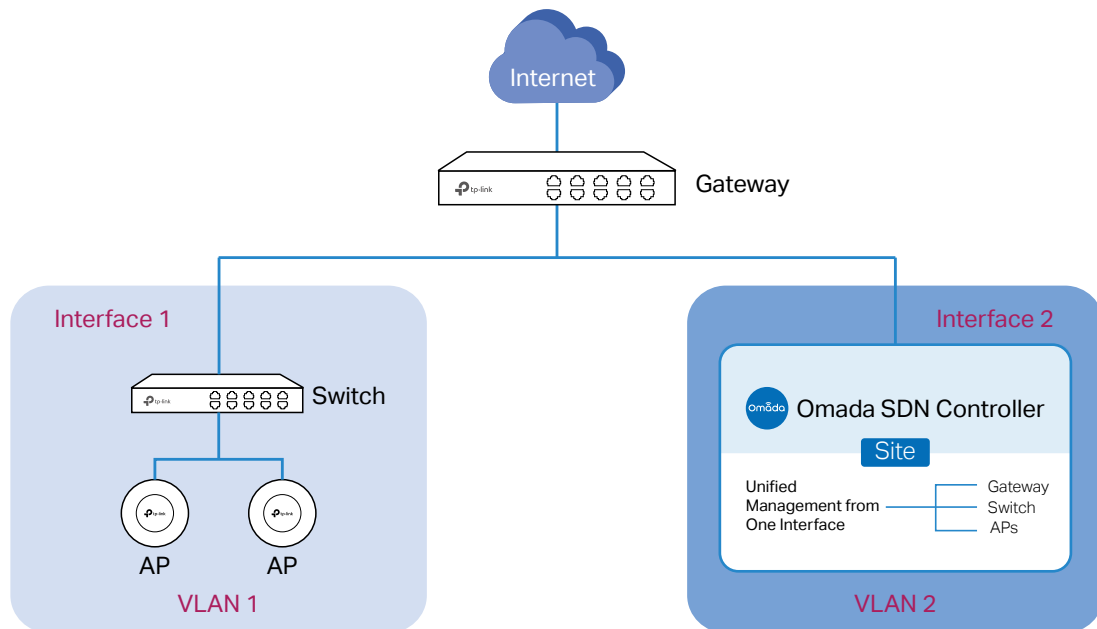
If the controller and devices are in the same LAN, subnet and VLAN, skip this step.

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

1. Set up the Network

■ Scenario 1: Across VLANs or Subnets

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



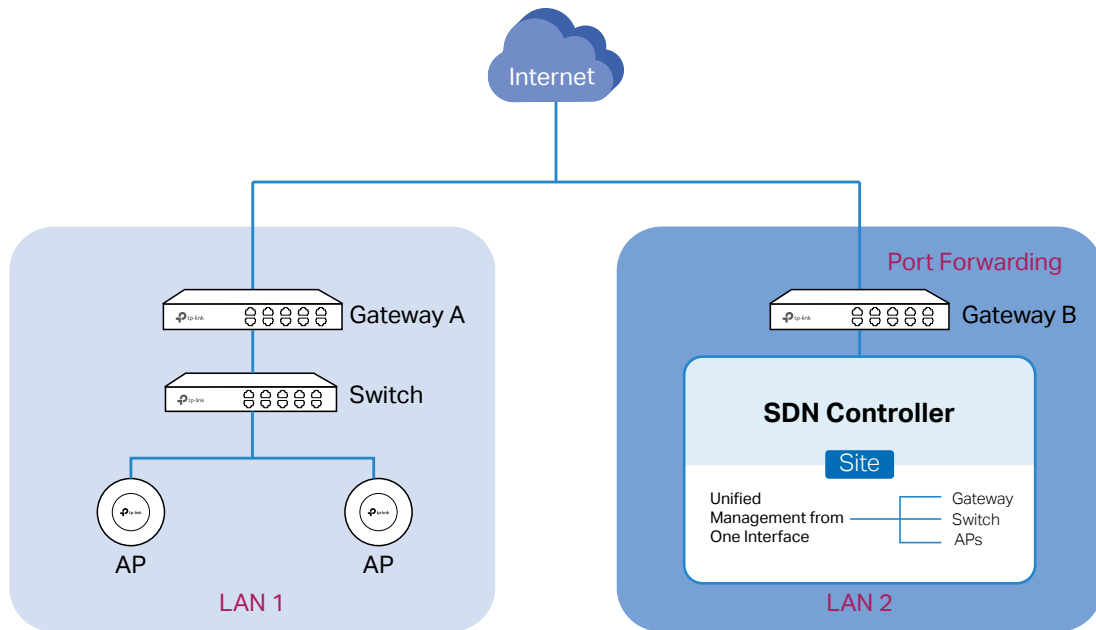
■ Scenario 2: Across LANs

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

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

- Use Port Forwarding

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



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

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

Create New Rule

Name:

Status: Enable

Source IP: Any
 Limited IP Address

Interface:

DMZ: Enable

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

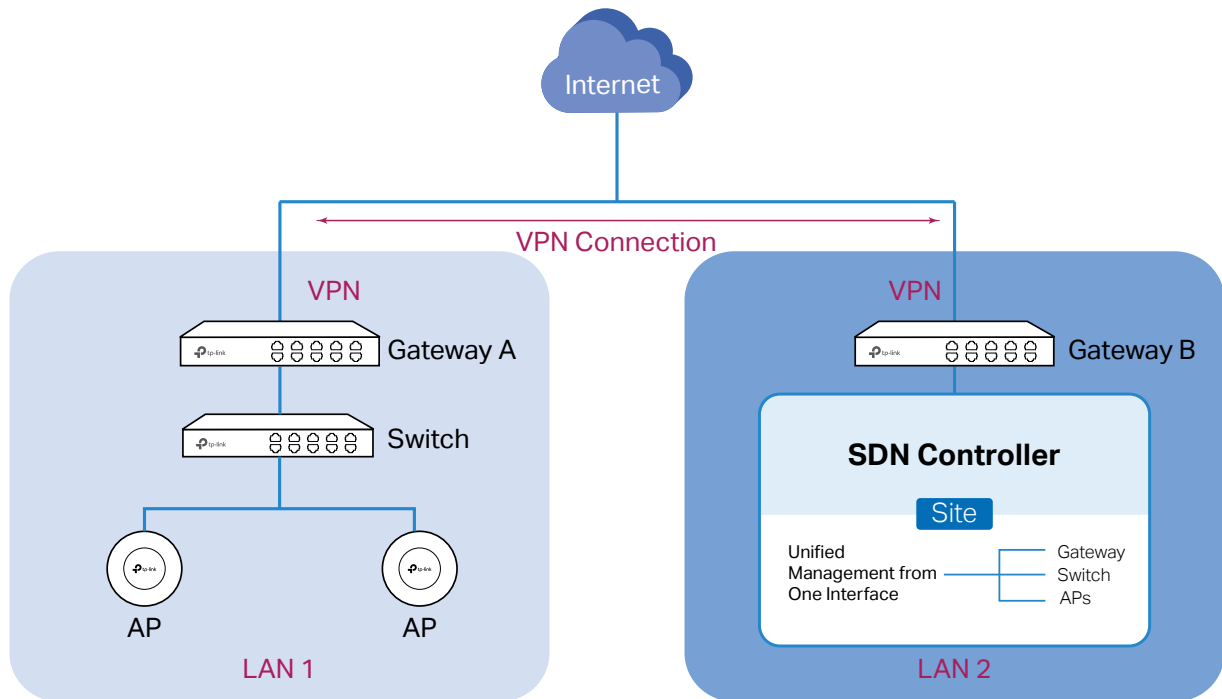
Destination IP:

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

Protocol: All
 TCP
 UDP

- Use VPN

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



2. (Optional) Test the network

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

Let's take a switch for example. Log into the web page of the switch in Standalone Mode. Then Go to [MAINTENANCE](#) > [Network Diagnostics](#) > [Ping](#) to load the following page, and specify Destination IP as the IP address of the controller (if you have configured Port Forwarding on the controller side, use the public WAN IP address of the gateway instead). Then click [Ping](#).

ⓘ Note:

To ping the router, please turn off Block WAN Ping on the [Settings](#) > [Network Security](#) > [Attack Defense](#) page.

Ping Config

Destination IP: (Format: 192.168.0.1 or 2001::1)

Ping Times: (1-10)

Data Size: bytes (1-1500)

Interval: milliseconds (100-1000)

[Ping](#)

Ping Result

Pinging 192.168.0.26 with 64 bytes of data:

Reply from 192.168.0.26 : bytes=64 time=19ms TTL=64

Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64

Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64

Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64

Ping statistics for 192.168.0.26 :

Packets: Sent=4, Received=4, Loss=0 (0%Loss)

Approximate round trip times in milliseconds:

Maximum=19ms, Minimum=3ms, Average=7ms

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

Prepare for Communication

Prepare for Device Discovery

Adopt the Devices

ⓘ Note:

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

Make sure that the controller can discover the devices.

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

■ Controller Inform URL

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

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

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

Cloud-Based Controller Management ?

Connection Status: Disabled

Cloud-Based Controller Management: Enable

Notes:
To enjoy centralized management on Omada Cloud-Based Controller, enable Cloud-Based Controller Management and add the device to the controller via its serial number.
You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.

Controller Inform URL

Inform URL/IP Address:

Notes:
Enter the inform URL or IP address of your controller to tell the device where to discover the controller.
This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.

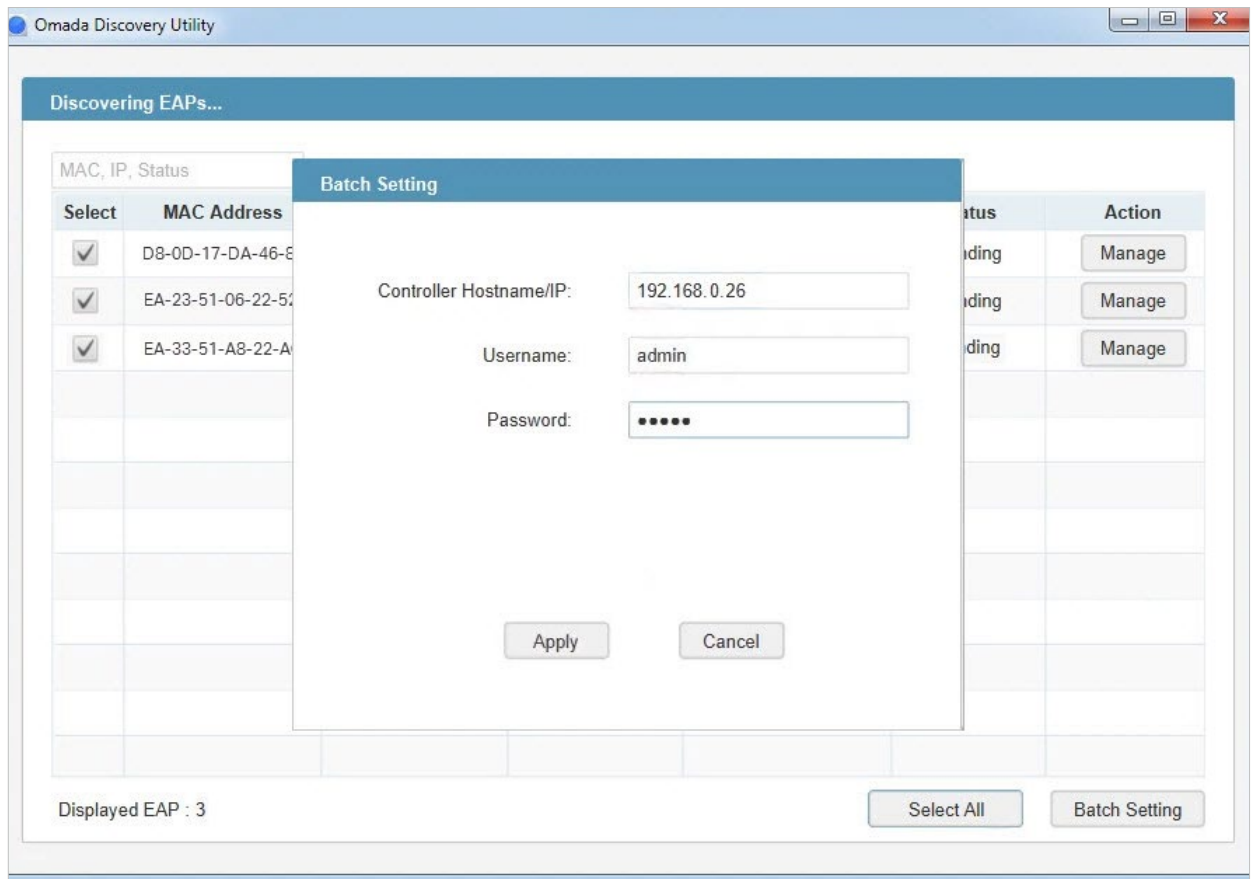
[Apply](#)

■ Discovery Utility

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

1. Download Discovery Utility from the https://www.tp-link.com/hk/support/download/omada-software-controller/#Omada_Discovery_Utility and then install it on your PC which should be located in the same LAN, subnet and VLAN as your devices.

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



■ DHCP Option 138

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

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

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

Edit Network

Name:

Purpose: Interface
 VLAN

LAN Interfaces: WAN/LAN2 WAN/LAN3 LAN1

VLAN: (1-4090) ⓘ

Gateway/Subnet: / ⓘ [Update DHCP Range](#)

| | |
|----------------------|-----------------------------|
| Gateway IP | 192.168.1.1 |
| Network Broadcast IP | 192.168.1.255 |
| Network IP Count | 254 |
| Network IP Range | 192.168.1.1 - 192.168.1.254 |
| Network Subnet Mask | 255.255.255.0 |

Domain Name: (Optional)

IGMP Snooping: Enable ⓘ

DHCP Server: Enable

DHCP Range: -

DNS Server: Auto
 Manual

Lease Time: minutes (2-2880)

Default Gateway: Auto
 Manual

DHCP Omada Controller: (Optional) ⓘ

Legal DHCP Servers: Enable ⓘ

Advanced DHCP Options

Option 60: (Optional) ⓘ

Option 66: (Optional) ⓘ

Option 138: (Optional) ⓘ

[Save](#) [Cancel](#)

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

Prepare for Communication

Prepare for Device Discovery

Adopt the Devices

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

The screenshot shows the Omada Controller interface. At the top, there's a navigation bar with 'tp-link omada | Omada Controller' and 'DST Organization: Global View'. Below this is the 'Controller Overview' section with various metrics: 2 Sites, 0 Gateways, 9 Switches, 287 APs, and 0 Clients. A dropdown menu for 'Organization' is open, showing 'Default' and 'Younity' options. Below the overview is the 'Site List' section with a search bar and a table of sites.

| NAME | COUNTRY/REGION | ALERTS | UPGRADE | GATEWAY | SWITCHES | EAPS | CLIENTS | ACTION |
|---------|----------------|--------|---------|---------|----------|-------------|-----------|------------------------|
| Default | Netherlands | 0 | | | 0 / 1 | 0 / 2 / 0 | 0 / 0 / 0 | [Edit] [Delete] [Home] |
| Younity | United States | 0 | | | 0 / 8 | 0 / 285 / 0 | 0 / 0 / 0 | [Edit] [Delete] [Home] |

2. Go to **Devices**, and devices which have been discovered by the controller are displayed.

The screenshot shows the 'Devices' section of the Omada Controller interface. It features a search bar at the top and a table of discovered devices. The table has columns for Device Name, IP Address, Status, Model, Version, Uptime, and Action. The status of devices is shown as 'CONNECTED', 'MANAGED BY OTHERS', or 'PENDING'.

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | ACTION |
|-------------------|--------------|-------------------|-----------------|---------|---------------------|---------------------------|
| 1C-61-B4-C5-48-83 | 192.168.0.1 | CONNECTED | ER605 v2.0 | 2.1.0 | 4day(s) 20h 22m ... | [Power] |
| 00-FF-00-05-40-5D | 192.168.0.18 | CONNECTED | TL-SG2428P v1.0 | 1.1.7 | 22day(s) 19h 49 ... | [Alert] [Power] [Refresh] |
| 00-00-FF-FC-30-92 | -- | MANAGED BY OTHERS | EAP770 v1.0 | -- | -- | [Checkmark] |
| 00-00-FF-FF-0D-28 | -- | PENDING | EAP225 v5.0 | -- | -- | [Checkmark] |
| 00-00-FF-FF-0F-BB | -- | PENDING | EAP225 v5.0 | -- | -- | [Checkmark] |

3. Click in the ACTION column of the devices which you want to add to the site. Wait until the STATUS turns into **Connected**. Then the devices are adopted by the controller and added to the current site. Once the devices are adopted, they are subject to central management in the site.

3.2.2 For Cloud-Based Controller

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

- 1) Connect to the internet.
- 2) Prepare for controller management.
- 3) Adopt the devices.

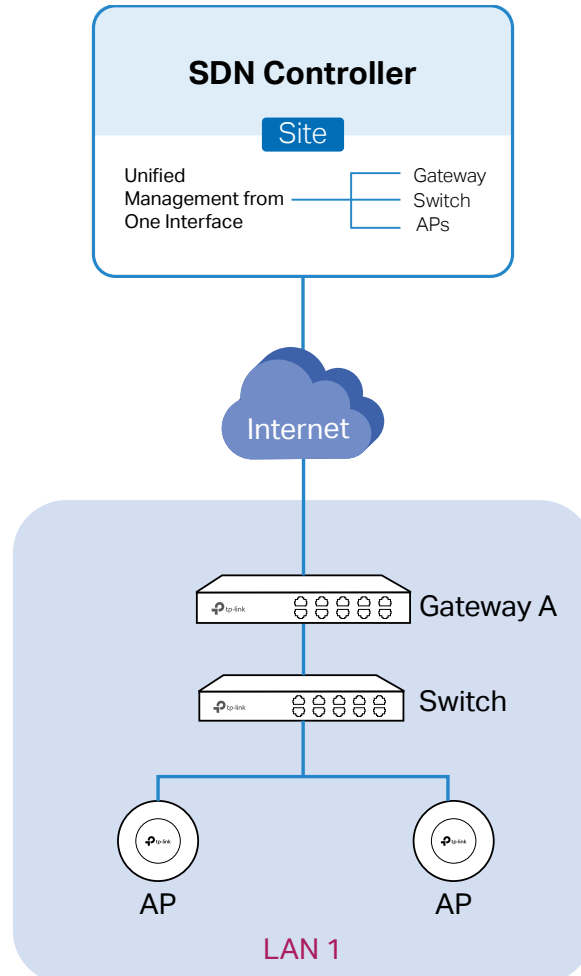
Connect to the Internet

Prepare for Controller Management

Adopt the Devices

1. Set up the network.

Make sure that your devices are connected to the internet.



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

2. (Optional) Test the network.

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

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

Ping Config

Destination IP: (Format: 192.168.0.1 or 2001::1)

Ping Times: (1-10)

Data Size: bytes (1-1500)

Interval: milliseconds (100-1000)

Ping

Ping Result

Pinging 8.8.8.8 with 64 bytes of data:

Reply from 8.8.8.8 : bytes=64 time=3ms TTL=64

Reply from 8.8.8.8 : bytes=64 time=3ms TTL=64

Reply from 8.8.8.8 : bytes=64 time=3ms TTL=64

Reply from 8.8.8.8 : bytes=64 time=3ms TTL=64

Ping statistics for 8.8.8.8 :

Packets: Sent=4, Received=4, Loss=0 (0%Loss)

Approximate round trip times in milliseconds:

Maximum=3ms , Minimum=3ms, Average=3ms

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

Connect to the Internet

Prepare for Controller Management

Adopt the Devices

ⓘ Note:

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

The Cloud-Based Controller Management feature allows the devices to be adopted by 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://www.tp-link.com/support/download/>.

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](#).

Cloud-Based Controller Management ?

Connection Status: Off-line

Cloud-Based Controller Management: [Enable](#)

Notes:
To enjoy centralized management on Omada Cloud-Based Controller, enable Cloud-Based Controller Management and add the device to the controller via its serial number.
You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.

Controller Inform URL

Inform URL/IP Address:

Notes:
Enter the inform URL or IP address of your controller to tell the device where to discover the controller.
This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.

[Apply](#)

Connect to the Internet

Prepare for Controller Management

Adopt the Devices

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

4

Configure the Network with the SDN Controller

This chapter guides you on how to configure the network with the SDN Controller. 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 routers, switches, and wireless access points. The chapter includes the following sections:

- [4. 1 Navigate the UI](#)
- [4. 2 Modify the Current Site Configuration](#)
- [4. 3 Configure Wired Networks](#)
- [4. 4 Configure Wireless Networks](#)
- [4. 5 Network Security](#)
- [4. 6 Transmission](#)
- [4. 7 Configure VPN](#)
- [4. 8 Create Profiles](#)
- [4. 9 Authentication](#)
- [4. 10 Services](#)
- [4. 11 CLI Configuration](#)

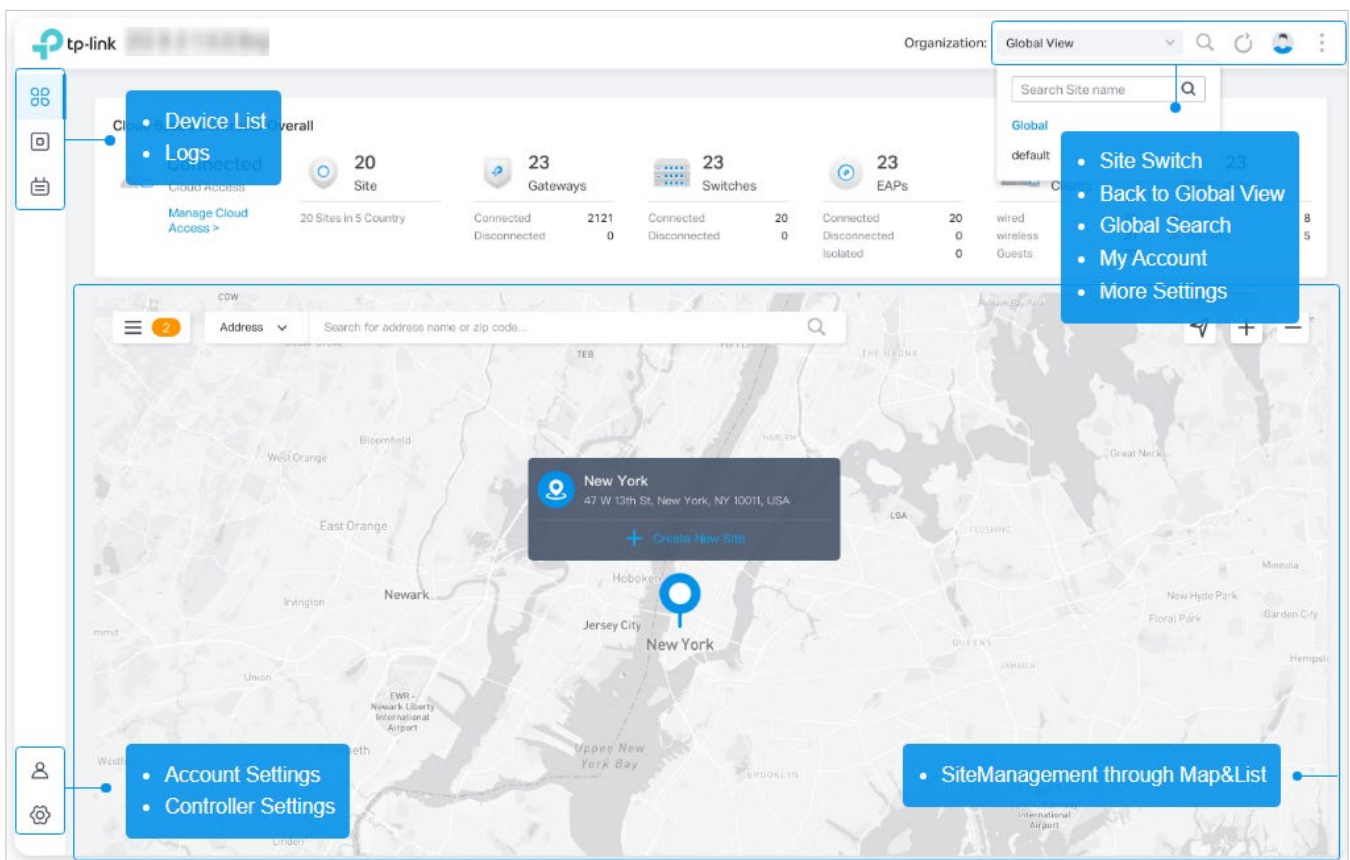
♥ 4.1 Navigate the UI

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

■ 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.



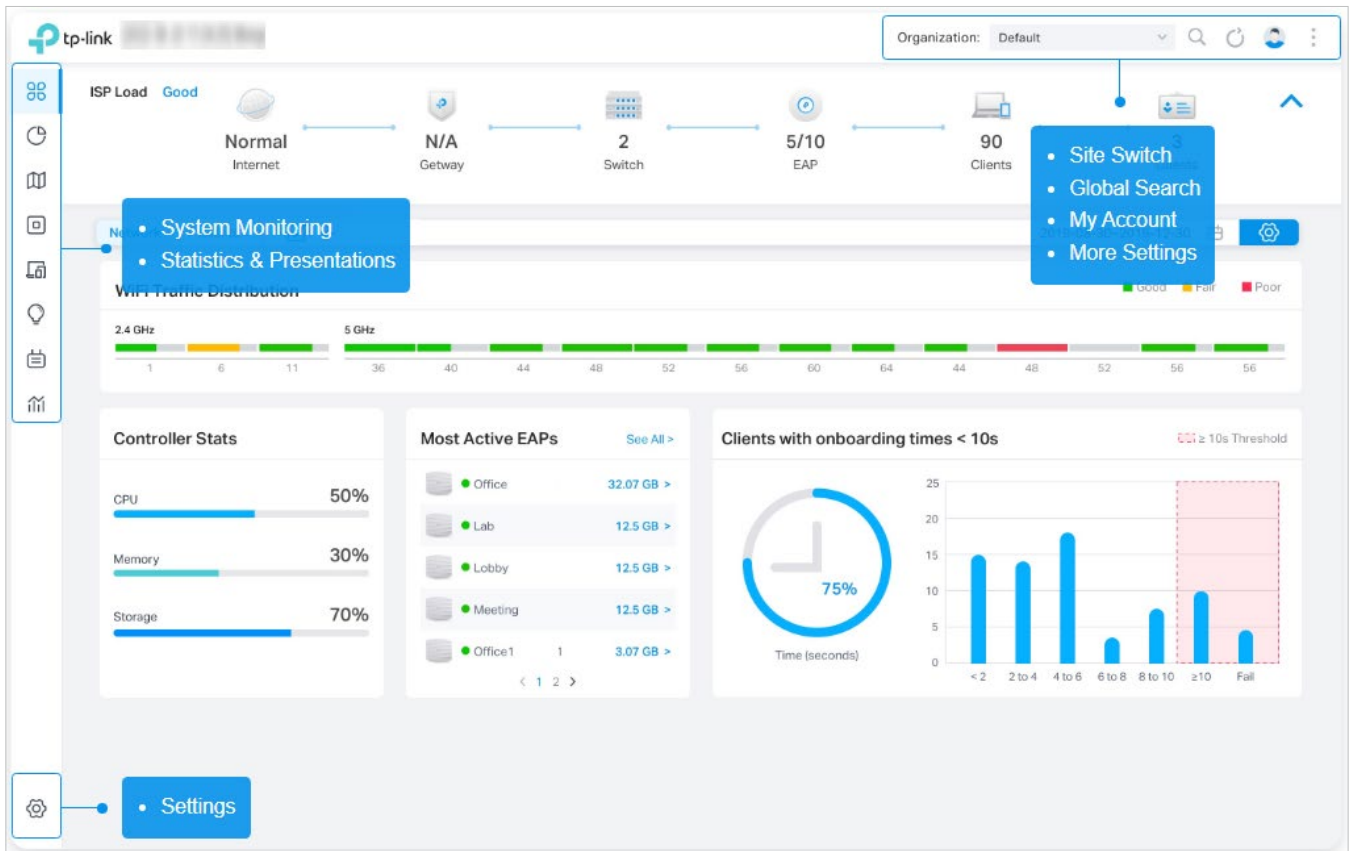
■ Site Overview

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

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

device and client.

- Settings—Configure all your network devices centrally.



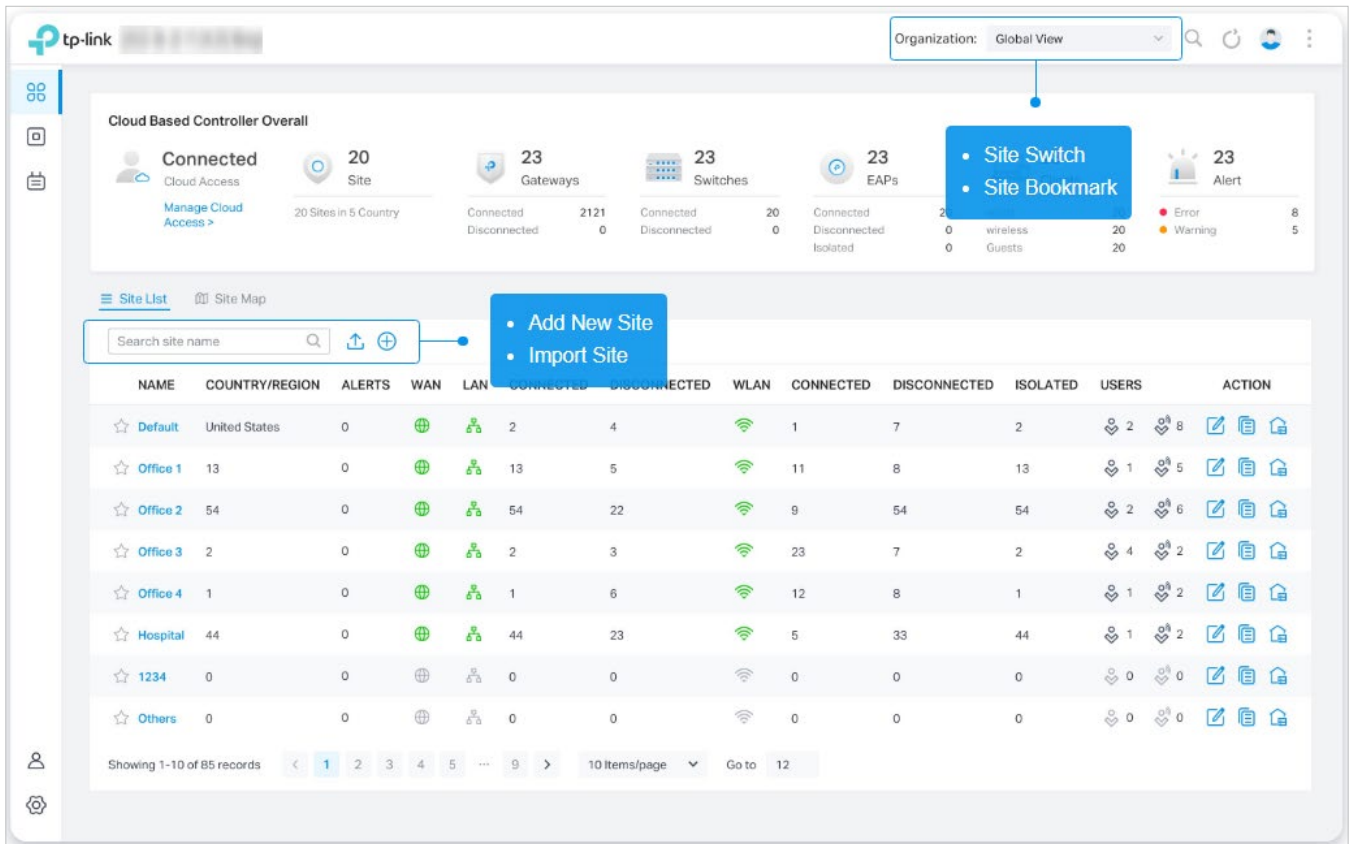
■ Site Overview

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

- Add New Site — Click Add New Site to add a new site, which is the logically separated network

location. The site is the largest unit for managing the network.

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

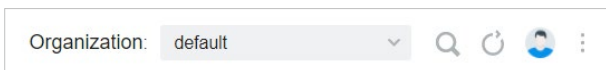


■ Network Monitoring

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

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

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




Organization Management

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.

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

Global Search Feature

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

My Account

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

More Settings

Click  to display Preferences, About, Tutorial and Feedback.











Preferences: Click to jump to Maintenance and customize the Controller UI depending on your needs. For details, refer to [5.3 Maintenance](#)

About: Click to display the controller version.

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

Feedback: Click to send your feedback to us.

The left-hand navigation bar provides access to:

| | |
|--|---|
|  Dashboard | <p>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.</p> |
|  Statistics | <p>Statistics provides a visual representation of the clients and network managed by the controller. The run charts show changes in device performances over time, including the status of switches and speed test results.</p> |
|  Map | <p>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.</p> |
|  Devices | <p>Device displays all TP-Link devices discovered on the site and their general information. This list view can change depending on your monitoring need through customizing the columns. You can click any device on the list to reveal the Properties window for more detailed information of each device and provisioning individual configurations to the device.</p> |
|  Clients | <p>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.</p> |
|  Insights | <p>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.</p> |
|  Logs | <p>Log shows log lines about varied activities of users, devices, and systems events, such as administrative actions and abnormal device behaviors. Comprehensive logs make historical information more accurate, readily accessible, and usable, which allows for proactive troubleshooting. And you can determine alert-level events and enable pushing notifications.</p> |
|  Tools | <p>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.</p> |
|  Reports | <p>Reports provides intuitive charts and detailed statistics concerning your network situation, managed devices, and connected clients.</p> |
|  Settings | <p>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.</p> |

♥ 4.2 Modify the Current Site Configuration

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

4.2.1 Site Configuration

Overview

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

Configuration

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

Site Configuration

Site Name:

Country/Region:

Time Zone: ⓘ

Daylight Saving Time: Enable

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

Time Offset:

Starts On: Week: Day: Month: Time:

Ends On: Week: Day: Month: Time:

Application Scenario:

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


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

Address: (Optional) [Refresh](#)

Site Name Specify the name of the current site. It should be no more than 64 characters.

Country/Region Select the location of the site.

Time Zone Select the time zone of the site.

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

4.2.2 Services

Overview

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

Configuration

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

Services

LED: Enable

Channel Limit: Enable [i](#)

Mesh: Enable [i](#)

Auto Failover: Enable [i](#)

Connectivity Detection:

Full-Sector DFS: Enable [i](#)

LLDP: Enable [i](#)


Remote Logging: Enable [i](#)

Syslog Server IP/Hostname:

Syslog Server Port: (1-65535)

Client Detail Logs: Enable [i](#)

Advanced Features: Enable

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

LED

Enable or disable LEDs of all devices in the site.

By default, the device follows the LED setting of the site it belongs to. To change the LED setting for certain devices, refer to [Chapter 6. Configure and Monitor Controller-Managed Devices](#).

Channel Limit

(For Outdoor APs) When enabled, outdoor APs do not use the channel with the frequency ranging from 5150 MHz to 5350 MHz to meet the local laws and regulations limit in EU countries.

Mesh

When enabled, APs supporting Mesh can establish the mesh network at the site.

Auto Failover

(For APs in the mesh network) Auto Failover is used to automatically maintain the mesh network. When enabled, the controller will automatically select a new wireless uplink for the AP if the original uplink fails.

To enable this feature, enable Mesh first.

| | |
|--|---|
| Connectivity Detection | <p>(For APs in the mesh network) Specify the method of Connection Detection when mesh is enabled.</p> <p>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.</p> <p>Auto (Recommended): Select this method and the mesh APs will send ARP request packets to the default gateway for the detection.</p> <p>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.</p> |
| Full-Sector DFS | <p>(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.</p> <p>To enable this feature, enable Mesh first.</p> |
| LLDP | <p>Click the checkbox to enable LLDP (Link Layer Discovery Protocol) for device discovery and auto-configuration of VoIP devices.</p> |
| Remote Logging | <p>With this feature configured, the controller will send generated site logs to the log server. When enabled, the following items are required:</p> <p>Syslog Server IP/Hostname: Enter the IP address or hostname of the log server.</p> <p>Syslog Server Port: Enter the port of the server.</p> <p>Client Detail Logs: With this feature enabled, the logs of clients will be sent to the syslog server.</p> |
| Advanced Features | <p>(For APs) When enabled, you can configure more features for APs in Advanced Features. When disabled, these features keep the default settings.</p> <p>For detailed configuration, refer to 4. 2. 3 Advanced Features.</p> |

4. 2. 3 Advanced Features

Overview

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

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

Configuration

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

Advanced Features

Fast Roaming: Enable [i](#)

AI Roaming: Enable [i](#)

Dual Band 11k Report: Enable [i](#)

Force-Disassociation: Enable [i](#)

Band Steering: [i](#)

Beacon Control

Beacon Interval: ms (40-100)

DTIM Period: (1-255)

RTS Threshold: (1-2347)

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

Airtime Fairness: Enable [i](#)

Fast Roaming

With this feature enabled, wireless clients that support 802.11k/v can improve fast roaming experience when moving among different APs.

By default, it is disabled. This feature is available for some certain devices.

AI Roaming

With Fast Roaming enabled, you can enable AI Roaming to facilitate Fast Roaming, which improves roaming experience of the wireless clients that support 802.11k/v. This feature is available for some certain devices.

Dual Band 11k Report

When disabled, the controller provides neighbor list that contains only neighbor APs in the same band with which the client is associated.

When enabled, the controller provides neighbor list that contains neighbor APs in both 2.4 GHz and 5 GHz bands.

This feature is available only when Fast Roaming is enabled. By default, it is disabled.

Force-Disassociation

With this feature disabled, the AP only issues an 802.11v roaming suggestion when a client's link quality drops below the predefined threshold and there is a better option of AP, but whether to roam or not is determined by the client.

With this feature enabled, the AP will force disassociate the client if it does not re-associate to another AP.

This feature is available only when Fast Roaming is enabled. By default, it is disabled.

Band Steering

Band steering can adjust the number of clients in 2.4 GHz, 5 GHz and 6 GHz bands to provide better wireless experience.

When enabled, multi-band clients will be steered to the 5 GHz and 6 GHz band according to the configured parameters. This function can improve the network performance because the 5 GHz and 6 GHz band supports a larger number of non-overlapping channels and is less noisy.

Beacon Control

Beacons are transmitted periodically by the AP to announce the presence of a wireless network for the clients. Click , select the band, and configure the following parameters of Beacon Control.

Beacon Interval: Specify how often the APs send a beacon to clients. By default, it is 100.

DTIM Period: Specify how often the clients check for buffered data that are still on the AP 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 has buffered data for client devices. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend that you keep the default interval, 1.

RTS Threshold: RTS (Request to Send) can ensure efficient data transmission by avoiding the conflict of packets. If a client wants to send a packet larger than the threshold, the RTS mechanism will be activated to delay packets of other clients in the same wireless network.

We recommend that you keep the default threshold, which is 2347. If you specify a low threshold value, the RTS mechanism may be activated more frequently to recover the network from possible interference or collisions. However, it also consumes more bandwidth and reduces the throughput of the packet.

Fragmentation Threshold: Fragmentation can limit the size of packets transmitted over the network. If a packet to be sent exceeds the Fragmentation threshold, the Fragmentation function will be activated, and the packet will be fragmented into several packets. By default, the threshold is 2346.

Fragmentation helps improve network performance if properly configured. However, too low fragmentation threshold may result in poor wireless performance because of the increased message traffic and the extra work of dividing up and reassembling frames.

Airtime Fairness: With this option enabled, each client connecting to the AP can get the same amount of time to transmit data so that low-data-rate clients do not occupy too much network bandwidth and network performance improves as a whole. We recommend you enable this function under multi-rate wireless networks.


4.2.4 Device Account

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

Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Site](#) and modify the username and password in [Device Account](#). Click [Save](#) and the new username and password are applied to all devices on the site.

Device Account

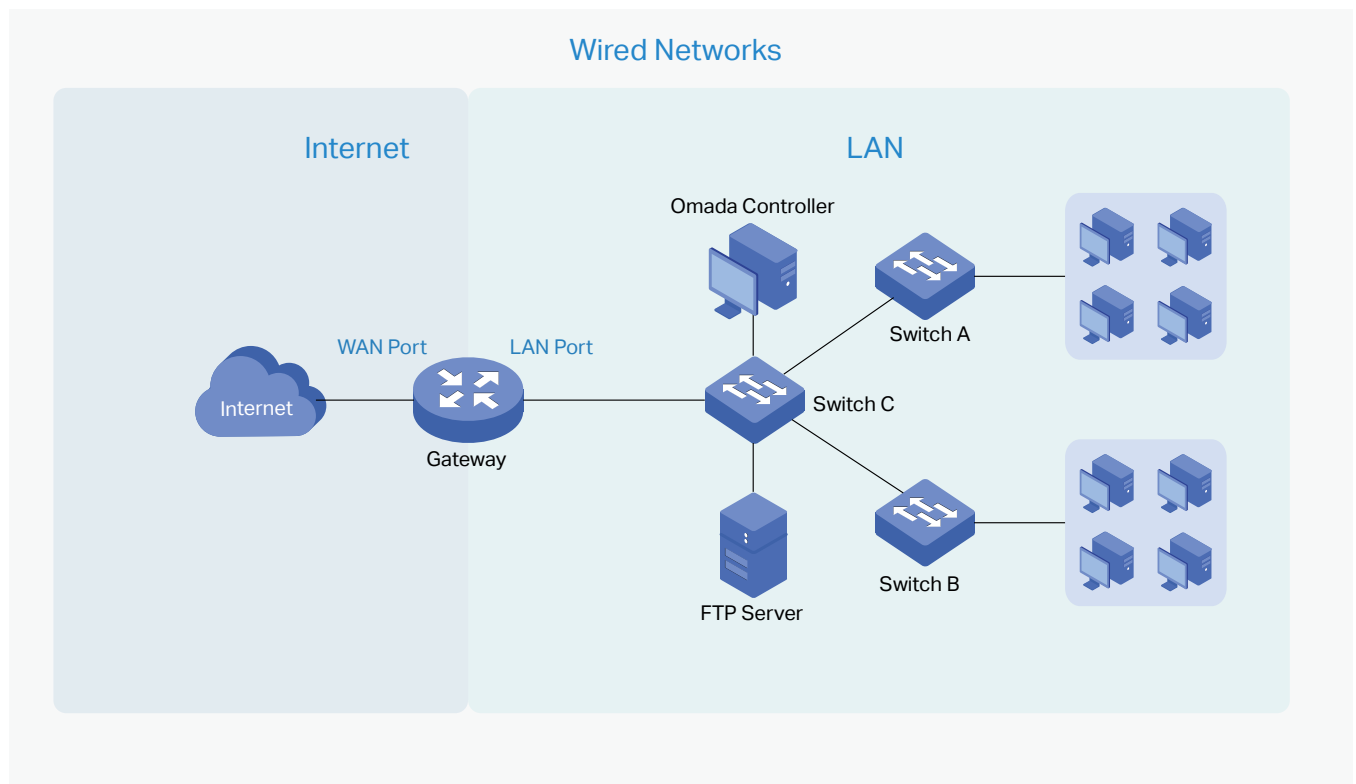
Username:

Password: 

♥ 4.3 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.

4.3.1 Set Up an Internet Connection

Configuration

To set up an internet connection, follow these steps:

- 1) Configure the number of WAN ports on the gateway based on needs.
- 2) Configure WAN Connections. You can set up the IPv4 connection, IPv6 connection, or both.
- 3) (Optional) Configure Load Balancing if more than one WAN port is configured.

Select WAN Mode

Configure WAN Connections

(Optional) Configure Load Balancing

Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Wired Networks](#) > [Internet](#) to load the following page. In [WAN Mode](#), configure the number of WAN ports deployed by the gateway and other parameters. Then click [Apply](#).

WAN Mode ?

WAN Settings Overrides:

?

- With WAN Settings Overrides disabled, the WAN settings of the newly adopted Omada gateway in standalone mode will take effect on the controller.
- When WAN Settings Overrides 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 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.
- If the adopted device does not support some pre-configurations, the relevant configurations will be deleted after adoption.

Gateway Model:

Online Detection Interval:

Custom Time: (1-3600)

?

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.

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.



Note:

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

- Set Up USB Modem Connection

Select a site from the drop-down list of **Organization**. Go to **Settings > Wired Networks > Internet**. In the **WAN Ports Config** section, click the edit icon of USB Modem and configure the parameters.

USB Modem

Description: (Optional)

USB Modem: No USB modem Connected.

Config Type: ▼

Location: ▼

Mobile ISP: ▼

SIM/UIM PIN: (Optional)

Connection Mode: Connect Automatically
 Connect Manually

Authentication Type: ▼

MTU Size: bytes ⓘ

Use the following DNS Servers: Enable

| | |
|--------------------|---|
| 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 on the device page, refer to 6. 2. 2 Monitor the Gateway . |
| Authentication Mode | Select the Authentication mode for the USB modem. The default value is Auto, and it is recommended to keep the default value. |
| MTU Size | Specify the MTU (Maximum Transmission Unit) of the USB WAN port. The default value is 1480, and it is recommended to keep the default value. MTU is the maximum data unit transmitted in the physical network. |
| Use the following DNS Servers | Enable the feature if you want to specify the Primary and Secondary DNS servers manually. |

- **Set Up IPv4 Connection**

Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Wired Networks](#) > [Internet](#). 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.

IPv4

Connection Type: Dynamic IP ▼

Advanced Settings

Unicast DHCP: Enable ⓘ

Primary DNS Server: . . . (Optional)

Secondary DNS Server: . . . (Optional)

Host Name: (Optional)

MTU: 1500 (576-1500, default:1500)

Internet VLAN: Enable

WAN IP Alias

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.

Internet VLAN

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.

Internet VLAN Priority

Priority is only available when Internet VLAN is enabled. The Internet 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.

IPv4

Connection Type: Static IP ▼

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . . (Optional)

Advanced Settings

Primary DNS Server: . . . (Optional)

Secondary DNS Server: . . . (Optional)

MTU: 1500 (576-1500, default:1500)

Internet VLAN: Enable

WAN IP Alias

| | |
|---|--|
| 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. |
| Internet VLAN | 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. |
| Internet VLAN Priority | Priority is only available when Internet VLAN is enabled. The Internet 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.

IPv4

Connection Type:

Username:

Password:

Advanced Settings

Get IP Address from ISP: Enable

Primary DNS Server: (Optional)

Secondary DNS Server: (Optional)

Connection Mode: Connect Automatically
 Connect Manually
 Time-based

Redial Interval: Seconds (1-99999)

Service Name: (Optional) ⓘ

MTU: (576-1492, default:1492)

MRU: (576-1492, default:1492)

MSS Clamping: Disable
 Auto
 Custom (532-1452)

Internet VLAN: Enable

Secondary Connection: None
 Static IP
 Dynamic IP

Username Enter the PPPoE username provided by your ISP.

Password Enter the PPPoE password provided by your ISP.

| | |
|---|--|
| Get IP address from ISP | <p>With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection.</p> <p>With this option disabled, you need to specify the IP Address provided by your ISP.</p> |
| Primary DNS Server / Secondary DNS Server | Enter the IP address of the DNS server provided by your ISP if there is any. |
| Connection Mode | <p>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.</p> <p>Connect Manually: You can manually activate or terminate the connection.</p> <p>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.</p> |
| Service Name | Keep it blank unless your ISP requires you to configure it. |
| MTU | <p>Specify the MTU (Maximum Transmission Unit) of the WAN port.</p> <p>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.</p> |
| 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 | <p>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</p> <p>Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties.</p> <p>Auto: Automatically calculate MSS value based on path MTU.</p> <p>Custom: Select this option to specify the MSS value. It should not exceed the MTU value.</p> |
| Internet VLAN | 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. |
| Internet VLAN Priority | Priority is only available when Internet VLAN is enabled. The Internet 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.

IPv4

Connection Type:

Username:

Password: 

VPN Server/Domain Name:

Get IP Address from ISP: Enable

Primary DNS Server: . . (Optional)

Secondary DNS Server: . . (Optional)

Connection Mode: Connect Automatically
 Connect Manually
 Time-based

Redial Interval: Seconds (1-99999)

MTU: (576-1460, default:1460)

MSS Clamping: Disable
 Auto
 Custom (532-1452)

Internet VLAN: Enable

Secondary Connection: Static IP
 Dynamic IP

| | |
|---------------------------------|--|
| 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 | <p>With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection.</p> <p>With this option disabled, you need to specify the IP address provided by your ISP.</p> |

| | |
|--|--|
| Primary DNS Server / Secondary DNS Server | Enter the IP address of the DNS server provided by your ISP if there is any. |
| Connection Mode | <p>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.</p> <p>Connect Manually: You can manually activate or terminate the connection.</p> <p>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.</p> |
| MTU | <p>Specify the MTU (Maximum Transmission Unit) of the WAN port.</p> <p>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.</p> |
| MSS Clamping | <p>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</p> <p>Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties.</p> <p>Auto: Automatically calculate MSS value based on path MTU.</p> <p>Custom: Select this option to specify the MSS value. It should not exceed the MTU value.</p> |
| Internet VLAN | 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. |
| Internet VLAN Priority | Priority is only available when Internet VLAN is enabled. The Internet 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 | <p>Select the connection type required by your ISP.</p> <p>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.</p> <p>Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection.</p> |

■ PPTP

Choose Connection Type as PPTP and configure the parameters.

IPv4

Connection Type:

Username:

Password:

VPN Server/Domain Name:

Get IP Address from ISP: Enable

Primary DNS Server: (Optional)

Secondary DNS Server: (Optional)

Connection Mode: Connect Automatically
 Connect Manually
 Time-based

Redial Interval: Seconds (1-99999)

MTU: (576-1420, default:1420)

MSS Clamping: Disable
 Auto
 Custom (532-1452)

Internet VLAN: Enable

Secondary Connection: Static IP
 Dynamic IP

| | |
|---|--|
| 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 | <p>With this option enabled, the gateway gets IP address from ISP when setting up the WAN connection.</p> <p>With this option disabled, you need to specify the IP address provided by your ISP.</p> |
| Primary DNS Server / Secondary DNS Server | Enter the IP address of the DNS server provided by your ISP if there is any. |

| | |
|------------------------|--|
| Connection Mode | <p>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.</p> <p>Connect Manually: You can manually activate or terminate the connection.</p> <p>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.</p> |
| MTU | <p>Specify the MTU (Maximum Transmission Unit) of the WAN port.</p> <p>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.</p> |
| MSS Clamping | <p>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</p> <p>Disabled: Disable the MSS Clamping function, and the gateway will not intervene in the MSS value negotiated by the communication parties.</p> <p>Auto: Automatically calculate MSS value based on path MTU.</p> <p>Custom: Select this option to specify the MSS value. It should not exceed the MTU value.</p> |
| Internet VLAN | <p>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.</p> |
| Internet VLAN Priority | <p>Priority is only available when Internet VLAN is enabled. The Internet 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.</p> |

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.

| | | |
|-------------------------|--|-----------|
| Connection Type: | Dynamic IP (SLAAC/DHCPv6) ▾ | |
| Get IPv6 Address: | <input checked="" type="radio"/> Automatically <input type="radio"/> Via SLAAC <input type="radio"/> Via DHCPv6 <input type="radio"/> Non-Address | |
| Prefix Delegation: | <input checked="" type="checkbox"/> Enable ⓘ | |
| Prefix Delegation Size: | <input type="text"/> | (48-64) ⓘ |
| DNS Address: | <input checked="" type="radio"/> Get from ISP Dynamically <input type="radio"/> Use the Following DNS Addresses | |

Get IPv6 Address

Select the proper method whereby your ISP assigns IPv6 address to your gateway.

Automatically: With this option selected, the gateway will automatically select SLAAC or DHCPv6 to get IPv6 addresses.

Via SLAAC: With SLAAC (Stateless Address Auto-Configuration) selected, your ISP assigns the IPv6 address prefix to the gateway and the gateway automatically generates its own IPv6 address. Also, your ISP assigns other parameters including the DNS server address to the gateway.

Via DHCPv6: With DHCPv6 selected, your ISP assigns an IPv6 address and other parameters including the DNS server address to the gateway using DHCPv6.

Non-Address: With this option selected, the gateway will not get an IPv6 address.

Prefix Delegation

Select Enable to get an address prefix by DHCPv6 server from your ISP, or Disable to designate an address prefix for your LAN port manually. Clients in LAN will get an IPv6 address with this prefix.

Prefix Delegation Size

With Prefix Delegation enabled, enter the Prefix Delegation Size to determine the length of the address prefix. If you are not sure about the value, you can ask your ISP.

DNS Address

Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually.

Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP.

Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

■ Static IP

Choose Connection Type as Static IP and configure the parameters.

| | | |
|-----------------------|--|----------------------------|
| Connection Type: | <input type="text" value="Static IP"/> | |
| IPv6 Address: | <input type="text"/> | (Format: 2001::) |
| Prefix Length: | <input type="text"/> | (1-128) ⓘ |
| Default Gateway: | <input type="text"/> | (Format: 2001::) |
| Primary DNS Server: | <input type="text"/> | (Format: 2001::) |
| Secondary DNS Server: | <input type="text"/> | (Optional. Format: 2001::) |

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

■ PPPoE

Choose Connection Type as PPPoE and configure the following parameters. Then click [Apply](#).

| | |
|-------------------------|--|
| Connection Type: | <input type="text" value="PPPoE"/> |
| | <input type="checkbox"/> Share the same PPPoE session with IPv4 |
| Username: | <input type="text"/> |
| Password: | <input type="password"/> |
| Get IPv6 Address: | <input checked="" type="radio"/> Automatically <input type="radio"/> Via SLAAC <input type="radio"/> Via DHCPv6 <input type="radio"/> Non-Address <input type="radio"/> Specified by ISP |
| Prefix Delegation: | <input checked="" type="checkbox"/> Enable i |
| Prefix Delegation Size: | <input type="text"/> (48-64) i |
| DNS Address: | <input checked="" type="radio"/> Get from ISP Dynamically <input type="radio"/> Use the Following DNS Addresses |

Share the same PPPoE session with IPv4

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

Username

Enter the username of your PPPoE account provided by your ISP.

Password

Enter the password of your PPPoE account provided by your ISP.

| | |
|-------------------------------|--|
| Get IPv6 Address | <p>Select the proper method whereby your ISP assigns IPv6 address to your gateway.</p> <p>Automatically: With this option selected, the gateway will automatically select the method to get IPv6 addresses between SLAAC and DHCPv6.</p> <p>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.</p> <p>Via DHCPv6: With DHCPv6 selected, your ISP assigns an IPv6 address and other parameters including the DNS server address to the gateway using DHCPv6.</p> <p>Non-Address: With this option selected, the gateway will not get an IPv6 address.</p> <p>Specified by ISP: With this option selected, enter the IPv6 address you get from your ISP.</p> |
| Prefix Delegation | <p>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.</p> |
| Prefix Delegation Size | <p>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.</p> |
| DNS Address | <p>Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually.</p> <p>Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP.</p> <p>Use the Following DNS Addresses: Enter the DNS address provided by the ISP.</p> |

■ 6to4 Tunnel

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

Connection Type: 6to4 Tunnel ▼

! If you want to configure the IPv6 address on the LAN side, it is recommended to use the SLAAC+Stateless DHCP or SLAAC+RDNSS dialing method on the LAN side. If you want to use the DHCPv6 configuration, ensure that the first 48 bits are the same as the 6to4 IPv6 address on the WAN side; otherwise IPv6 WAN-LAN connection may not work.

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

DNS Address

Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually.

Get from ISP Dynamically: The DNS address will be automatically assigned by the ISP.

Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

■ Pass-Through (Bridge)

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

Connection Type: Pass-Through(Bridge) ▼

• Set Up MAC Address

Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Wired 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.

Select WAN Mode

Configure WAN Connections

(Optional) Configure Load Balancing

ⓘ Note:

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

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

Load Balancing

Load Balancing Weight: : Pre-Populate

Application Optimized Routing: Enable i

Link Backup: Enable

Backup WAN: v

Primary WAN: v

Backup Mode:

Link Backup i

Always Link Primary i

Mode:

Enable backup link when any primary WAN fails

Enable backup link when all primary WANs fail

Load Balancing Weight

Specify the ratio of network traffic that each WAN port carries.

Alternatively, you can click [Pre-Populate](#) to test the speed of WAN ports and automatically fill in the appropriate ratio according to test result.

Application Optimized Routing

With Application Optimized Routing enabled, the router will consider the source IP address and destination IP address (or destination port) of the packets as a whole and record the WAN port they pass through. Then the packets with the same source IP address and destination IP address (or destination port) will be forwarded to the recorded WAN port.

This feature ensures that multi-connected applications work properly.

Link Backup

With Link Backup enabled, the router will switch all the new sessions from dropped lines automatically to another to keep an always on-line network.

Backup WAN / Primary WAN

The backup WAN port backs up the traffic for the primary WAN ports under the specified condition.

Backup Mode

Link Backup: The system will switch all the new sessions from dropped line automatically to another to keep an always on-link network.

Always Link Primary: Traffic is always forwarded through the primary WAN port unless it fails. The system will try to forward the traffic via the backup WAN port when it fails, and switch back when it recovers.

Mode

Select whether to enable backup link when any primary WAN fails or all primary WANs fail.

4.3.2 Configure LAN Networks

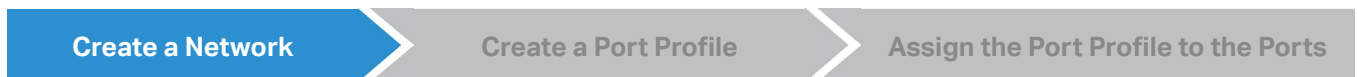
Overview

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.



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

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

Showing 1-1 of 1 records < 1 > 10 /page Go To page: adm1 **GO**

[+ Create New LAN](#)

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

Create New LAN

Name:

Purpose: Interface VLAN

Purpose

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

VLAN: Create the network as a Layer 2 VLAN.

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

■ Interface

Create New LAN

Name:

Purpose: Interface
 VLAN

LAN Interfaces: WAN/LAN1 WAN/LAN2 LAN1 LAN2

VLAN: (1-4090) ⓘ

Gateway/Subnet: / ⓘ

Domain Name: (Optional)

IGMP Snooping: Enable ⓘ

DHCP Server: Enable

DHCP Range: -

DNS Server: Auto
 Manual

Lease Time: 120 minutes (2-2880)

Default Gateway: Auto
 Manual

DHCP Omada Controller: (Optional) ⓘ

Legal DHCP Servers: Enable ⓘ

DHCP L2 Relay: Enable ⓘ

Advanced DHCP Options

Option 60: (Optional) ⓘ

Option 66: (Optional) ⓘ

Option 138: (Optional) ⓘ

Configure IPv6

LAN Interface

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

| | |
|-----------------------|--|
| VLAN | Enter a VLAN ID with the values between 1 and 4090. Each VLAN can be uniquely identified by VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame. |
| Gateway/Subnet | Enter the IP address and subnet mask in the CIDR format. The CIDR Notation here includes the IP address and subnet mask of the default gateway. The summary of the information that you entered will show up below in real time. |
| Domain Name | Enter the domain name. |
| IGMP Snooping | Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic. |
| DHCP Server | Click the checkbox to allow the Gateway to serve as the DHCP server for this network. A DHCP server assigns IP addresses, DNS server, default gateway, and other parameters to all devices in the network. Deselect the box if there is already a DHCP server in the network. |
| DHCP Range | Enter the starting and ending IP addresses of the DHCP address pool in the fields provided. For quick operation, click the Update DHCP Range beside the Gateway/Subnet entry to get the IP address range populated automatically, and edit the range according to your needs. |
| DNS Server | Select a method to configure the DNS server for the network. Auto: The DHCP server automatically assigns DNS server for devices in the network. It uses the IP address specified in the Gateway/Subnet entry as the DNS server address. Manual: Specify DNS servers manually. Enter the IP address of a server in each DNS server field. |
| Lease Time | Specify how long a client can use the IP address assigned from this address pool. |
| Default Gateway | Enter the IP address of the default gateway. Auto: The DHCP server automatically assigns default gateway for devices in the network. It uses the IP address specified in the Gateway/Subnet entry as the default gateway address. Manual: Specify default gateway manually. Enter the IP address of the default gateway in the field. |
| DHCP Omada Controller | Enter the IP address of the Controller. The DHCP server uses this IP address as Option 138 in DHCP packets to tell clients where the controller is. |
| Legal DHCP Servers | Click the checkbox to specify legal DHCP servers for the network. With legal DHCP servers configured, Gateways and Switches ensure that clients get IP addresses only from the DHCP servers specified here. |
| DHCP L2 Relay | Click the checkbox to enable DHCP L2 Relay for the network. |
| Option 60 | Enter the value for DHCP Option 60. DHCP clients use this field to optionally identify the vendor type and configuration of a DHCP client. Mostly it is used in the scenario where the APs apply for different IP addresses from different servers according to the needs. |

Option 66 Enter the value for DHCP Option 66. It specifies the TFTP server information and supports a single TFTP server IP address.

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

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

Configure IPv6

IPv6 Interface Type:

Gateway/Subnet: / ⓘ

DHCP Range: -

Lease Time: minutes (1-11520)

DHCPv6 DNS: Auto Manual

IPv6 Interface Type Configure the type of assigning IPv6 address to the clients in the local network.

None: IPv6 connection is not enabled for the clients in the local network.

DHCPv6: The gateway assigns an IPv6 address and other parameters including the DNS server address to each client using DHCPv6.

SLAAC+Stateless DHCP: The gateway assigns the IPv6 address prefix to each client and the client automatically generates its own IPv6 address. Also, the gateway assigns other parameters including the DNS server address to each client using DHCPv6.

SLAAC+RDNSS: The gateway assigns the IPv6 address prefix to each client and the client automatically generates its own IPv6 address. Also, the gateway assigns other parameters including the DNS server address to each client using the RDNSS option in RA (Router Advertisement).

Pass-Through: Select this type if the WAN ports of the gateway use the Pass-Through for IPv6 connections.

With DHCPv6 selected, configure the following parameters.

Gateway/Subnet Enter the IP address and subnet mask in the CIDR format. The CIDR notation here includes the IP address and subnet mask of the default gateway. The summary of the information that you entered will show up below in real time.

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

DNS Server

Select a method to configure the DNS server for the network.

Auto: With Auto selected, the DHCP server automatically assigns DNS server for devices in the network.

Manual: With Manual selected, enter the IP address of a server in each DNS server field.

With Pass-Through selected, configure the following parameters.

IPv6 Prefix Delegation Interface

Select the WAN port using Pass-Through (Bridge) for the IPv6 connection.

Create New LAN

Name:

Purpose: Interface
 VLAN

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

IGMP Snooping: Enable i

Legal DHCP Servers: Enable i

DHCP L2 Relay: Enable

Save Cancel

VLAN

Enter a VLAN ID with the values between 1 and 4090. Each VLAN can be uniquely identified by VLAN ID, which is transmitted and received as IEEE 802.1Q tag in an Ethernet frame.

IGMP Snooping

Click the checkbox to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.

Legal DHCP Servers

Click the checkbox to specify legal DHCP servers for the network. With legal DHCP servers configured, Gateways and Switches ensure that clients get IP addresses only from the DHCP servers specified here.

DHCP L2 Relay

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

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

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

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

+ Create New LAN

Create a Network

Create a Port Profile

Assign the Port Profile to the Ports

ⓘ Note:

- Three default port profiles are preconfigured on the controller. They can be viewed, but not edited or deleted.
 - All:** In the All profile, all networks except the default network (LAN) are configured as Tagged Network, and the native network is the default network (LAN). This profile is assigned to all switch ports by default.
 - Disable:** In the Disable profile, no networks are configured as the native network, Tagged Networks and Untagged Networks. With this profile assigned to a port, the port does not belong to any VLAN.
 - LAN:** In the LAN profile, the native network is the default network (LAN), and no networks are configured as Tagged Networks and Untagged Networks.
- When a network is created, the system will automatically create a profile with the same name and configure the network as the native network for the profile. In this profile, the network itself is configured as the Untagged Networks, while no networks are configured as Tagged Networks. The profile can be viewed and deleted, but not edited.

1. Go to [Wired Networks](#) > [LAN](#) > [Profiles](#) to load the following page.

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

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

[+ Create New Port Profile](#)

2. Click [+ Create New Port Profile](#) to load the following page, and configure the following parameters.

Create New Port Profile

NAME:

PoE: Keep the Device's Settings
 Enable
 Disable

Networks/VLANs

Native Network: ⓘ

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

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

Voice Network: ⓘ

Advanced Options

802.1X Control: ⓘ Force Unauthorized
 Force Authorized
 Auto

Port Isolation: Enable ⓘ

Flow Control: Enable

EEE: Enable ⓘ

Loopback Control: ⓘ Off
 Loopback Detection Port Based
 Loopback Detection VLAN Based ⓘ
 Spanning Tree

LLDP-MED: Enable ⓘ

Bandwidth Control: ⓘ Off
 Rate Limit
 Storming Control



DHCP L2 Relay: Enable






| | |
|-------------|---|
| Name | Enter a name to identify the port profile. |
| PoE | <p>Select the PoE mode for the ports.</p> <p>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.</p> <p>Enable: Enable PoE on PoE ports.</p> <p>Disable: Disable PoE on PoE ports.</p> |

| | |
|-------------------|--|
| 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. |
| 802.1X Control | <p>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.</p> <p>Auto: The port is unauthorized until the client is authenticated by the authentication server successfully.</p> <p>Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client.</p> <p>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.</p> |
| 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 | <p>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.</p> <p>Off: Disable loopback control on the port.</p> <p>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.</p> <p>Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the VLAN will be blocked.</p> <p>Spanning Tree: Select STP (Spanning Tree Protocol) 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.</p> <p>If you want to enable Spanning Tree for the switch, you also need to select the Spanning Tree protocol in the Device Config page. For details, refer to 6.3 Configure and Monitor Switches.</p> |
| LLDP-MED | <p>Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP devices.</p> |
| Bandwidth Control | <p>Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance.</p> <p>Off: Disable Bandwidth Control for the port.</p> <p>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.</p> <p>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.</p> |
| Ingress Rate Limit | <p>When Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.</p> |
| Egress Rate Limit | <p>When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.</p> |
| Broadcast Threshold | <p>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.</p> |
| Multicast Threshold | <p>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.</p> |
| UL-Frame Threshold | <p>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..</p> |

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

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

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


Showing 1-4 of 4 records < 1 > 10 /page Go To page: **GO**






[+ Create New Port Profile](#)



Note:

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

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

| Port | | LAG | | Edit Selected | | |
|--------------------------|---|-------|---|-------------------------------|---|---|
| <input type="checkbox"/> | # | Name | Status | Profile | ACTION | : |
| <input type="checkbox"/> | 1 | Port1 | ■ | All |  | |
| <input type="checkbox"/> | 2 | Port2 | ■ | FAE |  | |
| <input type="checkbox"/> | 3 | Port3 | ■ | All |  | |
| <input type="checkbox"/> | 4 | Port4 | ■ | All |  | |
| <input type="checkbox"/> | 5 | Port5 | ■ | All |  | |

2. Select the profile from the drop-down list to assign the port profile to the desired ports of the switch. You can enable profile overrides to customize the settings for the ports, and all the configuration here overrides the port profile. For details, refer to [Chapter 6. Configure and Monitor Controller-Managed Devices](#).

Edit Port1

Name:

Profile:
 [Manage Profiles](#)

Profile Overrides

♥ 4.4 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.

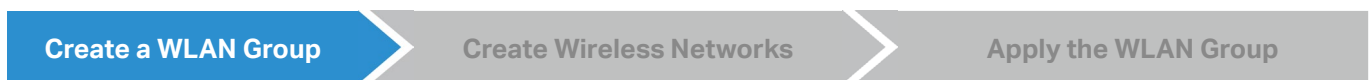
After setting up basic wireless networks, you can further configure WLAN Schedule, 802.11 Rate Control, MAC Filter, and other advanced settings.

4.4.1 Set Up Basic Wireless Networks

Configuration

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

- 1) Create a WLAN group.
- 2) Create Wireless Networks
- 3) Apply the WLAN group to your APs



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

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

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.

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

Add New WLAN Group ✕

Name:

Copy WLANs: Copy All SSIDs from the WLAN Group

Default
 Default
 tp-link

Save
Cancel

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

WLAN Group: ⓘ ✎ 🗑

SSID NAME
 Default
 test
 tp-link
 ⓘ No wired
 + Create New Group

| BAND | GUEST NETWORK | Portal | ACCESS CONTROL RULE | RATE LIMIT | VLAN | ACTION |
|---------------------------|---------------|--------|---------------------|------------|------|--------|
| No wireless networks yet. | | | | | | |

+ Create



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

WLAN Group: ⓘ ✎ 🗑

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

+ Create New Wireless Network

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

Note:

The 6 GHz band is only available for certain devices.

Create New Wireless Network

Network Name (SSID):

Device Type: EAP Gateway

Band: 2.4 GHz 5 GHz 6 GHz [i](#)

Guest Network: Enable [i](#)

Security:

Security Key: [i](#)

Advanced Settings

WLAN Schedule

802.11 Rate Control

MAC Filter

Multicast/Broadcast Management

DHCP Option 82

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

Device Type Select the type of devices that the wireless network can apply to.

Band Enable the radio band(s) for the wireless network. When 6GHz is turned on, Security cannot be PPSK with/without RADIUS since 6GHz does not support them.

Guest Network With Guest Network enabled, all the clients connecting to the SSID are blocked from reaching any private IP subnet.

Security Select the encryption method for the wireless network based on needs.

- Select the security strategy for the wireless network.

■ **None**

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

■ WPA-Personal

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

| | | |
|---------------|--------------|---|
| Security: | WPA-Personal | ▼ |
| Security Key: | | 🔒 |

Security Key

Specify a security key to encrypt the traffic.

■ WPA-Enterprise

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

| | | |
|-----------------|------------------|---|
| Security: | WPA-Enterprise | ▼ |
| RADIUS Profile: | Please Select... | ▼ |

RADIUS Profile

Select a RADIUS Profile, which records the settings of the authentication server and accounting server. You can create a RADIUS Profile by clicking [Create New Radius Profile](#) from the drop-down list of RADIUS Profile. For details, refer to [4.9 Authentication](#).

■ PPSK without RADIUS

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

| | | |
|---------------|---------------------|---|
| Security: | PPSK without RADIUS | ▼ |
| PPSK Profile: | Please Select... | ▼ |

[Manage PPSK Profile](#)

PPSK Profile

Select a PPSK Profile, which records the PPSK settings. You can create a PPSK Profile by clicking [Create New PPSK Profile](#) from the drop-down list of PPSK Profile. For details, refer to [4.8.4 PPSK](#).

■ PPSK with RADIUS

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

to record the traffic statistics. The SSID will not be applied to the device firmware not supporting PPSK.

| | | |
|-----------------------|-------------------------------|------------|
| Security : | PPSK with RADIUS | |
| RADIUS Profile : | | |
| Authentication type : | Generic Radius with bound MAC | |
| NAS ID : | | (Optional) |
| MAC Address Format : | aa:bb:cc:dd:ee:ff | |

RADIUS Profile

Select a RADIUS Profile, which records the settings of the authentication server and accounting server. You can create a RADIUS Profile by clicking [+ Create New Radius Profile](#) from the drop-down list of RADIUS Profile. For details, refer to [4.9 Authentication](#).

Authentication type

Choose the authentication type.

Generic Radius with bound MAC: This type needs to specify device MAC addresses.

NAS ID

Configure a Network Access Server Identifier (NAS ID) for the authentication. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups.

MAC Address Format

Select clients' MAC address format which the controller uses for authentication. Then configure the MAC addresses in the specified format as usernames for the clients on the RADIUS server.

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

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

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

[+ Create New Wireless Network](#)

Create a WLAN Group

Create Wireless Networks

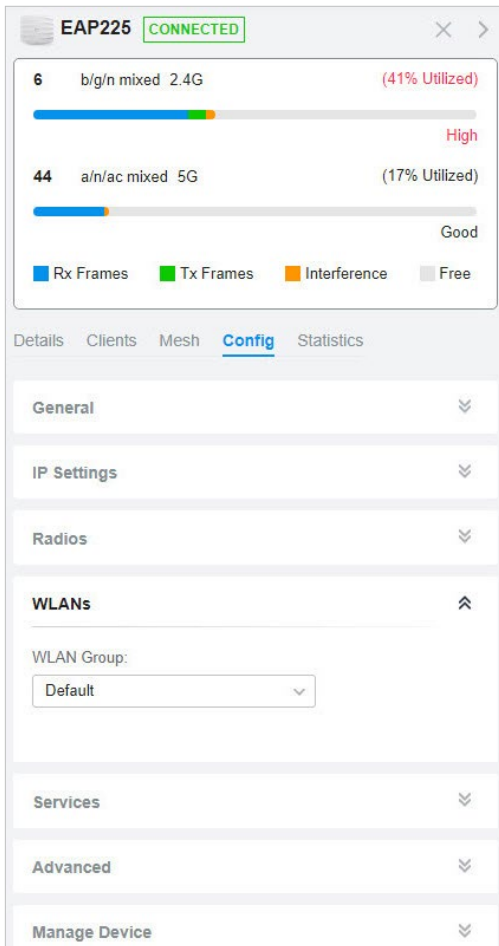
Apply the WLAN Group

Note:

The controller provides a default WLAN group. If you simply want to configure wireless networks for the default WLAN group and apply it to all your 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**.


| Search or select tag | | | | | | | | | | | |
|--|-------------------|------------|-----------|-------------------------|---------|-----------------|---------|----------|-----------|------------------|--------|
| All Gateway/Switches APs Overview Mesh Performance Config | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | CLIENTS | DOWN | UP | CHANNEL | ACTION |
| <input checked="" type="checkbox"/> | EA-23-51-06-22-52 | 10.0.1.70 | CONNECTED | EAP225-Outdoor(EU) v1.0 | 2.0.0 | 1 days 07:54:08 | 0 | 2.11 GB | 369.62 MB | 11(2.4G), 36(5G) | |
| <input checked="" type="checkbox"/> | EA-33-51-A8-22-A0 | 10.0.0.196 | CONNECTED | EAP225-Outdoor(EU) v1.0 | 2.0.0 | 0 days 06:15:18 | 1 | 13.61 MB | 3.00 MB | 11(2.4G), 36(5G) | |

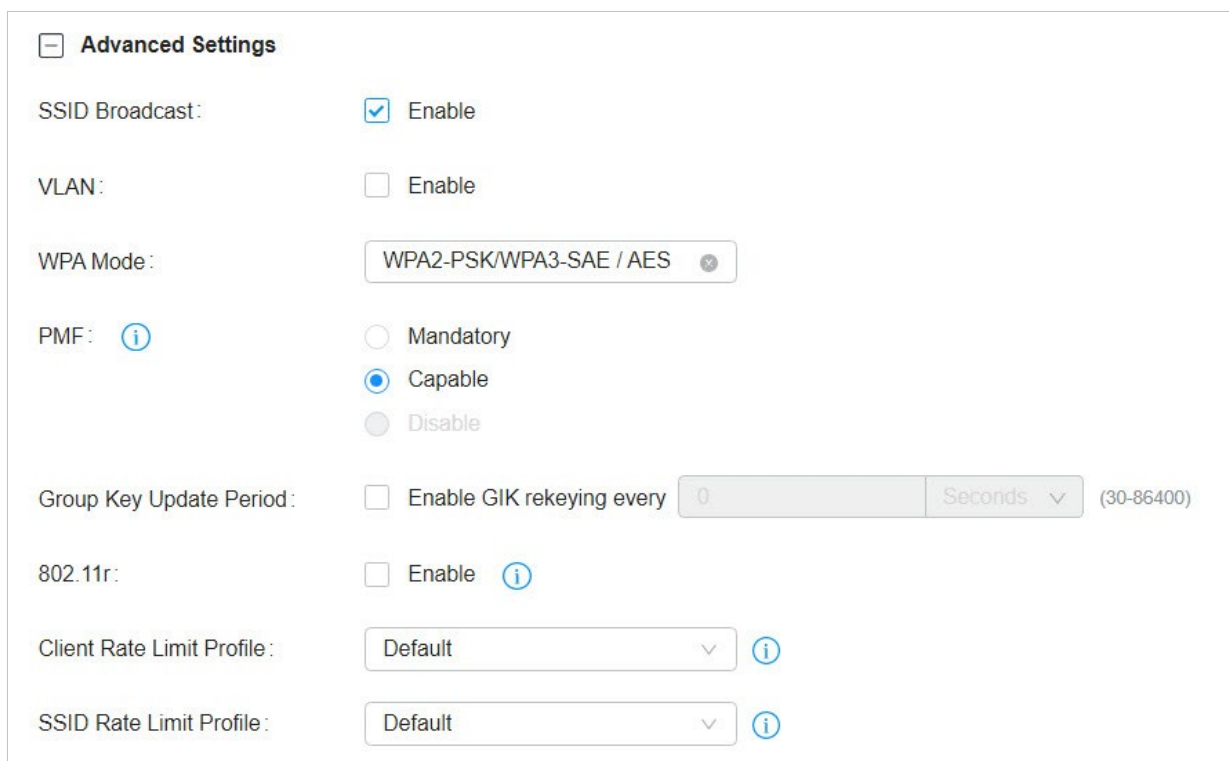
- In the Properties window, go to [Config](#) > [WLANs](#), select the WLAN group which you want to apply to the AP.







The screenshot shows a window titled "WLANs" with a search bar and a dropdown menu labeled "WLAN Group:" containing the option "Default".

4.4.2 Advanced Settings

Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Wireless Networks](#), click  in the ACTION column of the wireless network which you want to configure, and click [+ Advanced Settings](#) to load the following page. Configure the parameters and click [Apply](#).



The screenshot shows the "Advanced Settings" configuration page with the following options:

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

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

To set a wireless VLAN for the wireless network, enable this option and set a VLAN ID from 1 to 4094.

With this option enabled, traffic in different wireless networks is marked with different VLAN tags according to the configured VLAN IDs. Then the 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 | <p>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.</p> <p>Select the version of WPA according to your needs.</p> <p>Select the encryption type. Some encryption type is only available under certain circumstances.</p> <p>AES: AES stands for Advanced Encryption Standard.</p> <p>Auto: APs automatically decide the encryption type in the authentication process.</p> |
| PMF | <p>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.</p> <p>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.</p> <p>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.</p> <p>Mandatory: Only PMF-capable clients can connect to the network.</p> |
| Group Key Update Period | <p>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.</p> |
| 802.11r | <p>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.</p> |
| Client Rate Limit Profile | <p>Specify the profile to limit the download and upload rates of each client to balance bandwidth usage.</p> <p>You can use the default profile or custom a profile.</p> |
| SSID Rate Limit Profile | <p>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.</p> <p>You can use the default profile or custom a profile.</p> <p>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.</p> |

4.4.3 WLAN Schedule

Overview



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

Configuration

Select a site from the drop-down list of [Organization](#). Go to [Settings > Wireless Networks](#), click  in the ACTION column of the wireless network which you want to configure, and click [+ WLAN Schedule](#) to load the following page. Enable WLAN schedule and configure the parameters. Then click [Apply](#).

WLAN Schedule

WLAN Schedule: Enable

Action: Radio on  Radio off 

Time Range: [Manage Time Range Entries](#)

Action

Radio On: Turn on your wireless network within the time range you set, and turn it off beyond the time range.

Radio Off: Turn off your wireless network within the time range you set, and turn it on beyond the time range.

Time Range

Select the Time Range for the action to take effect. You can create a Time Range entry by clicking [+ Create New Time Range Entry](#) from the drop-down list of Time Range. For details, refer to [4. 8 Create Profiles](#).

4. 4. 4 802.11 Rate Control


Overview

Note:

802.11 Rate Control is only available for certain devices.

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

Configuration

Select a site from the drop-down list of [Organization](#). Go to [Settings > Wireless Networks](#), click  in the ACTION column of the wireless network which you want to configure, and click [+ 802.11 Rate Control](#) to load the following page. Select one or multiple bands to enable minimum data rate control according

to your needs, move the slider to determine what bit rates your wireless network allows, and configure the parameters. Then click [Apply](#).

Note:

The 6 GHz band is only available for certain devices.

802.11 Rate Control ⓘ

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

6 Mbps 54 Mbps

Lower Density Higher Density

ⓘ Limited range and no connectivity for 802.11b devices.

Disable CCK Rates (1/2/5.5/11 Mbps)

Require Clients to Use Rates at or Above the Specified Value

Send Beacons at 1 Mbps

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

6 Mbps 54 Mbps

Lower Density Higher Density

ⓘ Full device compatibility and range.

Require Clients to Use Rates at or Above the Specified Value

Send Beacons at 6 Mbps

Disable CCK Rates (1/2/5.5/11 Mbps)

Select whether to disable CCK (Complementary Code Keying), the modulation scheme which works with 802.11b devices. Disable CCK Rates (1/2/5.5/11 Mbps) is only available for 2.4 GHz band.

Require Clients to Use Rates at or Above the Specified Value

Select whether or not to require clients to use rates at or above the value specified on the minimum data rate controller slider.

Send Beacons at 1 Mbps/6 Mbps

Select whether or not to send Beacons at the minimum rate of 1Mbps for 2.4 GHz band or 6Mbps for 5 GHz band.

4.4.5 MAC Filter

Overview

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

Configuration

Select a site from the drop-down list of [Organization](#). Go to [Settings > Wireless Networks](#), click [✎](#) in the ACTION column of the wireless network which you want to configure, and click [+ MAC Filter](#) to load the following page. Enable MAC Filter and configure the parameters. Then click [Apply](#).

MAC Filter

MAC Filter: Enable

Policy: Allow List [i](#)
 Deny List [i](#)

MAC Addresses List: [Manage MAC Groups](#)

[Apply](#) [Cancel](#)

Policy

Allow List: Allow the connection of the clients whose MAC addresses are in the specified MAC Address List, while blocking others.

Deny List: Block the connection of the clients whose MAC address are in the specified MAC Addresses List, while allowing others.

MAC Address List

Select the MAC Group which you want to allow or block according to the policy. You can create new MAC group by clicking [+ Create New MAC Group](#) from the drop-down list of MAC Address List. For details, refer to [4. 8 Create Profiles](#).

4. 4. 6 Multicast/Broadcast Management

Overview

Multicast/Broadcast Management allows packet conversion and multicast filtering.

Configuration

Select a site from the drop-down list of [Organization](#). Go to [Settings > Wireless Networks](#), click [✎](#) in the ACTION column of the wireless network which you want to configure, and click [+ Multicast/Broadcast Management](#) to load the following page. Configure the parameters. Then click [Apply](#).

☐ Multicast/Broadcast Management

Multicast-to-Unicast Conversion: Enable
 Converse multicast to unicast when the channel utilization is below %

ARP-to-Unicast Conversion: Enable

IPv6-Multicast-to-Unicast Conversion: Enable

Multicast Filtering: Enable [i](#)

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 filter the multicast packets of the specified protocols. Improper settings may cause network issues.

4.4.7 AI WLAN Optimization

Overview

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

In [AI WLAN Optimization](#), the results of the last 10 scans are displayed. You can also enable automatic optimization to allow the controller to conduct RF optimization automatically and set optimization schedules. In [Optimization Log](#), the past optimization records are displayed, and you can also restore the previous optimization results as needed.

Configuration

ⓘ Note:

1. WiFi experience may be influenced during optimization. Please select the spare time to scan and optimize to reduce its impact on user experience.
 2. Because the APs should stay connected during optimization, please set a different time for AI WLAN Optimization and Reboot Schedule. It is recommended to stagger at least 10 minutes to avoid dissatisfactory results.
1. Select a site from the drop-down list of [Organization](#). Go to [Settings > Wireless Networks > AI WLAN Optimization](#).
 2. Click [Deploy Now](#) to begin the optimization. The controller will scan the wireless environment to conclude the optimum WLAN network configurations. You can view the optimization results in [Optimization Log](#).

AI WLAN Optimization

[Optimization Config](#)

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

[Deploy Now](#)

3. (Optional) Click [Optimization Config](#) if you want to custom configurations.

| | |
|---------------------------------------|--|
| Mode | Specify the optimization mode. Default: The controller will conduct the optimization with the default configurations. Custom: The controller will conduct the optimization with the configurations you set. |
| Automatic Channel Optimization | Enable this function, and the controller will scan the wireless environment to conclude the optimum operation channels for the APs and wireless routers. |
| Automatic Power Optimization | Enable this function, and the controller will scan the wireless environment to conclude the optimum transmission power for the APs and wireless routers. |
| Custom Channel Width | Select the channel width for each band, and the optimization will maintain the selected channel width. |
| Power Range | Select Custom if you want to optimize the power within the specified range. You can limit the transmit power range of each AP/wireless routers after the power deployment is completed. For high-density deployment, you can try to set a smaller power range. An over-low value may lead to limited coverage, while an over-high value may lead to strong interference. (Note: The deployment may fail if the minimum power you select exceeds the maximum power of the AP to be deployed.) |
| Power Threshold | Select Custom if you want to optimize the power within the specified threshold. You can adjust the power deployment override threshold according to the actual deployment height and spacing of APs/wireless routers, achieving optimal wireless coverage after RF optimization. The larger the threshold, the larger the adjusted overall power value. |

Excluded 5 GHz Channels

When enabled, you can specify the channels so they will not execute the automatic optimization.

4. (Optional) Set schedules for WLAN optimization, and save the settings.

Scheduled

Scheduled Optimization: Enable

Occurrence: Every at in Coordinated Universal Time [i](#)

Scheduled Optimization

Enable scheduled optimization, and the controller will automatically adjust the channels for the APs/wireless routers on a regular basis.

Occurrence

Set the schedule for regular WLAN optimization.

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

| Excluded APs List i | | | | |
|---|------------|--------|-------|--------|
| DEVICE NAME | IP ADDRESS | STATUS | MODEL | ACTION |
| + Add ⓘ No entry in the table. | | | | |

♥ 4.5 Network Security

Network Security is a portfolio of features designed to improve the usability and ensure the safety of your network and data. It implements policies and controls on multiple layers of defenses in the network.

4.5.1 ACL

Overview

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

The system provides three types of ACL:

■ Gateway ACL

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

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

■ Switch ACL

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

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

■ AP ACL

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

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

Configuration

To complete the ACL configuration, follow these steps:

- 1) Create an ACL with the specified type.

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

■ Configuring Gateway ACL

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

Create New Rule

Description:

Status: Enable

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

Direction:

Policy: Deny Permit


Protocols:

Log: Enable

Rule: i


Source

Type:




Please Select the type

Deny



Destination

Type:



Please Select the type

+ Advanced Settings

[Create](#) [Cancel](#)

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

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

| | |
|------------------|---|
| Direction | Select the 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 Networks > LAN to create one. The gateway will examine whether the packets are sourced from the selected network. |
| SSID | Select the SSID you have created. If no SSIDs have been created, go to Settings > Wireless Networks 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-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. |
| 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-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. |
| 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-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. |
|-------------------------------|--|

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

| | |
|--------------------------|---|
| 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 State New/Established/Related): Match the new, established, and related connection states.

Manual: If selected, you can manually specify the connection states to match.

Match State New: Match the connections of the initial state. For example, a SYN packet arrives in a TCP connection, or the router only receives traffic in one direction.

Match State Established: Match the connections that have been established. In other words, the firewall has seen the bidirectional communication of this connection.

Match State Related: Match the associated sub-connections of a main connection, such as a connection to a FTP data channel.

■ Configuring Switch ACL

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

Create New Rule

Name:

Status: Enable

Policy: Deny
 Permit

Protocols:

Time Range: Enable [i](#)


Ethertype: Enable

Bi-Directional: Enable

Rule: [i](#)

Source

Type:




Please Select the type

Deny

Destination

Type:



Please Select the type

ACL Binding

Binding Type: Ports
 VLAN

Ports: All Ports
 Custom Ports

[Create](#) [Cancel](#)

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

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

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

| | |
|---------------|--|
| Network | Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The switch will examine whether the packets are sourced from the selected network. |
| IP Group | Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address of the packet is in the IP Group. |
| IP-Port Group | Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address and port number of the packet are in the IP-Port Group. |
| MAC Group | Select the MAC Group you have created. If no MAC Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source MAC address of the packet is in the MAC Group. |
| IPv6 Group | Select the IPv6 Group you have created. If no IPv6 Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the source IP address of the packet is in the IPv6 Group. |

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


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

| | |
|------------------------|---|
| Network | Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The switch will examine whether the packets are forwarded to the selected network. |
| IP Group | Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address of the packet is in the IP Group. |
| IP-Port Group | Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address and port number of the packet are in the IP-Port Group. |
| MAC Group | Select the MAC Group you have created. If no MAC Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination MAC address of the packet is in the MAC Group. |
| IPv6 Group | Select the IPv6 Group you have created. If no IPv6 Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address of the packet is in the IPv6 Group. |
| IPv6-Port Group | Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The switch will examine whether the destination IP address and port number of the packet are in the IPv6-Port Group. |

- Bind the switch ACL to a switch port or a VLAN and click [Apply](#). Note that a switch ACL takes effect only after it is bound to a port or VLAN.

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

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

| Device List: | | Device Name | Ports/Lags | Status | Model | Firmware Version | | | | | | | | | | | | | | | | | | | | |
|-------------------------------------|---|-------------------------------------|---|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|---|---|---|----|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|---|-------------|---------------------------------|
| <input checked="" type="checkbox"/> |  | switch | Port <table border="0"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td> </tr> <tr> <td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td> </tr> </table> | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | CONNECTED | TL-SG2210MP | 1.0.0 Build 20200608 Rel7560 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | | | | | | | | | | | | | | | |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | |

VLAN: Select a VLAN and specify the switches as the interface to be bound with the ACL. If no VLANs have been created, you can select the default VLAN 1 (LAN), or go to [Settings > Wired Networks > LAN](#) to create one.

■ Configuring AP ACL

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

Create New Rule

Name:

Status: Enable

Policy: Deny
 Permit

Protocols:

Rule:


Source

Type:

IPGroup_Any

0/1 Items + Create

Deny



Destination

Type:

IPGroup_Any

0/1 Items + Create

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

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

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

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

| | |
|------------------------|---|
| Network | Select the network you have created. If no networks have been created, you can select the default network (LAN), or go to Settings > Wired Networks > LAN to create one. The AP will examine whether the packets are sourced from the selected network. |
| IP Group | Select the IP Group you have created. If no IP Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the source IP address of the packet is in the IP Group. |
| IP-Port Group | Select the IP-Port Group you have created. If no IP-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the source IP address and port number of the packet are in the IP-Port Group. |
| SSID | Select the SSID you have created. If no SSIDs have been created, go to Settings > Wireless Networks to create one. The AP will examine whether the SSID of the packet is the SSID selected here. |
| IPv6 Group | Select the IPv6 Group you have created. If no IPv6 Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the source IP address of the packet is in the IPv6 Group. |
| IPv6-Port Group | Select the IPv6-Port Group you have created. If no IPv6-Port Groups have been created, click +Create on this page or go to Settings > Profiles > Groups to create one. The AP will examine whether the source IP address and port number of the packet are in the IPv6-Port Group. |

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

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

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

4.5.2 URL Filtering

Overview

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

In URL filtering, the system compares the URLs in HTTP, HTTPS and DNS requests against the lists of URLs that are defined in URL Filtering rules, and intercepts the requests that are directed at a blocked URLs. These rules can be applied to specific clients or groups whose traffic passes through the gateway and 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 based on the sequence they are created. The rule created earlier is checked for a match with a higher priority. To reorder the rules, select a rule and drag it to a new position. If no rules match, the device forwards the packet because of an implicit Permit All clause.

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

Configuration

To complete the URL Filtering configuration, follow these steps:

- 1) Create a new URL Filtering rule with the specified type.
- 2) Define filtering criteria of the rule, including source, and URLs, and determine whether to forward the matched packets.

■ Configuring Gateway Rules

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

Create New Rule

Name:

Status: Enable

Policy: Deny
 Permit

Source Type:

Network:

URLs: ⓘ

[+ Add URL](#)

[Apply](#) [Cancel](#)

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

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

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

■ Configuring AP Rules

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

Create New Rule

Name:

Status: Enable

Policy: Deny
 Permit

Source Type:

SSID:

URLs: ⓘ

[+ Add URL](#)

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

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

URLs

Enter the URL address using up to 128 characters.

URL address should be given in a valid format. The URL which contains a wildcard(*) is supported. One URL with a wildcard(*) can match multiple subdomains. For example, with *.tp-link.com specified, community.tp-link.com will be matched.

4.5.3 MAC Filtering

Overview

MAC Filtering can drop or allow packets from certain devices passing through the router based on the MAC address of the devices. After the MAC filtering policy and MAC filtering list are configured, the router will apply the filter policy to the packets matching the MAC address, and thus limit network traffic and manage network access behaviors.

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Network Security](#) > [MAC Filtering](#).
2. Enable [MAC Filtering](#) and configure the parameters.

General

MAC Filtering:

Type: Allow packets with the MAC addresses listed below and deny the rest
 Deny packets with the MAC addresses listed below and allow the rest

Direction:

Type

Select the mode of MAC Filtering.

[Allow packets with the MAC addresses listed below and deny the rest](#): Select to allow packets with the listed MAC address to pass through the router, and packets with other MAC addresses will be dropped.

[Deny packets with the MAC addresses listed below and allow the rest](#): Select to drop packets with the listed MAC address, and packets with other MAC addresses will be allowed to pass through the router.

Direction

Select All when you want to apply the policy to traffic both from LAN to LAN and from LAN to WAN. Select LAN -> WAN when you want to apply the policy only to traffic from LAN to WAN.

3. Click [Add MAC Filtering](#) to add MAC addresses or groups to the list.

Name Specify the name for the entry.

Policy Choose [MAC Group](#) and specify the MAC groups of devices, then the MAC filtering policy will be applied to traffic with the MAC groups.

Choose [MAC Address](#) and specify the MAC addresses of devices, then the MAC filtering policy will be applied to traffic with the MAC addresses.

4.5.4 Attack Defense

Overview

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

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

The gateway provides two types of Attack Defense:

- **Flood Defense**

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

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

- **Packet Anomaly Defense**

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

Configuration

■ Configuring Flood Defense

Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Network Security](#) > [Attack Defense](#). In the Flood Defense, click the checkbox and set the corresponding limit of the rate at which specific packets are received.

Flood Defense

| | | | |
|--|-------|-------|-------------|
| <input type="checkbox"/> Multi-Connections TCP SYN Flood | 10000 | Pkt/s | (100-99999) |
| <input type="checkbox"/> Multi-Connections UDP Flood | 20000 | Pkt/s | (100-99999) |
| <input type="checkbox"/> Multi-Connections ICMP Flood | 1500 | Pkt/s | (100-99999) |
| <input type="checkbox"/> Stationary Source TCP SYN Flood | 4000 | Pkt/s | (100-99999) |
| <input type="checkbox"/> Stationary Source UDP Flood | 6000 | Pkt/s | (100-99999) |
| <input type="checkbox"/> Stationary Source ICMP Flood | 600 | Pkt/s | (100-99999) |

Multi-Connections TCP SYN Flood

A TCP SYN flood attack occurs when the attacker sends the target system with a succession of SYN (synchronize) requests. When the system responds, the attacker does not complete the connections, thus leaving the connection half-open and flooding the system with SYN messages. No legitimate connections can then be made.

With this feature enabled, the gateway limits the rate of receiving TCP SYN packets from all the clients to the specified rate.

Multi-Connections UDP Flood

A UDP flood attack occurs when the attacker sends a large number of UDP packets to a target host in a short time, the target host is busy with these UDP packets and cannot process normal services.

With this feature enabled, the gateway limits the rate of receiving UDP packets from all the clients to the specified rate.

Multi-Connections ICMP Flood

If an attacker sends many ICMP Echo messages to the target device, the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected.

With this feature enabled, the system limits the rate of receiving ICMP packets from all the clients to the specified rate.

Stationary Source TCP SYN Flood

A TCP SYN flood attack occurs when the attacker sends the target system with a succession of SYN (synchronize) requests. When the system responds, the attacker does not complete the connections, thus leaving the connection half-open and flooding the system with SYN messages. No legitimate connections can then be made.

With this feature enabled, the gateway limits the rate of receiving TCP SYN packets from a single client to the specified rate.

Stationary Source UDP Flood

A UDP flood attack occurs when the attacker sends a large number of UDP packets to a target host in a short time, the target host is busy with these UDP packets and cannot process normal services.

With this feature enabled, the gateway limits the rate of receiving UDP packets from a single client to the specified rate.

Stationary Source ICMP Flood

If an attacker sends many ICMP Echo messages to the target device, the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected.

With this feature enabled, the system limits the rate of receiving ICMP packets from a single clients to the specified rate.

■ Configuring Packet Anomaly Defense

Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Network Security](#) > [Attack Defense](#). In the Packet Anomaly Defense, click the checkbox and set the corresponding limit of the rate at which specific packets are received.

Packet Anomaly Defense

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

Block Fragment Traffic

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

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

4.5.5 Firewall

Overview

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

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

Configuration

■ Configuring State Timeouts

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

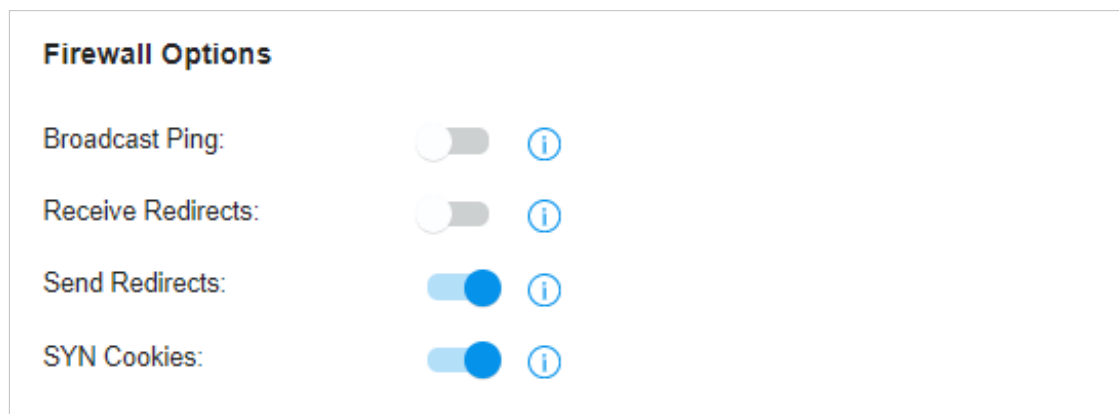
| State Timeouts | | | |
|------------------|-----------------------------------|---------|----------------|
| ICMP: | <input type="text" value="60"/> | Seconds | (1-21474836) ⓘ |
| Other: | <input type="text" value="600"/> | Seconds | (1-21474836) ⓘ |
| TCP Close: | <input type="text" value="10"/> | Seconds | (1-21474836) ⓘ |
| TCP Close Wait: | <input type="text" value="60"/> | Seconds | (1-21474836) ⓘ |
| TCP Established: | <input type="text" value="7440"/> | Seconds | (1-21474836) ⓘ |
| TCP FIN Wait: | <input type="text" value="120"/> | Seconds | (1-21474836) ⓘ |
| TCP Last ACK: | <input type="text" value="30"/> | Seconds | (1-21474836) ⓘ |
| TCP SYN Recv: | <input type="text" value="60"/> | Seconds | (1-21474836) ⓘ |
| TCP SYN Sent: | <input type="text" value="120"/> | Seconds | (1-21474836) ⓘ |
| TCP Time Wait: | <input type="text" value="120"/> | Seconds | (1-21474836) ⓘ |
| UDP Other: | <input type="text" value="60"/> | Seconds | (1-21474836) ⓘ |
| UDP Stream: | <input type="text" value="180"/> | Seconds | (1-21474836) ⓘ |

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

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

■ Configuring Firewall Options

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



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

4.5.6 IP-MAC Binding

Overview

ARP (Address Resolution Protocol) is used to map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations. However, if attackers send ARP spoofing packets with false IP address-to-MAC address mapping entries, the device will update the ARP table based

on the false ARP packets and record wrong mapping entries, which results in a breakdown of normal communication.

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

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Settings > Network Security > IP-MAC Binding](#).
2. Enable [ARP Spoofing Defense](#) and configure general settings. Click [Apply](#).

General

ARP Spoofing Defense: Enable

Interface: ... x ... x v

Permit the packets matching the IP-MAC Binding entries only

Send GARP packets when ARP attack is detected

Interval: ms (1-10000)

Apply
Cancel

[ARP Spoofing Defense](#) Check the box to globally enable ARP Spoofing Defense.

[Interface](#) Select the interface on which the entries will take effect.

[Permit the packets matching the IP-MAC Binding entries only](#) With this option enabled, when receiving a packet, the router will check whether the IP address, MAC address and receiving interface match any of the IP-MAC Binding entries. Only the matched packets will be forwarded. This feature can be enabled only when ARP Spoofing Defense is enabled.

[Send GARP packets when ARP attack is detected](#) With this option enabled, the router will send GARP packets to the hosts if it detects ARP spoofing packets on the network. The GARP packets will inform the hosts of the correct ARP information, which is used to replace the wrong ARP information in the hosts. This feature can be enabled only when ARP Spoofing Defense is enabled.

[Interval](#) Specify the time interval for sending GARP packets. The valid values are from 1 to 10000.

3. Click [Create New IP-MAC Binding Entry](#) and add an IP-MAC binding entry. Click [Apply](#).

Create New IP-MAC Binding Entry
×

IP Address:

MAC Address:

Interface:

Description: (Optional)

Status: Enable

Apply
Cancel

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

4.5.7 IDS/IPS

Overview

IDS/IPS is a security mechanism that detects intrusions based on attack characteristics. It can detect buffer overflows, Trojan horses, worms, SQL injections and other attacks to protect the network security of users.

ⓘ Note:

Using Intrusion Detection/Prevention may reduce maximum throughput speeds.

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Network Security](#) > [IDS/IPS](#).

2. Enable [Intrusion Detection/Prevention](#) and configure the parameters.

IDS/IPS ⓘ

Intrusion Detection/Prevention:

Type: Detect Only (IDS) Detect and Prevent (IPS)

⚠ Using Intrusion Detection/Prevention may reduce maximum throughput speeds.

GEO Enforcer: Enable ⓘ

Security Level: ⓘ

🛡 6 of 34 Threat Categories Enabled.

Effective Time: Enable

Type

Specify the working mode.

In IDS mode, the system will only report the threat log.

In IPS mode, the system will block the corresponding connection for 300s after a threat is detected.

GEO Enforcer

Enable geographic location identification of threat logs.

Security Level

Choose the protection level. A higher protection level means more threat types are detected, while a lower protection level only detects some important threats. You can also customize the protection level.

Effective Time

Specify the effective time period of the IDS/IPS module.

3. Apply the settings. When the system discovers a threat, the corresponding threat log will be displayed on the [Insights > Threat Management](#) page. For a specific threat log, you can choose a specified response strategy.

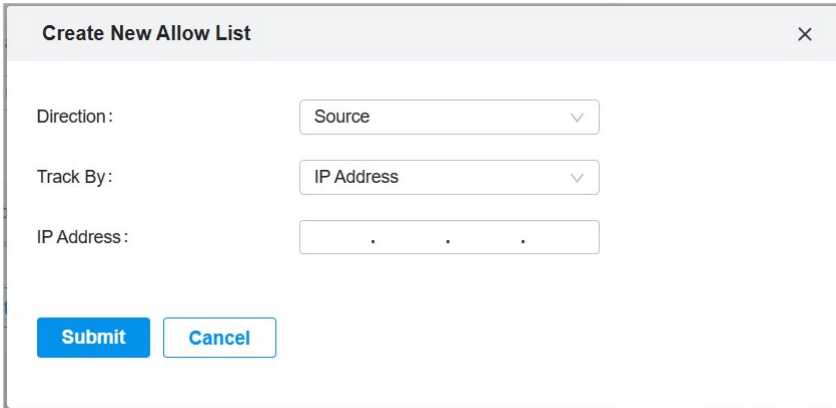
Block List

The Block List page displays all block entries added through the [Threat Management](#) page. Users can choose to block all traffic of the source IP in the threat log, or block all traffic between the source IP and the destination IP in the threat log.

Allow List

On the Allow List page, you can add, view, and edit the exemption entries of IDS/IPS detection, so that the specified objects will no longer trigger threat logs.

Click Create New Allow List and configure the parameters.



| | |
|--|---|
| Direction | Specify the location of the object (target) exempt from triggering the threat: source, destination, or both directions. |
| Track By | Specify the type of object (target) exempt from triggering the threat: IP address, Network, or Subnet. |
| IP Address/Network/ Subnet | Specify the value of the object. |

Signature Suppression

The Signature Suppression page displays all the signature suppression entries added through the Threat Management page, and the objects with signature suppressed will no longer trigger specific threat logs.

♥ 4.6 Transmission

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

4.6.1 Routing

Overview

- **Static Route**

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

- **Policy Routing**

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

Configuration

- **Static Route**

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

Create New Route

Name:

Status: Enable

Destination IP/Subnet: . . / [+ Add Subnet](#)

Route Type: Next Hop
 Interface

Next Hop: . .


Metric: (0-15)

[Create](#) [Cancel](#)

Name Enter the name to identify the Static Route entry.

Status Enable or disable the Static Route entry.

Destination IP/Subnet

Destination IP/Subnet identifies the network traffic which the Static Route entry controls. Specify the destination of the network traffic in the format of 192.168.0.1/24. You can click [+ Add Subnet](#) to specify multiple Destination IP/Subnets and click  to delete them.



Route Type



Next Hop: With Next Hop selected, your devices forward the corresponding network traffic to a specific IP address. You need to specify the IP address as Next Hop.

Interface: With Interface selected, your devices forward the corresponding network traffic through a specific interface. You need to specify the Interface according to your needs.

Metric

Define the priority of the Static Route entry. A smaller value means a higher priority. If multiple entries match the Destination IP/Subnet of the traffic, the entry of higher priority takes precedence. In general, you can simply keep the default value.

2. Click [Create](#). The new Static Route entry is added to the table. You can click  to edit the entry. You can click  to delete the entry.

| Search Static Route Entry <input type="text"/> | | | | | | | |
|--|--------------------------------------|----------------|----------|-----------|-------------|--------|---|
| NAME | ENABLED | DESTINATION IP | TYPE | INTERFACE | NEXT HOP | METRIC | ACTION |
| tp-link | ● | 192.168.2.3/24 | Next Hop | | 192.168.3.1 | 0 |   |

Showing 1-1 of 1 records < 1 > 10 /page Go To page: [GO](#)

[+ CreateNewRoute](#)

■ Policy Routing

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

Create New Routing

Name:

Status: Enable

Protocols: ▾

WAN: ▾

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

Routing Legend

Source

Type: ▾

LAN

MGMT VLAN

0/2 Items

Please Select...

→ →

Destination

Type: ▾

IPGroup_Any

0/1 Items + Create

Create
Cancel

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

Routing Legend



The Policy Routing entry takes effect only when the traffic using specified protocols matches the source and destination which are specified in the Routing Legend.





Select the type of the traffic source and destination.

Network: Select the LAN Interfaces for the traffic source or destination.

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

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

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

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

4.6.2 NAT

Overview

■ Port Forwarding

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

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

■ ALG

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

■ One-to-One NAT

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

Configuration

■ Port Forwarding

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

Create New Rule

Name:

Status: Enable

Source IP: Any
 Limited IP Address

Interface:

DMZ: Enable

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



Destination IP:





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

Protocol: All
 TCP
 UDP

| | |
|---------------------------|--|
| Name | Enter the name to identify the Port Forwarding rule. |
| Status | Enable or disable the Port Forwarding rule. |
| Source IP | <p>Any: The rule applies to traffic from any source IP address.</p> <p>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.</p> |
| Interface | Select the interface which the rule applies to. Traffic which is received through the interface is forwarded according to the rule. |

| | |
|-------------------------|---|
| DMZ | <p>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.</p> <p>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.</p> |
| 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 | <p>Network traffic is transmitted using either TCP or UDP protocol. Only the traffic which matches the Source Port and the Protocol is forwarded.</p> <p>If you want both TCP traffic and UDP traffic to be forwarded, select All.</p> |

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

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

■ **ALG**

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

ALG

FTP ALG: Enable

H.323 ALG: Enable

PPTP ALG: Enable

SIP ALG: Enable

IPsec ALG: Enable

| | |
|-----------|---|
| FTP ALG | <p>FTP ALG allows the FTP server and client to transfer data using the FTP protocol in one of the following scenarios:</p> <ul style="list-style-type: none">• 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 | <p>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:</p> <ul style="list-style-type: none">• One of the endpoints is in the LAN, while the other is on the internet.• The endpoints are in different LANs. |
| PPTP ALG | <p>PPTP ALG allows the PPTP server and client to set up a PPTP VPN in one of the following scenarios:</p> <ul style="list-style-type: none">• 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 | <p>SIP ALG allows the IP phones and multimedia devices to set up connections using the SIP protocol in one of the following scenarios:</p> <ul style="list-style-type: none">• One of the endpoints is in the LAN, while the other is on the internet.• The endpoints are in different LANs. |
| IPsec ALG | <p>IPsec ALG allows the IPsec endpoints to set up an IPsec VPN in one of the following scenarios:</p> <ul style="list-style-type: none">• One of the endpoints is in the LAN, while the other is on the internet.• The endpoints are in different LANs. |

■ One-to-One NAT

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

Create New Rule ⓘ

Name:

Status: Enable

Interface: ▼

Original IP: . .

Translated IP: . .

DMZ Forwarding: Enable

Description: (Optional)

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

2. Click [Create](#) to add the one-to-one NAT rule.

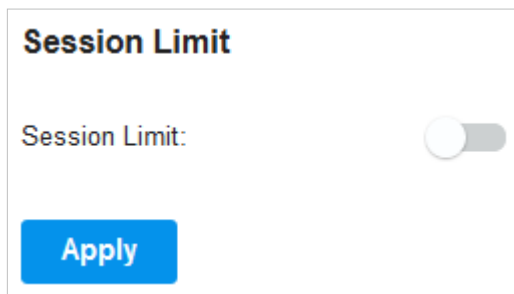
4.6.3 Session Limit

Overview

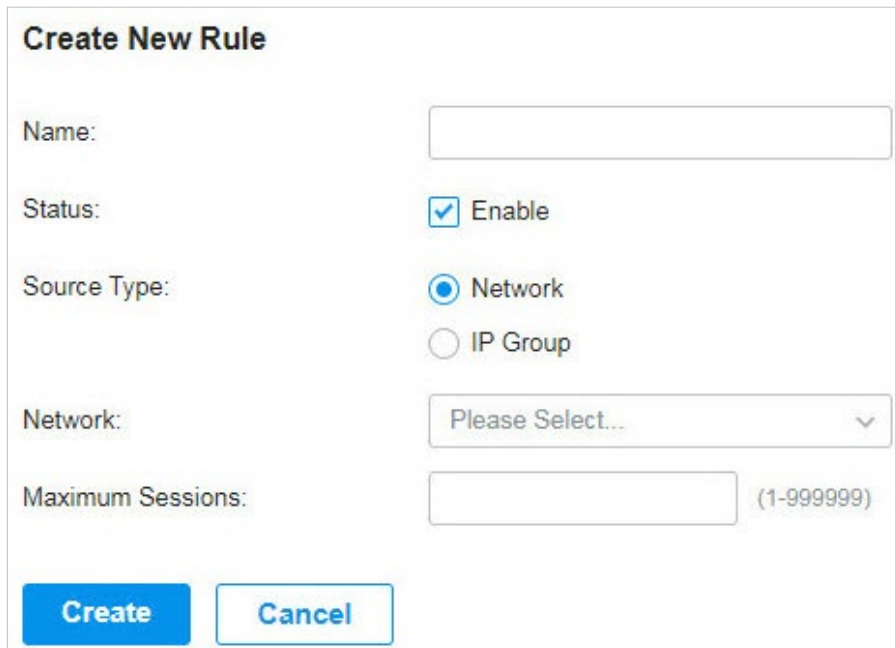
Session Limit optimizes network performance by limiting the maximum sessions of specific sources.

Configuration

1. Go to [Setting](#) > [Transmission](#) > [Session Limit](#). In [Session Limit](#), enable Session Limit globally and click [Apply](#).



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



Name Enter the name to identify the Session Limit rule.

Status Enable or disable the Session Limit rule.



Source Type



Network: Limit the maximum sessions of specific LAN networks. With this option selected, select the networks, which you can customize in [Wired Networks > LAN Networks](#). For detailed configuration of networks, refer to [4. 3. 2 Configure LAN Networks](#).

IP Group: Limit the maximum sessions of specific IP Groups. With this option selected, select the IP Groups, which you can customize in [Profiles > Groups](#). For detailed configuration of IP groups, refer to [4. 8 Create Profiles](#).

Maximum Sessions

Enter the maximum sessions of the specific sources.

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

| Session Limit Rule List | | | | |
|-------------------------|--------------------------------------|---|------------------|---|
| NAME | ENABLED | SOURCE | MAXIMUM SESSIONS | ACTION |
| tp-link | ● | Network: <input type="text" value="LAN"/> | 50000 |   |

[+ CreateNewRule](#)

4. 6. 4 Bandwidth Control

Overview

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

Configuration

- Go to [Setting > Transmission > Bandwidth Control](#). In [Bandwidth Control](#), enable Bandwidth Control globally and configure the parameters. Then click [Apply](#).

Bandwidth Control

Bandwidth Control:

Threshold Control: Enable Bandwidth Control when bandwidth usage reaches %

WAN

Upstream Bandwidth: Kbps [Test Speed](#)

Downstream Bandwidth: Kbps

[Apply](#) [Cancel](#)

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.

- In [Bandwidth Control Rule List](#), click **+ Create New Rule** to load the following page and configure the parameters.

Create New Rule

Name:

Status: Enable

Source Type: Network
 IP Group

Network:

WAN:



Upstream Bandwidth: Kbps



Downstream Bandwidth: Kbps

Mode: Shared Individual (i)

| | |
|--------------------|---|
| Name | Enter the name to identify the Bandwidth Control rule. |
| Status | Enable or disable the Bandwidth Control rule. |
| Source Type | <p>Network: Limit the maximum bandwidth of specific LAN networks. With this option selected, select the networks, which you can customize in Wired Networks > LAN Networks. For detailed configuration of networks, refer to 4. 3. 2 Configure LAN Networks.</p> <p>IP Group: Limit the maximum bandwidth of specific IP Groups. With this option selected, select the IP Groups, which you can customize in Profiles > Groups. For detailed configuration of IP groups, refer to 4. 8 Create Profiles.</p> |
| 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. |

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

| NAME | ENABLED | SOURCE | WAN | UPSTREAM BANDWIDTH | DOWNSTREAM BANDWIDTH | MODE | ACTION |
|---------|--------------------------------------|---|---------------------------------------|--------------------|----------------------|--------|---|
| tp-link | ● | Network: <input type="text" value="LAN"/> | <input type="text" value="WAN/LAN1"/> | 50000Kbps | 50000Kbps | Shared |   |

[+ CreateNewRule](#)

4.6.5 Gateway QoS

■ Bandwidth Control

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

Configuration

- Select a site from the drop-down list of **Organization**. Go to **Setting** > **Transmission** > **Gateway QoS**.

2. Click [Create New Rule](#).

Create New Rule

WAN Interface :

Status : Enable

UDP Bandwidth Control : Enable


Limited Bandwidth Ratio : %

Outbound TCP ACK Prioritize : Enable

Direction :

Inbound Bandwidth : Kbps

Outbound Bandwidth : Kbps



Class 1 : %

Class 2 : %

Class 3 : %

Others : %

3. Configure the parameters and click [Apply](#).**WAN Interface**

Select the WAN port. You can configure the QoS rule for a WAN port only when the port is enabled.

Status

Enable or disable QoS for the current entry.

UDP Bandwidth Control

Check the box to enable UDP bandwidth control.

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

■ Class Rule

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

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Setting](#) > [Transmission](#) > [Gateway QoS](#) > [Class Rule](#).

2. Click [Create New Class Rule](#).

Create New Class Rule

Status : Enable

IP Version : IPv4
 IPv6

Local Address :

Remote Address :

DSCP :

Service Name :

Qos Class :

3. Configure the parameters and click [Apply](#).

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

■ VoIP Prioritization

This page allows you to configure VoIP prioritization.

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Setting](#) > [Transmission](#) > [Gateway QoS](#) > [VoIP Prioritization](#).
2. Enable the first priority for VoIP SIP/RTP and enter the SIP UDP port. Then apply the settings.

VoIP Prioritization

Enable the First Priority for VoIP

SIP/RTP:

SIP UDP Port:

[Enable the First Priority for VoIP SIP/RTP](#) Check the box to enable prioritize VoIP traffic.

[SIP UDP Port](#) Enter the UDP port ID of the VoIP traffic.

■ Tag Outbound Traffic

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

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Setting](#) > [Transmission](#) > [Gateway QoS](#) > [Tag Outbound Traffic](#).
2. Check the box for your desired class and select the DSCP or Precedence value.

Tag Outbound Traffic

Class 1: Add DSCP or Precedence value

Class 2: Add DSCP or Precedence value

Class 3: Add DSCP or Precedence value

Others: Add DSCP or Precedence value

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

♥ 4.7 Configure VPN

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

4.7.1 VPN

Overview

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

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

■ IPsec

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

■ PPTP

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

■ L2TP

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

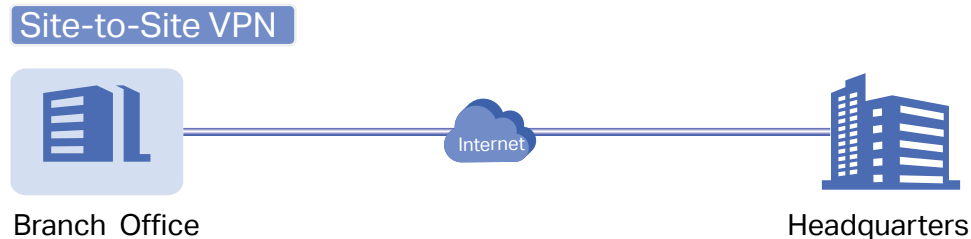
■ OpenVPN

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

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

■ Site-to-Site VPN

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



The gateway supports two types of Site-to-Site VPNs:

- Auto IPsec

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

- Manual IPsec

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

■ Client-to-Site VPN

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

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

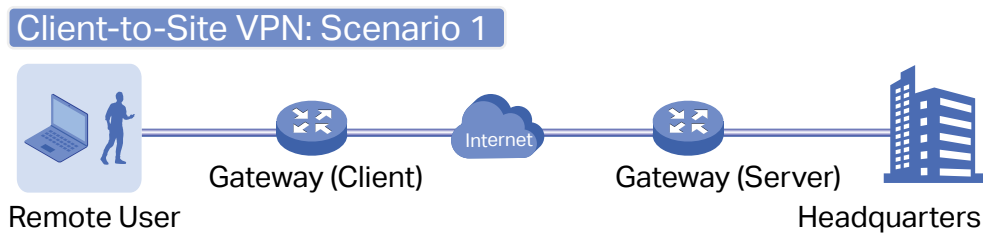
- VPN Server

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

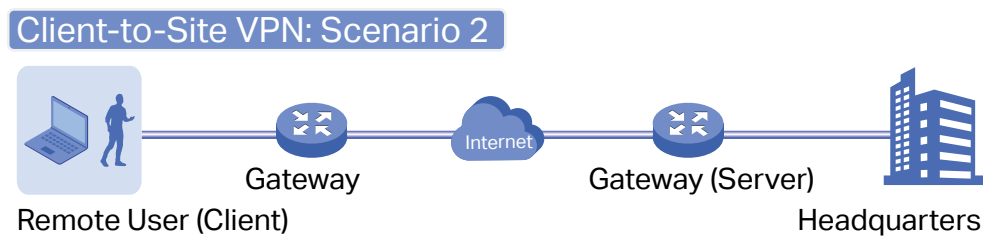
- VPN Client

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

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



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



Note:

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

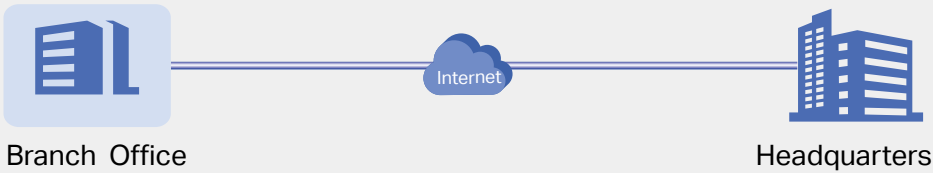
In scenario 2, you need to configure VPN server on the gateway, and then configure the VPN client software program on the remote user's laptop or PC, while the remote user's gateway doesn't need any VPN configuration.

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

 Create a VPN Policy

 Select the purpose of the VPN

Site-to-Site VPN



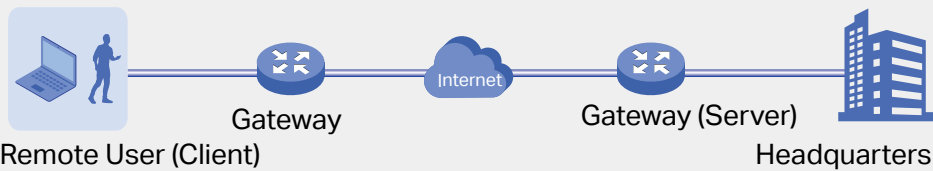
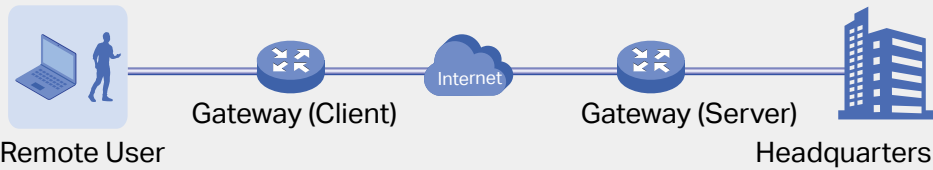
Auto IPsec VPN


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

Manual IPsec VPN

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

Client-to-Site VPN



 Select the role of the gateway and VPN tunneling protocol

VPN Server

VPN Client

L2TP

L2TP

PPTP

PPTP

IPsec

IPsec (Only for VPN client software)

OpenVPN

OpenVPN

Configuration

To complete the VPN configuration, follow these steps:

- 1) Create a new VPN policy and select the purpose of the VPN according to your needs. Select Site-to-Site if you want the network connected to another. Select Client-to-Site if you want some hosts connected to the network.
- 2) Select the VPN tunneling protocol and configure the VPN policy based on the protocol.

■ Configuring Site-to-Site VPN

The gateway supports two types of Site-to-Site VPNs: [Auto IPsec](#) and [Manual IPsec](#).

- Configuring Auto IPsec VPN

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

Create New VPN Policy

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type: Auto IPsec
 Manual IPsec

Remote Site:

[Create](#) [Cancel](#)

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

| | |
|--------------------------|--|
| Name | Enter a name to identify the VPN policy. |
| Status | Click the checkbox to enable the VPN policy. |
| Purpose | Select the purpose for the VPN as Site-to-Site VPN . |
| VPN Type | Select the VPN type as Auto IPsec . With Auto IPsec, the controller automatically creates an IPsec VPN tunnel between two sites on the same controller. The VPN connection is bidirectional. That is, creating an Auto IPsec VPN from site A to site B also provides connectivity from site B to site A, and nothing is needed to be configured on site B. |

Remote Site Select the site on the other end of the Auto IPsec VPN tunnel. Make sure that the selected remote site has an online gateway within the same controller.

- Configuring Manual IPsec VPN

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

Create New VPN Policy

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type: Auto IPsec
 Manual IPsec

Remote Gateway:

Remote Subnets: /

[+ Add Subnet](#)

Local Network Type: Network
 Custom IP

Local Networks: [i](#)

Pre-Shared Key:

WAN:

[+ Advanced Settings](#)

[Create](#) [Cancel](#)

- Enter a name to identify the VPN policy and select the purpose as Site-to-Site VPN. Refer to the following table to configure the basic parameters and click [Create](#).

Name Enter a name to identify the VPN policy.

Status Click the checkbox to enable the VPN policy.

| | |
|--------------------|--|
| Purpose | Select the purpose for the VPN as Site-to-Site VPN . |
| VPN Type | Select the VPN type as Manual IPsec . |
| Remote Gateway | Enter an IP address or a domain name as the gateway on the remote peer of the VPN tunnel. |
| Remote Subnets | Enter the IP address range of LAN on the remote peer of the VPN tunnel. Remote subnets should not be in the same network segment as the local LAN. |
| Local Network Type | <p>Specify whether to apply the VPN policy to specific local networks or IP addresses.</p> <p>Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks.</p> <p>Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.</p> |
| Pre-Shared Key | <p>Enter the pre-shared key(PSK). Both peer gateways must use the same pre-shared secret key for authentication.</p> <p>A pre-shared key is a string of characters that is used as an authentication key. Both peer gateways create a hash value based on the same pre-shared key and other information. The hash values are then exchanged and verified to authenticate the other party.</p> <p>The pre-shared keys should be long and random for security. Short or predictable pre-shared keys can be easily broken in brute-force attacks. To maintain a high level of security, administrators are recommended to update the pre-shared key periodically.</p> |
| WAN | Select the WAN port on which the IPsec VPN tunnel is established. |

3. Click [Advanced Settings](#) to load the following page.

☰

Advanced Settings

Phase-1 Settings

Key Exchange Version: IKEv1 i
 IKEv2

Proposal: SHA1 - AES256 - DH2 ▼

Exchange Mode: Main Mode
 Aggressive Mode

Negotiation Mode: Initiator Mode
 Responder Mode

Local ID Type: IP Address
 Name

Remote ID Type: IP Address
 Name

SA Lifetime: 28800 seconds (60-604800)

DPD: Enable

DPD Interval: 10 seconds (1-300)

Phase-2 Settings

Encapsulation Mode: Tunnel Mode
 Transport Mode

Proposal: ESP - SHA1 - AES256 ▼

PFS: None ▼

SA Lifetime: 28800 seconds (120-604800)

Create
Cancel

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

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

Refer to the following table to complete the configurations according to your actual needs and click [Create](#).

For Phase-1 Settings:

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

| | |
|------------------------------|--|
| Local ID Type | Specify the type of Local ID which indicates the authentication identifier sent to the peer for IKE negotiation. |
| | IP Address: Select IP Address to use the IP address for authentication. |
| | Name: Select Name, and then enter the name in the Local ID field to use the name as the ID for authentication. |
| | Note that the type and value of Local ID should be the same as Remote ID given for the remote peer of the VPN tunnel. |
| Local ID | When the Local ID Type is configured as Name, enter a name for the local device as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name). |
| Remote ID Type | Specify the type of Remote ID which indicates the authentication identifier received from the peer for IKE negotiation. |
| | IP Address: Select IP Address to use the IP address for authentication. |
| | Name: Select Name, and then enter the name in the Remote ID field to use the name as the ID for authentication. |
| | Note that the type and value of Remote ID should be the same as Local ID given for the remote peer of the VPN tunnel. |
| Remote ID | When the Remote ID Type is configured as Name, enter a name of the remote peer as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name). |
| SA Lifetime | Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted. |
| DPD | Check the box to enable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive. |
| DPD Interval | Specify the interval between sending DPD requests with DPD enabled. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA. |
| For Phase-2 Settings: | |
| Phase-2 Settings | The purpose of Phase 2 negotiations is to establish the Phase-2 SA (also called the IPsec SA). The IPsec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic. |
| Encapsulation Mode | Specify the Encapsulation Mode as Tunnel Mode or Transport Mode. When both ends of the tunnel are hosts, either mode can be chosen. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, Tunnel Mode is recommended to ensure safety. |

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

■ **Configuring Client-to-Site VPN**

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

[Configuring the gateway as a VPN server using L2TP](#)

[Configuring the gateway as a VPN server using PPTP](#)

[Configuring the gateway as a VPN server using IPsec](#)

[Configuring the gateway as a VPN server using OpenVPN](#)

[Configuring the gateway as a VPN client using L2TP](#)

[Configuring the gateway as a VPN client using PPTP](#)

[Configuring the gateway as a VPN client using OpenVPN](#)

- Configuring the gateway as a VPN server using L2TP

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

Create New VPN Policy

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type:

IPsec Encryption: Encrypted
 Unencrypted
 Auto

Authentication Mode: Local
 LDAP

Local Network Type: Network
 Custom IP

Local Networks: ⓘ

Pre-Shared Key:

WAN:

IP Pool Type: IP Address/Mask
 IP Address Range

IP Pool: / ⓘ

Primary DNS Server:

Secondary DNS Server: (Optional)

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

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

| | |
|-----------------------------|--|
| IPsec Encryption | <p>Specify whether to enable the encryption for the tunnel.</p> <p>Encrypted: Select Encrypted to encrypt the L2TP tunnel by IPsec (L2TP over IPsec). With Encrypted selected, enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication.</p> <p>Unencrypted: With Unencrypted selected, the L2TP tunnel will not be encrypted by IPsec.</p> <p>Auto: With Auto selected, the L2TP server will determine whether to encrypt the tunnel according to the client 's encryption settings. And enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication.</p> |
| Authentication Mode | Select the authentication mode: Local or LDAP. |
| Local Network Type | <p>Specify whether to apply the VPN policy to specific local networks or IP addresses.</p> <p>Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks.</p> <p>Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.</p> |
| Pre-shared Key | Enter the pre-shared secret key when IPsec Encryption is selected as Encrypted and Auto. Both peer routers must use the same pre-shared secret key for authentication. |
| WAN | Select the WAN port on which the L2TP VPN tunnel is established. Each WAN port supports only one L2TP VPN tunnel when the gateway works as a L2TP server. |
| IP Pool Type | Specify the format of the IP pool. |
| IP Pool | If you selected IP Address/Mask type, enter the IP address and subnet mask to decide the range of the VPN IP pool. If you select IP Address Range type, enter the start and end IP addresses of the VPN IP pool. |
| Primary DNS Server | Enter the IP address of the primary DNS server provided by your ISP. |
| Secondary DNS Server | (Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down. |

3. Add the VPN users account to validate remote hosts. To create VPN users, refer to [4. 7. 2 VPN User](#).

- Configuring the gateway as a VPN server using PPTP

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

Create New VPN Policy

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type:

MPPE Encryption: Encrypted
 Unencrypted
 Auto

Authentication Mode: Local
 LDAP

Local Network Type: Network
 Custom IP

Local Networks: ⓘ

WAN:

IP Pool Type: IP Address/Mask
 IP Address Range

IP Pool: / ⓘ

Primary DNS Server:

Secondary DNS Server: (Optional)

[Create](#) [Cancel](#)

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

| | |
|-------------------------------------|--|
| Name | Enter a name to identify the VPN policy. |
| Status | Click the checkbox to enable the VPN policy. |
| Purpose | Select the purpose for the VPN as Client-to-Site VPN . |
| VPN Type | Select the VPN type as VPN Server - PPTP . |
| MPPE Encryption | Specify whether to enable MPPE (Microsoft Point-to-Point Encryption) for the tunnel. Encrypted : With Encrypted selected, the PPTP tunnel will be encrypted by MPPE. Unencrypted : With Unencrypted selected, the PPTP tunnel will be not encrypted by MPPE. |
| Authentication Mode | Select the authentication mode: Local or LDAP. |

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

3. Add the VPN users account to validate remote hosts. To create VPN users, refer to [4. 7. 2 VPN User](#).
- Configuring the gateway as a VPN server using IPsec
1. Select a site from the drop-down list of [Organization](#). Go to [Settings > VPN](#). Click [+ Create New VPN Policy](#) to load the following page.

Create New VPN Policy

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type:

Remote Host:

Local Network Type: Network
 Custom IP

Local Networks: ⓘ

Pre-Shared Key:

WAN:

IP Pool: / ⓘ

Primary DNS Server: . .

Secondary DNS Server: . . (Optional)

Advanced Settings

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

| | |
|-----------------------------|---|
| Name | Enter a name to identify the VPN policy. |
| Status | Click the checkbox to enable the VPN policy. |
| Purpose | Select the purpose for the VPN as Client-to-Site VPN . |
| VPN Type | Select the VPN type as VPN Server - IPsec . |
| Remote Host | Enter an IP address or a domain name of the host on the remote peer of the VPN tunnel. 0.0.0.0 represents any IP address. |
| Local Network Type | Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses. |
| Pre-Shared Key | Enter the pre-shared key(PSK). Both peer gateways must use the same pre-shared secret key for authentication. A pre-shared key is a string of characters that is used as an authentication key. Both VPN peers create a hash value based on the same pre-shared key and other information. The hash values are then exchanged and verified to authenticate the other party. The pre-shared keys should be long and random for security. Short or predictable pre-shared keys can be easily broken in brute-force attacks. To maintain a high level of security, administrators are recommended to update the pre-shared key periodically. |
| WAN | Select the WAN port on which the IPsec VPN tunnel is established. |
| IP Pool | Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router. |
| Primary DNS Server | Enter the IP address of the primary DNS server provided by your ISP. |
| Secondary DNS Server | (Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down. |

3. Click Advanced Settings to load the following page.

- **Advanced Settings**

Phase-1 Settings

Key Exchange Version: IKEv1 i IKEv2

Proposal: SHA1 - AES256 - DH2 v

Exchange Mode: Main Mode Aggressive Mode

Negotiation Mode: Initiator Mode Responder Mode

Local ID Type: IP Address Name

Remote ID Type: IP Address Name

SA Lifetime: 28800 seconds (60-604800)

DPD: Enable

DPD Interval: 10 seconds (1-300)

Phase-2 Settings

Encapsulation Mode: Tunnel Mode Transport Mode

Proposal: ESP - SHA1 - AES256 v

PFS: None v

SA Lifetime: 28800 seconds (120-604800)

Create
Cancel

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

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

Refer to the following table to complete the configurations according to your actual needs and click [Create](#).

For Phase-1 Settings:

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

| | |
|------------------------------|---|
| Local ID Type | <p>Specify the type of Local ID which indicates the authentication identifier sent to the peer for IKE negotiation.</p> <p>IP Address: Select IP Address to use the IP address for authentication.</p> <p>Name: Select Name, and then enter the name in the Local ID field to use the name as the ID for authentication.</p> <p>Note that the type and value of Local ID should be the same as Remote ID given for the remote peer of the VPN tunnel.</p> |
| Local ID | <p>When the Local ID Type is configured as Name, enter a name for the local device as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).</p> |
| Remote ID Type | <p>Specify the type of Remote ID which indicates the authentication identifier received from the peer for IKE negotiation.</p> <p>IP Address: Select IP Address to use the IP address for authentication.</p> <p>Name: Select Name, and then enter the name in the Remote ID field to use the name as the ID for authentication.</p> <p>Note that the type and value of Remote ID should be the same as Local ID given for the remote peer of the VPN tunnel.</p> |
| Remote ID | <p>When the Remote ID Type is configured as Name, enter a name of the remote peer as the ID in IKE negotiation. The name should be in the format of FQDN (Fully Qualified Domain Name).</p> |
| SA Lifetime | <p>Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.</p> |
| DPD | <p>Check the box to enable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.</p> |
| DPD Interval | <p>Specify the interval between sending DPD requests with DPD enabled. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA.</p> |
| For Phase-2 Settings: | |
| Phase-2 Settings | <p>The purpose of Phase 2 negotiations is to establish the Phase-2 SA (also called the IPsec SA). The IPsec SA is a set of traffic specifications that tell the device what traffic to send over the VPN, and how to encrypt and authenticate that traffic.</p> |
| Encapsulation Mode | <p>Specify the Encapsulation Mode as Tunnel Mode or Transport Mode. When both ends of the tunnel are hosts, either mode can be chosen. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, Tunnel Mode is recommended to ensure safety.</p> |

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

- Configuring the gateway as a VPN server using OpenVPN

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

Create New VPN Policy

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type:

Account Password: Enable

Tunnel Mode: Split
 Full

Protocol: TCP
 UDP

Service Port: (1-65535)

Authentication Mode: Local
 LDAP

Local Network Type: Network
 Custom IP

Local Networks: ⓘ

WAN:

IP Pool: / ⓘ


Primary DNS Server: . .




Secondary DNS Server: . . (Optional)

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

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

| | |
|-----------------------------|--|
| Purpose | Select the purpose for the VPN as Client-to-Site VPN . |
| VPN Type | Select the VPN type as VPN Server - OpenVPN . |
| Account Password | Specify whether VPN clients need to enter a user account to access the VPN tunnel. When enabled, you need to create accounts on the VPN User page. |
| Tunnel Mode | Select the tunnel mode: Split or Full. Full tunneling uses the VPN for all your traffic, whereas split tunneling sends part of your traffic through a VPN and part of it through the open network. Full tunneling is more secure than split tunneling. |
| Protocol | Select the communication protocol for the gateway which works as an OpenVPN Server. Two communication protocols are available: TCP and UDP. |
| Service Port | Enter a VPN service port to which a VPN device connects. |
| Authentication Mode | Select the authentication mode: Local or LDAP. LDAP is used for SSO (single sign-on), which enables users to use the same password in multiple services. |
| Local Network Type | Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses. |
| WAN | Select the WAN port on which the VPN tunnel is established. Each WAN port supports only one OpenVPN tunnel when the gateway works as a OpenVPN server. |
| IP Pool | Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer router. |
| Primary DNS Server | Enter the IP address of the primary DNS server provided by your ISP. |
| Secondary DNS Server | (Optional) Enter the IP address of the secondary DNS server, which provides redundancy in case the primary DNS server goes down. |

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

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

Showing 1-2 of 2 records < 1 > 10 /page Go To page: [GO](#)

[+ Create New VPN Policy](#)

- Configuring the gateway as a VPN client using L2TP

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

Create New VPN Policy ⓘ

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type:

Working Mode: NAT
 Routing

Username:

Password:

IPsec Encryption: Encrypted
 Unencrypted
 Auto

Remote Server:

Remote Subnets: /

[+ Add Subnet](#)

Local Network Type: Network
 Custom IP

Local Networks: ⓘ

Pre-Shared Key:

WAN:

[Create](#) [Cancel](#)

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

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

| | |
|---------------------------|--|
| Working Mode | <p>Specify the Working Mode as NAT or Routing.</p> <p>NAT: With NAT (Network Address Translation) mode selected, the L2TP client uses the assigned IP address as its source addresses of original IP header when forwarding L2TP packets.</p> <p>Routing: With Routing selected, the L2TP client uses its own IP address as its source addresses of original IP header when forwarding L2TP packets.</p> |
| Username | <p>Enter the username used for the VPN tunnel. This username should be the same as that of the L2TP server.</p> |
| Password | <p>Enter the password of user. This password should be the same as that of the L2TP server.</p> |
| IPsec Encryption | <p>Specify whether to enable the encryption for the tunnel.</p> <p>Encrypted: Select Encrypted to encrypt the L2TP tunnel by IPsec (L2TP over IPsec). With Encrypted selected, enter the Pre-shared Key for IKE authentication. VPN server and VPN client must use the same pre-shared secret key for authentication.</p> <p>Unencrypted: With Unencrypted selected, the L2TP tunnel will be not encrypted by IPsec.</p> |
| Remote Server | <p>Enter the IP address or domain name of the L2TP server.</p> |
| Remote Subnets | <p>Enter the IP address and subnet mask to specify the remote network. It's always the IP address range of LAN on the remote peer of the VPN tunnel.</p> |
| Local Network Type | <p>Specify whether to apply the VPN policy to specific local networks or IP addresses.</p> <p>Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks.</p> <p>Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.</p> |
| Pre-shared Key | <p>Enter the pre-shared secret key when the L2TP tunnel is encrypted by IPsec. Both peer gateways must use the same pre-shared secret key for authentication.</p> |
| WAN | <p>Select the WAN port on which the VPN tunnel is established.</p> |

- Configuring the gateway as a VPN client using PPTP

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

Create New VPN Policy

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type:

Working Mode: NAT
 Routing

Username:

Password:

MPPE Encryption: Encrypted
 Unencrypted
 Auto

Remote Server:

Remote Subnets: /

[+ Add Subnet](#)

Local Network Type: Network
 Custom IP

Local Networks: ⓘ

WAN:

[Create](#) [Cancel](#)

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

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

| | |
|---------------------------|--|
| Working Mode | <p>Specify the Working Mode as NAT or Routing.</p> <p>NAT: With NAT (Network Address Translation) mode selected, the PPTP client uses the assigned IP address as its source addresses of original IP header when forwarding PPTP packets.</p> <p>Routing: With Routing selected, the PPTP client uses its own IP address as its source addresses of original IP header when forwarding PPTP packets.</p> |
| Username | <p>Enter the username used for the VPN tunnel. This username should be the same as that of the PPTP server.</p> |
| Password | <p>Enter the password of user. This password should be the same as that of the PPTP server.</p> |
| MPPE Encryption | <p>Specify whether to enable the encryption for the tunnel.</p> <p>Encrypted: Select Encrypted to encrypt the PPTP tunnel by MPPE.</p> <p>Unencrypted: With Unencrypted selected, the PPTP tunnel will be not encrypted by MPPE.</p> |
| Remote Server | <p>Enter the IP address or domain name of the PPTP server.</p> |
| Remote Subnets | <p>Enter the IP address and subnet mask to specify the remote network. It's always the IP address range of LAN on the remote peer of the VPN tunnel.</p> |
| Local Network Type | <p>Specify whether to apply the VPN policy to specific local networks or IP addresses.</p> <p>Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks.</p> <p>Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses.</p> |
| WAN | <p>Select the WAN port on which the VPN tunnel is established.</p> |

- Configuring the gateway as a VPN client using OpenVPN

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

Create New VPN Policy

Name:

Status: Enable

Purpose: Site-to-Site VPN
 Client-to-Site VPN

VPN Type:

Mode: Certificate
 Certificate+Account

Remote Server: : (1-65535)

Local Network Type: Network
 Custom IP

Local Networks: ⓘ

WAN:

Configuration:

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

| | |
|--------------------------|--|
| Name | Enter a name to identify the VPN policy. |
| Status | Click the checkbox to enable the VPN policy. |
| Purpose | Select the purpose for the VPN as Client-to-Site VPN . |
| VPN Type | Select the VPN type as VPN Client - OpenVPN . |
| Mode | Select the access mode according to VPN requirements. Certificate : Select this option if the VPN tunnel only requires the certificate. Certificate+Account : Select this option if the VPN tunnel requires the certificate and VPN user account. If selected, configure the following parameters: Username : Enter the username for the VPN tunnel. Password : Enter the password for the VPN tunnel. |

| | |
|--------------------|--|
| Remote Server | Enter the IP address or domain name of the OpenVPN server. |
| Local Network Type | Specify whether to apply the VPN policy to specific local networks or IP addresses. Network: Specify the local networks of the VPN tunnel. The VPN policy will be only applied to the selected local networks. Custom IP: Specify the IP addresses of the VPN tunnel. The VPN policy will be only applied to the specified IP addresses. |
| WAN | Select the WAN port on which the VPN tunnel is established. |
| Configuration | Click <input type="button" value="Import"/> to import the OpenVPN file that ends in .ovpn generated by the OpenVPN server. Only one file can be imported. If the certificate file and configuration file are generated singly by the OpenVPN server, combine two files and import the whole file. |

4.7.2 VPN User

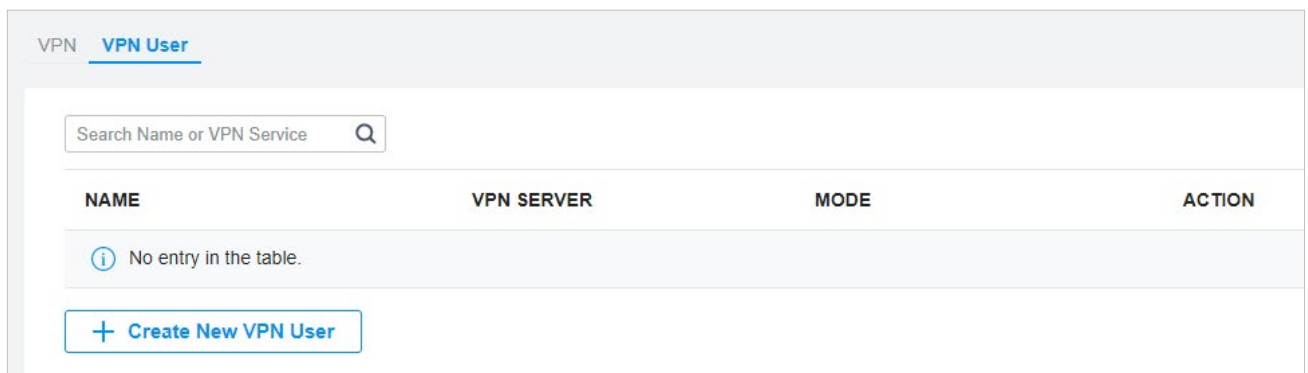
Overview

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

Configuration

To configure the VPN users, follow these steps:

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



2. Specify the parameters and click [Create](#).

Create New VPN User

Username:

Password:

Protocol: L2TP/PPTP ▼

VPN Server: Please Select... ▼

Local IP Address: (Optional)

Mode: Client i Network Extension Mode i

Maximum Connections: (1-100)

[Create](#) [Cancel](#)

Username Enter the username used for the VPN tunnel. The client use the username for the validation before accessing the network.

Password Enter the password of user. The client uses the password for the validation before accessing the network.

Protocol Select the protocol type for the VPN tunnel.

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

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

Local IP Address (Optional) Specify the local IP address of the VPN tunnel.

Mode Specify the connection mode for the VPN users.

Client: This mode allows the client to request for an IP address and the server supplies the IP addresses from the VPN IP Pool. With this mode selected, set maximum number of concurrent VPN connections with the same account in [Maximum Connections](#).

Network Extension Mode: This mode allows only clients from the configured subnet to connect to the server and obtain VPN services. With this mode selected, specify the subnets in [Remote Subnets](#).

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

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

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

| NAME | VPN SERVER | MODE | ACTION |
|------|---------------------------|--------|--------|
| user | L2TP Server: VPN Server 1 | Client | |

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

[+ Create New VPN User](#)



Filter the entries.



View and edit the account information of users.



Delete the VPN user.

4.7.3 IPsec Failover

Overview

IPsec Failover is used to configure the backup group of the IPsec connection. When the primary connection in the group is interrupted, it will try to use the secondary connection to dial up to maintain the stability of the VPN network.

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Settings > VPN > IPsec Failover](#). Click [Create New IPsec Failover](#) to add a new entry.

Create New IPsec Failover ⓘ

Group Name:

Primary Tunnel:

Secondary Tunnel:

Automatic Failback:

Gateway Failover Timeout: seconds (10-3600)

[Create](#) [Cancel](#)

Group Name

Enter a name to identify the IPsec Failover group.

| | |
|------------------------------------|---|
| Primary Tunnel | Specify the IPsec primary connection. |
| Secondary Tunnel | Specify the IPsec secondary connection. |
| Automatic Failback | Select this function to automatically switch back to the primary connection when it is reachable. When selected, specify the Gateway Failover Timeout time, then the system will query whether the primary connection is reachable within the time, and if yes, it will switch back to the primary connection. |

4.7.4 SSL VPN

Overview

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

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

Configuration

■ SSL VPN Server

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

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

SSL VPN Server Resource Management User Group User List Locked Out User

SSL VPN Server

SSL VPN Server:

WAN:

Virtual IP Pool: -

Primary DNS:

Secondary DNS: (Optional)

Listen on Port: (1-65535)

Authentication Type: Local Authentication RADIUS Authentication

Username Lockout:

IP Lockout:

Idle Timeout:

Full Mode:

[Apply](#) [Cancel](#) [Export Certificate](#)

2. Configure the parameters according to your needs. Click [Apply](#).

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

| | |
|----------------------------|--|
| Authentication Type | Select the authentication for the clients: Local Authentication or RADIUS Authentication . |
| | If you selected RADIUS Authentication , configure the following parameters: |
| | RADIUS Server: Select a RADIUS server profile. |
| | Authentication Type: Select the authentication protocol for the RADIUS server. |
| | Max Requests: Specify the maximum number of requests sent when no response is received. |
| | Request Timeout: Specify the maximum interval for request timeout. After timeout, the request will be sent again. |
| | NAS IP: Specify the IP address for the router to communicate with the RADIUS server. |

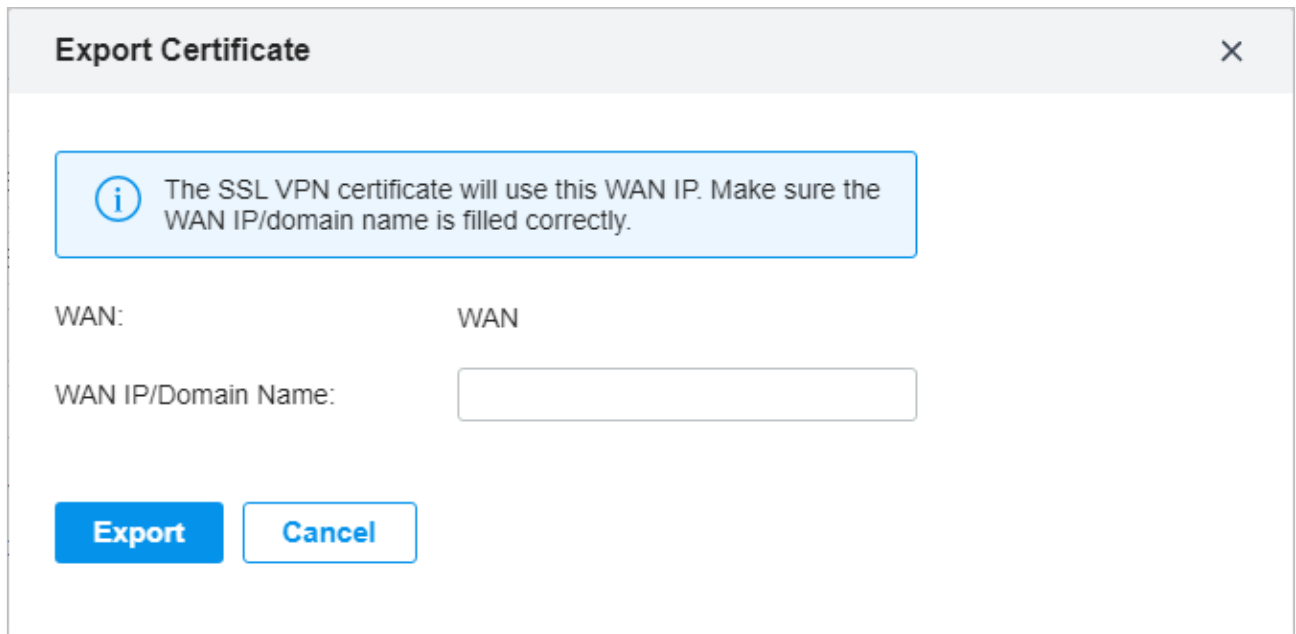
| | |
|-------------------------|--|
| Username Lockout | When enabled, you can lock out a username in case of excessive login attempts. |
| | Max Login Attempts: Specify the maximum failed login attempts for a username. If the number of attempts reaches this amount, the username will be locked out. |
| | Lockout Duration: Specify how long the username will be locked out. |

| | |
|-------------------|--|
| IP Lockout | When enabled, you can lock out an IP address in case of excessive login attempts. |
| | Max Login Attempts: Specify the maximum failed login attempts for a login IP. If the number of attempts reaches this amount, the login IP will be locked out. |
| | Lockout Duration: Specify how long the login IP will be locked out. |

| | |
|---------------------|--|
| Idle Timeout | When enabled, the VPN tunnel will close automatically if there is no traffic for the specified amount of time. |
|---------------------|--|

| | |
|------------------|---|
| Full Mode | When enable, all traffic will go through the SSL VPN tunnel. When disabled, only the resource-related traffic will go through the tunnel. |
|------------------|---|

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



Export Certificate ×

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

WAN: WAN

WAN IP/Domain Name:

[Export](#) [Cancel](#)

■ Resource Management

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

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

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

2. Click [Create New Tunnel Resource](#) to load the following page. Configure the parameters and click [Confirm](#).

Create New Tunnel Resource
✕

Name:

Resource Type:

IP/Mask: /

Protocol:

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

Confirm
Cancel

Name Specify a name for the entry.

Resource Type Select the type for the resources: [IP Address](#) or [Domain Name](#).

If you selected [IP Address](#), configure the following parameters:

IP/Mask: Specify IP range the clients can access.

Protocol: Select the protocol type that the client can access in the IP range, and the router will filter illegal packets through firewall rules. By default, the value is ALL, and it means there is no restriction on the client.

If you selected [Domain Name](#), specify domain name the clients can access.

3. Click [Create New Resource Group](#) to load the following page. Configure the parameters and click [Confirm](#).

Create New Resource Group
✕

Resource Group:

Resources:

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

Confirm
Cancel

Resource Group Specify a name for the resource group.

Resources

Select the resources for the group.

■ User Group

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

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

Create New User Group
×

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

Resource Group List:

Group Name

Specify a name for the user group.

Resource Group List

Select the resource group for the user group.

■ User List

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

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

- Click [Create New User](#) to load the following page. Configure the parameters and click [Confirm](#).

Create New User
✕

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

Password: (1-64 characters, using a combination of letters, digits, and symbols)

Max Concurrent Users: (1-100)

Expiration Date:

User Group:

Status:

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

■ Locked Out User

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

- Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [VPN](#) > [SSL VPN](#) > [Locked Out User](#).

2. Click [Add Locked Out User](#) to load the following page. Configure the parameters and click [Confirm](#).

Add Locked Out User
✕

Type: Username ▼

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

Locked Out Duration: 0h ▼ 01m ▼

Confirm
Cancel

Type

Specify the locked out type.

If you selected [Username](#), specify the username of a locked out user.

If you selected [IP Address](#), specify the IP address of a locked out user.

Lockout Duration

Specify how long the entry will be locked out.

4.7.5 WireGuard VPN

Overview

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

■ WireGuard

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [VPN](#) > [WireGuard](#).

2. Click [Create New WireGuard](#). Configure the parameters and click [Apply](#).

Edit Wireguard

Name:

Status: Enable

MTU: (576-1440)

Listen Port: (1-65535)

Local IP Address:

Private Key:

[Apply](#) [Cancel](#)

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

■ Peers

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

2. Click [Create New Peer](#). Configure the parameters and click [Apply](#).

Edit Peer

Name:

Status: Enable

Interface: ▾

Endpoint: (Optional)

Endpoint Port: (Optional)

Allow Address: / [+ Add Subnet](#)

Persistent Keepalive: (0-65535 second)

Comment: (0-128 characters)

Public Key:

Preshared Key: (Optional)

[Apply](#) [Cancel](#)

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

♥ 4.8 Create Profiles

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

4.8.1 Time Range

Overview

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

Configuration

To configure the time range profiles, follow these steps:

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

| NAME | DAY MODE | TIME RANGE | ACTION |
|---|----------|------------|--------|
| <i>i</i> No time range profiles yet. | | | |
| + Create New Time Range | | | |

2. Enter a Name for the new entry, select the Day Mode, and specify the time range. Click [+Add](#) to add a new time period, click [Apply](#) to save the entry. After saving the newly added entry, you can apply

them to site configuration. To apply the customized time range profiles in configuration, refer to [4. 3 WLAN Schedule](#), and [4. 10. 8 Port Schedule](#).

Create New Time Range

Name:

Day Mode: Every Day Weekday Weekend Customized

Every Day

08:00 am 06:00 pm

08:00 am 06:00 pm

[+ Add](#)

| | |
|-----------------|---|
| Name | Enter a name for the new entry, and it is a string with 1 to 64 ASCII symbols. |
| Day Mode | <p>Select Every Day, Weekday, Weekend, or Customized first before specifying the time range for each day.</p> <p>Every Day: You only need to set the time range once, and it will repeat every day.</p> <p>Weekday: You only need to set the time range once, and it will repeat every weekday from Monday to Friday.</p> <p>Weekend: You only need to set the time range once, and it will repeat every Saturday and Sunday.</p> <p>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.</p> |

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

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

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

[+ Create New Time Range](#)

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



Edit the parameters in the entry.



Delete the entry.

4.8.2 Groups

Overview

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

Configuration

To configure the group profiles, follow these steps:

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Profiles](#) > [Groups](#). Click [+Create New Group](#) to add a new group profile.

| NAME ↕ | TYPE | COUNT | ACTION |
|---------------|------------|-------|--------|
| IPGroup_Any | IP Group | 1 | |
| IPv6Group_Any | IPv6 Group | 1 | |

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

[+ Create New Group](#)

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

Create New Group

Name :

Type: IP Group
 IPv6 Group
 IP-Port Group
 IPv6-Port Group
 MAC Group
 Location Group

IP Subnets : . . /

[+ Add Subnet](#)

- **To create an IP group profile:**
Choose the [IP Group](#) type and specify IP subnets.
- **To create an IPv6 group profile:**
Choose the [IPv6 Group](#) type and specify IPv6 addresses.
- **To Create an IP-Port group profile:**
Choose the [IP-Port Group](#) type and specify the IP-Port type and ports, while it is optional to specify IP subnets. If you only specify ports without entering any IP subnets, it means the group contains the specified ports for all IP addresses.
- **To create an IPv6-Port group profile:**
Choose the [IPv6-Port Group](#) type and specify the IP-Port type and ports, while it is optional to specify IPv6 addresses. If you only specify ports without entering any IPv6 addresses, it means the group contains the specified ports for all IPv6 addresses.
- **To configure a MAC group profile:**
Choose the [MAC Group](#) type and add MAC addresses in the MAC Addresses List.



Add

Add MAC address individually.

 **Batch Add**

Add MAC addresses in batches. You can enter the MAC addresses and names in the input box or import them with files in the format of Excel, txt, and text.

If you want to use the newly added MAC address(es) and names when they conflict with the existing ones, check the box to override the current MAC addresses in the list.

Note:

1. Each MAC address and name should be entered on a new line. The MAC address and name should be separated by a space.
2. Octets in a MAC address should be separated by a hyphen. For example, AA-BB-CC-DD-EE-FF.

 **Add from Client List**















Add MAC addresses from the clients that are connected to the devices controlled by the SDN Controller.

■ To configure a location group profile:

Choose the [Location Group](#) type and select locations. You can enter a description for identification.

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.

| NAME | TYPE | COUNT | ACTION |
|-------------------|-----------------|-------|---|
| IP Group_1 | IP Group | 2 |   |
| IPv6Group_Any | IPv6 Group | 1 |  |
| IP-Port Group_1 | IP-Port Group | 1 |   |
| IPGroup_Any | IP Group | 1 |  |
| IPv6 Group_1 | IPv6 Group | 1 |   |
| IPv6-Port Group_1 | IPv6-Port Group | 3 |   |
| Location Group_1 | Location Group | 1 |   |
| MAC Group_1 | MAC Group | 1 |    |

4.8.3 Rate Limit


Overview

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

Configuration

To configure the rate limit profiles, follow these steps:

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


| NAME | Download Limit | Upload Limit | ACTION |
|---------|----------------|--------------|---|
| Default | Unlimited | Unlimited |  |

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

[+ Create New Rate Limit Profile](#)

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.

Create New Rate Limit Profile

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

Name:

Download Limit: Enable






Upload Limit: Enable

Apply Cancel

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

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

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

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

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

[+ Create New Rate Limit Profile](#)

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



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



Delete the entry.

4.8.4 PPSK

Overview

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

Configuration

To configure the PPSK profiles, follow these steps:

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

| NAME | SSID | ACTION |
|------------------------|------|--------|
| No entry in the table. | | |

[+ Create New PPSK Profile](#)

2. Enter a name for the new profile.

3. Add new entries to the PPSK profile.

- **Method 1: Add entries manually**

Click [Add](#) and select [Manually](#) for PPSK Generation. Configure the parameters.

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

Apply the settings. The new PPSK entry will be created.

- **Method 2: Add entries automatically**

Click [Add](#) and select [Auto](#) for PPSK Generation. Configure the parameters and apply the settings.

| | |
|-----------------------------------|---|
| Number of PPSK | Enter the number of PPSK entries to create. |
| PPSK Name Prefix | Enter the prefix of the names for the created PPSK entries. |
| Passphrase Length | Enter the passphrase length. |
| VLAN Assignment | (Optional) Enter the VLAN ID, and the client who uses the passphrase for authentication will be assigned to the specified VLAN. |

Apply the settings. New PPSK entries will be created automatically.

- **Method 3: Export and Import entries in batch**

After creating PPSK entries, you can click [Export](#) to save them to a file locally, then access another site and click [Import](#) to import them in batches from the file.

template and fill in your PPSK information. Then import the file.' Below this is a 'Choose File:' label, a text input field containing 'Please select a file.', and a 'Browse' button with an upload icon. At the bottom left are 'Import' and 'Cancel' buttons."/>

4. After saving the newly added profile, you can apply them to wireless networks, refer to [4. 4. 1 Set Up Basic Wireless Networks](#).

4.8.5 Gateway QoS Service

Overview

In Gateway QoS Service, you can define service type entries that will appear as matching conditions for you to choose when configuring the rules of related modules like QoS. The default entries cannot be edited or deleted. You can add other entries if your service type is not in the list.

Configuration

To configure the Gateway QoS Service profiles, follow these steps:

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Profiles](#) > [Gateway QoS Service](#). Click [+Create New Gateway QoS Service](#) to add a new profile .

Create New Gateway QoS Service

Service Name:

Protocol:

Source Port Range: - (0-65535)

Destination Port Range: - (0-65535)

Description: (Optional)

2. Configure the parameters.

| | |
|--|---|
| Service Name | Enter a name to identify the profile. |
| Protocol | Specify the protocol for the service. The system predefined protocols include TCP, UDP, TCP/UDP and ICMP. For other protocols, select the option Other. |
| Source Port Range | Specify the source port range for the service. Packets whose source port and destination port are both in the range are considered as the target packets. |
| Destination Port Range | Specify the destination port range for the service. Packets whose source port and destination port are both in the range are considered as the target packets. |
| Type | Specify the type of the ICMP packets. 255 means all types are included. ICMP packets with both the type and code fields matched are considered as the target packets. |
| Code | Specify the code of the ICMP packets. 255 means all codes are included. ICMP packets with both the type and code fields matched are considered as the target packets. |
| Protocol Number | Specify the protocol number of the packets. Packets matched with the protocol number are considered as the target packets. |
| Description | Enter a description for identification. |

3. Click [Apply](#) to save the profile. Now you can select the predefined entry of service type when configuring rules of related modules like QoS.

4.8.6 Bonjour Service

Overview

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

Configuration

To configure the Bonjour Service profiles, follow these steps:

1. Select a site from the drop-down list of [Organization](#). Go to [Settings > Profiles > Bonjour Service](#). Click [+Create New Bonjour Service](#) to add a new profile .

2. Configure the parameters.

| | |
|------------------------------|--|
| Service Name | Enter a name to identify the profile. |
| Service ID | Specify the domain name corresponding to the mDNS service. It is used to identify and filter mDNS packets. |

3. Click [Apply](#) to save the profile.

4.8.7 RADIUS Profile

Overview

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

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

the database when the users are requesting to access the network, and provides authorization and accounting services for them.

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

Configuration

■ Configure the Built-in RADIUS Profile (for Software/Hardware Controller only)

- Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Profiles](#) > [RADIUS Profile](#).
- The Software/Hardware Controller provides a Built-in RADIUS Profile. Click the edit icon of the profile, then click [Add New RADIUS User](#).
- Configure the parameters and save the settings.

Authentication Type

Select the Authentication Type.

User Authentication: Select this option and enter the user [Name](#) and [Password](#) for authentication.

MAC Authentication: Select this option and enter the [MAC Address](#) for authentication.

VLAN ID

Enter a VLAN ID to assign VLANs to users.

Session-Timeout

Configure the authentication expiration time for users.

Rate Limit When enabled, you can set limits for [Uplink Rate](#) and [Downlink Rate](#) of each client to balance bandwidth usage.

This function applies to the portal service only.

Traffic Limit When enabled, you can set limits for [Uplink Traffic](#) and [Downlink Traffic](#) of each client.

This function applies to the portal service only.

■ Create New RADIUS Profile

- a. Select a site from the drop-down list of [Organization](#). Go to [Settings > Profiles > RADIUS Profile](#).
- b. Click [Create New RADIUS Profile](#). Configure the parameters and save the settings.

Create New RADIUS Profile

Name:

VLAN Assignment: Enable VLAN Assignment for Wireless Network [i](#)

Authentication Server 1

Authentication Server IP:

Authentication Port: (1-65535)

Authentication Password: [🔑](#)

[+](#) [Add New Authentication Server](#)

RADIUS Accounting: Enable

Name Enter a name to identify the RADIUS profile.

VLAN Assignment This feature allows the RADIUS server to place a wireless user into a specific VLAN based on the credentials supplied by the user. To use the feature, you should create the specific VLAN first. And the user-to-VLAN mappings must be already stored in the RADIUS server database.

Note:

1. VLAN Assignment is not currently supported when a client is authenticated by Portal with External RADIUS Server or RADIUS Hotspot.
2. VLAN Assignment is applicable only when the device supports the feature. To make this feature work properly, it is recommended to upgrade your devices to the latest firmware version.

Authentication Server IP Enter the IP address of the authentication server.

Authentication Port Enter the UDP destination port on the authentication server for authentication requests.

Authentication Password Enter the password that will be used to validate the communication between network devices and the RADIUS authentication server.

| | |
|--------------------------------|--|
| RADIUS Accounting | Click the checkbox to enable RADIUS Accounting to meet billing needs. This feature is only available for APs with Portal to account for wireless clients. |
| Interim Update | Click the checkbox to enable Interim Update. By default, the RADIUS accounting process needs only start and stop messages to the RADIUS accounting server. With Interim Update enabled, network devices will periodically send an Interim Update (a RADIUS Accounting Request packet containing an "interim-update" value) to the RADIUS server. An Interim Update updates the user's session duration and current data usage. |
| Interim Update Interval | Enter an appropriate interval between the updates of users' session duration and current data usage. |
| Accounting Server IP | Enter the IP address of the RADIUS accounting server. |
| Accounting Port | Enter the UDP destination port on the RADIUS server for accounting requests. |
| Accounting Password | Enter the password that will be used to validate the communication between network devices and the RADIUS accounting server. |

4.8.8 LDAP Profiles

Overview

The Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for maintaining and accessing directory information over a network. LDAP Authentication allows you to bind the device to an LDAP server and use that server to authenticate LAN clients.

Configuration

To configure the LDAP profiles, follow these steps:

1. Select a site from the drop-down list of [Organization](#). Go to [Settings > Profiles > LDAP Profile](#). Click [+Create New LDAP Profile](#) to add a new profile .

Create New LDAP Profile

Status: Enable

Name:

Bind Type: ▼

Server Address:

Destination Port:

Use SSL: Enable

Common Name Identifier:

Base Distinguished Name: 🔍

2. Configure the parameters.

| | |
|--------------------------|---|
| Status | Check the box to enable LDAP Authentication. |
| Name | Specify the profile name. |
| Bind Type | Select the LDAP Authentication mode: Anonymous Mode, Simple Mode, or Regular Mode. |
| Server Address | Enter the IP address of the LDAP server. |
| Destination Port | Enter the port ID of the LDAP server. By default, the port ID is 389 when SSL is disabled and 636 when SSL is enabled. |
| Use SSL | Determine whether to use SSL for LDAP communication. |
| Regular DN | Specify the distinguished name (DN) of the administrator account. This parameter is required in Regular mode. |
| Regular Password | Specify the password of the administrator account. This parameter is required in Regular mode. |
| Common Name Identifier | Specify the common name for user authentication. It is usually "cn". |
| Base Distinguished Name | Specify the user identifier for user authentication. You can click the icon next to it to search and select from the LDAP directory tree. |
| Additional Filter | Specify the filter for user authentication. It is not supported in Simple Mode and is optional in other modes. |
| Group Distinguished Name | Specify the group identifier for user authentication. It is not supported in Simple Mode and is optional in other modes. |

- Click **Apply** to save the profile. Now you can select the predefined entry of LDAP profile when configuring rules of related modules like LDAP Server.

♥ 4.9 Authentication

Authentication is a portfolio of features designed to authorize network access to clients, which enhances the network security. Authentication services include [4.9.1 Portal](#), [4.9.2 802.1X](#) and [4.9.3 MAC-Based Authentication](#), covering all the needs to authenticate both wired and wireless clients.

4.9.1 Portal

Overview

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

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

The controller provides several types of Portal authentication:

■ No Authentication

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

■ Simple Password

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

■ Hotspot

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

• Voucher

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

• Local User

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

• SMS

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

- **RADIUS**

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

- **Form Auth**

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

- **RADIUS Server**

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

- **External Portal Server**

The option of External Portal Server is designed for the developers. They can customize their own authentication type like Google account authentication according to the interface provided by 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. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Authentication](#) > [Portal](#).

- On **Portal** tab, click **Create New Portal**. Specify the portal name and enable **Portal**.

Create New Portal

Portal Name:

Portal: 💡 Controller Online Required.

SSID & Network: ⓘ

Authentication Type:

Authentication Timeout:

Daily Limit: Enable ⓘ

HTTPS Redirection: Enable ⓘ

Landing Page: ⓘ The Original URL
 The Promotional URL

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

■ No Authentication

Authentication Timeout Select the login duration. Clients will be off-line after the authentication timeout.

Daily Limit Click the checkbox to enable Daily Limit. With this feature enabled, after authentication times out, clients cannot get authenticated again until the next day. With this feature disabled, after authentication times out, clients can get authenticated again without limit.

■ Simple Password

Password Specify the password for the portal.

Authentication Timeout Select the login duration. Clients will be off-line after the authentication timeout.

■ Hotspot

Type Select one or more authentication types according to your needs. Clients can access the network after passing any type of the authentication.

With different types of Hotspot selected, configure the related parameters.

- **Voucher Portal**

| | |
|---------|--|
| Voucher | Select Voucher and click Voucher Manager to manage the voucher codes. Refer to 7.2.3 Vouchers for detailed information about how to create vouchers. |
|---------|--|

- **Local User Portal**

| | |
|------------|---|
| Local User | Select Local User and click User Management to manage the information of the login accounts. Refer to 7.2.4 Local Users for detailed information about how to create Local Users. |
|------------|---|

- **SMS Portal**

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

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

- **RADIUS Portal**

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

| | |
|------------------------|--|
| Authentication Timeout | Clients are required to enter the correct username and password which are stored in the RADIUS server to pass the authentication. |
| RADIUS Profile | Select the RADIUS profile you have created. If no RADIUS profiles have been created, click + Create New RADIUS Profile from the drop-down list or Manage RADIUS Profile to create one. The RADIUS profile records the information of the RADIUS server which provides a method for storing the authentication information centrally. |
| Authentication Mode | Select the authentication protocol for the RADIUS server. Two authentication protocols are available: PAP and CHAP. |

| | |
|---------------------------------------|---|
| NAS ID | Configure a Network Access Server Identifier (NAS ID) on the portal. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups. |
| Disconnected Requests | With the feature enabled, the controller will listen on the receiver port for disconnect requests from the RADIUS server. When the controller receives the disconnect requests in correct format, the controller will terminate the RADIUS authentication session of the clients. Note that the feature is available only when the controller is accessible to the RADIUS server. |
| Receiver Port | Specify the port on which the controller listens when there are disconnect requests from the RADIUS server. Make sure that the specified port is not in use. |
| Status | The entry displays the status of the receiver port, including Running, Disabled, and Error. Running means that the port is available, Disabled means that the port is closed, and Error means that the port is already in use. |

- **Configuring Form Authentication**

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

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

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

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

- **RADIUS Server**

| | |
|--|--|
| Authentication Timeout | Select the login duration. Clients will be off-line after the authentication timeout. |
| RADIUS Profile | Select the RADIUS profile you have created. If no RADIUS profiles have been created, click Create New RADIUS Profile from the drop-down list or click Manage RADIUS Profile to create one. The RADIUS profile records information of the RADIUS server including the IP address, port and so on. |
| NAS ID | Configure a Network Access Server Identifier (NAS ID) on the portal. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups. |
| Disconnected Requests | With the feature enabled, the controller will listen on the receiver port for disconnect requests from the RADIUS server. When the controller receives the disconnect requests in correct format, the controller will terminate the RAIDIUS authentication session of the clients. Note that the feature is available only when the controller is accessible to the RADIUS server. |

| | |
|--------------------------------------|--|
| Receiver Port | Specify the port on which the controller listens when there are disconnect requests from the RADIUS server. Make sure that the specified port is not in use. |
| Status | The entry displays the status of the receiver port, including Running, Disabled, and Error. Running means that the port is available, Disabled means that the port is closed, and Error means that the port is already in use. |
| Authentication Mode | Select the authentication protocol for the RADIUS server. |
| Portal Customization | Select Local Web Portal or External Web Portal. The authentication login page of Local Web Portal is provided by the built-in portal server of the controller. The External Web Portal is provided by external portal server. Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field. |

■ External LDAP Server

| | |
|--|--|
| Authentication Timeout | Select the login duration. Clients will be off-line after the authentication timeout. |
| LDAP Profile | Select the LDAP profile you have created. If no LDAP profiles have been created, click Create New LDAP Profile from the drop-down list or click Manage LDAP Profile to create one. The LDAP profile records information of the LDAP server including the server address, port and so on. |
| Portal Customization | Select Local Web Portal or External Web Portal. The authentication login page of Local Web Portal is provided by the built-in portal server of the controller. The External Web Portal is provided by external portal server. Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field. |

■ External Portal Server

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

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.

Portal Customization

Type: Edit Current Page
 Import Customized Page

Default Language: ⓘ

Background: Solid Color
 Picture

Background Picture: ⓘ

Logo: Enable

Logo Picture: ⓘ

Logo Size: Small Medium Large

Logo Position: Upper Middle Lower

Button Color: # 0492eb 100%

Button Text color: # ffffff 100%

Button Position: Upper Middle Lower

Button Text:

Welcome Information: Enable

Terms of Service: Enable

Copyright: Enable

Show Redirection Countdown Enable
 After Authorized:

| | |
|--------------------------------------|--|
| Type | <p>Select the type of the Portal page.</p> <p>Edit Current Page: Edit the related parameters to customize the Portal page based on the provided page.</p> <p>Import Customized Page: Click <input type="button" value="Import"/> to import your unique Portal page for branding it as per your business.</p> |
| Default Language | <p>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.</p> |
| Background | <p>Select the background type.</p> <p>Solid Color: Configure your desired background color by entering the hexadecimal HTML color code manually or through the color picker.</p> <p>Picture: Click <input type="button" value="Choose"/> and select a picture from your PC as the background.</p> |
| Logo | <p>Click to show the logo on the portal page.</p> |
| Logo Picture | <p>Click <input type="button" value="Choose"/> and select a picture from your PC as the logo.</p> |
| Logo Size/ Logo Position | <p>Adjust the logo size and position on the Portal Page.</p> |
| Input Box Color/ Input Text Color | <p>(For certain authentication 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.</p> |
| Button Color/ Button Text Color | <p>Configure your desired background and text color for the button by entering the hexadecimal HTML color code manually or through the color picker.</p> |
| Button Position | <p>Select the button position on the Portal Page.</p> |
| Button Text | <p>Enter the text for the button.</p> |
| Welcome Information | <p>Click the checkbox and enter text as the welcome information.</p> <p>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.</p> |
| Terms of Service | <p>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.</p> |
| Copyright | <p>Click the checkbox and enter text as the copyright in the following box.</p> <p>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.</p> |

Show Redirection
Countdown After
Authorized

When enabled, the system will show the portal's redirection countdown.

Click [Advertisement Options](#) and customize advertisement pictures on the authentication page if needed.

Advertisement Options

Advertisement: Enable

Picture Resource: (1-5 Pictures) ⓘ

Advertisement Duration Time: (1-30)

Picture Carousel Interval: (1-10)

Allow Users To Skip Advertisement: Enable

[Advertisement](#)

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

[Picture Resource](#)

Click and select pictures from your PC as the advertisement pictures. When several pictures are added, they will be played in a loop.

[Advertisement Duration Time](#)

Enter the duration time for the advertisement pictures. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.

[Picture Carousel Interval](#)

Enter the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.

[Allow Users To Skip Advertisement](#)

Click the checkbox to allow users to skip the advertisement.

(Optional) Access Control

On [Access Control](#) tab, you can configure access control rules if needed.

Access Control

Pre-Authentication Access: Enable [i](#)

Pre-Authentication Access List: [+](#) Add

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

Authentication-Free Client: Enable [i](#)

Authentication-Free Client List: [+](#) Add

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

Apply
Cancel

Pre-Authentication Access

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

Pre-Authentication Access List

Click [+](#) Add to configure the IP range or URL which unauthenticated clients are allowed to access.

Authentication-Free Policy

Click the checkbox to enable Authentication-Free Policy. With this feature enabled, you can allow certain clients to access the internet without Portal authentication.

Authentication-Free Client List

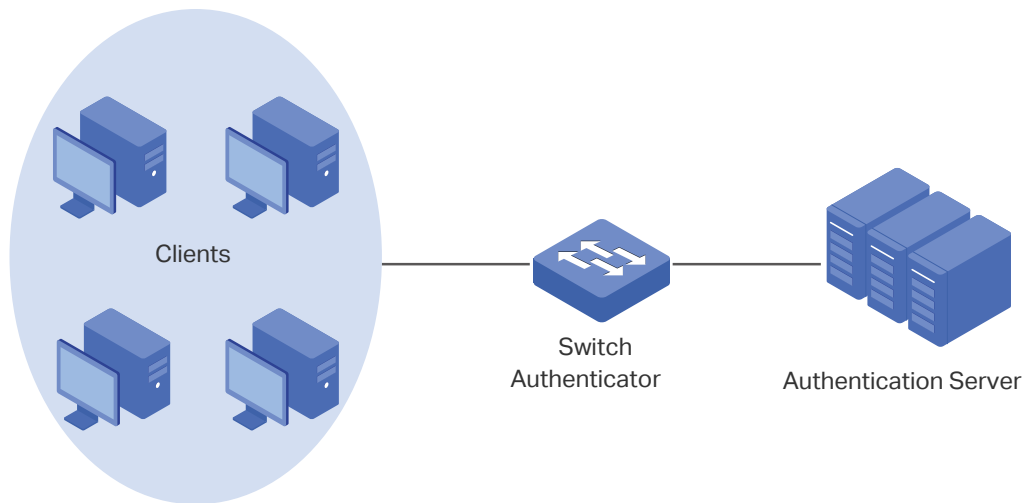
Click [+](#) Add and enter the IP address or MAC address of Authentication-Free clients.

4.9.2 802.1X

Overview

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

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



■ Client

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

■ Authenticator

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

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

■ Authentication Server

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

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

Configuration

To complete the 802.1X configuration, follow these steps:

- 1) Click to enable 802.1X.
- 2) Select the RADIUS profile you have created and configure other parameters.
- 3) Select the ports on which 802.1X Authentication will take effect.

Enable 802.1X

Configure RADIUS Profile and Parameters

Select the Ports

Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Authentication](#) > [802.1X](#). Click to enable 802.1X.

802.1X

802.1X: 💡 Switch Required.

Enable 802.1X

Configure RADIUS Profile and Parameters

Select the Ports

Select the RADIUS profile you have created. If no RADIUS profiles have been created, click [+ Create New RADIUS Profile](#) from the drop-down list or [Manage RADIUS Profile](#) to create one. The RADIUS profile records the information of the RADIUS server which acts as the authentication server during 802.1X authentication.

Basic Info

RADIUS Profile: Please Select... ▾ [Manage RADIUS Profile](#)

Authentication Protocol: PAP
 EAP

Authentication Type: Port Based
 MAC Based

MAB: Enable

Authentication Protocol

Select the authentication protocol for exchanging messages between the switch and RADIUS server. As a bridge between the client and RADIUS server, the switch forwards messages for them. It uses AP packets to exchange messages with the client, and processes the messages according to the specified authentication protocol before forwarding them to the RADIUS server.

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

AP: The AP packets are encapsulated in other protocol (such as RADIUS) packets, and transmitted to the authentication server. To use this authentication mechanism, the RADIUS server should support AP attributes.

Authentication Type

Select the 802.1X authentication type.

Port Based: After a client connected to the port gets authenticated successfully, other clients can access the network via the port without authentication.

MAC Based: Clients connected to the port need to be authenticated individually. The RADIUS server distinguishes clients by their MAC addresses.

VLAN Assignment

This feature allows the RADIUS server to send the VLAN configurations to the port dynamically. After the port is authenticated, the RADIUS server assigns the VLAN based on the username of the client connecting to the port. The username-to-VLAN mappings must be already stored in the RADIUS server database. This feature is available only when the 802.1X authentication type is Port Based.

MAB

MAB (MAC Authentication Bypass) allows clients to be authenticated without any client software installed. MAB is useful for authenticating devices without 802.1X capability like IP phones. When MAB is enabled on a port, the switch will learn the MAC address of the client automatically and send the authentication server a RADIUS access request frame with the client's MAC address as the username and password. MAB takes effect only when 802.1X authentication is enabled on the port.

Enable 802.1X

Configure RADIUS Profile and Parameters

Select the Ports

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

| <input type="checkbox"/> | DEVICE NAME | PORTS | STATUS | MODEL | FIRMWARE VERSION |
|--------------------------|-------------|--|-----------|-------|------------------|
| <input type="checkbox"/> | | 1 2 Port <input checked="" type="checkbox"/> <input type="checkbox"/> | CONNECTED | | 2.0.4 |

Note:

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

4.9.3 MAC-Based Authentication**Overview**

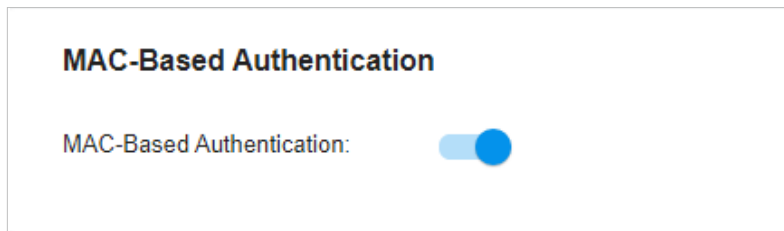
MAC-Based Authentication allows or disallows clients access to wireless networks based on the MAC addresses of the clients. In this authentication method, the controller takes wireless clients' MAC addresses as their usernames and passwords for authentication. The RADIUS server authenticates the MAC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

Note:

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

Configuration

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



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

Basic Info

SSID:

RADIUS Profile: [Manage RADIUS Profile](#)

NAS ID: (Optional)

MAC-Based Authentication Fallback: Enable ⓘ

MAC Address Format: ⓘ

Empty Password: Enable ⓘ

SSID

Select one or more SSIDs for MAC-based authentication to take effect.

RADIUS Profile

Select the RADIUS profile you have created. If no RADIUS profiles have been created, click [+ Create New RADIUS Profile](#) from the drop-down list or [Manage RADIUS Profile](#) to create one. The RADIUS profile records the information of the RADIUS server which acts as the authentication server during MAC-Based Authentication.

| | |
|-----------------------------------|---|
| NAS ID | Configure a Network Access Server Identifier (NAS ID) for the authentication. Authentication request packets from the controller to the RADIUS server carry the NAS ID. The RADIUS server can classify users into different groups based on the NAS ID, and then choose different policies for different groups. |
| MAC-Based Authentication Fallback | For the wireless network configured with both MAC-Based Authentication and Portal, if you enable this feature, a wireless client needs to pass only one authentication. The client tries MAC-Based Authentication first, and is allowed to try Portal authentication if it failed the MAC-Based Authentication. If you disable this feature as default, a wireless client needs to pass both the MAC-Based Authentication and portal authentication for internet access, and will be denied if it fails either of the authentication. |
| MAC Address Format | Select clients' MAC address format which the controller uses for authentication. Then configure the MAC addresses in the specified format as usernames for the clients on the RADIUS server. |
| Empty Password | Click to allow a blank password for MAC-Based Authentication. With this option disabled, the password will be the same as the username. |

♥ 4.10 Services

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

4.10.1 DHCP Reservation

Overview

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

Configuration

- To manually add DHCP Reservation entries:

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Services](#) > [DHCP Reservation](#).
2. Click [+Create New DHCP Reservation Entry](#) and configure the parameters. Then click [Apply](#).

Create New DHCP Reservation Entry ✕

Network:

MAC Address:

IP ADDRESS:

Description: (Optional)

Status: Enable

Apply
Cancel

[Network](#) Select the network the DHCP reservation entry is used for.

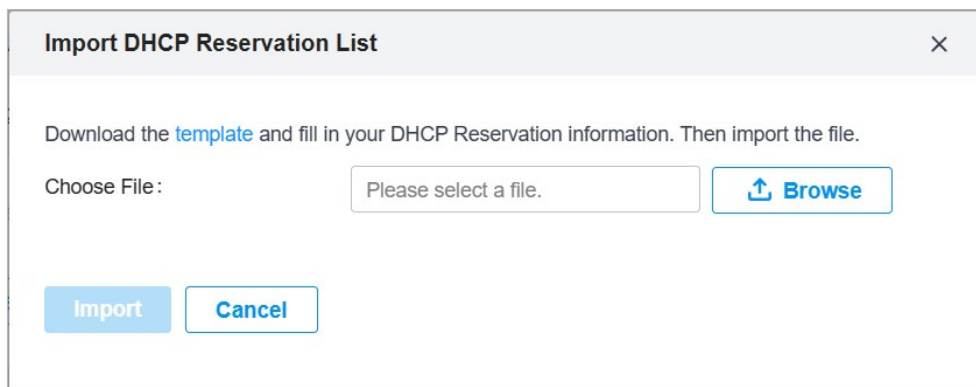
[MAC Address](#) Specify the MAC address of the device for which you want to reserve an IP address.

[IP Address](#) Specify the fixed IP address for the device.

| | |
|-------------|---|
| Description | Enter description for the entry for identification. |
| Status | Enable or disable the entry. |

■ **To import DHCP Reservation entries in batch:**

1. Select a site from the drop-down list of [Organization](#). 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.

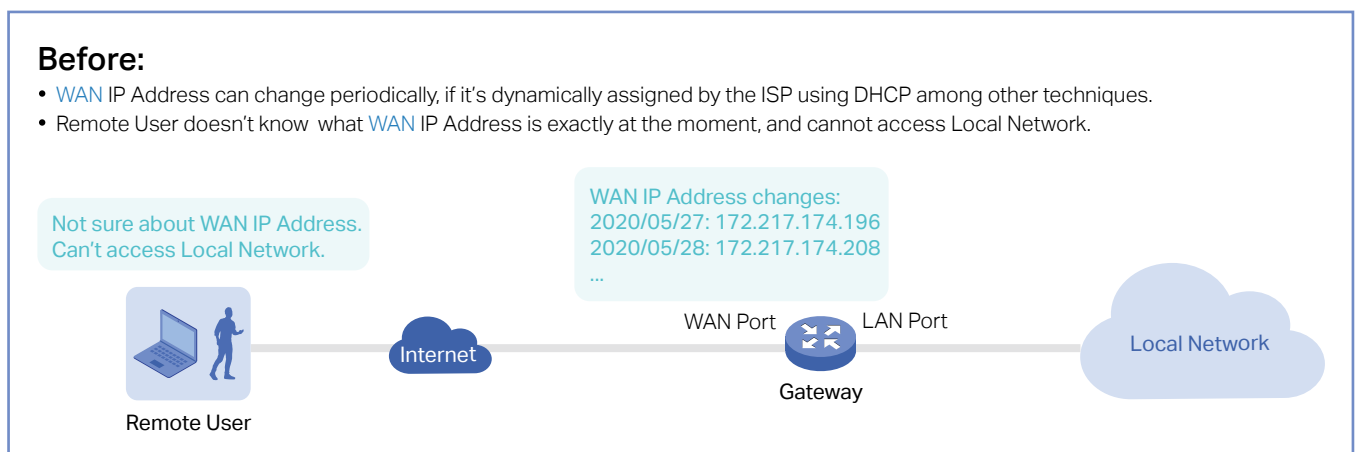


4. 10. 2 Dynamic DNS

Overview

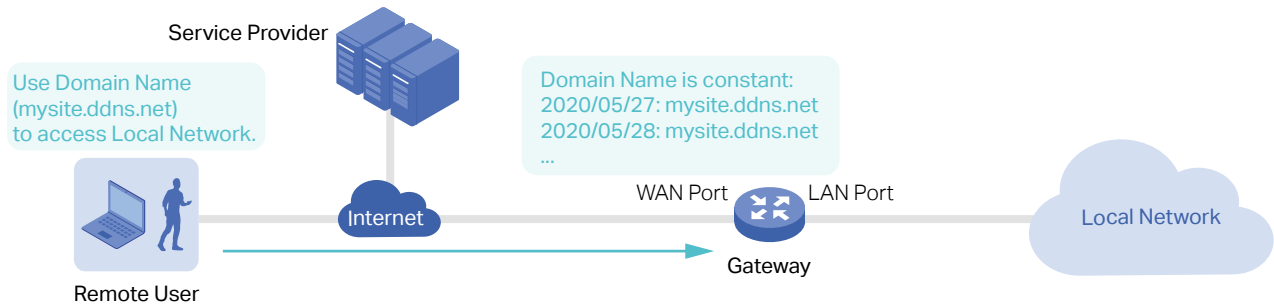
WAN IP Address of your gateway can change periodically because your ISP typically employs DHCP among other techniques. This is where Dynamic DNS comes in. Dynamic DNS assigns a fixed domain name to the WAN port of your gateway, which facilitates remote users to access your local network through WAN Port.

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



After:

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

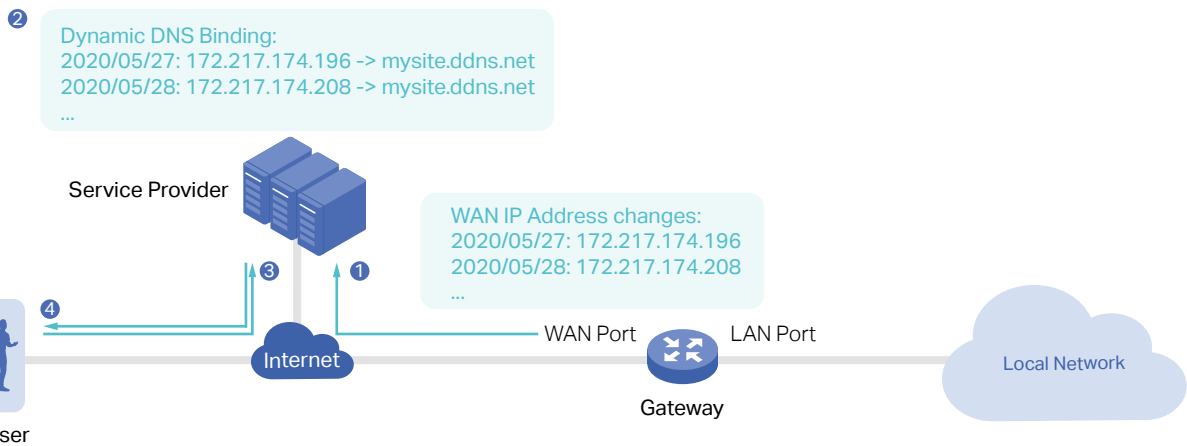


Prerequisite:

- Choose one **Service Provider** from the four that the controller supports, i.e. **DynDNS, No-IP, Peanuthull, Comexe**.
- 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 actually uses to access Local Network through **WAN Port**.



Configuration

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

Create New Dynamic DNS Entry

Service Provider:

Status: Enable

Interface: SFP WAN
 WAN

Username: [Go To Register](#) ⓘ

Password:

Domain Name:

Interval Mode: Fixed Custom

Update Interval:

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

4. 10. 3 mDNS

Overview

mDNS (Multicast DNS) Repeater can help forward mDNS request/reply packets between different VLANs. With this function, you can create a forwarding rule to allow the devices in the specified Client

VLAN to discover the mDNS service in the specified Service VLAN. You can also specify the services to be forwarded.

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Services](#) > [mDNS](#).
2. Click [Create New Rule](#). Configure the parameters.

Create New Rule

Name:

Status: Enable

Device Type: AP
 Gateway

Bonjour Service: [Manage Bonjour Service](#)

Services Network

VLAN: (Range: 1-4094. Enter only one VLAN.)

Client Network

VLAN: (Range: 1-4094. Enter one or multiple VLANs. For example: 1,2-100)

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

3. Apply the settings.

4.10.4 SNMP

Overview

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

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

ⓘ Note:

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

Configuration

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

SNMPv1 & SNMPv2c

SNMPv1 & SNMPv2c:

Community String:

SNMPv3

SNMPv3:

Username:

Password:

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

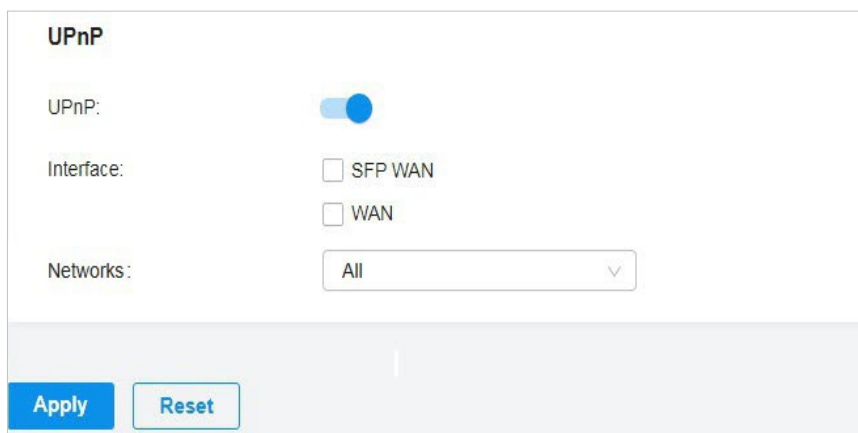
4. 10. 5 UPnP

Overview

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

Configuration

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



[Interface](#) Select the WAN port where UPnP takes effect.

[Networks](#) Select the LAN interface where UPnP takes effect.

4. 10. 6 SSH

Overview

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

ⓘ Note:

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

Configuration

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

SSH

SSH Login:

SSH Server Port: (22 or 1025-65535)

Layer 3 Accessibility: Enable [i](#)

[Apply](#) [Reset](#)

SSH Server Port

Specify the SSH Server Port which your network devices use for SSH connections. You need to configure the SSH Server Port correspondingly on your SSH terminal.

Layer 3 Accessibility

With this feature enabled, the SSH terminal from a different subnet can access your devices via SSH. With this feature disabled, only the SSH terminal in the same subnet can access your devices via SSH.

4. 10. 7 Reboot Schedule

Overview

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

Configuration

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




Create New Reboot Schedule

Name:

Status: Enable

Occurrence: Every on at in [America/Bogota](#) [i](#)

Devices List:

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

Showing 1-3 of 3 records < 1 > 5 /page Go To page: [GO](#)

[Create](#) [Cancel](#)

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

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

4.10.8 Port Schedule

Overview

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

Configuration

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

Create New Port Schedule

Name:

Status: Enable

Type: PoE Schedule
 Port Schedule

This function only affects PoE power supply.

Time Range: [Manage Time Range Entries](#)

Device List:

| | DEVICE NAME | PORTS | STATUS | MODEL | FIRMWARE VERSION |
|--------------------------|-------------------|---|-----------|-------|------------------|
| <input type="checkbox"/> | 00-0A:EB-45-F7-A5 | <div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="margin-right: 10px;"> <input type="checkbox"/> 1 <input type="checkbox"/> 3 <input type="checkbox"/> 5 <input type="checkbox"/> 7 <input type="checkbox"/> 9 </div> <div> <input type="checkbox"/> 2 <input type="checkbox"/> 4 <input type="checkbox"/> 6 <input type="checkbox"/> 8 <input type="checkbox"/> 10 </div> </div> | CONNECTED | | -- |

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

Create **Cancel**

| | |
|--------|--|
| Name | Enter the name to identify the schedule entry. |
| Status | Enable or disable the schedule entry. |

| | |
|---------------------|--|
| Type | <p>Type:Specify the schedule type:</p> <p>PoE Schedule: This function only affects PoE power supply.</p> <p>Port Schedule: This function affects LAN connections of ports but does not affect PoE power supply. To avoid network problems, please check your topology and related configurations before turning off ports.</p> |
| Time Range | <p>When the Type is PoE Schedule, select the time range when the PoE switches will supply power to the powered devices.</p> <p>when the Type is Port Schedule, select the time range when the switches will turn on the designated ports.</p> <p>You can create a Time Range entry by clicking Create New Time Range Entry from the drop down list.</p> |
| Devices List | <p>When Type is PoE Schedule, select the PoE switch and PoE port to apply the schedule.</p> <p>When Type is Port Schedule, select the switch and port to apply the schedule.</p> |

2. Click **Create**. The new schedule entry will be added to the table.

4. 10.9 IPTV

Overview

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

Configuration

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

IGMP

IGMP Proxy:

IGMP Version: v2 ▼

IGMP Interface: Please Select... ▼

IGMP Proxy

Enable IGMP Proxy.

IGMP Proxy sends IGMP querier packets to the LAN ports to detect if there is any multicast member connected to the LAN ports.

IGMP Version

Select the IGMP version as V2 or V3. The default is IGMP V2.

IGMP Interface

Select the WAN port on which the IGMP Proxy takes effect.

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

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

IPTV

IPTV:

Mode: Bridge
 Custom (i)

WAN Port: Please Select... ▼

WAN/LAN1 Mode: Internet ▼

WAN/LAN2 Mode: Internet ▼

LAN1 Mode: Internet ▼

LAN2 Mode: Internet ▼

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

4. 10. 10 Upgrade Schedule

Overview

Upgrade Schedule allows you to schedule the device upgrade as desired. You can set recurring upgrades or a one-time schedule. When configuring multiple schedules, set different execution times if possible. If execution times overlap, new schedule will not be executed before the current task completes.

Configuration

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

Add Upgrade Schedule




Name:

Status: Enable

Type: Execute Auto Upgrade Once
 Repeat

Occurrence: at at in Coordinated Universal Time ⓘ

Device List:

| <input type="checkbox"/> | DEVICE NAME | STATUS | MODEL | FIRMWARE VERSION |
|-------------------------------------|--|-----------|----------------------|----------------------|
| <input checked="" type="checkbox"/> |  <input type="text"/> | CONNECTED | <input type="text"/> | <input type="text"/> |
| <input checked="" type="checkbox"/> |  <input type="text"/> | CONNECTED | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> |  <input type="text"/> | CONNECTED | <input type="text"/> | <input type="text"/> |

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

Name Enter the name to identify the schedule entry.

Status Enable or disable the upgrade schedule.

Type Specify whether to execute auto upgrade once or repeat it.

Occurrence Specify the time for automatic upgrade.

Devices List Select the devices that will upgrade according to the set schedule.

4. 10. 11 DNS Proxy

Overview

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

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

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

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Settings > Services > DNS Proxy](#).
2. Configure the parameters, then save the settings.

DNS Proxy

DNS Proxy: Enable

Proxy Type: DNSSEC DoH DoT

DNS Server: [+ Add](#)

Bogus DNS Reply:

[Save](#) [Cancel](#)

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

4. 10. 12 DNS Cache

Overview

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

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Settings > Services > DNS Cache](#).

2. Enable [DNS Cache](#), configure the parameters, then save the settings.

DNS Cache

Enable DNS Cache: Enable

TTL: seconds (Optional, 1 - 86400)

[Save](#) [Cancel](#)

[Enable DNS Cache](#) Enable or disable DNS Cache.

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

4. 10. 13 Export Data

Overview

You can export data to monitor or debug your devices.

Configuration

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

2. Go to [Settings](#) > [Services](#) > [Export Data](#). Select the type of data from the export list and click [Export](#).

Export Data

Export List:

Mode:

Default Columns

All Columns

Current Display Columns

⚠ If you select All or Current Display Columns, data exporting will be time-consuming if there are lots of devices.

Format:

Send Email: Enable

💡 We recommend enabling SMTP. Otherwise export may fail.

Report Name:

Occurrence: Every at in Coordinated Universal Time ⓘ

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

Export List

Device List: Export the list of managed devices.

Client List: Export the list of all clients that are connected to the networks.

Insight-Rogue AP List: Export the list of the rogue APs scanned before.

Log List: Export the list of the logs generated by the controller.

Authorized Client List: Export the list of authorized clients.

Voucher Codes: Export the list of the voucher codes.

Mode

Select the columns to export. We recommend selecting **Default Columns**, which include commonly needed columns such as DEVICE NAME, MAC ADDRESS, MODEL, etc. If you select **All Columns** or **Current Display Columns**, data exporting will be time-consuming if there are lots of devices.

Site

Choose one or multiple sites to export data.

Note: In site view, only the data of current site can be exported.

Format

The data can be exported to the file in the format of .CSV or .XLSX.

Send Email

If you want to send the exported data via email, enable **Send Email** and configure the parameters below:

Report Name: Specify the report name of the email to send.

Occurrence: Specify when to send the email.

Send to: Specify the email addresses to send the exported data to.

♥ 4.11 CLI Configuration

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

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

■ Site CLI

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

■ Device CLI

Device CLI supports batch configuration of selected devices.

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

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

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

General Precautions

1. The GUI and CLI configuration should be planned globally according to the actual network topology and requirements.
2. To avoid conflicts, it is recommended not to use the CLI to configure the existing functions of the GUI.
 - a. When adopting a new device, the Controller will apply configurations to the device in the order of GUI, Site CLI, and then Device CLI. If there is a configuration conflict, the configuration applied last takes effect.
 - b. CLI profiles (including Site CLI profiles and Device CLI profiles) will only be sent to devices once after applied, unless the "Apply Again" button in the Application Result is clicked to trigger the full configurations application.
 - c. When a device upgrades its firmware, the Controller will apply the full configurations to the device in the order of GUI, Site CLI, and then Device CLI.
 - d. Since the configurations applied later will overwrite the previous configurations, the configuration results of different devices may be different after the same function has been modified repeatedly via GUI, Site CLI and Device CLI.
3. The Controller will not verify the existing GUI and CLI configurations of devices. Be sure to check the existing configurations before performing new configurations. Otherwise, unexpected results may occur after the configurations are applied, and the devices may even go offline.
4. To avoid configuration conflicts, if you really need to use the CLI to configure a certain function, it is recommended not to configure it via GUI at the same time.

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

Repeated Configurations

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

- a. It is recommended to confirm the currently effective commands via the CLI configuration viewing function "Show Running Config".
- b. If you need to cancel a certain configuration, use the "no" command.
- c. If you need to modify a certain configuration, you can enter a new command to overwrite the configuration.
- d. Apply the final configuration, and confirm that the function is configured correctly and takes effect via the CLI configuration viewing function.

Execution Failures

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

- a. Use the CLI configuration viewing function (Show Running Config) to confirm the commands that have taken effect. If you need to cancel them, you can enter "no" commands and apply them to devices.
- b. Troubleshoot and correct the command error, regenerate the CLI configuration, and apply it to devices.

Command Modification

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

- a. Use the CLI configuration view function (Show Running Config) to confirm the commands that have taken effect, and sort out the commands that need to be canceled.
- b. Enter "no" commands to cancel the configurations, and apply them to devices.

Prohibited Commands

1. CLI commands such as modifying user name and password, managing VLAN, SDM profile, reboot, reset, upgrade, import and export configurations have been prohibited. When using other CLI commands, please also pay attention to avoid affecting the management of the Controller.
2. Device CLI supports the variable function. The variable content does not have too many restrictions, for example, you can enter CLI commands, but it is not recommended to use it in this way.

4.11.1 Site CLI

Overview

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

Configuration

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

Create New Site CLI Profile

Name:

Description: (Optional)

CLI:

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

[Import CLI from Device](#) [Import CLI from File](#)

Note:

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

2.If a command starts with the ! character, the command will be ignored.

ⓘ Note:

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

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

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

| NAME | DESCRIPTION | STATUS | ACTION |
|-------------------|--|----------|---|
| Loopback Interval | Modify the loopback detection interval | Inactive | Edit Delete Apply |

Showing 1-1 of 1 records < 1 > 10 / page Go To page: [Go](#)

[+ Create New Site CLI Profile](#)

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

ⓘ **Note:**

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

Configurations applied.

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

[View CLI Details](#) [Cancel](#)

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

ⓘ **Note:**

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

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

Select 0 of 2 items [Select All](#) Showing 1-2 of 2 records < 1 > 10 / page Go To page: [Go](#)

4. 11.2 Device CLI

Overview

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

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

Configuration

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

Create New Device CLI Profile

1 CLI Template ————— 2 Device Variable Settings

Name:

Description: (Optional)

CLI:

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

Variables:

Note:

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

[Import CLI from Device](#) [Import CLI from File](#)

[Next](#) [Cancel](#)

! Note:

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

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

2. Click [Next](#). Select the devices to apply the CLI profile.

Choose Device:

[Save](#) [← Back](#)

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

| NAME | DEVICE NAME | DESCRIPTION | STATUS | ACTION |
|--------------------|-------------|---------------------|----------|---|
| Multicast Snooping | Switch | Drop Unknown Groups | Inactive | Edit Delete Apply |

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

[+ Create New Device CLI Profile](#)

4. Click [Apply](#) to apply the CLI. The profile will change to active state and apply configurations to the devices you selected.

Note:

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

Configurations applied.

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

[View CLI Details](#) [Cancel](#)

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

Note:

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

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

Select 0 of 2 items [Select All](#) Showing 1-2 of 2 records < 1 > 10 / page Go To page: Go

5

Configure the SDN Controller

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

- [5. 1 Manage the Controller](#)
- [5. 2 Manage Your Controller Remotely via Cloud Access](#)
- [5. 3 Maintenance](#)
- [5. 4 Migration](#)
- [5. 5 Auto Backup](#)

♥ 5.1 Manage the Controller

5.1.1 General Settings

Configuration

Select **Global** from the drop-down list of Organization in the upper right corner. Go to **Settings > Controller**. In **General Settings**, configure the parameters and click **Save**.


■ For Hardware Controller

General Settings

Controller Name:

Time Zone:

Daylight Saving Time: Enable

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


Time Offset:

Starts On: Week: Day: Month: Time:

Ends On: Week: Day: Month: Time:

Primary NTP Server:

Secondary NTP Server:

Reset Button: 

Network Settings: Static DHCP

IP Address:

Netmask:

Gateway:

Primary DNS:

Secondary DNS: (Optional)


Controller Name

Specify the Controller Name to identify the controller.

Time Zone

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

Daylight Saving Time

Enable the feature if your country/region implements DST. When it is enabled, the icon  will appear on the upper right, showing the DST settings and status.

| | |
|---|---|
| Time Offset | Select the time added in minutes when Daylight Saving Time starts. |
| Starts On | Specify the time when the DST starts. The clock will be set forward by the time offset you specify. |
| Ends On | Specify the time when the DST ends. The clock will be set back by the time offset you specify. |
| Primary NTP Server/ Secondary NTP Server | Enter the IP address of the primary and secondary NTP (Network Time Protocol) server. NTP servers assign network time to the controller. |
| Reset Button | With this feature enabled, the controller can be reset via reset button. |
| Network Settings | <p>Select one way for the controller to get IP settings.</p> <p>Static: You need to specify the IP address, Netmask, Gateway, Primary DNS, and Secondary DNS for the controller.</p> <p>DHCP: The controller get IP settings from the DHCP server. If the controller fails to get IP settings from the DHCP server, it will use the Fallback IP Address and Fallback Netmask.</p> |

■ For Software Controller / Cloud-Based Controller

General Settings

Controller Name:

Time Zone: ⓘ

Daylight Saving Time: Enable

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

Time Offset:

Starts On: Week: Day: Month: Time:

Ends On: Week: Day: Month: Time:

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

5. 1. 2 Mail Server

Overview


With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. The Mail Server feature works with the SMTP (Simple Mail Transfer Protocol) service provided by an email service provider.

Configuration

1. Log in to your email account and enable the SMTP (Simple Mail Transfer Protocol) Service. For details, refer to the instructions of your email service provider.

2. Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings > Controller Settings](#). In [Mail Server](#), enable SMTP Server and configure the parameters. Then click [Save](#).

Mail Server

 With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. For security reasons, we recommend that you configure Mail Server carefully.

SMTP Server: Enable


SMTP:

Port: (1-65535)

SSL: Enable

Authentication: Enable

Username:

Password: 

Sender Address: (Optional)

Test SMTP Server: Send Test Email to

| | |
|--------------------------------|--|
| SMTP | Enter the URL or IP address of the SMTP server according to the instructions of the email service provider. |
| Port | Configure the port used by the SMTP server according to the instructions of the email service provider. |
| SSL | Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between the controller and the SMTP server. |
| Authentication | Enable or disable Authentication according to the instructions of the email service provider. If Authentication is enabled, the SMTP server requires the username and password for authentication. |
| Username | When Authentication is enabled, enter your email address as the username. |
| Password | When Authentication is enabled, enter the authentication code as the password, which is provided by the email service provider when you enable the SMTP service. |

| | |
|-----------------------|--|
| Sender Address | (Optional) Specify the sender address of the email. If you leave it blank, the controller uses your email address as the Sender Address. |
|-----------------------|--|

| | |
|-------------------------|--|
| Test SMTP Server | Test the Mail Server configuration by sending a test email to an email address that you specify. |
|-------------------------|--|

5.1.3 History Data Retention

Overview

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

Configuration

Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings > Controller Settings](#). In [History Data Retention](#), configure the parameters and click [Save](#).

History Data Retention

Clients' History Data: Enable

When enabled, known clients, client history and client logs will be recorded. This will occupy much storage space.

Client History:

Known Client:

Time-Based Settings

The settings below will affect the graphical display of Statistics and Network Report.

Time Series with 5 Minutes Granularity: 2 Days

Time Series with Hourly Granularity: 7 Days

Time Series with Daily Granularity:

Time Series with Weekly Granularity:

Others

Portal Authentication Records:

Log:

Rogue AP:

| | |
|------------------------------|--|
| Clients' History Data | When enabled, known clients, client history and client logs will be recorded. This will occupy much storage space. |
|------------------------------|--|

| | |
|-----------------------|--|
| Client History | Specify the retention time of client online and offline records. Corresponding to Insight-Past Connection. |
|-----------------------|--|

| | |
|--|---|
| Known Client | Specify the retention time of known client data. Corresponding to Insight-Known Clients. |
| Time Series with 5 Minutes Granularity | Displays the retention time of AP, switch, gateway, and client data. Corresponding to 5-minute statistics. |
| Time Series with Hourly Granularity | Displays the retention time of AP, switch, gateway, and client data. Corresponding to hourly statistics. |
| Time Series with Daily Granularity | Specify the retention time of AP, switch, gateway, and client data. Corresponding to daily statistics. |
| Time Series with Weekly Granularity | Specify the retention time of client data. Corresponding to weekly statistics. |
| Portal Authentication Records | Specify the retention time of portal authorization records. Corresponding to Insight-Past Portal Authorization. |
| Log | Specify the retention time of logs. |
| Rogue AP | Specify the retention time of scanned Rogue APs. Corresponding to Insight-Rogue APs. |

5. 1. 4 Customer Experience Improvement Program

Configuration

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

Customer Experience Improvement Program

Participate in the [customer experience improvement program](#) and help improve the quality and performance of TP-Link products by sending statistics and usage information.

5. 1. 5 HTTPS Certificate

Overview

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

ⓘ Note:

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

Configuration

Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings > Controller Settings](#). In [HTTPS Certificate](#), select your file format, import your SSL certificate and configure the parameters. Then click [Save](#).

HTTPS Certificate

i If you have assigned a domain name to the Omada Controller for login, to eliminate the "untrusted certificate" error message that will appear in the login process, you can import the corresponding SSL certificate and private key here. The certificate and private key are issued by the certificate authority. Note that you should restart your controller for the imported SSL certificate to take effect.

File Format:

SSL Certificate:

Keystore Password: **i**

File Format

Select the format of your certificate, and import the certificate file.

Keystore Password

(For JKS) Enter the keystore password if your SSL certificate has the keystore password. Otherwise, leave it blank.

Private Key Password

(For PFX) Enter the private key password if your SSL certificate has the private key password. Otherwise, leave it blank.

i Note:

For the PEM-formatted certificate:

- Starts with: -----BEGIN CERTIFICATE-----
- Ends with: -----END CERTIFICATE-----
- Certificate chain is supported and no blank line is allowed between two certificate chains.

For the PEM-formatted key:

- RSA encryption is required.
- Starts with: -----BEGIN RSA PRIVATE KEY-----
- Ends with: -----END RSA PRIVATE KEY -----
- The key can be placed behind certificate file, and they can be imported together.

5.1.6 Access Config

Overview

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

ⓘ Note:

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

Configuration

Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings](#) > [Controller Settings](#). In [Access Config](#), configure the parameters and click [Save](#).

Access Config

Controller Hostname/IP: ⓘ

Auto Refresh IP: ⓘ

Redirect HTTP to HTTPS: ⓘ

HTTPS Port for Controller Management: (443 or 1024-65535)

HTTP Port for Controller Management: (80 or 1024-65535)

ⓘ Once applying the change of HTTPS port, HTTP port and HTTP Redirect, restart the controller to make the change effective. After restart, visit the following URLs to log in to the Omada Controller:

http://[Omada Controller Host's IP address or URL]:[HTTP Port]

https://[Omada Controller Host's IP address or URL]:[HTTPS Port]

HTTPS Port for Portal: (1024-65535)

HTTP Port for Portal: (80 or 1024-65535)

ⓘ Once applying the change of HTTPS and HTTP port, restart the controller to make the change effective. For security, the HTTPS and HTTP port for Portal should be different from that for controller management.

| | |
|--|---|
| Controller Hostname/IP | Enter the hostname or IP address of the controller which will be used as the Controller URL in the notification email for resetting your controller password. You can keep it default and IP address recognized by the controller will be used as the Controller URL. |
| Auto Refresh IP | (Only for hardware controller) Enable the feature and the hardware controller will refresh its IP address automatically. |
| Redirect HTTP to HTTPS | With this option enabled, HTTP requests will be redirected to HTTPS connections. |
| HTTPS Port for Controller Management | Specify the HTTPS port used by the controller for management. After setting the port, you can visit <code>https://[Controller Host's IP address or URL]:[HTTPS Port]</code> to log in to the Controller. |
| HTTP Port for Controller Management | Specify the HTTP port used by the controller for management. After setting the port, you can visit <code>https://[Controller Host's IP address or URL]:[HTTP Port]</code> to log in to the Controller. |
| HTTPS Port for Portal | Specify the HTTPS port used by the controller for Portal. |
| HTTP Port for Portal | Specify the HTTP port used by the controller for Portal. |

♥ 5.2 Manage Your Controller Remotely via Cloud Access

Overview

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

Configuration

To manage your controller from anywhere, follow these steps:

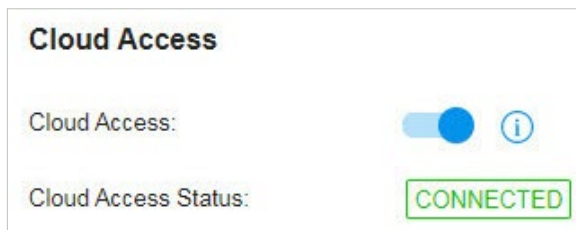
1. Prepare your controller for Cloud Access

■ For Software Controller / Hardware Controller:

ⓘ Note:

- Before you start, make sure your Software Controller Host or Hardware Controller has access to the internet.
- If you have enabled cloud access and bound your TP-Link ID in the quick setup wizard, skip this step.

1) Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings > Cloud Access](#). Enable Cloud Access.



2) Enter your TP-Link ID and password. Then click [Log In and Bind](#).

Log In and Bind Your TP-Link ID ✕

ⓘ Enter the email address and password of your TP-Link ID. Note that it is not the account that you have used to log in to this controller.

TP-Link ID: [No TP-Link ID? Register Now](#)

Password:


Log In and Bind

Cancel

■ For Cloud-Based Controller

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

2. Access your controller through Cloud Service

Go to <https://omada.tplinkcloud.com> and login with your TP-Link ID and password. A list of controllers that have been bound with your TP-Link ID will appear. Then click  Launch to manage the controller.



| NAME | MAC ADDRESS | LOCAL IP | STATUS | SITES | DEVICES | CLIENTS | ALERTS | VERSION | FIRMWARE | ACTION |
|-------------------------|-------------|-----------|--------|-------|---------|---------|--------|---------|----------|---|
| Omada Controller_381C5F | - | 10.0.3.23 | Online | 2 | 1 | 0 | 37 | 4.0.7 | - |  Launch  Unbind |

Page Size: 10 << < 1 > >>

♥ 5.3 Maintenance

5.3.1 Controller Status

Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings > Maintenance](#). In [Controller Status](#), you can view the controller-related information and status.

| Controller Status | |
|---------------------|--------------------------|
| Controller Name: | Omada Controller_737B60 |
| MAC Address: | FC-AA-14-55-FB-5D |
| System Time: | Nov 25, 2022 10:33:13 am |
| Uptime: | 22m 0s |
| Controller Version: | 5.8.3 |

| | |
|------------------------------------|---|
| Controller Name | Displays the controller name, which identifies the controller. You can specify the controller name in 5.1.1 General Settings . |
| MAC Address | Displays the MAC address of the controller. |
| System Time | Displays the system time of the controller. The system time is based on the time zone which you configure in 5.1.1 General Settings . |
| Uptime | Displays how long the controller has been working. |
| Controller Version | Displays the software version of the controller. |

5.3.2 User Interface

Overview

You can customize the User Interface settings of the controller according to your preferences.

Configuration

Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings](#) > [Maintenance](#). In [User Interface](#), configure the parameters and click [Apply](#).

User Interface

Language:

Use 24-Hour Time:

Statistic/DashBoard Timezone:

Fixed Menu:

Dark Settings:

Show Pending Devices: ⓘ

Refresh Button:

Refresh Interval:

Enable WebSocket Connection:

Controller Update Notification: ⓘ

Devices Update Notification: ⓘ

| | |
|--|--|
| Language | Select the language to display the user interface. |
| Use 24-Hour Time | With Use 24-Hour Time enabled, time is displayed in a 24-hour format. With Use 24-Hour Time disabled, time is displayed in a 12-hour format. |
| Statistic/Dashboard Timezone | <p>Select which Timezone the time of statistics and the dashboard is based on.</p> <p>Site's: Site's Timezone is set in Site Configuration of the corresponding site.</p> <p>Browser's: Browser's Timezone is synchronized with the browser configuration.</p> <p>Controller's: Controller's Timezone is set in General Settings of the controller.</p> <p>UTC: UTC (Coordinated Universal Time) is the common time standard across the world.</p> |
| Fixed Menu | With Fixed Menu enabled, the menu icons are fixed and do not prompt menu texts when your mouse hovers on them. |
| Dark Settings | When enabled, the system will switch to a dark theme. |

| | |
|--|---|
| Show Pending Devices | With this option enabled, the devices in Pending status will be shown, and you can determine whether to adopt them. With this option disabled, they will not be shown, thus you cannot adopt any new devices. |
| Refresh Button | Enable or disable Refresh Button in the upper right corner of the configuration page. |
| Refresh Interval | Select how often the controller automatically refreshes the data displayed on the page. |
| Enable WebSocket Connection | With WebSocket Connection enabled, the controller updates in real time some part of its data on the web interface, which is transmitted using the WebSocket service, so that you don't need to refresh them manually. |
| Controller Update Notification | With this feature enabled, you will receive an update notification when a new controller version is available. |
| Devices Update Notification | With this feature enabled, you will receive an update notification when a new firmware version for your device is available. |

5.3.3 Backup & Restore

Overview

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

Configuration

■ Backup

Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings](#) > [Maintenance](#) > [Backup & Restore](#) > [Backup](#), click [Export](#) to export and save the backup file.

If you want to export the data to a file server, configure the parameters accordingly and click [Export](#).

Backup & Restore

Backup

Retained Data Backup: Settings Only ▾

i Retained Data Backup has been set as Settings Only, no data will be backed up. Note that all configurations and data about licenses will not be backed up, including Auto-Activation, Auto-Renewal and license logs.

Retain User Info: Enabled **i**

Export: Export to Local File
 Export to File Server

[Export](#)

Retained Data Backup

Select the time range in the drop-down menu of Retained Data Backup. Only configuration and data within the time range is backed up. If you select Settings Only, only configuration (no data) is backed up.

Retain User Info

Select this option if you want to retain local and cloud user information.

Export

Select where you want to export the data to.

Export to Local File: Export and save the data locally. It is not supported when accessing the controller via cloud.

Export to File Server: Export and save the data to a file server. Select the desired file server type (FTP / TFTP / SFTP / SCP) and configure the parameters.

■ Restore

Go to [Settings](#) > [Maintenance](#) > [Backup & Restore](#) > [Restore](#). In [Backup & Restore](#) section, Click [Browse](#) and select a backup file from your computer or file server. Click [Restore](#).

Import

Select where you store the restore file.

[Import from Local File](#): Import the data locally. It is not supported when accessing the controller via cloud.

[Import from File Server](#): Import the data from a file server. Select the desired file server type (FTP / TFTP / SFTP / SCP) and configure the parameters.

Restore

Select the backup file to restore the information.

■ Export for Support

Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings](#) > [Maintenance](#) > [Export for Support](#). You can export configuration data and running logs for technical support to diagnose network problems. The exported data will not contain users' personal information.

Export Running Logs

Click to export running logs.

Export Configuration Data

Click to export configuration data.

ⓘ Note:

Configuration data cannot be imported into the controller through restore.

♥ 5.4 Migration

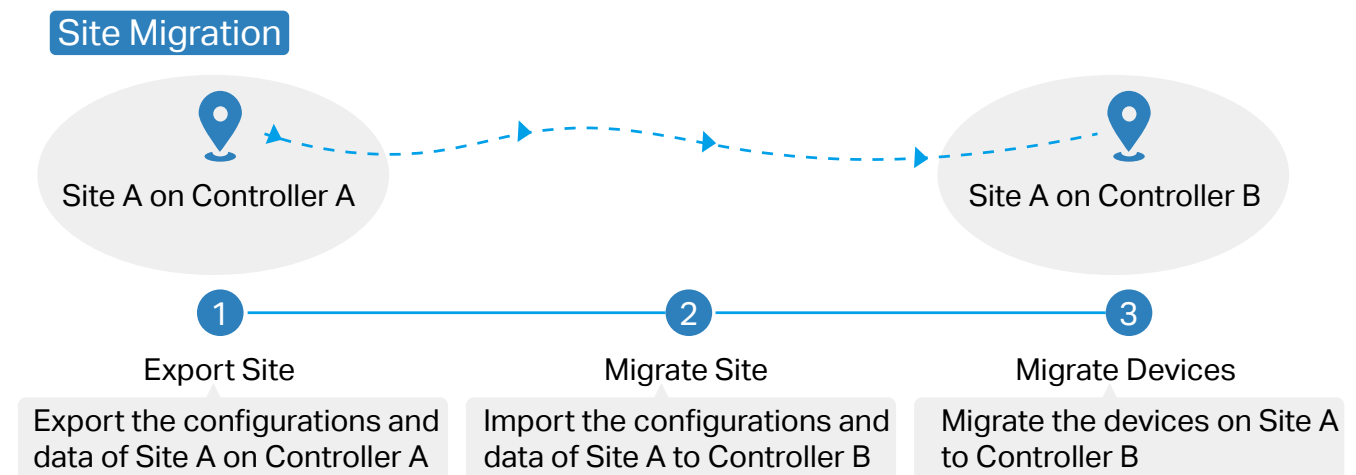
Migration services allow users to migrate the configurations and data to any other controller. Migration services include [5.4.1 Site Migration](#) and [5.4.2 Controller Migration](#), covering all the needs to migrate both a single site and the whole controller.

5.4.1 Site Migration

Overview

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

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



Step1: Export Site

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

Step2: Migrate Site

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

Step3: Migrate Devices

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

Configuration

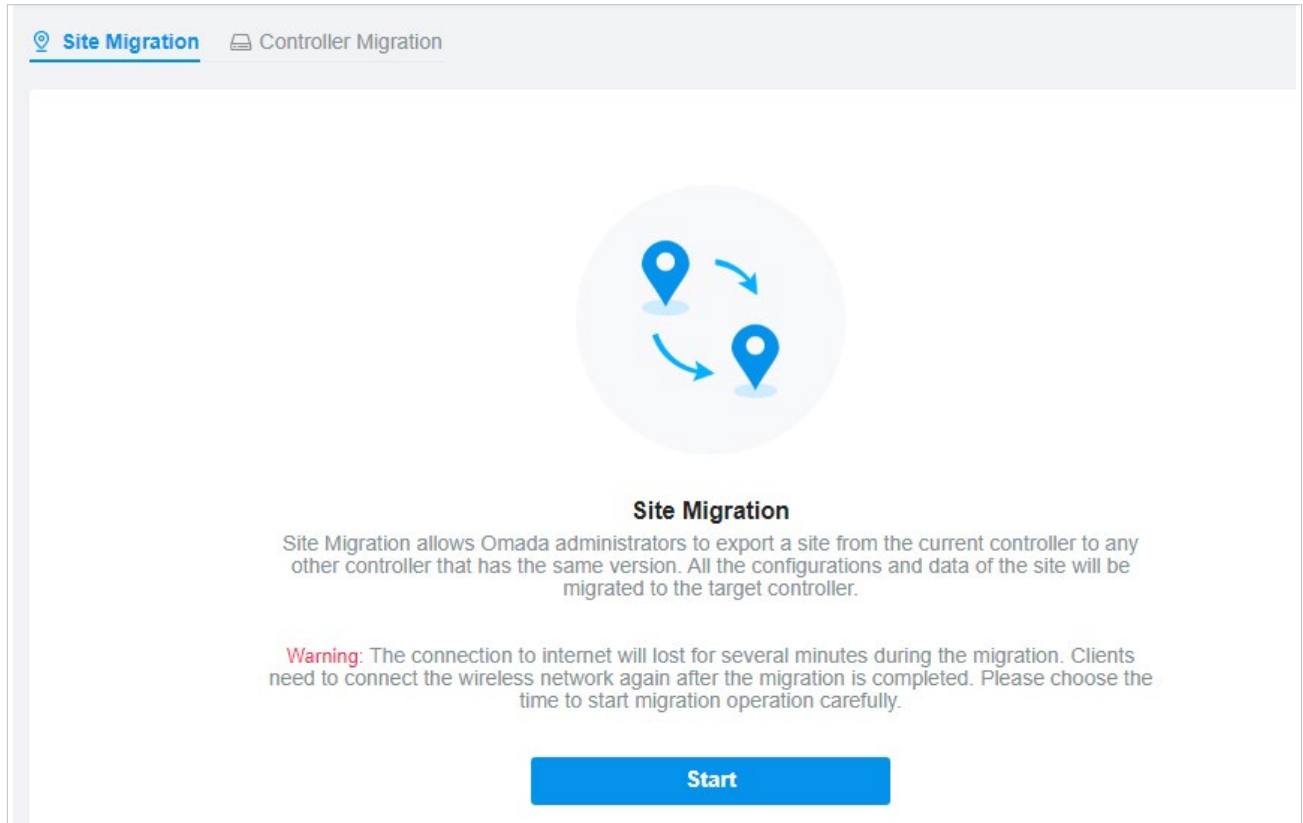
To migrate a site to another controller, follow these steps below.

ⓘ Note:

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

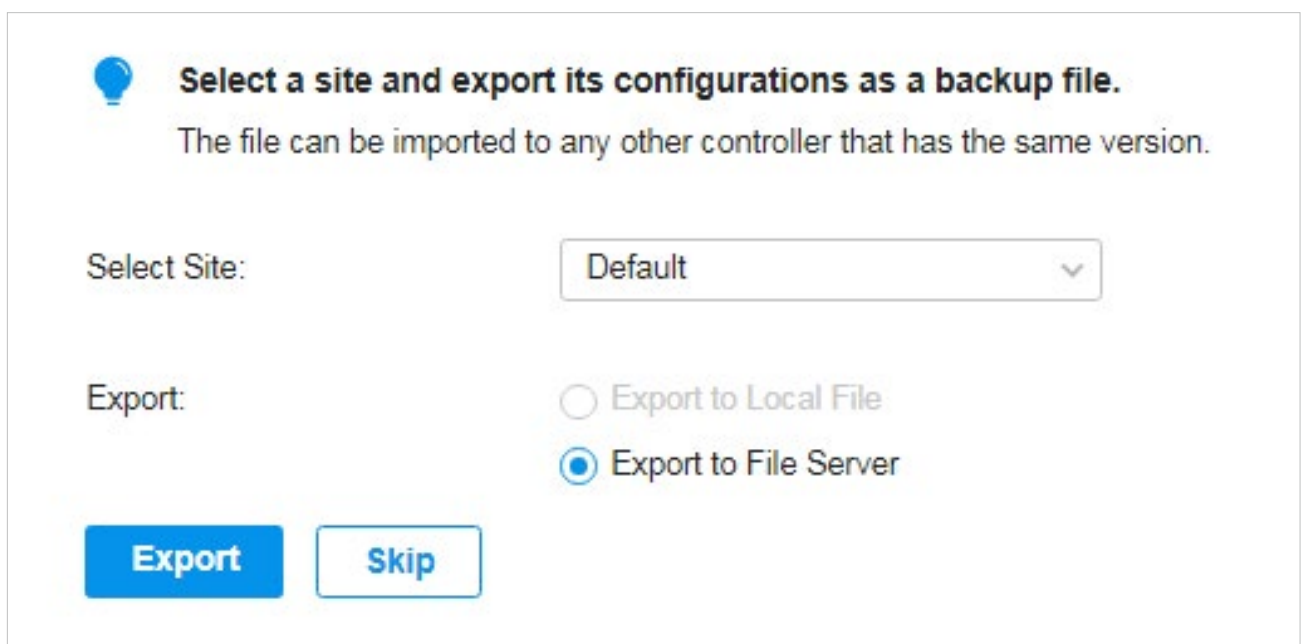
Export Site**Migrate Site****Migrate Devices**

1. Select **Global** from the drop-down list of Organization in the upper right corner. Go to **Settings > Migration**. On the Site Migration tab, click start button on the following page.




The screenshot shows the 'Site Migration' page in the Omada controller interface. At the top, there are two tabs: 'Site Migration' (active) and 'Controller Migration'. The main content area features a circular icon with two location pins and arrows indicating migration. Below the icon, the heading 'Site Migration' is followed by a descriptive paragraph: 'Site Migration allows Omada administrators to export a site from the current controller to any other controller that has the same version. All the configurations and data of the site will be migrated to the target controller.' A red warning message states: 'Warning: 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.' At the bottom center, there is a blue 'Start' button.

2. Select the site to be imported into the second controller in the **Select Site** drop-down list. Select where you want to export and save the backup file. Click **Export** to download the file of the current site. If you have backed up the file, click **Skip**.



The screenshot shows a dialog box titled 'Select a site and export its configurations as a backup file.' Below the title, it says 'The file can be imported to any other controller that has the same version.' There are two main sections: 'Select Site:' with a dropdown menu currently showing 'Default', and 'Export:' with two radio button options: 'Export to Local File' (unselected) and 'Export to File Server' (selected). At the bottom, there are two buttons: 'Export' (blue) and 'Skip' (white with blue border).



1. Start and log in to the target controller, click **Sites:** Site A in the top right corner of the screen and select  **Import Site**, and then the following window will pop up. Note that for controller v 4.3.0 and above, only the file from the controller with the same major and minor version number can be imported.

Import Site
✕



Site Name:

Choose File: Browse

i For controller v 4.3.0 and above, only the file from the controller with the same major and minor version number can be imported.

Import
Cancel

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


 **Site Migration**
 Controller Migration

✓ Export Site

2 **Migrate Site**

3 Migrate Devices

4 Done

 **To migrate your site, import the backup file into your target controller.**

Log into the target controller and go to **Site Management** to click the **Import Site** in the **Site Management** drop-down menu and upload the backup file of your site.

Confirm
Skip



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

The screenshot shows the 'Site Migration' interface. At the top, there are two tabs: 'Site Migration' (active) and 'Controller Migration'. Below the tabs is a progress bar with four steps: 'Export Site' (checked), 'Migrate Site' (checked), '3 Migrate Devices' (active), and '4 Done'. Below the progress bar, there is a light blue lightbulb icon followed by the text: 'Select the devices to be migrated and enter the URL or IP address of your target controller. The selected devices will try to discover the target controller.' At the bottom, there is a label 'Controller IP/Inform URL:' followed by a text input field containing '10.0.3.23'.

Note:

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

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



Site Migration Controller Migration

Export Site — Migrate Site — **3 Migrate Devices** — 4 Done

Select the devices to be migrated and enter the URL or IP address of your target controller.
The selected devices will try to discover the target controller.

Controller IP/Inform URL:

Device List:

| <input checked="" type="checkbox"/> | DEVICE NAME | STATUS | MODEL |
|-------------------------------------|---|-----------|-----------------|
| <input checked="" type="checkbox"/> |  CC-32-E5-A4-B1-AC | CONNECTED | TL-ER7206 V1.0 |
| <input checked="" type="checkbox"/> |  switch | CONNECTED | TL-SG2008P V1.0 |

Select 2 of 2 items [select all](#)
Showing 1-2 of 2 records < 1 > 10 /page Go To page: **GO**

Migrate Devices

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

Site Migration Controller Migration

Export Site — Migrate Site — Migrate Devices — **4 Done**

Migration succeeded! We suggest you forget the successfully migrated devices.
Go to the Device page of your target controller and check if the migrated devices are visible and connected. This process may take several minutes.

Device List:

| <input checked="" type="checkbox"/> | DEVICE NAME | STATUS | MODEL |
|-------------------------------------|-------------------|-----------|-----------------|
| <input checked="" type="checkbox"/> | CC-32-E5-A4-B1-AC | CONNECTED | TL-ER7206 V1.0 |
| <input checked="" type="checkbox"/> | CC-32-E5-69-B5-B0 | CONNECTED | TL-SG2008P V1.0 |

Select 2 of 2 items [select all](#) Showing 1-2 of 2 records < 1 > 10 /page Go To page: [GO](#)

[Forget Devices](#)

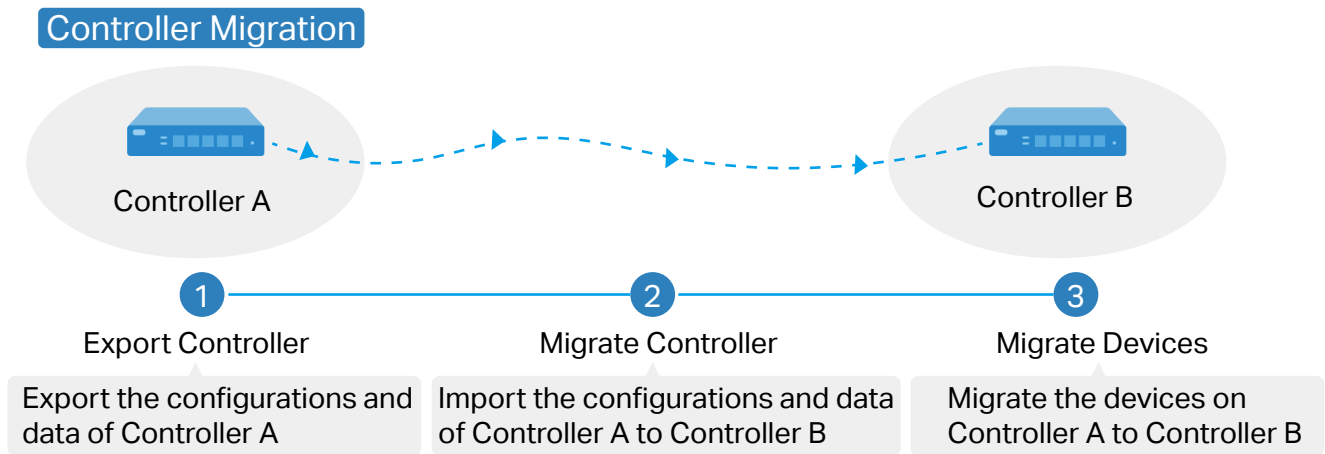
- When the migration process is completed, all the configuration and data are migrated to the target controller. You can delete the previous site if necessary.

5.4.2 Controller Migration

Overview

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

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



Step1: Export Controller

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

Step2: Migrate Controller

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

Step3: Migrate Devices

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

Configuration

To migrate your controller, follow these steps below.

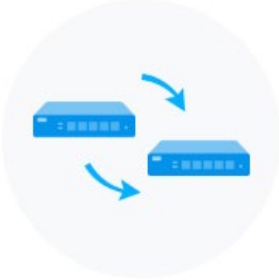
ⓘ Note:

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

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

1. Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings](#) > [Migration](#). On the Controller Migration tab, click start button on the following page.

Site Migration [Controller Migration](#)




Controller Migration

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


Warning: 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.

Start

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

 **Export the configurations and data of your current controller as a backup file.**
The file can be imported to any other controller that has the same version.

Retained Data Backup:

 Retained Data Backup has been set as Settings Only, no data will be backed up. Note that all configurations and data about licenses will not be backed up, including Auto-Activation, Auto-Renewal and license logs.

Export:

Export to Local File
 Export to File Server

Export Controller

Migrate Controller

Migrate Devices

1. Log in to the target controller. Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings > Maintenance > Backup & Restore](#). Click [Browse](#) to locate and choose the backup file of the previous controller. Then click [Restore](#) to upload the file.

Backup & Restore

Backup

Retained Data Backup:

i Retained Data Backup has been set as Settings Only, no data will be backed up. Note that all configurations and data about licenses will not be backed up, including Auto-Activation, Auto-Renewal and license logs.

Export: Export to Local File Export to File Server

Export

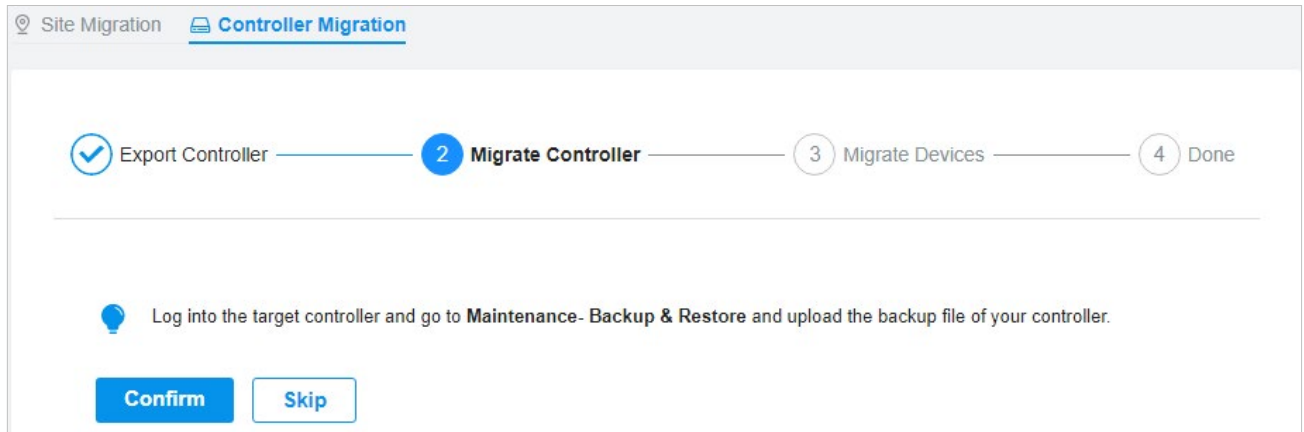
Restore

Import: Import from Local File Import from File Server

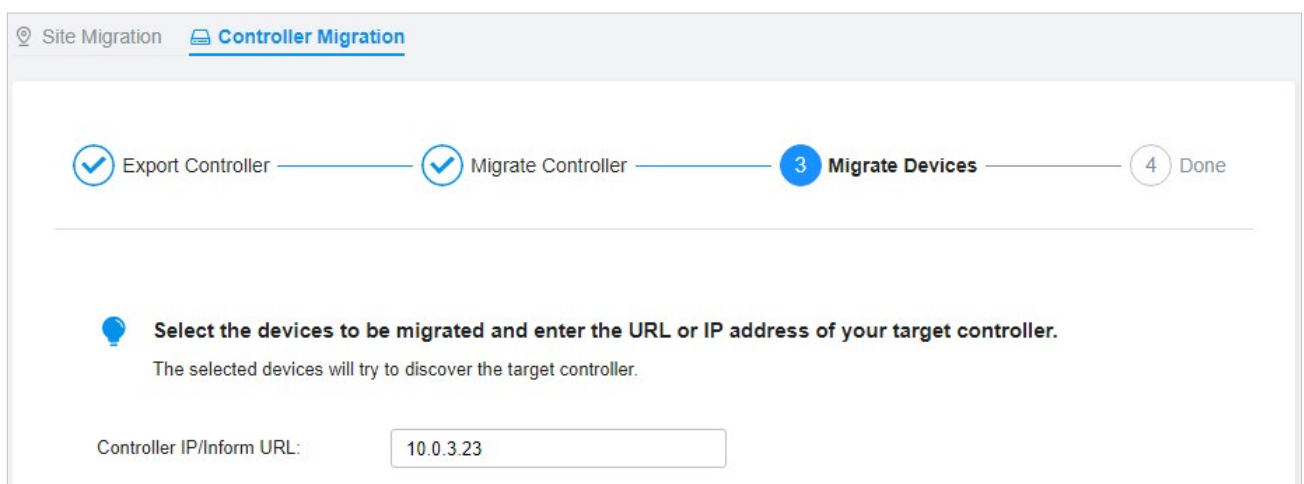
Restore: **Browse**

Restore **i**

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



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



ⓘ **Note:**

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

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



Site Migration [Controller Migration](#)

Export Controller — Migrate Controller — **3 Migrate Devices** — 4 Done

Select the devices to be migrated and enter the URL or IP address of your target controller.
The selected devices will try to discover the target controller.

Controller IP/Inform URL:

Device List:

| <input checked="" type="checkbox"/> | DEVICE NAME | STATUS | MODEL |
|-------------------------------------|---|-----------|------------------|
| <input checked="" type="checkbox"/> |  CC-32-E5-A4-B1-AC | CONNECTED | TL-ER6120 v3.0 |
| <input checked="" type="checkbox"/> |  CC-32-E5-69-B5-B0 | CONNECTED | T1500G-10MPS v2. |

Select 2 of 2 items [select all](#) Showing 1-2 of 2 records < 1 > 10 /page Go To page: [GO](#)

[Migrate Devices](#)

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

Site Migration [Controller Migration](#)

Export Controller —
 Migrate Controller —
 3 Migrate Devices —
 4 Done

Select the devices to be migrated and enter the URL or IP address of your target controller.
 The selected devices will try to discover the target controller.

Controller IP/Inform URL:

Device List:

| <input checked="" type="checkbox"/> | DEVICE NAME | STATUS | MODEL |
|-------------------------------------|-------------------|-----------|------------------|
| <input checked="" type="checkbox"/> | CC-32-E5-A4-B1-AC | CONNECTED | TL-ER6120 v3.0 |
| <input checked="" type="checkbox"/> | CC-32-E5-69-B5-B0 | CONNECTED | T1500G-10MPS v2. |

Select 2 of 2 items [select all](#) Showing 1-2 of 2 records < 1 > 10 /page Go To page: [GO](#)

[Forget Devices](#)

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

♥ 5.5 Auto Backup

Overview

With Auto Backup enabled, the controller will be scheduled to back up the configurations and data automatically at the specified time. You can easily restore the configurations and data when needed.

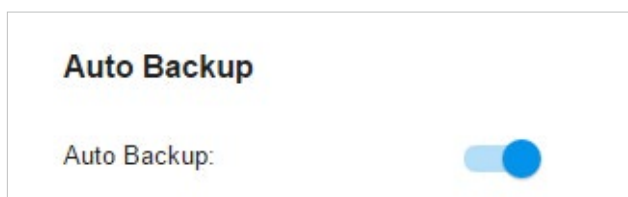
ⓘ Note:

- For OC200, Auto Backup is available only when it is powered by a PoE device and a storage device is connected to its USB port.
- On the Cloud-Based Controller, you have no need to configure Auto Backup. It will automatically save your configurations and data on the cloud.

Configuration

To configure Auto Backup, follow these steps:

1. Select [Global](#) from the drop-down list of Organization in the upper right corner. Go to [Settings > Maintenance > Auto Backup](#). Click to enable Auto Backup.



2. Configure the following parameters to specify the rules of Auto Backup. Click [Apply](#).

Auto Backup

Auto Backup:

Occurrence: Every at in (UTC) Coordinated Universal Time ⓘ

Retained Data Backup:




ⓘ Retained Data Backup has been set as 30 days, data only in recent 30 days will be backed up. Note that all configurations and data about licenses will not be backed up, including Auto-Activation, Auto-Renewal and license logs.

Storage: Save to Local File (the same path as the controller software)
 Save to File Server




Maximum Number of Files: (1-50)

| | |
|--------------------------------|--|
| Occurrence | <p>Specify when to perform Auto Backup regularly. Select Every Day, Week, Month, or Year first and then set a time to back up files.</p> <p>Note the time availability when you choose Every Month. For example, if you choose to automatically backup the data on the 31st of every month, Auto Backup will not take effect when it comes to the month with no 31st, such as February, April, and June.</p> |
| Retained Data Backup | <p>Select the length of time in days that data will be backed up.</p> <p>Settings Only: Back up controller settings only.</p> <p>7 Days/1 Month/2 Months/3 Months/6 Months/1 Year: Back up the data in the recent 7 days/1 month/2 months/3 months/6 months/1 year.</p> <p>All Time: (Only for Software Controller) Back up all data in the controller.</p> |
| Storage | <p>Select where you want to save the backup file.</p> <p>Save to Local File: The backup file will be saved as a local file.</p> <p>Save to File Server: The backup file will be saved in the specified file server. Four types of file server are available: FTP, TFTP, SFTP, and SCP.</p> |
| Saving Path | (Only for Hardware Controller) Select a path to save the backup files. |
| Maximum Number of Files | Specify the maximum number of backup files to save. |

You can view the name, backup time and size of backup files in [Backup Files List](#).

| Backup Files List | | | |
|-------------------------------------|---------------------------|---------|---|
| FILE NAME | BACKUP TIME | SIZE | ACTION |
| autobackup_30days_20230525_1026.cfg | 2023-05-25 10:26:00 am | 7.37 KB |    |

To restore, export or delete the backup file, click the icon in the [Action](#) column.

| | |
|---|---|
|  | <p>Restore the configurations and data in the backup file. All current configurations will be replaced after the restoration.</p> <p>To keep the backup data safe, please wait until the operation is finished. This will take several minutes.</p> |
|  | Export the backup file. The exported file will be saved in the saving path of your web browser. |
|  | Delete the backup file. |

 **Note:**

- If the backup file is saved to file server and the type SCP / TFTP is selected, it will not included in the Backup Files List, and it cannot be exported, restored, or deleted.
 - To back up data manually and restore the data to the controller, refer to [5. 3. 3 Backup & Restore](#) to configure Backup&Restore.
 - The configuration of cloud users can be neither backed up nor restored. To add cloud users, please refer to [9. 4 Manage and Create Cloud User Accounts](#).
-

6

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:

- [6. 1 Introduction to the Devices Page](#)
- [6. 2 Configure and Monitor the Gateway](#)
- [6. 3 Configure and Monitor Switches](#)
- [6. 4 Configure and Monitor APs](#)

6.1 Introduction to the Devices Page

Overview

The Devices page displays all TP-Link devices discovered by the controller and their general information. For an easy monitoring of the devices, you can customize the column and filter the devices for a better overview of device information. Also, quick operations and Batch Edit are available for configurations.

| Search or select tag <input type="text"/> | | | | | | | |
|--|---------------|-----------------------|-------|------------------------|---------------------|-----------------------|--|
| All Gateway/Switches APs Batch Action ▼ | | | | | | | |
| DEVICE NAME | IP ADDRESS | STATUS ▼ | MODEL | VERSION ↑ | UPTIME | ACTION ⋮ | |
| | 192.168.0.1 | CONNECTED | | 2.0.0 | 23h 16m 25s | | |
| | 192.168.0.103 | CONNECTED | | 1.0.3 | 15day(s) 5h 1m 2... | | |
| | -- | PENDING | | -- | | | |
| | -- | MANAGED BY OTHERS | | -- | | | |
| | 192.168.0.101 | CONNECTED | | 3.1.0 | 22h 31m 24s | | |
| | -- | MANAGED BY OTHERS | | -- | | | |
| | 192.168.0.100 | CONNECTED | | 5.0.4 | 22h 25m 50s | | |
| | 192.168.0.105 | CONNECTED | | 5.0.7 | 21h 39m 59s | | |

Showing 1-8 of 8 records < 1 > 10 /page Go To page: GO

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

PENDING

The device is in Standalone Mode or with factory settings, and has not been adopted by the controller. To adopt the device, click , and the controller will use the default username and password to adopt it. When adopting, its status will change from Adopting, Provisioning, Configuring, to Connected eventually.

ISOLATED

(For APs in the mesh network) The AP once managed by the controller via a wireless connection now cannot reach the gateway. You can rebuild the mesh network by connecting it to an AP in the Connected status, then the isolated AP will turn into a connected one. For detailed configuration, refer to [Mesh](#).

CONNECTED

The device has been adopted by the controller and you can manage it centrally. A connected device will turn into a pending one after you forget it.

MANAGED BY OTHERS

The device has already been managed by another controller. You can reset the device or provide the username and password to unbind it from another controller and adopt it in the current controller.

HEARTBEAT MISSED

A transition status between Connected and Disconnected.

Once connected to the controller, the device will send inform packets to the controller in a regular interval to maintain the connection. If the controller does not receive its inform packets in 30 seconds, the device will turn into the Heartbeat Missed status. For a heartbeat-missed device, if the controller receives an inform packet from the device in 5 minutes, its status will become Connected again; otherwise, its status will become Disconnected.

DISCONNECTED

The connected device has lost connection with the controller for more than 5 minutes.



(For APs in the mesh network) When this icon appears with a status icon, it indicates the 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 [5.4 Migration](#).

Configuration

■ Customize the Column

To customize the columns, click next to [Action](#) and check the boxes of information type.

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



| Search or select tag | | | | | | | |
|---|---------------|-------------------|----------------------|---------|---------------------|--------|--|
| All Gateway/Switches APs Batch Action | | | | | | | |
| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | ACTION | |
| B4-B0-24-59-F5-9D | 192.168.0.1 | CONNECTED | ER605 v2.0 | 2.0.0 | 23h 16m 25s | | |
| 00-0A-EB-45-F7-B1 | 192.168.0.103 | CONNECTED | TL-SG2210MP v1.0 | 1.0.3 | 15day(s) 5h 1m 2... | | |
| 00-00-FF-FF-0E-8C | -- | PENDING | EAP245 v4.0 | -- | | | |
| 00-00-FF-FF-20-6F | -- | MANAGED BY OTHERS | EAP670 v1.0 | -- | | | |
| 00-5F-67-DF-56-46 | 192.168.0.101 | CONNECTED | EAP235-Wall(US) v1.0 | 3.1.0 | 22h 31m 24s | | |

■ 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.

Group 1








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  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 Header or the **Action** column to quickly adopt, locate, upgrade, or reboot the device.

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

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | |
|------------------------|--------------|-----------|-------------------|---------|------------------|-----|
| TP-Link_Test_Gatew... | 192.168.0.1 | CONNECTED | TL-ER7206 v1.0 | 1.1.0 | 1 days 03:35:44 | ⏸ |
| TP-Link_Test_Swiftc... | 192.168.0.37 | CONNECTED | TL-SG2210MP v1.0 | 1.0.0 | 10 days 16:57:04 | 📍 ⏸ |
| TP-Link_Test_Swiftc... | 192.168.0.41 | CONNECTED | TL-SG2210MP v1.0 | 1.0.0 | 11 days 19:56:36 | 📍 ⏸ |
| TP-Link_Test_Swiftc... | 192.168.0.21 | CONNECTED | TL-SG3428X v1.0 | 1.0.1 | 0 days 01:20:48 | 📍 ⏸ |
| TP-Link_Test_Swiftc... | 192.168.0.77 | CONNECTED | TL-SG3428XMP v1.0 | 1.0.1 | 0 days 00:33:34 | 📍 ⏸ |

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.

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | CLIENTS | DOWN | UP | CHANNEL | ACTION |
|--------------------|---------------|--------------|----------------------|---------|------------------|---------|---------|---------|---------|--------|
| TP-Link_Test_Eap_4 | 192.168.0.104 | ADOPT FAILED | EAP235-Wall(US) v1.0 | 1.0.2 | 16 days 10:42:33 | 0 | 0 Bytes | 0 Bytes | -- | Retry |
| TP-Link_Test_Eap_5 | 192.168.0.105 | ADOPT FAILED | EAP235-Wall(US) v1.0 | 1.0.2 | 10 days 23:14:11 | 0 | 0 Bytes | 0 Bytes | -- | Retry |


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 **X** 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.

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



Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click .



Click to maximize the Properties window. You can also use the icon on pages other than the Devices page.



Click to close the Properties window of the chosen device(s). Note that the unsaved configuration will be lost.



The number on the lower-right shows the number of devices in the batch configuration.

♥ 6.2 Configure and Monitor the Gateway

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

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

The screenshot shows a network management interface. On the left, there is a table listing devices:

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | DOWN |
|-------------------|---------------|-----------|-----------------|---------|-----------------|------------------|
| CC-32-E5-A4-B1-AC | 192.168.0.1 | CONNECTED | TL-ER7206 v1.0 | 1.0.0 | 4 days 18:27:40 | -- |
| CC-32-E5-69-B5-B0 | 192.168.0.135 | CONNECTED | TL-SG2210P v1.0 | 1.0.3 | 8 days 21:56:16 | 949.25 MB 1.05 G |

Below the table, there are pagination controls: "Showing 1-2 of 2 records", "1" (selected), "5/page", "Go To page:", and a "GO" button. There is also a "+ Add Devices" button.

On the right, a detailed view for the selected device "CC-32-E5-A4-B1-..." is shown. It includes a status indicator "CONNECTED" and a legend for port types: Disabled (grey), Disconnected (dark grey), 1000 Mbps (green), 10/100 Mbps (orange), 2.5 Gbps (cyan), 5 Gbps (blue), 10 Gbps (dark blue), WAN (globe icon), and LAN (network icon). Below the legend, there are tabs for "Details", "Networks", "Ports", "Config", and "Statistics". The "Overview" tab is active, showing:

- MAC Address: CC-32-E5-A4-B1-AC
- Model: TL-ER7206 v1.0
- Firmware Version: 1.0.0 Build 20200509 Rel.71443
- CPU Utilization: 1%
- Memory Utilization: 13%
- LAN IP Address: 192.168.0.1
- Uptime: 4 days 18:27:40

At the bottom of the detailed view, there is a "WAN" section.

! Note:

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

6.2.1 Configure the Gateway

In the Properties window, 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.

The legend shows icons for different port statuses and types:


- Disabled: Grey square
- Disconnected: Dark grey square
- 1000 Mbps: Green square
- 10/100 Mbps: Orange square
- 2.5 Gbps: Cyan square
- 5 Gbps: Blue square
- 10 Gbps: Dark blue square
- WAN: Globe icon
- LAN: Network icon

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


| | |
|----------|-----------|
| Port | 1 |
| Status | 1000 Mbps |
| Tx Bytes | 34.70 MB |
| Rx Bytes | 59.61 MB |



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.

Overview 

| | |
|-------------------|--|
| MAC Address: | Public IP Address: |
| 40-ED-00-52-BB-E5 | 192.168.0.1 |
| Model: | Firmware Version: |
| ER706W v1.0 | 1.0.0 Build 20230712 Rel.61 639(4555) |
| CPU Utilization: | Memory Utilization: |
| 3% | 40% |
| LAN IP Address: | Uptime: |
| 192.168.0.1 | 3day(s) 2h 1m 28s |
| Temperature: | |
| 56°C | |

Radios 

| | |
|--------------|---|
| SFP WAN/LAN1 | Link Down  |
| WAN2 | Online  |












Networks

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

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

Ports

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

| Name | Status | ACTION |
|-----------|---|---|
| WAN |  |  |
| WAN/LAN1 |  |  |
| WAN/LAN2 |  |  |
| LAN1 |  |  |
| LAN2 |  |  |
| USB Modem |  | |

Showing 1-6 of 6 records < 1 >

To configure a port, click [✎](#) in the table.

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 send a copy of traffic 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.

[All \(1\)](#) [Users \(1\)](#) [Guests \(0\)](#) [History >](#)

Client name or MAC

| NAME | MAC | SSID/N |
|----------------------------------|-------------------|--------|
| DESKTOP-STTAJ... | EC-F4-BB-35-D4-06 | LAN |

Showing 1-1 of 1 records < 1 >

Mesh (for wireless routers only)

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

[All \(1\)](#) [Users \(1\)](#) [Guests \(0\)](#) [History >](#)

Client name or MAC

| NAME | MAC | SSID/N |
|----------------------------------|-------------------|--------|
| DESKTOP-STTAJ... | EC-F4-BB-35-D4-06 | LAN |

Showing 1-1 of 1 records < 1 >

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.

General
⤴

Name:

LED:
 Use Site Settings
 On
 Off

Longitude:

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

Latitude:

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

Address:
 ↻ Refresh
(Optional)

Apply
Cancel

Name Specify a name of the device.

LED Select the way that device's LEDs work.

Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to [4. 2. 2 Services](#).

On/Off: The device's LED will keep on/off.

Longitude / Latitude / Address Configure the parameters according to where the site is located. These fields are optional.

■ Radios (for wireless routers only)

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

Radios ⤴

2.4 GHz
5 GHz

Status: Enable

Wireless Mode: Auto ▼

Channel Width: Auto ▼

Channel: Auto ▼

Tx Power (EIRP): Auto ▼

Note : The EIRP transmit power includes the antenna gain.

Apply
Cancel

| | |
|----------------------|--|
| 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 router to improve wireless performance. If you select Auto for the channel setting, the router scans available channels and selects the channel where the least amount of traffic is detected. |
| Tx Power | <p>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.</p> <p>Low: $\text{Min. TxPower} + (\text{Max. TxPower} - \text{Min. TxPower}) * 20\%$ (round off the value)</p> <p>Medium: $\text{Min. TxPower} + (\text{Max. TxPower} - \text{Min. TxPower}) * 60\%$ (round off the value)</p> <p>High: Max. TxPower</p> <p>Custom: Specify the value manually.</p> |

■ 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 [4.4 Configure Wireless Networks](#).


WLANs

WLAN Group:
Default

| Name | Band | Overri des | Enable |
|------|-------------------|---------------|-------------------------------------|
| 123 | 2.4 GHz, 5 GHz | | <input checked="" type="checkbox"/> |

Showing 1-1 of 1 records < 1 >


Apply **Cancel**

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

WLANs>SSID Override

SSID Override: Enable

SSID:
tp-link

Password:
..... 

VLAN: Enable

VLAN ID:
1 (1-4094)

Save **Cancel**

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](#), and for detailed configuration of SNMP service, refer to [4.10.4 SNMP](#).

Services ⤴

SNMP Manage

Location:

Contact:

■ Advanced

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

Advanced ⤴

Hardware Offload: Enable (i)

LLDP: Enable

Echo Server:

Auto

Custom

2.4 GHz 5 GHz

Load Balance

Maximum Associated Clients: Enable

RSSI Threshold: Enable (i)

QoS

No Acknowledgement: Enable (i)

Unscheduled Automatic Power Save Delivery: Enable (i)

OFDMA

OFDMA: Enable (i)

Apply Cancel

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 [4.6 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.

Maximum Associated Clients

Enable this function and specify the maximum number of connected clients. If the connected client reaches the maximum number, the router 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 router.

| | |
|---|--|
| No Acknowledgement | Enable this function to specify that the router 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. |
| OFDMA | (Only for models supporting 802.11 ax) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improve 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.

Manage Device
⤴

Custom Upgrade

Choose the firmware file and upgrade the device.

⤴ **Browse**

Move to Site

Move this device to another site of this controller.

Please Select... ▾

Move

Force Provision

Click Force Provision to synchronize the configurations of the device with the controller. The device will be disconnected from the controller temporarily, and be adopted again to get the configurations from the controller.

Force Provision

Forget This Device

If you no longer wish to manage a device, you may forget it. After forgotten, the device will be removed from the controller and get reset.

Forget

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.


Download

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. |
| | <p> Note:</p> <p>Firmware updates are required for earlier devices to obtain complete information.</p> |

■ Common Settings

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

Common Settings ⤴

[Settings->Wired Networks->Internet](#)

To configure the network of the WAN port, go to the **Settings->Wired Networks->Internet** page.

[Settings->Wired Networks->LAN](#)

To view and configure the settings of the network interfaces, go to the **Settings->Wired Networks->LAN** page.

[Settings->VPN](#)

To view and configure the VPN network, go to the **Settings->VPN** page.

[Settings->Network Security](#)

To view and configure the Firewall and ACL rules for the network, go to the **Settings->Network Security** page.

[Settings->Transmission->Routing](#)

To view and configure Routing on the gateway, go to the **Settings->Transmission->Routing** page.

[Settings->Transmission->NAT](#)

To view and configure NAT on the gateway, go to the **Settings->Transmission->NAT** page.

[Settings->Services](#)

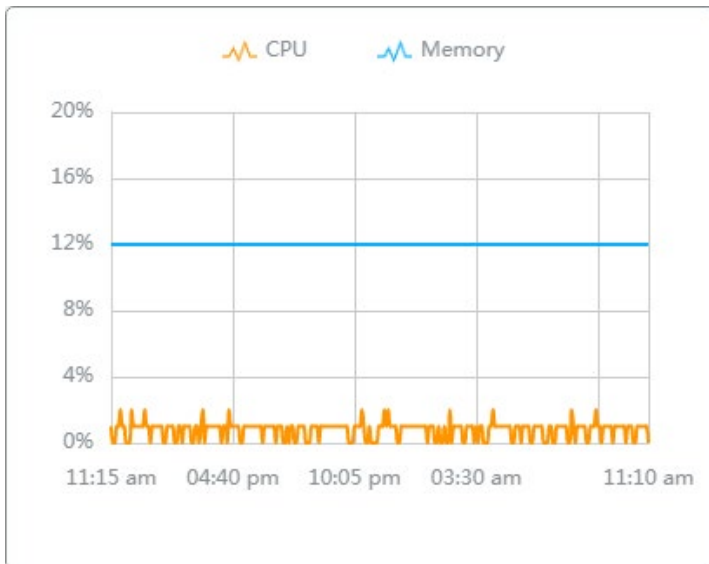
To view and configure the network services, go to the **Settings->Services** page.

6.2.2 Monitor the Gateway

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

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.



♥ 6.3 Configure and Monitor Switches

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

To open the Properties window, click the entry of a switch, or click [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.

The screenshot displays the network management interface. On the left, the 'Device List' window shows a table of devices:

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME |
|-------------------|--------------|-----------|-----------------|---------|----------|
| 1C-61-B4-C5-48-83 | 192.168.0.1 | CONNECTED | ER605 v2.0 | 2.1.0 | 4day(s) |
| 00-FF-00-05-40-5D | 192.168.0.18 | CONNECTED | TL-SG2428P v1.0 | 1.1.7 | 22day(s) |

Below the table, it indicates 'Showing 1-2 of 2 records' and '10 /page'. On the right, the 'Properties' window for the switch '00-FF-00-05-40-5D' is open, showing an 'Overview' tab with the following details:

- Serial Number: [REDACTED]
- Model: TL-SG2428P v1.0
- MAC Address: [REDACTED]
- IP Address: 192.168.0.18
- IPv6 Address: [REDACTED]
- Firmware Version: 1.1.7
- CPU Utilization: 10%
- Memory Utilization: 47%
- Uptime: 22day(s) 17h 16m 40s
- Remaining PoE Power: 97.80% / 244.50W
- Fan Status: Normal

ⓘ Note:

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

6.3.1 Configure Switches






















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

Ports

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



■ Port

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

| Port | | LAG | Edit Selected | | |
|--------------------------|----|--------|---|---------|---|
| <input type="checkbox"/> | # | Name | Status | Profile | ACTION |
| <input type="checkbox"/> | 1 | Port1 |  | All |  |
| <input type="checkbox"/> | 2 | Port2 |  | All |  |
| <input type="checkbox"/> | 3 | Port3 |  | All |   |
| <input type="checkbox"/> | 4 | Port4 |  | All |  |
| <input type="checkbox"/> | 5 | Port5 |  | All |  |
| <input type="checkbox"/> | 6 | Port6 |  | All |  |
| <input type="checkbox"/> | 7 | Port7 |  | All |  |
| <input type="checkbox"/> | 8 | Port8 |  | All |  |
| <input type="checkbox"/> | 9 | Port9 |  | All |  |
| <input type="checkbox"/> | 10 | Port10 |  | All |  |

Status

Displays the port status in different colors.

: The port profile is Disabled. To enable it, click  to change the profile.

: The port is enabled, but no device or client is connected to it.


: The port is running at 1000 Mbps.

: The port is running at 10/100 Mbps.

Profile

Displays the profile applied to the port.

Action

: Click to edit the port name and configure the profile applied to the port.

: (For PoE ports) Click to reboot the connected powered devices (PDs).

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

Edit Port1

Name:

Profile:
 [Manage Profiles](#)

Profile Overrides

| | |
|-----------------------------------|---|
| 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 4.3 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.

Edit Port1

Name:

Profile: [Manage Profiles](#)

Profile Overrides

Operation:

Switching

Mirroring (i)

Aggregating

PoE Mode:

Off

802.3at/af

802.1X Control:

Auto

Force Authorized

Force Unauthorized

Link Speed:

Auto

Manual

Port Isolation: Enable (i)

Flow Control: Enable

EEE: Enable

Loopback Control:

Off

Loopback Detection Port Based

Loopback Detection VLAN Based

Spanning Tree

LLDP-MED: Enable

Bandwidth Control: (i)

Off

Rate Limit

Storm Control (

DHCP L2 Relay: Enable

Format:

Circuit ID: (Optional)

Remote ID: (Optional)

| | |
|------------------|---|
| PoE Mode | <p>(Only for PoE ports) Select the PoE (Power over Ethernet) mode for the port.</p> <p>Off: Disable PoE function on the PoE port.</p> <p>802.3at/af: Enable PoE function on the PoE port.</p> |
| 802.1X Control | <p>Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to Settings > Authentication > 802.1X.</p> <p>Auto: The port is unauthorized until the client is authenticated by the authentication server successfully.</p> <p>Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client.</p> <p>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.</p> |
| Link Speed | <p>Select the speed mode for the port.</p> <p>Auto: The port negotiates the speed and duplex automatically.</p> <p>Manual: Specify the speed and duplex from the drop-down list manually.</p> |
| Port Isolation | <p>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.</p> |
| Flow Control | <p>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.</p> |
| EEE | <p>Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.</p> |
| Loopback Control | <p>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.</p> <p>Off: Disable loopback control on the port.</p> <p>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.</p> <p>Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the VLAN will be blocked.</p> <p>Spanning Tree: Select STP (Spanning Tree Protocol) 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.</p> |

| | |
|---------------------------|--|
| 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 | <p>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.</p> <p>Off: Disable Bandwidth Control for the port.</p> <p>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.</p> <p>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.</p> |
| 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 | <p>When Storm Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit.</p> <p>Drop: With Drop selected, the port will drop the subsequent frames when the traffic exceeds the limit.</p> <p>Shutdown: With Shutdown selected, the port will be shutdown when the traffic exceeds the limit.</p> |
| Recover Time | With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time. |
| DHCP L2 Relay | Click the checkbox to enable DHCP L2 Relay for the network. |
| Format | <p>Select the format of option 82 sub-option value field.</p> <p>Normal: The format of sub-option value field is TLV (type-length-value).</p> <p>Private: The format of sub-option value field is just value.</p> |

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

Profile Overrides

Operation:

Switching

Mirroring (i)

Aggregating

Unselected Selected

| | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | | |

LAG: LAG1

PoE Mode:

Off

802.3at/af

Link Speed:

Auto

Manual

Auto / Auto v

Bandwidth Control:

Off

Rate Limit

Ingress Rate Limit: Enable

Egress Rate Limit: Enable

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.

Profile Overrides

Operation:

Switching

Mirroring ⓘ

Aggregating

Unselected Selected

| | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | | |

LAG ID:

(1-8)

Static LAG

Active LACP

Passive LACP

Apply
Cancel
Remove Overrides

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](#).

| Port | | LAG | | | |
|--------|------|--------------------------------------|----------------|---------|---|
| LAG ID | Name | Status | Ports | Profile | ACTION |
| 1 | LAG1 | ■ | Port 9,Port 10 | All |   |

Status

Displays the status in different colors.

■: The LAG profile is Disable. To enable it, click  to change the profile.

■: The port is enabled, but no device or client is connected to it.

■: The LAG ports are running at 1000 Mbps.

■: The LAG port are running at 10/100 Mbps.


Ports


Displays the port number of LAG ports.

Profile

Displays the profile applied to the port.

Action

: Click to edit the port name and configure the profile applied to the port.

: Click to delete the LAG. Once deleted, the ports will be configured as the default All profile and Switching operation. You can configure the ports under the Port tab.

Click [✎](#) to configure the LAG name and the applied profile.

Edit LAG1

Name:

Profile:
 [Manage Profiles](#)

i Configurations of PoE, 802.1x and LLDP-MED in the profile do not take effect on LAG ports.

Profile Overrides

| | |
|--------------------------|---|
| 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 4.3 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.

Profile Overrides

Unselected Selected

| | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | | |

LAG ID:
 (1-8)

Static LAG
 Active LACP
 Passive LACP

Link Speed: Auto
 Manual

Port Isolation: Enable ⓘ

Flow Control: Enable

EEE: Enable ⓘ

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

Bandwidth Control: Off
 Rate Limit
 Storm Control

DHCP L2 Relay: Enable

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 | <p>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.</p> <p>Off: Disable loopback control on the port.</p> <p>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.</p> <p>Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the VLAN will be blocked.</p> <p>Spanning Tree: Select STP (Spanning Tree Protocol) 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.</p> |
| Bandwidth Control | <p>Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance.</p> <p>Off: Disable Bandwidth Control for the port.</p> <p>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.</p> <p>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.</p> |
| Ingress Rate Limit | <p>With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.</p> |
| Egress Rate Limit | <p>With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.</p> |
| Broadcast Threshold | <p>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.</p> |
| Multicast Threshold | <p>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.</p> |
| Unknown Unicast Threshold | <p>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.</p> |
| DHCP L2 Relay | <p>Click the checkbox to enable DHCP L2 Relay for the network.</p> |

| | |
|---------------------|--|
| 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 the device name and LED settings of the switch, and categorize it via device tags.

The screenshot shows the 'Config' tab selected in a navigation menu. The 'General' section is expanded, showing the following configuration options:

- Name:** A text input field containing the MAC address '00-0A-E3-AB-D7-B7'.
- LED:** Three radio button options: 'Use Site Settings' (selected), 'On', and 'Off'.
- Device Tags:** A dropdown menu with the text 'Please Select...' and a downward arrow.
- Jumbo:** A text input field containing '1518', followed by the label 'Bytes' and a range '(1518-9216)'.
- Hash Algorithm:** A dropdown menu with the text 'SRC MAC+DST MAC' and a downward arrow.

| | |
|-------------|--|
| 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 4. 2. 2 Services . |
| | On/Off: The device's LED will keep on/off. |
| Device Tags | Select a tag from the drop-down list or create a new tag to categorize the device. |
| 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. |


■ 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.


| Name | VLAN | Enable |
|--------|------|-------------------------------------|
| LAN | 1 | <input checked="" type="checkbox"/> |
| Test A | 10 | <input type="checkbox"/> |
| Test B | 101 | <input type="checkbox"/> |


Showing 1-3 of 3 records < 1 >

Apply Cancel

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

VLAN Interface > Edit Interface

Management VLAN: Enable 


 The controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the [Configuration Guide](#) before you configure this feature.

IP Address Mode:

Static


DHCP

Use Fixed IP Address: Enable

 Gateway Required

Network:

IP Address:

Fallback IP Address: Enable 

Fallback IP Address:

Fallback IP Mask:

Fallback Gateway:

(Optional)

DHCP Option12:

(Optional)

DHCP Mode:

None

DHCP Server

DHCP Relay

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/Secondary 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 on 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  to edit the settings, and click  to delete it.

The screenshot shows the 'Static Route' configuration page. At the top right is a '+ Add' button. Below it is a table with the following columns: Destination IP, Enabled, Next Hop, and ACTION. The table contains one row with the following data: Destination IP: 192.168.0.3/32, Enabled: , Next Hop: 10.0.0.1, and ACTION:  . At the bottom left, it says 'Showing 1-1 of 1 records' with navigation arrows and the number '1'.

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

The screenshot shows the 'Static Route > Add New Route' configuration form. It includes the following fields and options:

- Status: Enable
- IP Version: IPv4, IPv6
- Destination IP/Subnet: Input field with a subnet button (+ Add Subnet)
- Next Hop: Input field
- Distance: Input field (1-255)
- Buttons: Apply, Cancel

| | |
|-------------------------------|---|
| Status | Click the checkbox to enable or disable the static route. |
| IP Version | Select IPv4 or IPv6. |
| Destination IP/ Subnet / | 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. |
| Destination IP/ Prefix Length | You can click + Add Subnet to specify multiple entries or click  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.

Services ⤴

VLAN

Management VLAN:
LAN

 To configure the Management VLAN, please go to [VLAN Interface](#). Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the [Configuration Guide](#) before you configure this feature.

Loopback Control

Loopback Detection: Enable

Spanning Tree:

Off
 STP
 RSTP

SNMP [Manage](#)

Location:

Contact:

| | |
|---------------------------|---|
| Management VLAN | <p>Display the name of the current Management VLAN.</p> <p>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.</p> <p>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.</p> |
| Loopback Detection | <p>When enabled, the switch checks the network regularly to detect the loopback.</p> <p>Note that Loopback Detection and Spanning Tree are not available at the same time.</p> |
| Spanning Tree | <p>Select a mode for Spanning tree. This feature is available only when Loopback Detection is disabled.</p> <p>Off: Disable Spanning Tree on the switch.</p> <p>STP: Enable STP (Spanning Tree Protocol) 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.</p> <p>RSTP: Enable RSTP (Rapid Spanning Tree Protocol) to prevent loops in the network. RSTP provides the same features as STP with faster spanning tree convergence.</p> <p>Priority: When STP/RSTP enabled, specify the priority for the switch 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.</p> |
| SNMP | <p>(Only for configuring a single device) Configure SNMP to write down the location and contact detail. You can also click Manage to jump to Settings > Services > SNMP, and for detailed configuration of SNMP service, refer to 4. 10. 4 SNMP.</p> |

■ IP Settings (Only for configuring a single device)

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

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

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

IP Settings ⤴

Mode:

DHCP

Static

Fallback IP: Enable ⓘ

Fallback IP Address:

192 . 168 . 0 . 25

Fallback IP Mask:

255 . 255 . 255 . 0

Fallback Gateway:

. . . (Optional)

Apply **Cancel**

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

IP Settings ⤴

Mode:

DHCP

Static

IP Address:

IP Mask:

Gateway:

Primary DNS Server:

 (Optional)

Secondary DNS Server:

 (Optional)

Apply **Cancel**

■ 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.

Manage Device ⤴

Custom Upgrade

Please choose the firmware file and upgrade the device.

[Browse](#)

Copy Configuration

Select another device at the current site to copy its configurations.

Please Select... ▼

[Copy](#)

Move to Site

Move this device to another site of this controller.

Please Select... ▼

[Move](#)

Force Provision

Click Force Provision to synchronize the configurations of the device with the controller. The device will be disconnected from the controller temporarily, and be adopted again to get the configurations from the controller.

[Force Provision](#)

Forget This Device

If you no longer wish to manage a device, you may forget it. After forgotten, the device will be removed from the controller and get reset.

[Forget](#)

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.

[Download](#)

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.

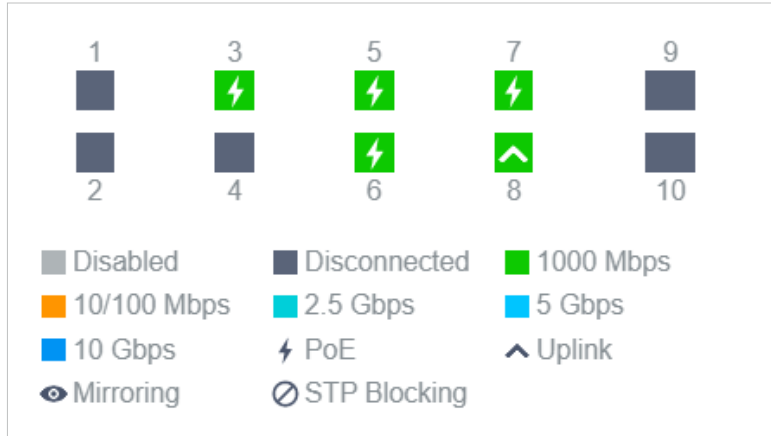
| | |
|--|--|
| Force Provision | (Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller. |
| Forget 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. |
| <p> Note:</p> <p>Firmware updates are required for earlier devices to obtain complete information.</p> | |





6.3.2 Monitor Switches

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

Monitor Panel

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



| | |
|--|--|
|  PoE | A PoE port connected to a powered device (PD). |
|  Uplink | An uplink port connected to WAN. |
|  Mirroring | A mirroring port that is mirroring another switch port. |
|  STP Blocking | A port in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocol 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.

| | |
|-----------|-----------------------|
| Port | 3 |
| Name | Port3 |
| Status | 1000 Mbps Full Duplex |
| Tx Bytes | 343.59 MB |
| Rx Bytes | 353.98 MB |
| Profile | All |
| PoE Power | 4.3 W |

| | |
|----------------|---|
| 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 4.8 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 mirrored. |
| 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.

Overview ⤴

| | |
|--|-----------------------------|
| S/N: ██████████ | Model: TL-SG3428XMP v1.0 |
| MAC Address: ██████████ | IP Address: 192.168.0.11 |
| Firmware Version: 1.0.2 Build 20210119 Rel.75169 | CPU Utilization: 5% |
| Memory Utilization: 30% | Uptime: 5 days 23:14:42 |
| Remaining PoE Power: 97.53% / 374.50W | Fan Status: Normal |

■ **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.

Uplink ⤴

| | |
|--------------------------|--|
| Port: 8 | Uplink Device: CC-32-E5-A4-B1-AC |
| Model: TL-ER7206 v1.0 | Speed & Duplex: 1000 Mbps Full Duplex |
| Rx Bytes: 491.79 MB | Tx Bytes: 497.95 MB |

- **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.

| Downlink ⤴ | | | |
|---|--------------|-----------------------|-----------------------------|
| Port | Model | Device-MAC | Status |
| 3 | EAP660 HD | B0-95-75-E6-48- 3C | 1000 Mbps Full Duplex |

Showing 1-1 of 1 records < 1 >

Clients

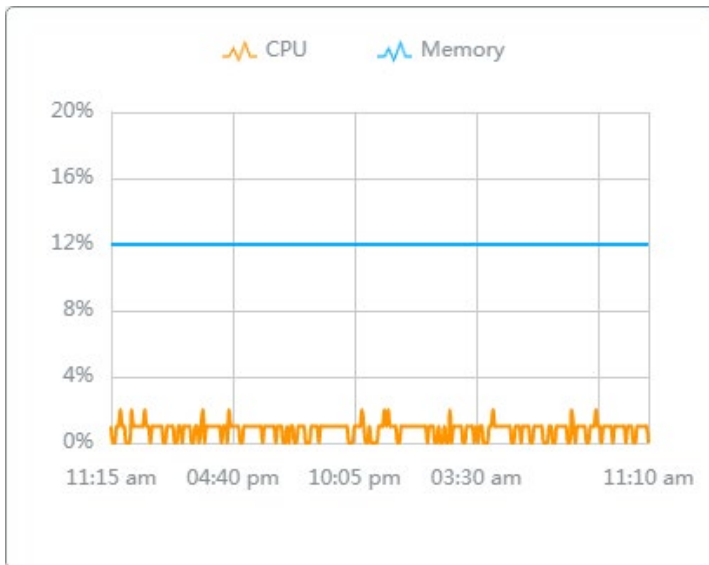
In Clients, you can view the information of clients connected to the switch, including the client name, IP address and the connected port. You can click the client name to open its Properties window.

| # | Name | IP Address |
|---|------------------------------|---------------|
| 7 | OC200_72C6FB | 192.168.0.132 |
| 8 | TP-Link-PC | 192.168.0.145 |

Showing 1-2 of 2 records < 1 >

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 [8.2 View the Statistics of the Network](#).



▼ 6.4 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.

The screenshot displays the AP Properties window. On the left, a table lists APs with columns for Device Name, IP Address, Status, Model, Version, Uptime, Clients, and Down. The table contains 7 records. The selected AP, TP-Link_Test_Eap_6, is highlighted in blue. On the right, a detailed view for the selected AP shows various metrics and configuration options. The 'Overview' tab is active, displaying MAC Address, IP Address, Model, Firmware Version, CPU Utilization, Memory Utilization, and Uptime. Below the overview, there are sections for 'Uplink (Wireless)' and 'Radios'.

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | CLIENTS | DOWN |
|--------------------|---------------|--------------|----------------------|---------|------------------|---------|-----------|
| TP-Link_Test_Eap_0 | 192.168.0.100 | CONNECTED | EAP690E HD(EU) v1.0 | 1.0.2 | 16 days 23:14:38 | 4 | 125.76 GB |
| TP-Link_Test_Eap_1 | 192.168.0.101 | CONNECTED | EAP245(EU) v4.0 | 1.0.2 | 16 days 23:13:29 | 3 | 210.87 GB |
| TP-Link_Test_Eap_2 | 192.168.0.102 | DISCONNECTED | EAP235-Wall(US) v1.0 | 1.0.2 | -- | 0 | 210.87 GB |
| TP-Link_Test_Eap_3 | 192.168.0.103 | DISCONNECTED | EAP235-Wall(US) v1.0 | 1.0.2 | -- | 0 | 210.87 GB |
| TP-Link_Test_Eap_4 | 192.168.0.104 | ADOPT FAILED | EAP235-Wall(US) v1.0 | 1.0.2 | 16 days 10:42:33 | 0 | 0 Bytes |
| TP-Link_Test_Eap_5 | 192.168.0.105 | ADOPT FAILED | EAP235-Wall(US) v1.0 | 1.0.2 | 10 days 23:14:11 | 0 | 0 Bytes |
| TP-Link_Test_Eap_6 | 192.168.0.106 | CONNECTED | EAP235-Wall(US) v1.0 | 1.0.2 | 15 days 11:14:35 | 3 | 210.87 GB |

ⓘ Note:

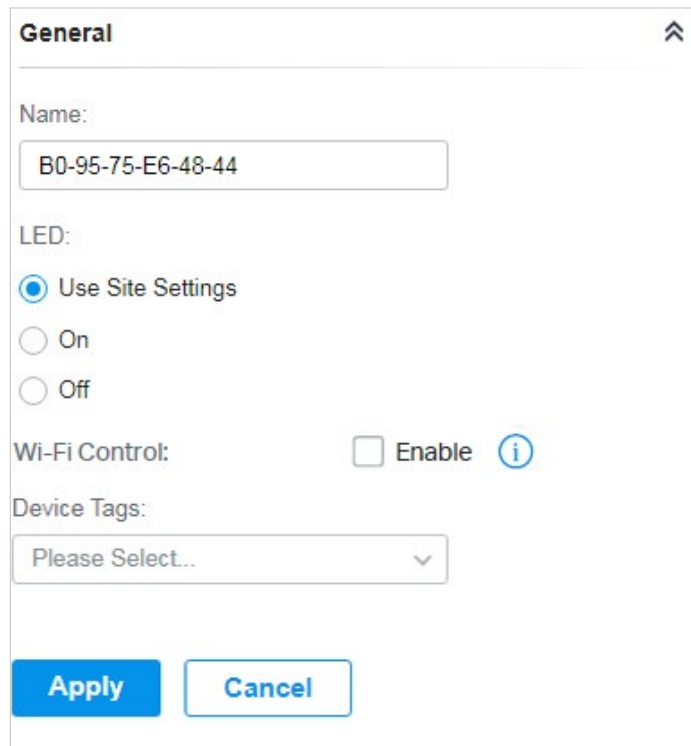
- The available functions in the window vary due to the model and status of the device.
- In Batch Config, you can only configure the selected devices, and the unaltered configurations will keep the current settings.
- In Batch Config, if some functions, such as the 5 GHz band, are available only on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

6.4.1 Configure APs

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 the device name and LED settings of the AP, and categorize it via device tags.



Name (Only for configuring a single device) Specify a name of the device.

LED Select the way that device's LEDs work.

Use Site Settings: The device's LED will work following the settings of the site. To view and modify the site settings, refer to [4. 2. 2 Services](#).

On/Off: The device's LED will keep on/off.

Wi-Fi Control (Only for Certain wall plate 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.

■ 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.

IP Settings ⤴

Mode:

DHCP
 Static

Use Fixed IP Address: Enable

🔔 Gateway Required

Network:

IP Address:

Fallback IP: Enable ⓘ

Fallback IP Address:

Fallback IP Mask:

Fallback Gateway:
 (Optional)

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

IP Settings ⤴

Mode:

DHCP

Static

IP Address:

IP Mask:

Gateway:

Primary DNS Server:

 (Optional)

Secondary DNS Server:

 (Optional)

Apply **Cancel**

■ 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.

Radios
⤴

2.4 GHz

5 GHz-1

5 GHz-2

6 GHz

Status: Enable

Channel Width:

Channel:

Tx Power (EIRP):

Note : The EIRP transmit power includes the antenna gain.

Apply

Cancel

Status

If you disable the frequency band, the radio on it will turn off.

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: $\text{Min. TxPower} + (\text{Max. TxPower} - \text{Min. TxPower}) * 20\%$ (round off the value)

Medium: $\text{Min. TxPower} + (\text{Max. TxPower} - \text{Min. TxPower}) * 60\%$ (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 [4. 4 Configure Wireless Networks](#).

ⓘ **Note:**


The 6 GHz band is only available for certain devices.

WLANs ⌵

WLAN Group:

| Name | Band | Overrides | Enable |
|------------------------|-----------------------------|-----------|-------------------------------------|
| EAP_t st | 2.4 GHz, 5 GHz, 6 GHz | | <input checked="" type="checkbox"/> |
| EAP_t st_IPC | 2.4 GHz, 5 GHz, 6 GHz | | <input checked="" type="checkbox"/> |
| EAP_t st_gue. .. | 2.4 GHz, 5 GHz, 6 GHz | | <input type="checkbox"/> |


Showing 1-3 of 3 records < 1 >

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

WLANs>SSID Override ⤴

SSID Override: Enable

SSID:

Password:
 

VLAN: Enable

VLAN ID:
 (1-4094)

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.

Services
⤴

VLAN

Management VLAN: Enable

LAN(1) ▼

! The controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the [Configuration Guide](#) before you configure this feature.

SNMP Manage

Location:

Contact:

Web Server

Layer-3 Accessibility: Enable

LLDP:

Use Site Settings

On

Off

Apply
Cancel

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 [4.3 Configure Wired Networks](#).

The management VLAN is a VLAN created to enhance the network security. Without Management VLAN, the configuration commands and data packets are transmitted in the same network. There are risks of unauthorized users accessing the management page and modifying the configurations. A management VLAN can separate the management network from the data network and lower the risks.

SNMP

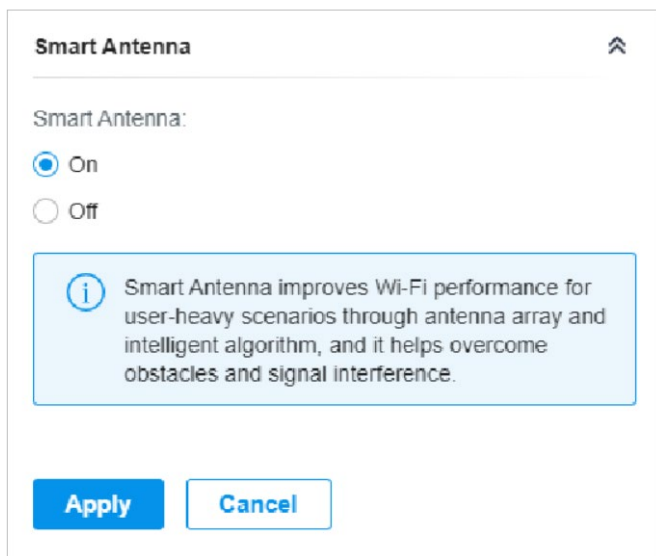
(Only for configuring a single device) Configure SNMP to write down the location and contact detail. You can also click [Manage](#) to jump to [Settings > Services > SNMP](#), and for detailed configuration of SNMP service, refer to [4.10.4 SNMP](#).

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

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.



The image shows a configuration dialog box titled "Smart Antenna". At the top right of the dialog is an upward-pointing arrow icon. Below the title, the text "Smart Antenna:" is followed by two radio button options: "On" (which is selected) and "Off". Below these options is a light blue information box with a circular icon containing the letter 'i'. The text inside the information box reads: "Smart Antenna improves Wi-Fi performance for user-heavy scenarios through antenna array and intelligent algorithm, and it helps overcome obstacles and signal interference." At the bottom of the dialog are two buttons: "Apply" and "Cancel".

■ 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.

Advanced

2.4GHz 5GHz

Load Balance

Maximum Associated Clients: Enable

(1-511)

RSSI Threshold: Enable ⓘ

(-95-0 dBm)

ETH Port Settings

ETH1 VLAN: Enable

(1-4094)

ETH2 VLAN: Enable

ETH3 VLAN: Enable

ETH3 PoE Out: Enable

QoS

Wi-Fi Multimedia (WMM): Enable ⓘ

No Acknowledgement: Enable ⓘ

Unscheduled Automatic Power Save Delivery: Enable ⓘ

OFDMA

OFDMA: Enable ⓘ

| | |
|---|--|
| 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 Wall Plate AP) Enable this function and add the corresponding AP's LAN port to the VLAN specified here. Then the hosts connected to this AP can only communicate with the devices in this VLAN. |
| ETH3 PoE Out | (Only for Wall Plate AP with the PoE out port) Enable this function to supply power to the connected device on this port. |
| Wi-Fi Multimedia (WMM) | With WMM enabled, the 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) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improve 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.

Manage Device ⤴

Custom Upgrade

Please choose the firmware file and upgrade the device.

[Browse](#)

Copy Configuration

Select another device at the current site to copy its configurations.

Please Select... ▼

[Copy](#)

Move to Site

Move this device to another site of this controller.

Please Select... ▼

[Move](#)

Force Provision

Click Force Provision to synchronize the configurations of the device with the controller. The device will be disconnected from the controller temporarily, and be adopted again to get the configurations from the controller.

[Force Provision](#)

Forget This Device

If you no longer wish to manage a device, you may forget it. After forgotten, the device will be removed from the controller and get reset.

[Forget](#)

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.

[Download](#)

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.

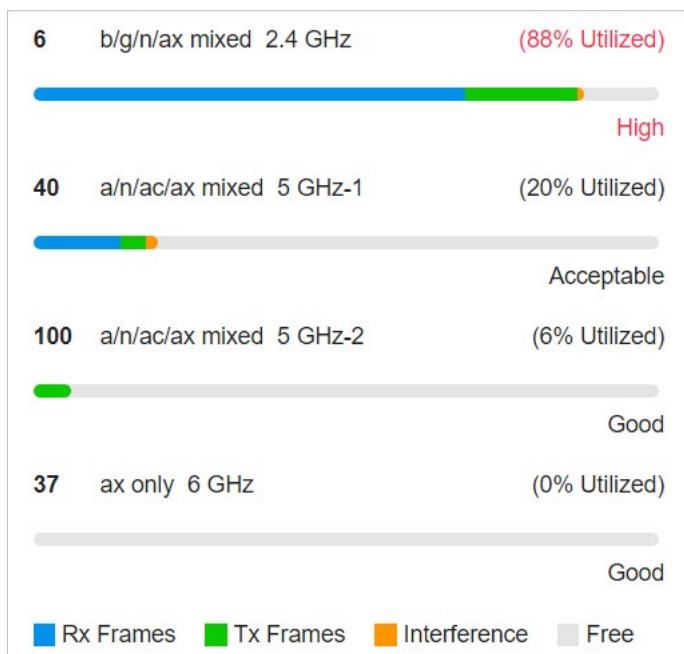
| | |
|--------------------------------------|--|
| Force Provision | (Only for configuring a single device) Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations 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. |
| | <p>Note:</p> <p>Firmware updates are required for earlier devices to obtain complete information.</p> |

6.4.2 Monitor APs

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

Monitor Panel

The monitor panel illustrates the active channel information on each radio band, including the 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) | 51% / 32% / 4% |
| Tx Pkts/Bytes | 4195 / 847.04 KB |
| Rx Pkts/Bytes | 24247 / 6.47 MB |
| Tx Error/Dropped | 0.0% / 0.0% |
| Rx Error/Dropped | 0.0% / 0.0% |

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

| Overview ⤴ | |
|---|-------------------------------------|
| MAC Address: | IP Address: |
| 40-3F-8C-00-01-10 | 192.168.0.100 |
| Model: | Firmware Version: |
| EAP690E HD(EU) v1.0 | 1.0.0 Build 20220708 Rel. 3 6560 |
| CPU Utilization: | Memory Utilization: |
| 4% | 22% |
| Uptime: | |
| -- | |

■ 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.

| LAN ⤴ | |
|--|------------|
| Rx Packets: | Rx Bytes: |
| 4724 | 936.73 KB |
| Rx Dropped Packets: | Rx Errors: |
| 0 | 0 |
| Tx Packets: | Tx Bytes: |
| 822 | 647.23 KB |
| Tx Dropped Packets: | Tx Errors: |
| 0 | 0 |

■ **Uplink (Wireless) (Only for devices in the Connected  status)**

Click [Uplink \(Wireless\)](#) to view the traffic information related to the uplink AP, including the signal strength, transmission rate, ratio of packets number and size, and dynamic downstream rate.

Uplink (Wireless)

| | |
|---|----------------|
| Uplink Device: | Signal: |
| CC-32-E5-F7-DD-1C | -22 dBm |
| Tx Rate: | Rx Rate: |
| 104Mbps | 526Mbps |
| Down Pkts/Bytes: | Up Pkts/Bytes: |
| 29 / 9.11 KB | 18 / 2.50 KB |
| Activity Speed:  | |
| 1.16 KB /s | |

■ 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.

Radios ⤴

2.4 GHz

5 GHz-1

5 GHz-2

6 GHz

| | |
|----------------------|----------------|
| Mode: | Channel Width: |
| 802.11b/g/n/ax mixed | 20/40MHz |
| Channel: | Tx Power: |
| 6 / 2437MHz | 20 |
| Rx Packets: | Rx Bytes: |
| 0 | 0 |
| Rx Dropped Packets: | Rx Errors: |
| 0 | 0 |
| Tx Packets: | Tx Bytes: |
| 2550 | 726.87 KB |
| Tx Dropped Packets: | Tx Errors: |
| 0 | 0 |

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.

| Name | MAC | SSID |
|--------------------------|-------------------|----------|
| Client_0 | 20-47-DA-2E-23-1D | EAP_test |
| Client_3 | 44-55-C4-06-EF-75 | EAP_test |
| Client_6 | D4-62-EA-B4-21-E8 | EAP_test |
| Client_9 | C0-9F-05-24-0C-EF | EAP_test |

Showing 1-4 of 4 records < 1 >

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.

| START TIME | END TIME | Name | MAC |
|--------------------------|--------------------------|----------|-------------------|
| Dec 20, 2020 01:10:46 am | Dec 20, 2020 01:10:46 am | Client_0 | 20-47-DA-2E-23-1D |
| Jan 21, 2021 03:34:29 am | Jan 21, 2021 03:34:29 am | Client_1 | 9C-28-F7-9B-9B-08 |
| Jan 24, 2021 03:52:33 pm | Jan 24, 2021 03:52:33 pm | Client_2 | A4-F1-E8-C2-FC-3F |

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

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

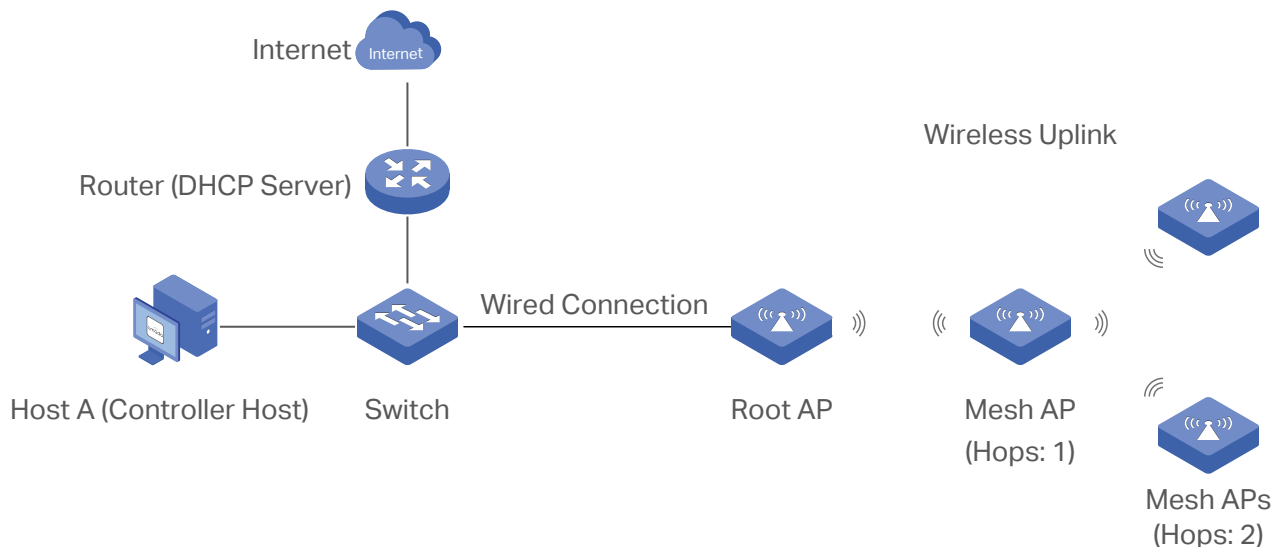
Mesh is used to establish a wireless network or expand a wired network through wireless connection on 5 GHz radio band. In practical application, it can help users to conveniently deploy APs without requiring Ethernet cable. After mesh network establishes, the APs can be configured and managed in the 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.

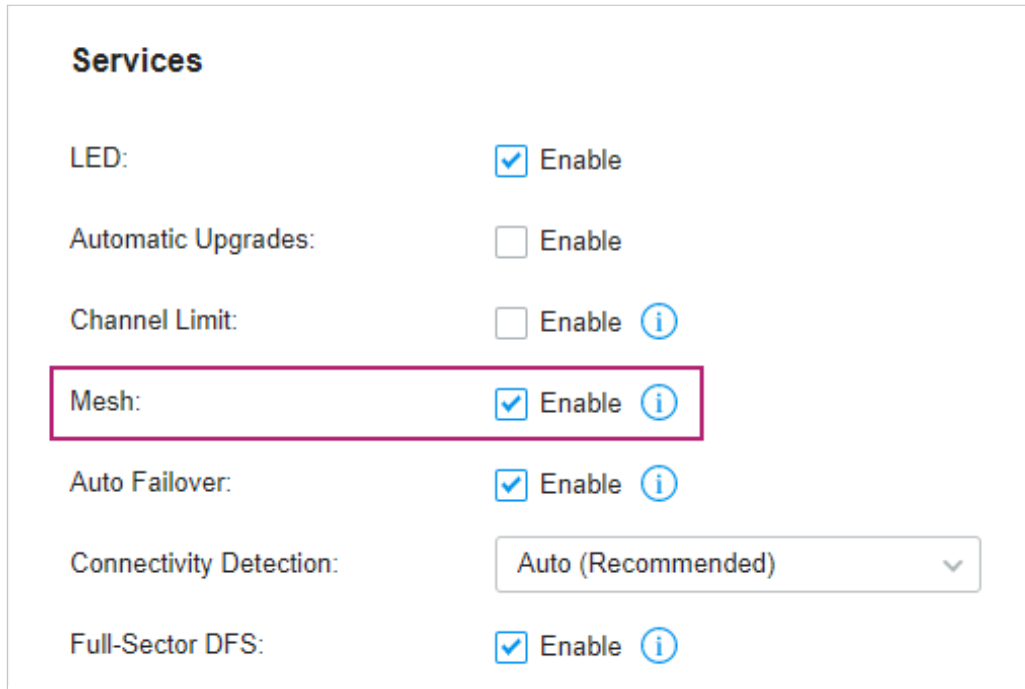


After all the APs are adopted, a mesh network is established. The APs connected to the network via wireless connection also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

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](#) 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.

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | ACTION |
|-------------------|---------------|-----------|-------------------------|---------|------------------|--------|
| 00-EA-DE-5B-E3-11 | 192.168.0.1 | CONNECTED | TL-R605 v1.0 | 1.0.0 | 24 days 21:57:58 | |
| 60-32-B1-8D-3D-F6 | 192.168.0.133 | CONNECTED | TL-SG2008 v3.0 | 3.0.0 | 8 days 04:36:20 | |
| EA-33-51-A8-22-A0 | 192.168.0.187 | CONNECTED | EAP225-Outdoor(EU) v1.0 | 5.0.0 | 1 days 05:09:10 | |


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


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 with the icon  in the controller. Click  to adopt the AP in Pending (Wireless) status in the [Devices](#) list.

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | ACTION |
|-------------------|---------------|---|-------------------------|---------|------------------|---|
| 00-EA-DE-5B-E3-11 | 192.168.0.1 | CONNECTED | TL-R605 v1.0 | 1.0.0 | 24 days 21:57:58 |  |
| 60-32-B1-8D-3D-F6 | 192.168.0.133 | CONNECTED | TL-SG2008 v3.0 | 3.0.0 | 8 days 04:36:20 |   |
| EA-23-51-06-22-52 | -- | PENDING  | EAP225-Outdoor v1.0 | -- | -- |  |
| EA-33-51-A8-22-A0 | 192.168.0.187 | CONNECTED | EAP225-Outdoor(EU) v1.0 | 5.0.0 | 1 days 08:23:27 |   |

Showing 1-4 of 4 records < 1 > 5 /page Go To page: GO

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) with the icon  within your controller.

- 2) For the AP that has been managed by the Controller before and cannot reach the gateway, it goes into Isolated status when it is discovered by controller again. Click  to connect the Uplink AP in the [Devices](#) list.

| DEVICE NAME | IP ADDRESS | STATUS | MODEL | VERSION | UPTIME | ACTION |
|-------------------|---------------|-----------|-------------------------|---------|------------------|---|
| 00-EA-DE-5B-E3-11 | 192.168.0.1 | CONNECTED | TL-R605 v1.0 | 1.0.0 | 24 days 21:49:55 |  |
| 60-32-B1-8D-3D-F6 | 192.168.0.133 | CONNECTED | TL-SG2008 v3.0 | 3.0.0 | 8 days 04:28:00 |   |
| EA-23-51-06-22-52 | 192.168.0.7 | ISOLATED | EAP225-Outdoor(EU) v1.0 | 5.0.0 | 0 days 00:02:53 |  |
| EA-33-51-A8-22-A0 | 192.168.0.187 | CONNECTED | EAP225-Outdoor(EU) v1.0 | 5.0.0 | 1 days 08:15:23 |   |


Showing 1-4 of 4 records < 1 > 5 /page Go To page: GO

The following page will be shown as below, click [Link](#) to connect the Uplink AP.

EA-23-51-06-22-... ISOLATED ✕ >

Details Mesh Config

Uplinks ⤴

| AP Name | Channel | Signal | ACTION |
|-------------------|---------|---------|---|
| EA-33-51-A8-22-A0 | 44 | -67 dBm | Link  |

Showing 1-1 of 1 records < 1 > [Rescan](#)

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.

Details Clients **Mesh** Config Tools Statistics

This AP is a wired AP currently

Downlinks

| AP Name | Signal |
|-------------------|---------|
| EA-23-51-06-22-52 | -68 dBm |

Showing 1-1 of 1 records 1

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.

Uplinks

| AP Name | Channel | Signal | Hop | Downlink | ACTION |
|-------------------|---------|---------|-----|----------|----------------------|
| CC-32-E5-F7-DD-1C | 36 | -46 dBm | 0 | 0 | |
| EA-23-51-06-22-52 | 36 | -40 dBm | 0 | 0 | Link |

Showing 1-2 of 2 records 1 [Rescan](#)



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 [4. 2. 2 Services](#).

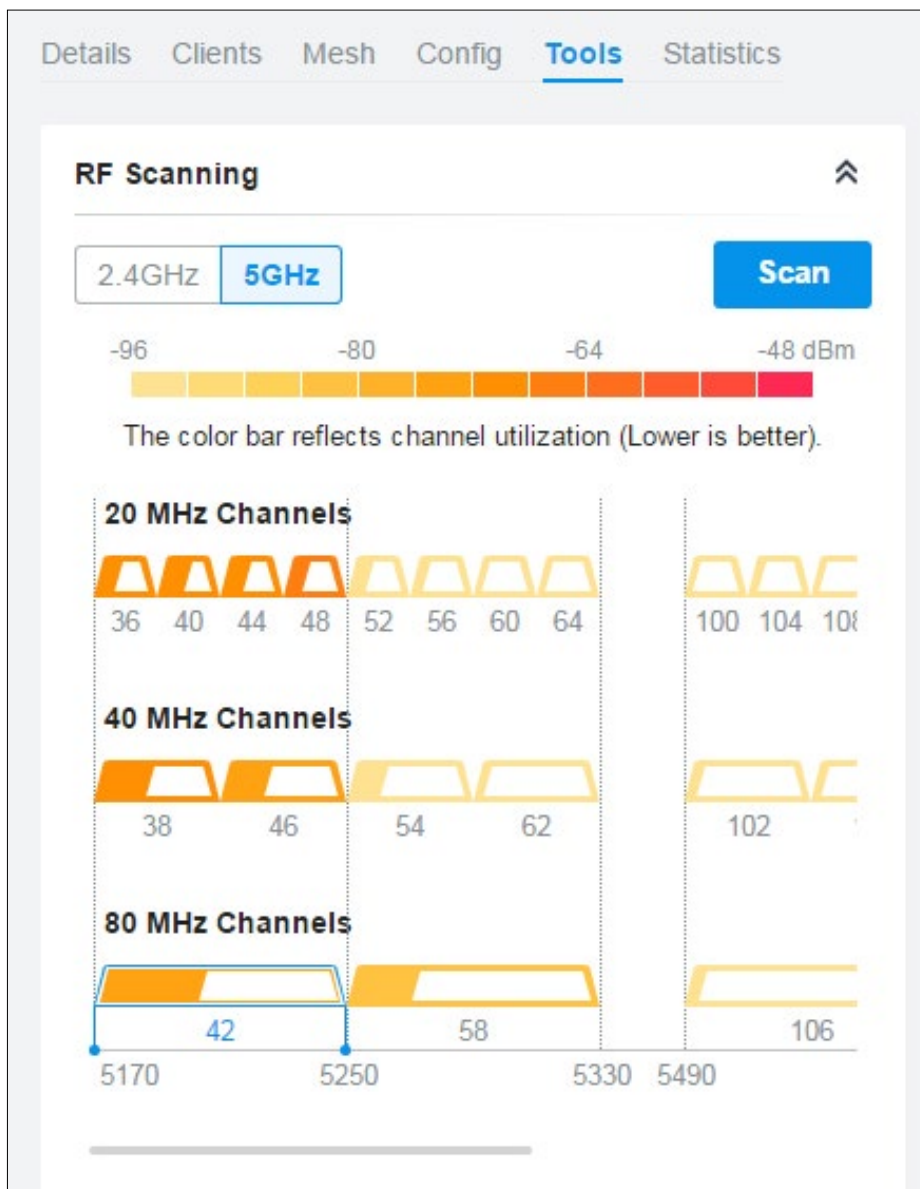
Tools

In Tools, you can enable RF Scanning to scan the RF (Radio Frequency) environments around the AP, which is useful for spectral analysis in channel selection and planning.

ⓘ Note:

- The RF scanning may take several minutes. During the scanning, all clients using this AP will be disconnected, and the AP will be offline. You should select a spare time of network to start scanning.
- The APs in the mesh network do not support RF Scanning.

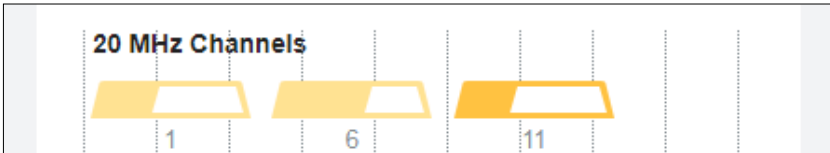
Select each frequency band to view and analyze the scan results.



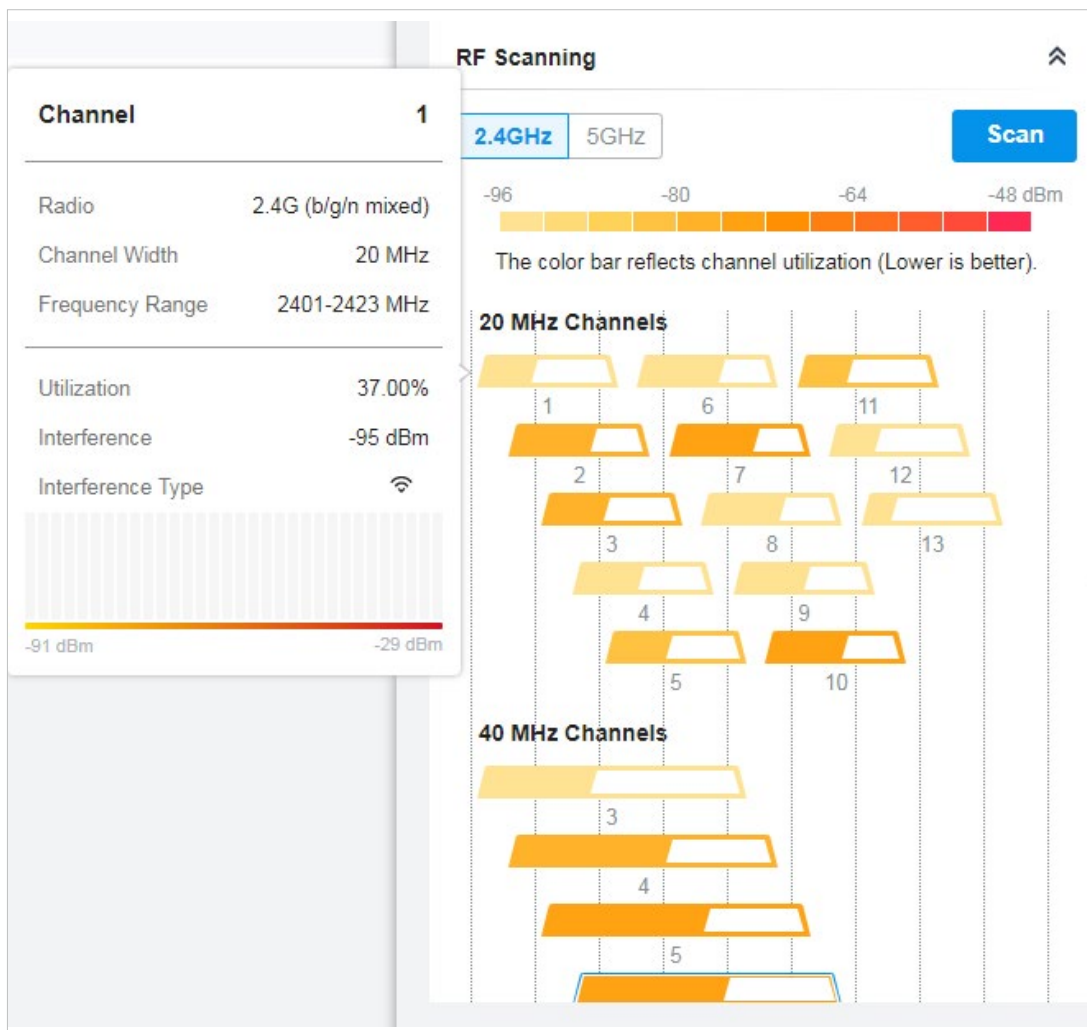
Each colored bar graph displays the information about channel utilization and interference on a channel. The filling area of the bar represents the channel utilization. And the larger filling area means the higher utilization, which indicates the channel is busier in transmitting data. The color shade represents the level of interference. And the legend is displayed at the top.

The results of different bands are displayed in different channel widths.

The number below the bar graph displays the corresponding channel number for each channel width option. For example, channels 42, 58 and 106 are three of the 80 MHz channels. And the channel outline in blue is in use currently.



You can hover the cursor over a channel option for more details.

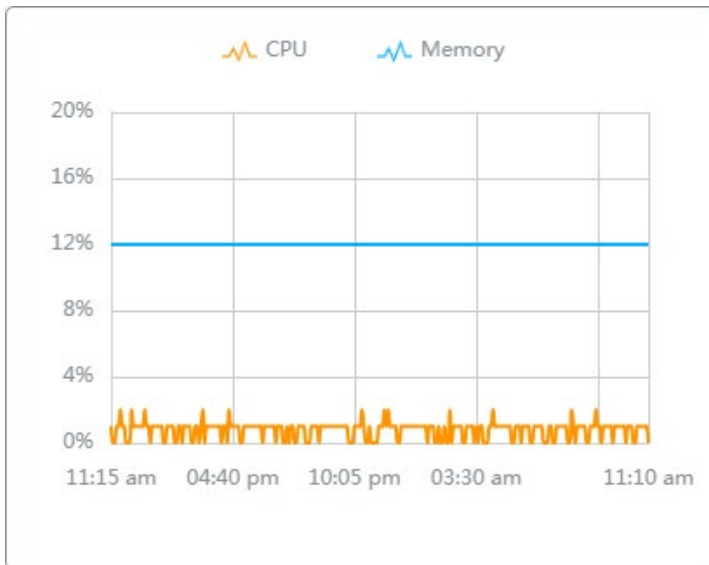


| | |
|------------------------|--|
| Radio | Displays the radio that the AP uses. |
| Channel Width | Displays the width of the channel. |
| Used Channels | Displays the channels in use. |
| Frequency Range | Displays the range of frequencies. |
| Utilization | Displays the percentage of the frequency range already in use. |

| | |
|-------------------|--|
| Interference | Displays the level of interference. |
| Interference Type | Displays the type of interface, including MWO (Microwave Oven), CW (Continuous Wave), WLAN (Wi-Fi signals) and FHSS (Frequency Hopping Spread Spectrum). |

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 [8.2 View the Statistics of the Network](#).



7

Monitor and Manage the Clients

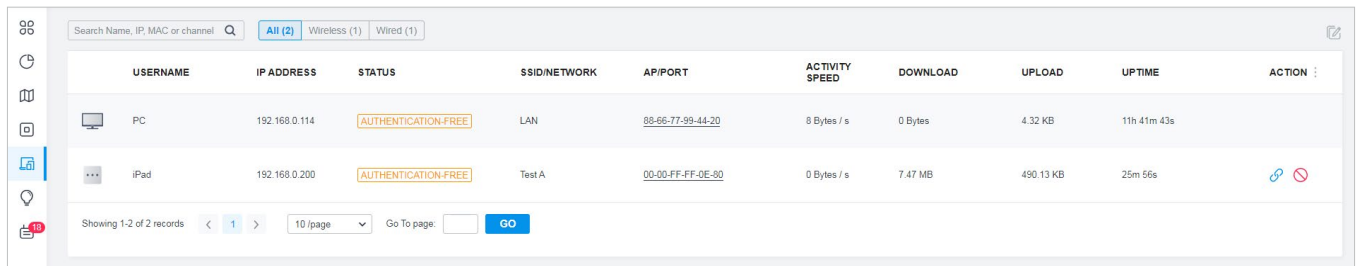
This chapter guides you on how to monitor and manage the clients through the Clients page using the clients table and the properties window and the Hotspot Manager system. To view clients that have connected to the network in the past, refer to [View the Statistics During the Specified Period with Insight](#).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

- [7.1 Manage Wired and Wireless Clients in Clients Page](#)
- [7.2 Manage Client Authentication in Hotspot Manager](#)

♥ 7.1 Manage Wired and Wireless Clients in Clients Page

7.1.1 Introduction to Clients Page

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



| USERNAME | IP ADDRESS | STATUS | SSID/NETWORK | API/PORT | ACTIVITY SPEED | DOWNLOAD | UPLOAD | UPTIME | ACTION |
|----------|---------------|---------------------|--------------|-------------------|----------------|----------|-----------|-------------|--|
| PC | 192.168.0.114 | AUTHENTICATION-FREE | LAN | 88-66-77-99-44-20 | 0 Bytes / s | 0 Bytes | 4.32 KB | 11h 41m 43s | |
| iPad | 192.168.0.200 | AUTHENTICATION-FREE | Test A | 00-00-FF-FF-0E-80 | 0 Bytes / s | 7.47 MB | 490.13 KB | 25m 56s | link refresh |

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

PENDING

The client has not passed the portal authentication and it is not connected to the internet.

AUTHORIZED

The client has been authorized and is connected to the internet.

CONNECTED

The client is connected to internet via non-portal network.


AUTHENTICATION-FREE


The client does not need to be authorized and it is connected to the internet.

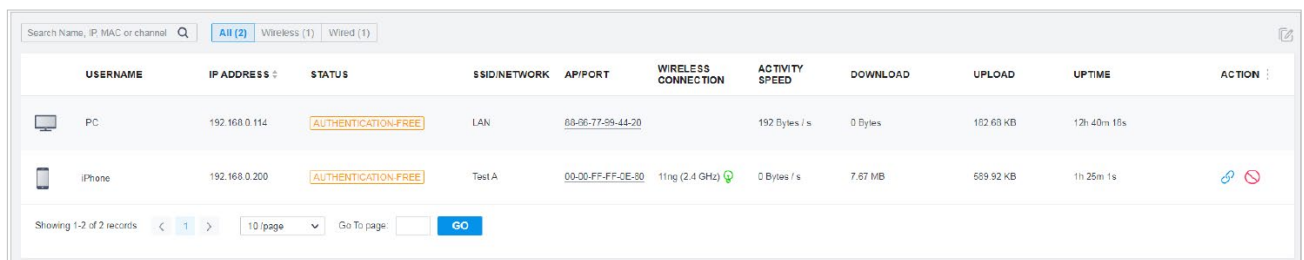
7.1.2 Using the Clients Table to Monitor and Manage the Clients


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

■ Customize the Information Columns


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

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



| USERNAME | IP ADDRESS | STATUS | SSID/NETWORK | API/PORT | WIRELESS CONNECTION | ACTIVITY SPEED | DOWNLOAD | UPLOAD | UPTIME | ACTION |
|----------|---------------|---------------------|--------------|-------------------|--|----------------|----------|-----------|-------------|--|
| PC | 192.168.0.114 | AUTHENTICATION-FREE | LAN | 88-66-77-99-44-20 | | 192 Bytes / s | 0 Bytes | 102.60 KB | 12h 40m 16s | |
| iPhone | 192.168.0.200 | AUTHENTICATION-FREE | Test A | 00-00-FF-FF-0E-80 | 11mg (2.4 GHz)  | 0 Bytes / s | 7.67 MB | 589.92 KB | 1h 25m 1s | link refresh |

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

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 or channel Q

Filter clients using the search box based on username, IP address, MAC address or channel.

All (2)

Wireless (1)

Wired (1)

Filter clients based on their connection type.

All (2)

2.4 GHz (0)

5 GHz (2)

(For wireless clients) Filter wireless clients based on the frequency band they are using.

All (2)

Users (0)

Guests (2)

(For wireless clients) Filter wireless clients based on the type of connected wireless network. Guests are clients connected to the guest network, which you can set during the [Quick Setup](#), [creating wireless networks](#), etc.

■ **Quick Operations**

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

Click to block the client in the chosen site. You can view blocked clients in [8. 5. 1 Known Clients](#).

(With portal authentication enabled) Click to manually authorize the client that has not passed the portal authentication.

(With portal authentication enabled) Click to unauthorize the client that has passed the portal authentication.

(For wireless clients) Click to reconnect the wireless client to the wireless network.


■ **Multiple Select for Batch Configuration**







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

| USERNAME | IP ADDRESS | STATUS | SSID/NETWORK | AP/PORT | ACTIVITY SPEED | DOWNLOAD | UPLOAD | UPTIME | ACTION |
|----------|---------------|---------------------|--------------|-------------------|----------------|----------|-----------|-------------|--------|
| PC | 192.168.0.114 | AUTHENTICATION-FREE | LAN | 88-66-77-99-44-20 | 192 Bytes / s | 0 Bytes | 182.68 KB | 12h 40m 18s | |
| iPhone | 192.168.0.200 | AUTHENTICATION-FREE | Test A | 00-00-FF-FF-0E-80 | 0 Bytes / s | 7.67 MB | 589.92 KB | 1h 25m 1s | |

Showing 1-2 of 2 records
< 1 >
10 /page
Go To page:
[GO](#)

7.1.3 Using the Properties Window to Monitor and Manage the Clients

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

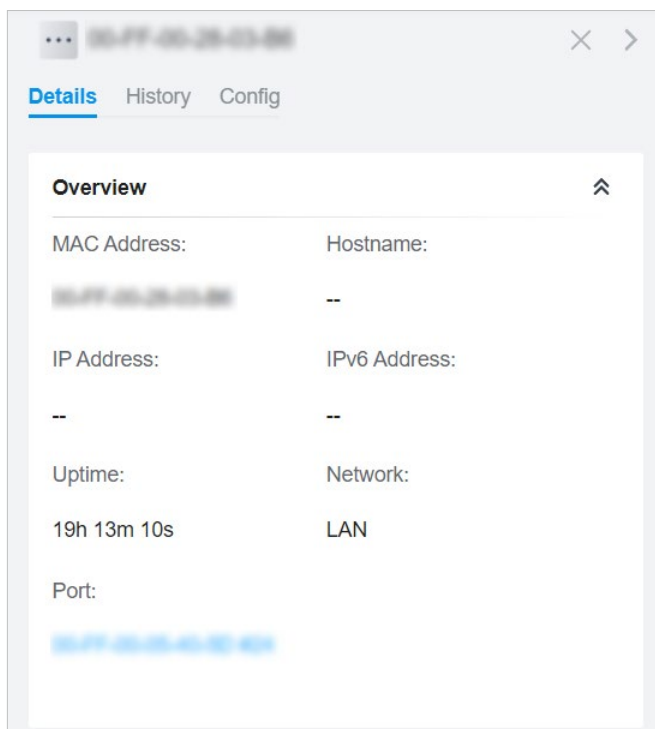
| | |
|---|--|
|  | Click to select multiple clients and add them to the Properties window for batch monitoring and management. |
|  | Click to minimize the Properties window to an icon. To reopen the minimized Properties window, click  . |
|  | Click to maximize the Properties window. You can also use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

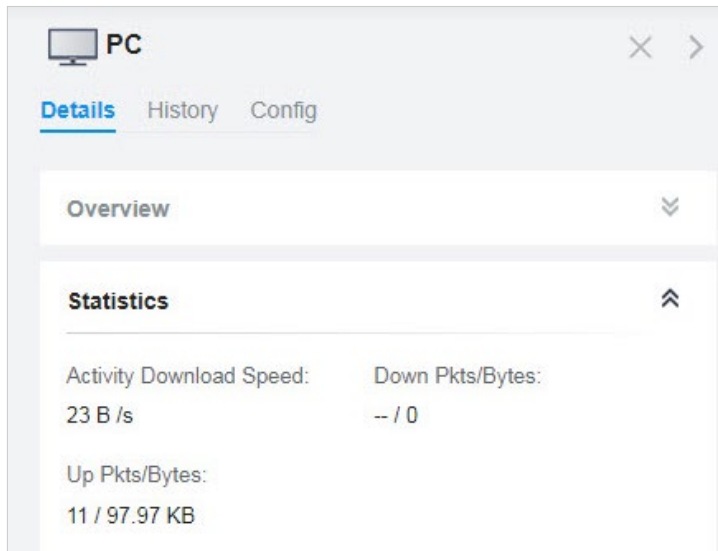
Monitor and Manage a Single Client

■ Monitor a Single Client

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

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

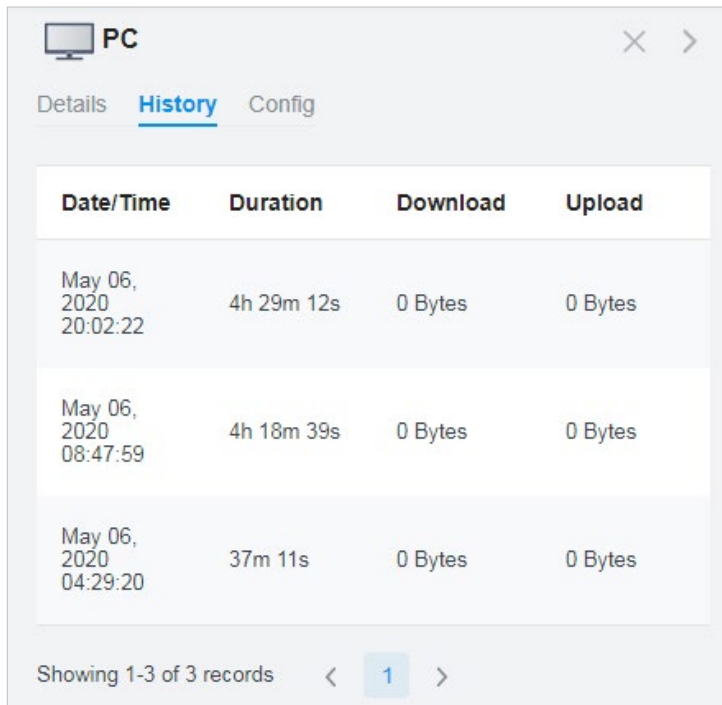




The screenshot shows a window titled "PC" with a close button and a right arrow. Below the title bar are three tabs: "Details" (selected), "History", and "Config". The "Overview" section is collapsed, and the "Statistics" section is expanded. The statistics are as follows:

| Activity | Value |
|-----------------|---------------|
| Download Speed | 23 B /s |
| Down Pkts/Bytes | -- / 0 |
| Up Pkts/Bytes | 11 / 97.97 KB |

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



The screenshot shows a window titled "PC" with a close button and a right arrow. Below the title bar are three tabs: "Details", "History" (selected), and "Config". The window displays a table of connection history records:

| Date/Time | Duration | Download | Upload |
|-----------------------|------------|----------|---------|
| May 06, 2020 20:02:22 | 4h 29m 12s | 0 Bytes | 0 Bytes |
| May 06, 2020 08:47:59 | 4h 18m 39s | 0 Bytes | 0 Bytes |
| May 06, 2020 04:29:20 | 37m 11s | 0 Bytes | 0 Bytes |

At the bottom, it says "Showing 1-3 of 3 records" with a pagination control showing "1" in a blue box, flanked by left and right arrows.

■ Manage a Single Client

In Config, you can configure the following parameters:

The screenshot shows a configuration window for a client with MAC address 00-FF-00-28-03-B6. The window has tabs for 'Details', 'History', and 'Config'. The 'Config' tab is active. The configuration options are as follows:

- Name:** 00-FF-00-28-03-B6
- Rate Limit:** Enable ⓘ
- Rate Limit:** Custom
- Download Limit:** Enable
- Download Limit:** 0 Kbps
- Upload Limit:** Enable
- Upload Limit:** 0 Kbps
- Use Fixed IP Address:** Enable ⓘ
- Network:** Please Select...
- IP Address:** . . .
- Lock To AP:** Enable ⓘ
- Select AP:** Please Select... ⓘ

At the bottom of the window are two buttons: 'Apply' and 'Cancel'.

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

Rate Limit Select an existing rate limit profile, create a new rate limit profile or customize the rate limit for the client.

Custom: Specify the download/upload rate limit based on needs.

Note: Rate Limit on this page is only available for the clients connected to the APs. To limit the rate of the clients connected to the gateway or switch, go to Bandwidth Control page.

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.

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 [4.3 Configure Wired Networks](#).

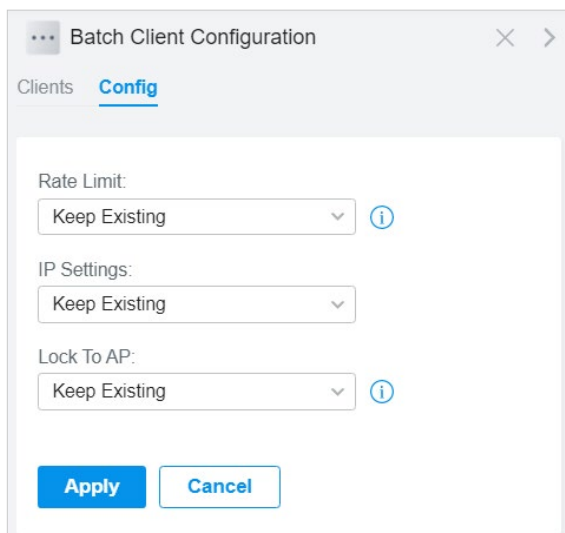
Note: A gateway is required for this function. Otherwise, you cannot set a fixed IP address for the client.

Lock To AP

Enable the function, and select one or multiple APs, then the client will be locked to the selected APs. This feature helps prevent a static client from roaming frequently between multiple APs.

Monitor and Manage Multiple Clients

To manage multiple clients at the same time, click , select multiple clients, and click [Edit Selected](#). Then you can configure the following parameters under the Config tab.



Batch Client Configuration

Clients **Config**

Rate Limit:
Keep Existing ⓘ

IP Settings:
Keep Existing

Lock To AP:
Keep Existing ⓘ

Apply Cancel

Rate Limit

Select an existing rate limit profile, create a new rate limit profile or customize the rate limit for the clients.

Keeping Existing: The rate limit of the chosen clients will remain their current settings.

Custom: Specify the download/upload rate limit based on needs.

Disabled: The rate limit of the chosen clients will be disabled.

Note: Rate Limit on this page is only available for the clients connected to the APs. To limit the rate of the clients connected to the gateway or switch, go to Bandwidth Control page.

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.

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 [4.3 Configure Wired Networks](#). Note that a gateway is required for this function. Otherwise, you cannot set fixed IP addresses for the chosen clients.

Lock To AP

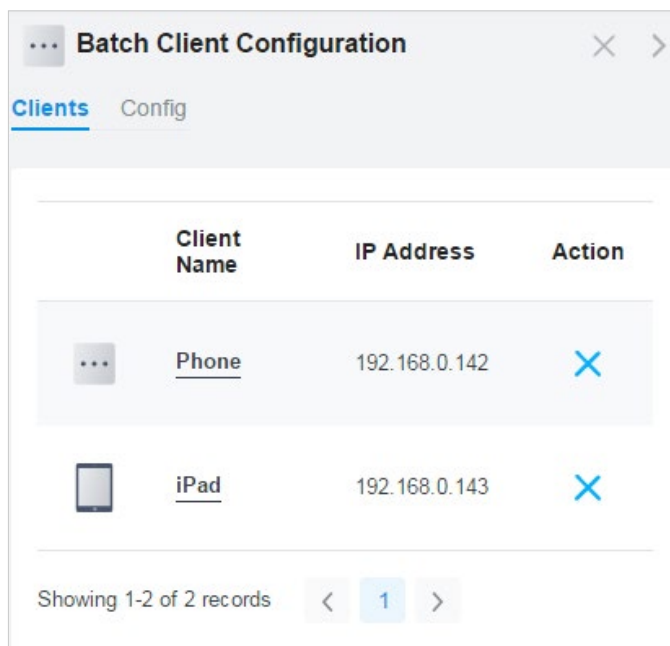
Lock to AP helps prevent static clients from roaming frequently between multiple APs.

Keeping Existing: Keep the current settings of the chosen clients.





Disabled: Disable Lock to AP of the chosen clients.

Enable: Enable Lock to AP, and select one or multiple APs, then the chosen clients will be locked to the selected APs.

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



The screenshot shows a window titled "Batch Client Configuration" with a "Clients" tab selected. The table below lists two clients: "Phone" and "iPad". Each client has an icon, a name, an IP address, and an "Action" column with a blue "X" icon for removal.


| Client Name | IP Address | Action |
|---|---------------|---|
|  Phone | 192.168.0.142 |  |
|  iPad | 192.168.0.143 |  |

Showing 1-2 of 2 records < 1 >

♥ 7.2 Manage Client Authentication in Hotspot Manager

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

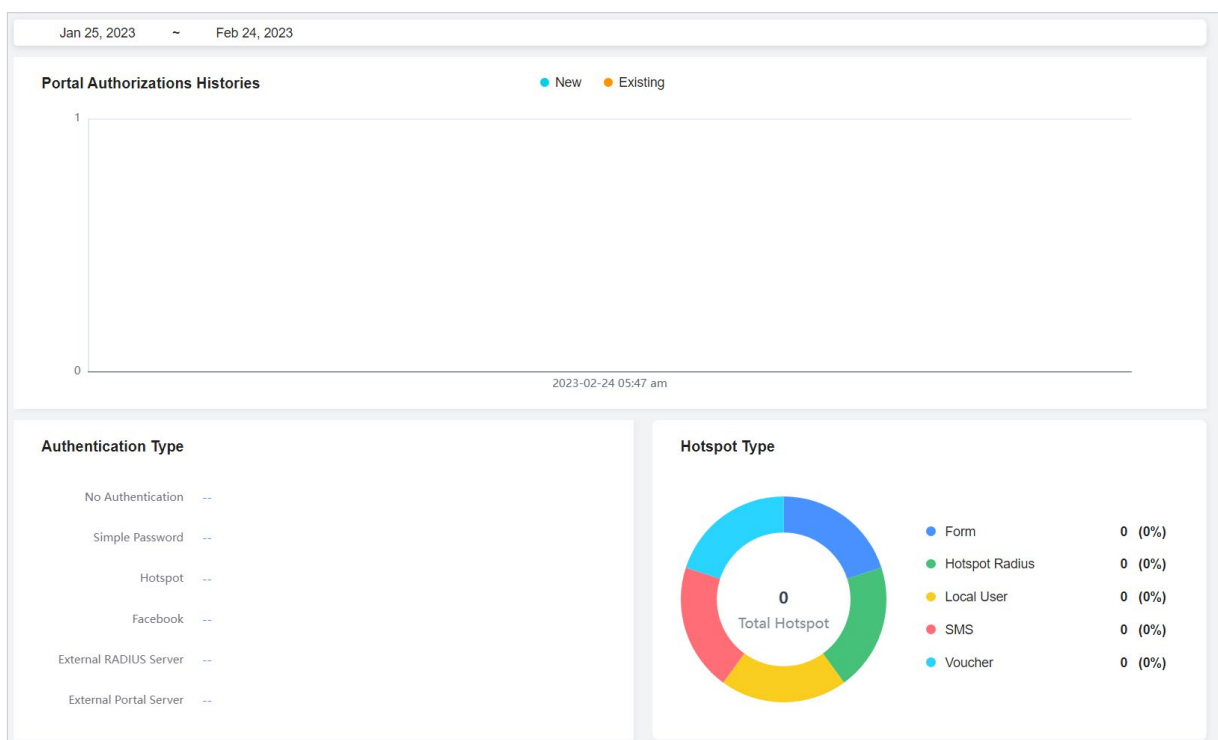
| | |
|------------------------------------|--|
| Dashboard | Monitor portal authorizations at a glance through different visualizations. |
| Authorized Clients | View the records of the connected and expired portal clients. |
| Vouchers | Create vouchers for Portal authentication, and view and manage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

To access the system, click [Hotspot Manager](#) from the drop-down list of [Organization](#). To log out of the system, click the account icon  at the upper-right corner, then click [Log Out](#).

7.2.1 Dashboard

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

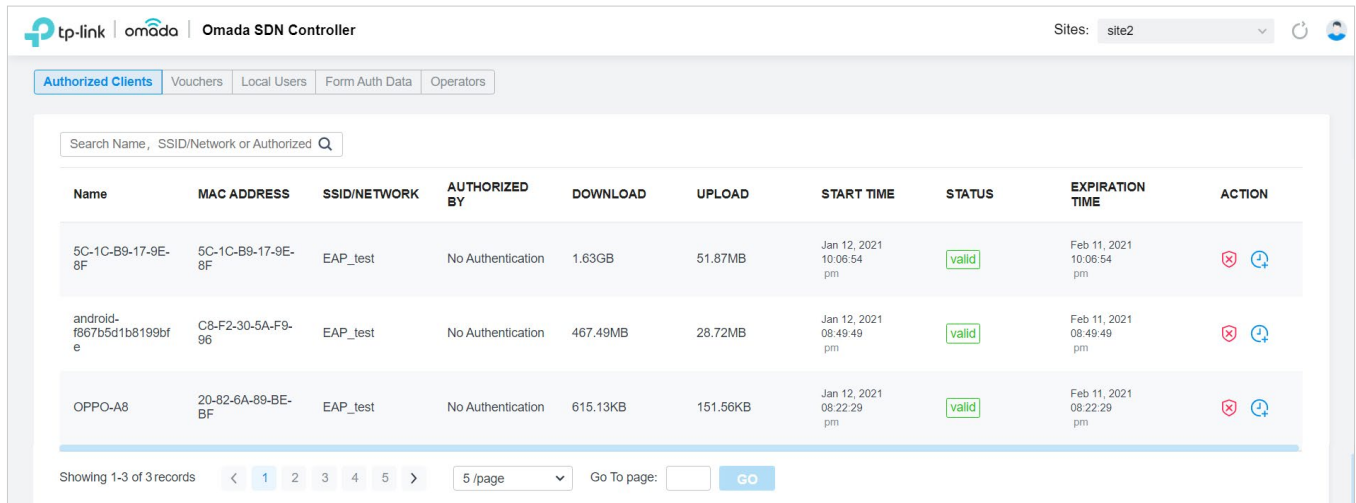
To open the dashboard, click [Hotspot Manager](#) from the drop-down list of [Organization](#) and click [Dashboard](#) in the pop-up page. Specify the time period to view portal authorization histories.









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 Manager](#) from the drop-down list of [Organization](#) and click [Authorized Clients](#) in the pop-up page. You can search certain clients using the search box, view their detailed information in the table, and manage them using the action column.



| Name | MAC ADDRESS | SSID/NETWORK | AUTHORIZED BY | DOWNLOAD | UPLOAD | START TIME | STATUS | EXPIRATION TIME | ACTION |
|--------------------------|-------------------|--------------|-------------------|----------|----------|--------------------------|--------|--------------------------|---|
| 5C-1C-B9-17-9E-8F | 5C-1C-B9-17-9E-8F | EAP_test | No Authentication | 1.63GB | 51.87MB | Jan 12, 2021 10:06:54 pm | valid | Feb 11, 2021 10:06:54 pm |   |
| android-f867b5d1b8199bfe | C8-F2-30-5A-F9-96 | EAP_test | No Authentication | 467.49MB | 28.72MB | Jan 12, 2021 08:49:49 pm | valid | Feb 11, 2021 08:49:49 pm |   |
| OPPO-A8 | 20-82-6A-89-BE-BF | EAP_test | No Authentication | 615.13KB | 151.56KB | Jan 12, 2021 08:22:29 pm | valid | Feb 11, 2021 08:22:29 pm |   |

Showing 1-3 of 3 records < 1 2 3 4 5 > 5 /page Go To page:



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 Vouchers

The Vouchers tab is used to create vouchers and manage unused voucher codes. With voucher configured and codes created, you can distribute the voucher codes generated by the controller to clients for them to access the network via portal authentication. For detailed configurations, refer to [4.9.1 Portal](#).

Create vouchers

Follow the steps below to create vouchers for authentication:

1. Click [Hotspot Manager](#) from the drop-down list of [Organization](#) and click [Vouchers](#) in the pop-up page.

- Click **+Create Vouchers** on the lower-left, and the following window pops up. Configure the following parameters and click **Save**.

Create Vouchers

Portal:

Code Length: (6-10)

Amount: (1-500)

Type: Limited Usage Counts (1-999) ⓘ
 Limited Online Users

Duration Type: Voucher Duration ⓘ
 Client Duration ⓘ

Duration:

ⓘ Download Limit, Upload Limit, and 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 page.

Rate Limit:

Download Limit: Enable Kbps (1-10485760)

Upload Limit: Enable Kbps (1-10485760)

Traffic Limit: Enable ⓘ Limit traffic to MB (1-10485760)

Description: (Optional)

| | |
|----------------------|---|
| 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. |
| Amount | Specify the number of voucher codes you want to create. |
| Type | <p>Select a type to limit the usage counts or the number of authorized users of a voucher code.</p> <p>Limited Usage Counts: The voucher code can only be used for a limited number of times within its valid period.</p> <p>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.</p> |
| Duration Type | Specify whether to limit the voucher duration or client duration. |

| | |
|-------------------------------|---|
| 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 . |
| Description (optional) | Enter notes for the created voucher code(s), and the input description is displayed in the voucher list under the voucher tab. |

3. The voucher codes are generated and displayed in the table.

| <input type="checkbox"/> | Code | Created Time | DOWNLOAD | UPLOAD | TRAFFIC | Notes | Duration | Type | PORTAL | Action |
|--------------------------|--------|--------------------------------|------------|------------|---------|-------|------------|------|----------------|--------|
| <input type="checkbox"/> | 809532 | Feb 07, 2021 05:28:07 pm | 23.00 Kbps | 22.00 Mbps | | | 8.00 Hours | 1 | Portal_Default | |
| <input type="checkbox"/> | 550740 | Feb 07, 2021 09:28:07 pm | 23.00 Kbps | 22.00 Mbps | | | 8.00 Hours | 1 | Portal_Default | |
| <input type="checkbox"/> | 249399 | Feb 07, 2021 05:28:07 pm | 23.00 Kbps | 22.00 Mbps | | | 8.00 Hours | 1 | Portal_Default | |
| <input type="checkbox"/> | 667766 | Feb 07, 2021 09:28:07 pm | 23.00 Kbps | 22.00 Mbps | | | 8.00 Hours | 1 | Portal_Default | |
| <input type="checkbox"/> | 866876 | Feb 07, 2021 05:28:07 pm | 23.00 Kbps | 22.00 Mbps | | | 8.00 Hours | 1 | Portal_Default | |

Select 0 of 5 items [select all](#) Showing 1-5 of 5 records < 1 > 10 /page Go To page: [GO](#)




[+ Create Vouchers](#)





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.



The voucher code can only be used for a limited number of times within its valid period. The number on the right shows the limited number of authentication times.

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

| | |
|---|---|
| 307690 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> | 084520 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> |
| 924665 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> | 232608 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> |
| 701945 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> | 473875 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> |
| 141716 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> | 999934 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> |
| 825813 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> | 180815 <u>Valid for 8h</u> <u>Limited Usage Counts One</u> |

5. Distribute the vouchers to clients, and then they can use the codes to pass authentication. If a voucher code expires, it will be automatically removed from the list.
6. To delete certain vouchers manually, click  to delete a single voucher, or  [Delete](#) to delete multiple voucher codes at a time.

7.2.4 Local Users

The Local Users tab is used to create user accounts for authentication. With the Local User configured, clients are required to enter the username and password to pass the authentication. You can create multiple accounts and assign them to different users. For detailed configurations, refer to [4.9.1 Portal](#).

Create Local Users

There are two ways to create local user accounts: create accounts on the page and import from a file. To create local user accounts, follow the steps below.

1. Click [Hotspot Manager](#) from the drop-down list of [Organization](#) and click [Local Users](#) in the pop-up page.
2. Create Local User accounts through two different ways.

■ Create Local User accounts

Click [+Create User](#) on the lower-left, and the following window pops up. Configure the following parameters and click [Save](#).

Create User

Portal:

Username:

Password:

Status: Enable

Authentication Timeout:

MAC Address Binding Type:

Maximum Users: (1-2048)

Name: (Optional)

Telephone: (Optional)

! Download Limit, Upload Limit, and 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 page.

Rate Limit:

Download Rate Limit: Enable Kbps (1-10485760)

Upload Rate Limit: Enable Kbps (1-10485760)

Traffic Limit: Enable Limit traffic to MB (1-10485760)

Portal

Select the portal for which the local users will take effect.

Username

Specify the username. The username should be different from the existing ones, and it is not editable once it is created.

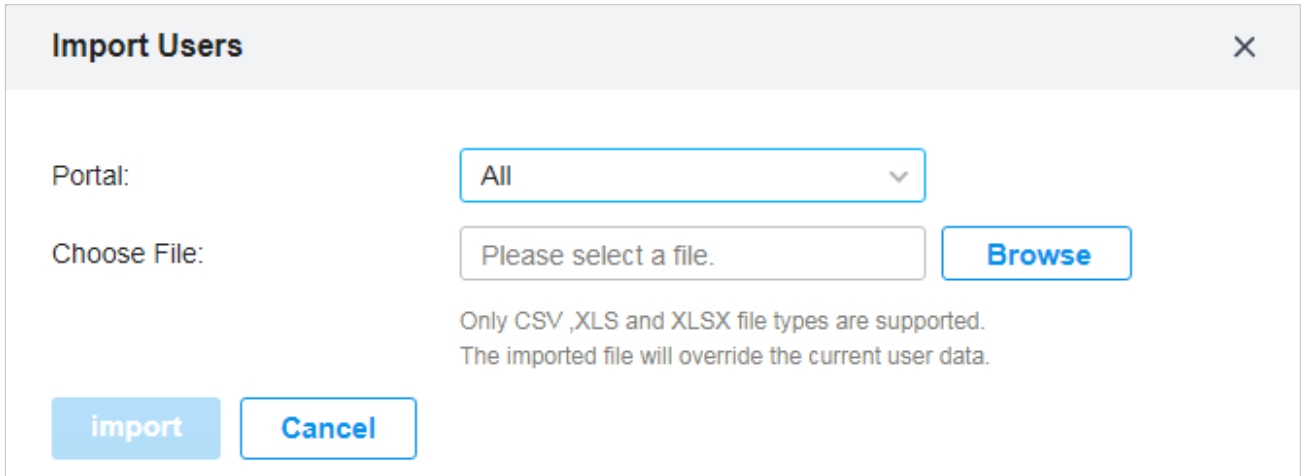
Password

Specify the password. Local users are required to enter the username and password to pass authentication and access the network.

| | |
|---------------------------------|---|
| Status | When the status is enabled, it means the user account is valid. You can disabled the user account, and enable it later when needed. |
| Authentication Timeout | Specify the authentication timeout for local users. After timeout, the users need to log in again on the authentication page to access the network. |
| MAC Address Binding Type | <p>There are three types of MAC binding: No Binding, Static Binding and Dynamic Binding.</p> <p>No Binding: No MAC address is bound to the local user account.</p> <p>Static Binding: Bind a MAC address to this user account manually. Then only the user with the this MAC address can use the username and password to pass the authentication.</p> <p>Dynamic Binding: The MAC address of the first user that passes the authentication will be bound to this account. Then only this user can use the username and password to pass the authentication.</p> |
| Maximum Users | Specify the maximum number of users that can use this account to pass the authentication. |
| Name (optional) | Specify a name for identification. |
| Telephone (optional) | Specify a telephone number for identification. |
| Rate Limit | <p>Select an existing rate limit profile, create a new rate limit profile or customize the rate limit for the local users.</p> <p>Custom: Specify the download/upload rate limit based on needs.</p> |
| Download/Upload Limit | <p>Click the checkbox and specify the rate limit for download/upload for users of the local user account. The value of the download/upload rate can be set in Kbps or Mbps.</p> <p>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.</p> |
| Traffic Limit | <p>Click the checkbox and specify the daily/weekly/monthly/total traffic limit for the local user account, and the value of the traffic limit can be set in MB or GB. Once the limited is reached, the user(s) can no longer access the network using this account.</p> <p>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.</p> |

■ **Create Local User accounts from files.**

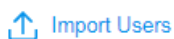
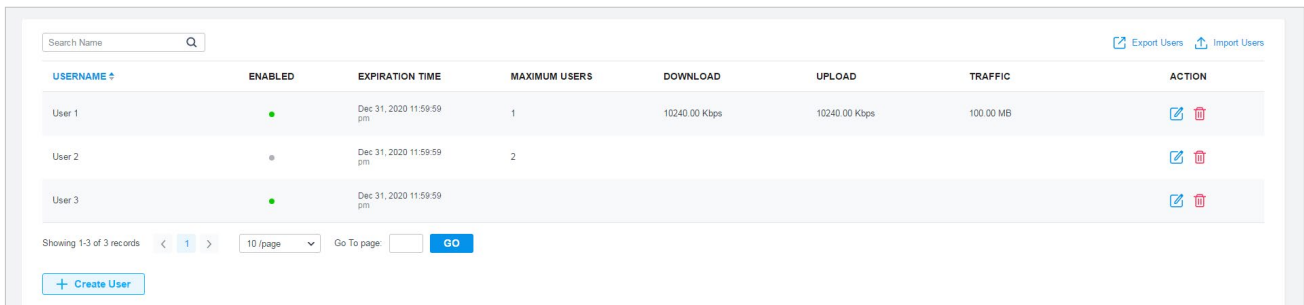
Click [Import Users](#) on the upper-right, and the following window pops up. Select a file in the format of CVS or Excel, and click **Import**. To see required parameters and corresponding explanation, refer to [Create Local User accounts](#). Note that the imported file will override the current user data.



Portal

Select the portal to which the local users will be imported.

3. The local user account(s) will be created and displayed in the module. You can view the information of the created local users, search certain accounts through the name, and use icons for management.



Click to add local user(s) from files in the format of CVS or Excel. It is recommended when you need to create local users in batches. Select the portals based on needs, and the local users will be imported to the chosen portal.

Note that the imported file will override the current user data.



Click to export the local user(s) to files in the format of CVS or Excel. Select the portals based on needs, and the local users of the chosen portal will be exported.



Click to edit the parameters for the local user.



Click to delete the local user.


7.2.5 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 Manager](#) from the drop-down list of [Organization](#) and click [Form Auth Data](#) in the pop-up page.
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  for more management options.

| FORM AUTH NAME | PORTAL | CREATED TIME | RESPONSES | ACTION |
|-----------------------------------|---------------------------|--------------------------|-----------|---|
| Survey 1 Published | ● Not in Use | Aug 15, 2023 01:32:34 am | 0 |    |
| Survey 2 Unpublished | ● Not in Use | Aug 15, 2023 01:33:18 am | 0 |    |

7.2.6 Operators

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


Create Operators


To create operator accounts, follow the steps below.

1. Click [Hotspot Manager](#) from the drop-down list of [Organization](#) and click [Operators](#) in the pop-up page.
2. Click [Create Operator](#) on the lower-left, and the following window pops up.


Create Operator

Username:

Password: 


Role: Admin 







Description: (Optional)

Site Privileges: Please Select... 

Save
Cancel

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.



| USERNAME | PASSWORD | ROLE | NOTES | ACTION |
|------------|---|--------|------------|---|
| Operator 1 |  | Admin | for site 1 |   |
| Operator 2 |  | Viewer | for site 2 |   |

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

+ Create Operator

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



Monitor the Network

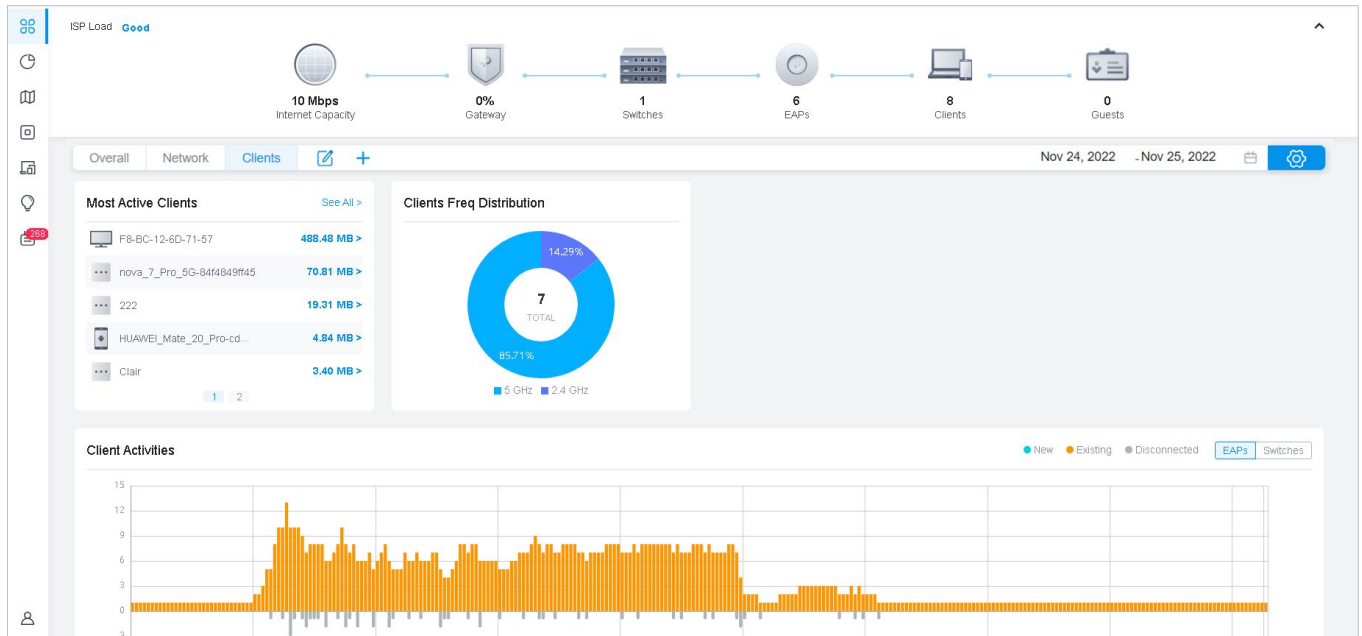
This chapter guides you on how to monitor the network devices, clients, and their statistics. Through visual and real-time presentations, the SDN Controller keeps you informed about the accurate status of the managed network. This chapter includes the following sections:

- [8.1 View the Status of Network with Dashboard](#)
- [8.2 View the Statistics of the Network](#)
- [8.3 Monitor the Network with Map](#)
- [8.4 Monitor the Network with Reports](#)
- [8.5 View the Statistics During Specified Period with Insight](#)
- [8.6 View and Manage Logs](#)
- [8.7 Monitor the Network with Tools](#)

8.1 View the Status of Network with Dashboard

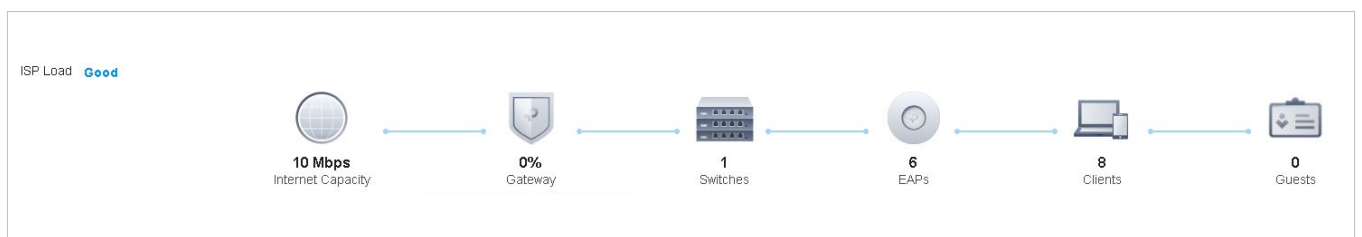
8.1.1 Page Layout of Dashboard

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

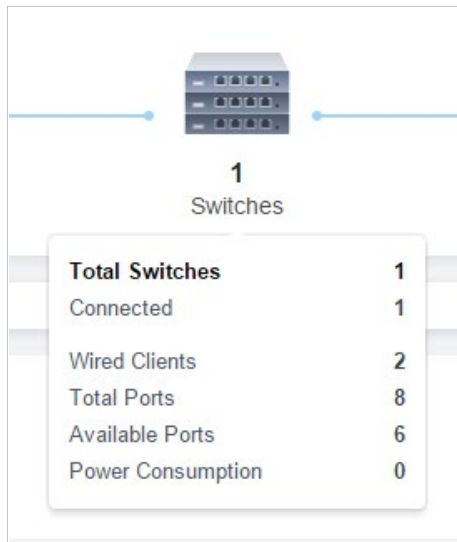


Topology Overview

Topology Overview on the top shows the status of ISP Load and numbers of devices, clients and guests. ISP Load has four statuses: Unknown, Good, Medium, Poor.

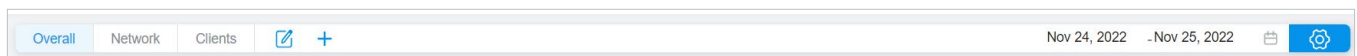


You can hover the cursor over the gateway, switch, AP, client or guest icons to check their status. For detailed information, click the icon here to jump to the [Devices](#) or [Clients](#) section.







Tab Bar

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




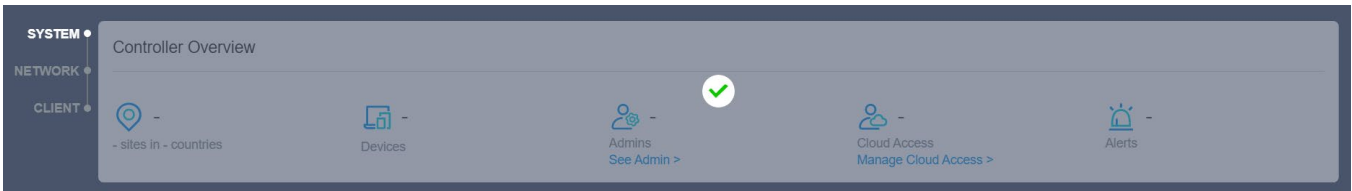
| | |
|--------------------------|---|
| Overview | Displays Controller Overview and Association Failures by default. |
| Network | Displays Alerts, Wi-Fi Traffic Distribution, Wi-Fi Summary and Traffic Activities by default. |
| Clients | Displays Most Active Clients, Clients Freq Distribution, and Client Activities by default. |

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

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

8.1.2 Explanation of Widgets

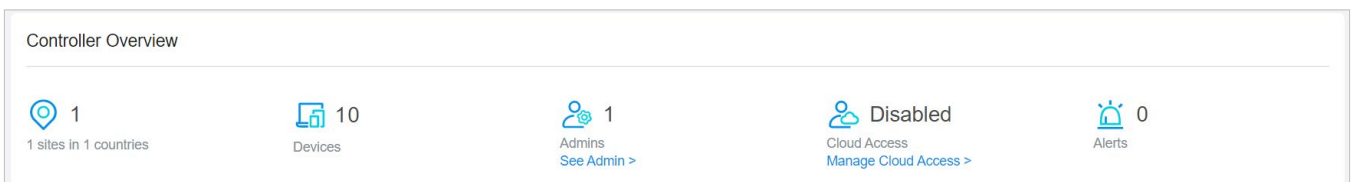
The widgets are divided into three categories: [System](#), [Network](#) and [Client](#). You can click the  icon to add or remove the widgets.



| | |
|-------------------------|--|
| System | Controller Overview |
| Network | Alerts, ISP Load, VPNs, Most Active EAPs, Most Active Switches, Wi-Fi Traffic Distribution, Wi-Fi Summary, Switching Summary, Traffic Distribution, Client Distribution, Traffic Activities, Retried Rate/Dropped Rate, Top Devices Usage, PoE Utilization, Top Interference |
| Client | Most Active Clients, Longest Client Uptime, Clients Freq Distribution, Client Activities, Clients Association Activities, Association Failures, Clients SSID Distribution, Clients with on Boarding Times, Clients with RSSI |

System

The Controller Overview widget in System displays the general information about the controller, including sites, devices, Admin accounts, Cloud Access, and alerts. You can click [See Admin](#) to view and manage Admin accounts, or click [Manage Cloud Access](#) to configure cloud access. For details, refer to [9 Manage Accounts of the SDN Controller](#).



Network

Widgets in Network use lists and charts to illustrate the traffic status of wired and wireless networks in the site, including traffic statistics, the most active devices, VPN connection, distribution, **PoE utilization**, and interference.

■ Alerts

The Alerts widget displays the total number of unarchived alerts happened in the site and details of the latest five. To view all the alerts and archive them, click [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 [8.6 View and Manage Logs](#).

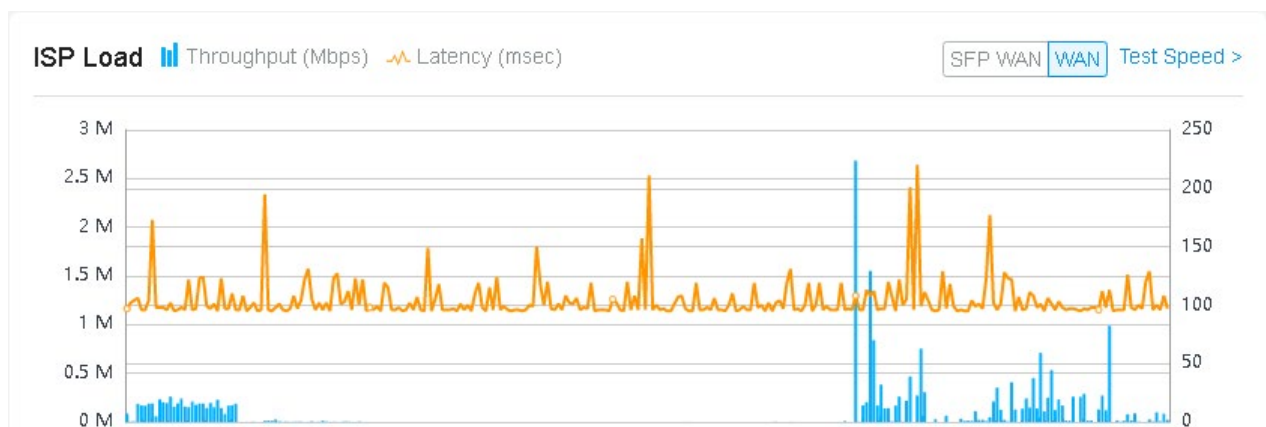
Alerts See All >

11 Alerts

- 2022-05-28 09:35:03 am ⚙ CC-32-E5-A4-B1-AC detected Ping of Death attack and dropped 2 packets.
- 2022-05-28 07:33:17 am ⚙ CC-32-E5-A4-B1-AC detected Ping of Death attack and dropped 16 packets.
- 2022-05-27 07:25:20 pm ⚙ CC-32-E5-A4-B1-AC detected Ping of Death attack and dropped 16 packets.
- 2022-05-27 07:07:15 pm ⚙ CC-32-E5-A4-B1-AC detected Ping of Death attack and dropped 16 packets.

■ 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 [8.2 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

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

| L2TP/PPTP VPN | | | | | IPsec VPN | | | |
|---|--------|---------|-----------------|-----------------|---|--------|----------------------------|----------------------------------|
| NAME | STATUS | TUNNELS | AVERAGE TX DATA | AVERAGE RX DATA | NAME | STATUS | TUNNEL ID | DATA FLOW |
| ppIp | ● | 3 | 24.59 KB | 23.68 KB | VPN1 | ● | 192.168.0.1 192.168.0.2 | 192.168.2.0/24 192.168.1.0/24 |
| l2tp | ● | 3 | 7.96 KB | 50.15 KB | VPN2 | ● | 192.168.1.1 192.168.1.2 | 192.168.2.0/24 192.168.1.0/24 |
| < 1 > Go To page: <input type="text"/> GO | | | | | < 1 2 > Go To page: <input type="text"/> GO | | | |

| OpenVPN | | | | SSL VPN | | | |
|---|--------|---------|---------------------------|---|--------|---------------|---------------------------|
| NAME | STATUS | TUNNELS | STATISTICS | NAME | STATUS | LOGIN IP | STATISTICS |
| VPN1 | ● | 2 | ↑ 0.00 Bytes ↓ 9.77 KB | VPN1 | ● | 192.168.55.33 | ↑ 0.00 Bytes ↓ 9.77 KB |
| VPN2 | ● | 2 | ↑ 953.67 MB ↓ 9.77 KB | VPN2 | ● | 192.168.55.33 | ↑ 953.67 MB ↓ 9.77 KB |
| VPN3 | ● | 2 | ↑ 0.00 Bytes ↓ 0.00 Bytes | VPN3 | ● | 192.168.55.33 | ↑ 0.00 Bytes ↓ 0.00 Bytes |
| VPN4 | ● | 2 | ↑ 9.54 MB ↓ 9.77 KB | VPN4 | ● | 192.168.55.33 | ↑ 9.54 MB ↓ 9.77 KB |
| < 1 2 > Go To page: <input type="text"/> GO | | | | < 1 2 > Go To page: <input type="text"/> GO | | | |

Name Displays the name of VPN server/client.

Status Displays the connection status of VPN server/client.

Tunnels Displays the number of VPN tunnels for the VPN server.

Average Tx Data Displays the average transmitted traffic of the VPN server/client.

Average Rx Data Displays the average received traffic of the VPN server/client.

Statistics Displays the upstream and downstream traffic of the VPN server/client.

Login IP Displays the login IP of the SSL VPN.

Tunnel ID Displays the direction of the IPsec VPN tunnel.

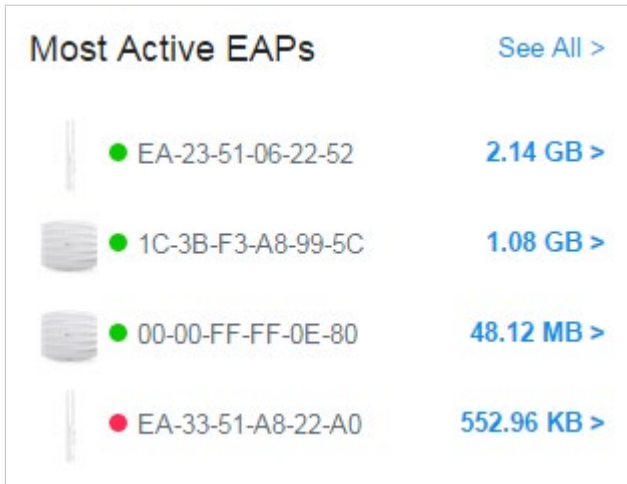
Data Flow Displays the data flow of the IPsec VPN tunnel.

■ Most Active EAPs/Most Active Switches

These two widgets can display, respectively, 15 most active EAPs and switches in the site based on the total number of traffic within the time range. Only the devices that has been adopted by the controller will be displayed.

To view all the devices discovered by the controller, click [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 [6 Configure and Monitor Controller-Managed Devices](#).



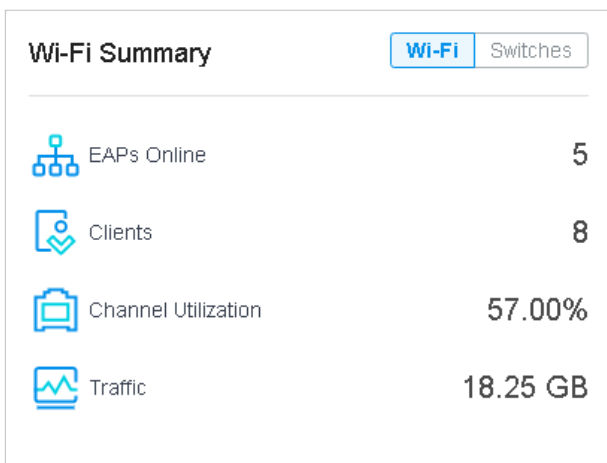
■ **Wi-Fi Traffic Distribution**

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.



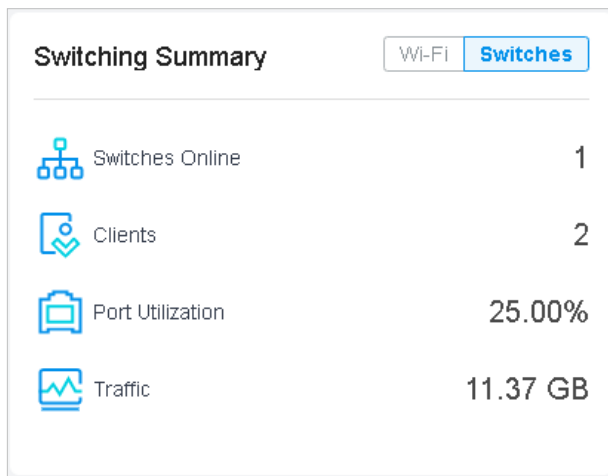
■ **Wi-Fi Summary**

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.



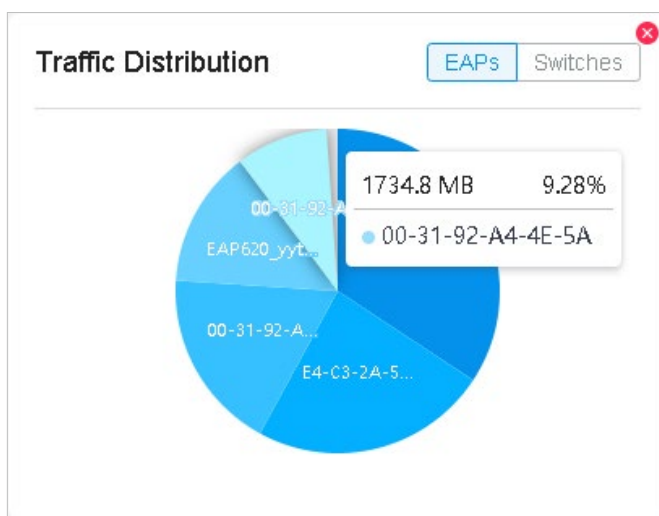
■ Switching Summary

The Switching Summary widget summarizes the real-time status of switches in the site, including the number of connected switches and clients, the port utilization, and the total amount 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

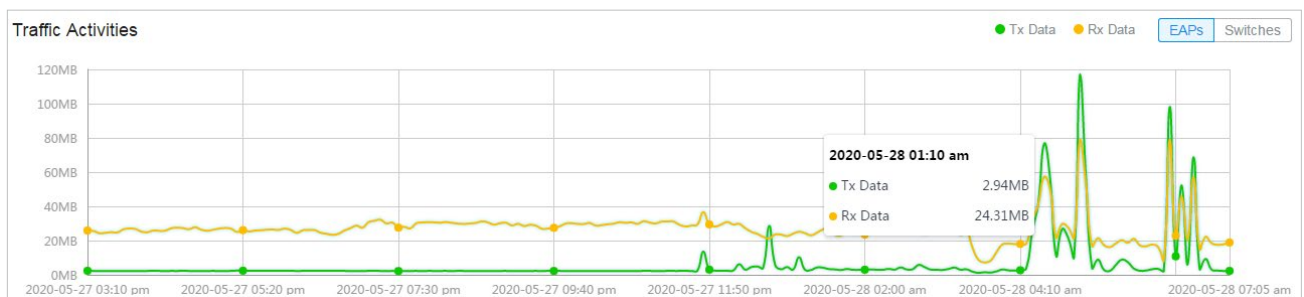
device category the clients connected to, the middle is by the device name, and the outer is by the frequency band. You can hover the cursor over the slice to view specific values.



■ Traffic Activities

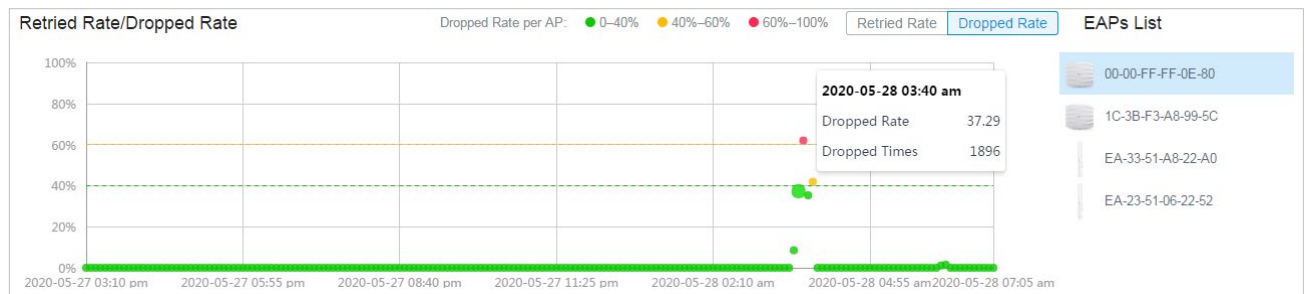
The Traffic Activities widget displays the Tx and Rx data of EAPs and switches within the time range. Only activities of the devices in the connected status currently will be counted.

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 [8.2 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

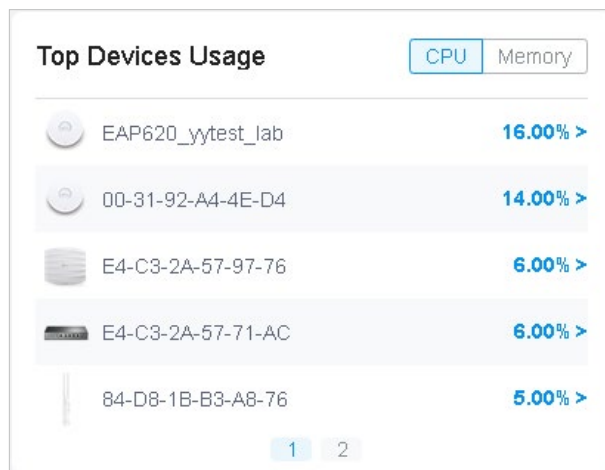
Displays the percentage of packets that needed to be re-sent because they were corrupted upon arriving at the proper destination.

Dropped Rate

Displays the percentage of packets that were dropped before reaching their intended destination.

■ **Top Devices Usage**

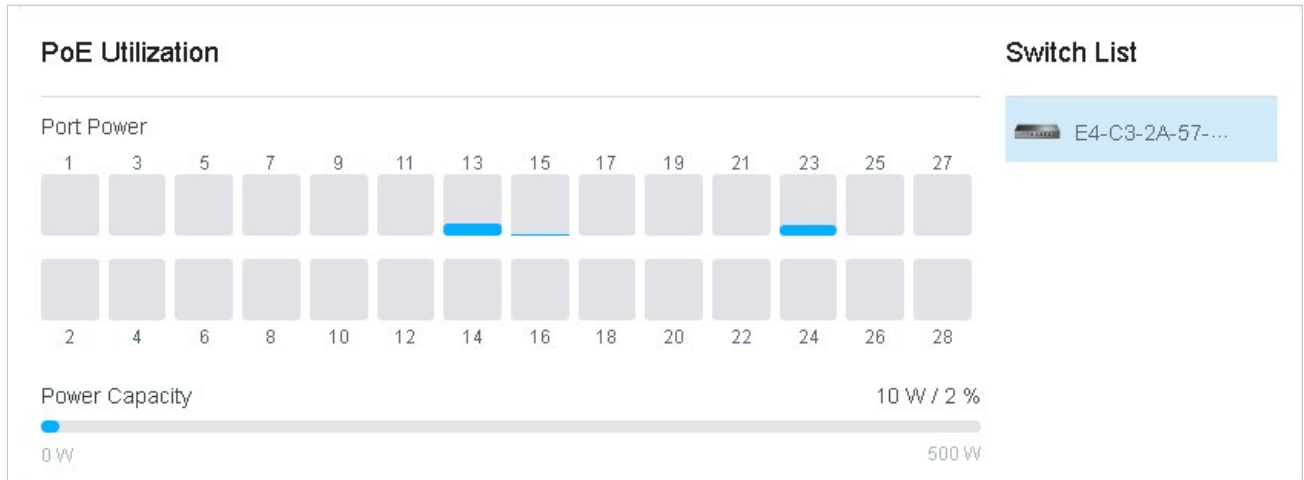
The Top Devices Usage widget displays the CPU utilization and memory utilization of devices within the time range. Click the tab to select the CPU or memory for display. Click the traffic number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to [6 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 2.4 GHz band or 5 GHz band. Click the traffic number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to [6 Configure and Monitor Controller-Managed Devices](#).



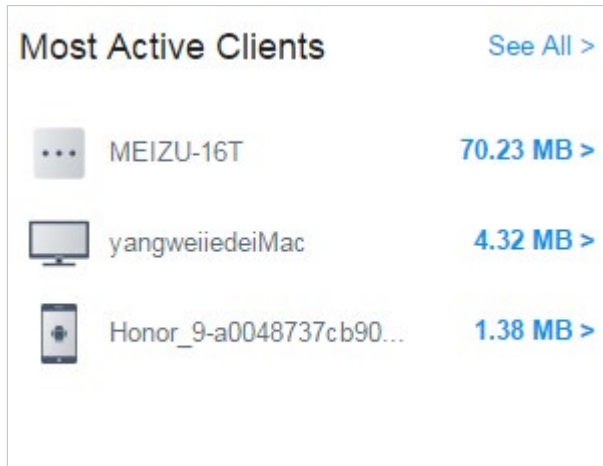
Client

Widgets in Clients use lists and charts to illustrate the traffic status of wired and wireless clients in the site, including the most active clients, activity statistics and distribution.

■ Most Active Clients

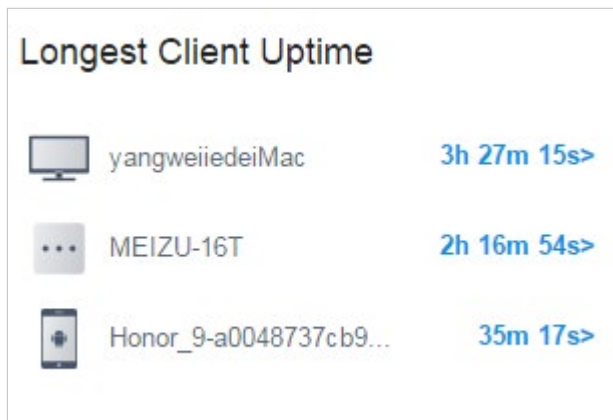
The Most Active Clients widget can display 15 most active clients. Only the clients in the connected status currently will be displayed.

To view all the clients connected to the network, click [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 [7.1 Manage Wired and Wireless Clients in Clients Page](#).



■ Longest Client Uptime

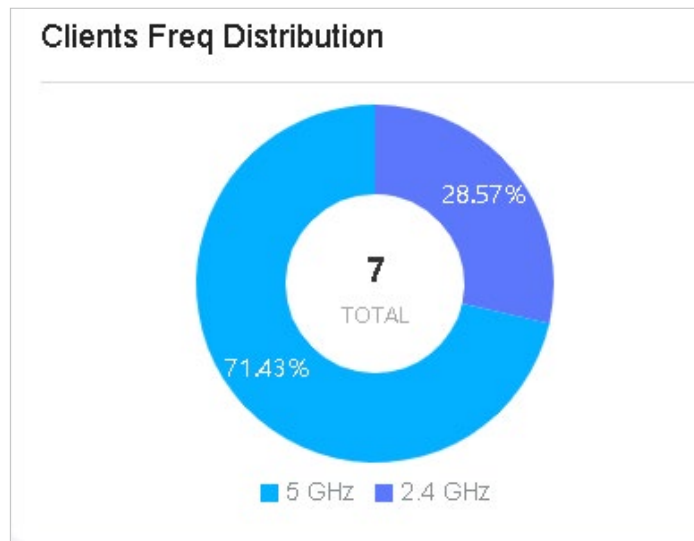
The Longest Client Uptime widget can display up to 15 clients sorted by the uptime. Only the clients in the connected status currently will be displayed. You can also click the uptime in the widget to open the client's Properties window for further configurations and monitoring. For details, refer to [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 5 GHz band and 2.4 GHz band 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

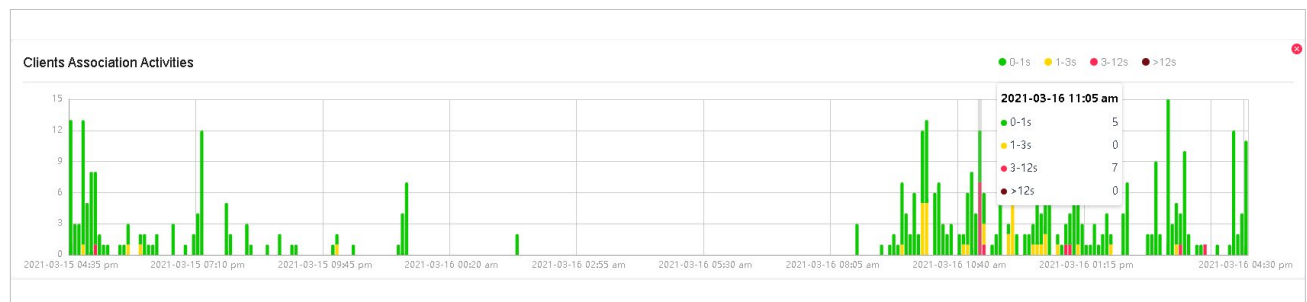
connect to the two bands. You can hover the cursor over the slice to view the number of clients in 2.4 GHz or 5 GHz band.



■ 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.

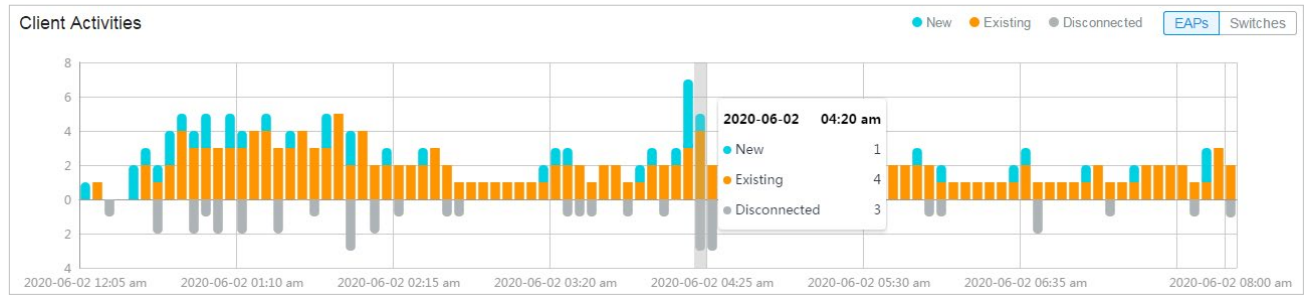


■ Client Activities

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.

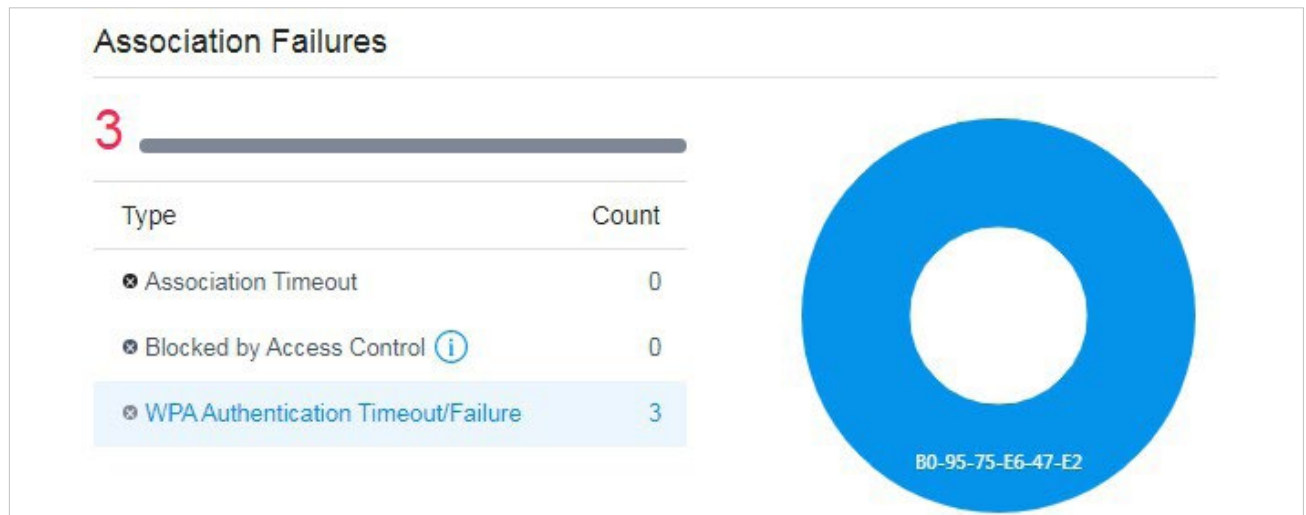
The total value of a column shows the total number of connected clients in this time period, and the segments in three colors shows the change of client number compared with the last time period.

Blue represents the newly connected clients, orange is the clients have been connected in the last period, and gray is the newly disconnected clients.



■ Association Failures

The Association Failures widget list three failure types and the times of clients failed to connect to the EAPs' networks in the site. A single bar is next to the count to show the proportion of the three failure reasons using gray colors from dark to light. Click the reason in the list to view the distribution of failures on EAPs.

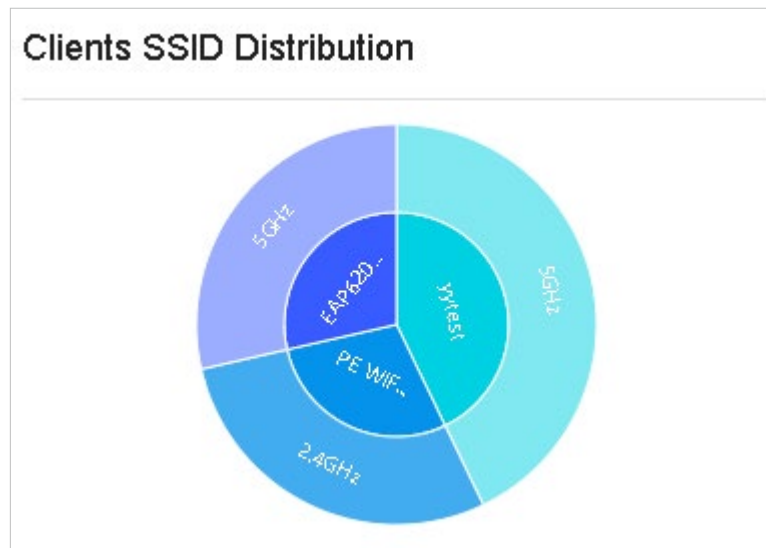


| | |
|--|--|
| Association Timeout | The connection failed because of session timeout. |
| Blocked by Access Control | The connection failed because the client has been blocked. For details about blocked clients, refer to 8. 5. 1 Known Clients . |
| WPA Authentication Timeout/Failure | The connection failed because the client did not pass the authentication due to authentication timeout or wrong password. |

■ Clients SSID Distribution

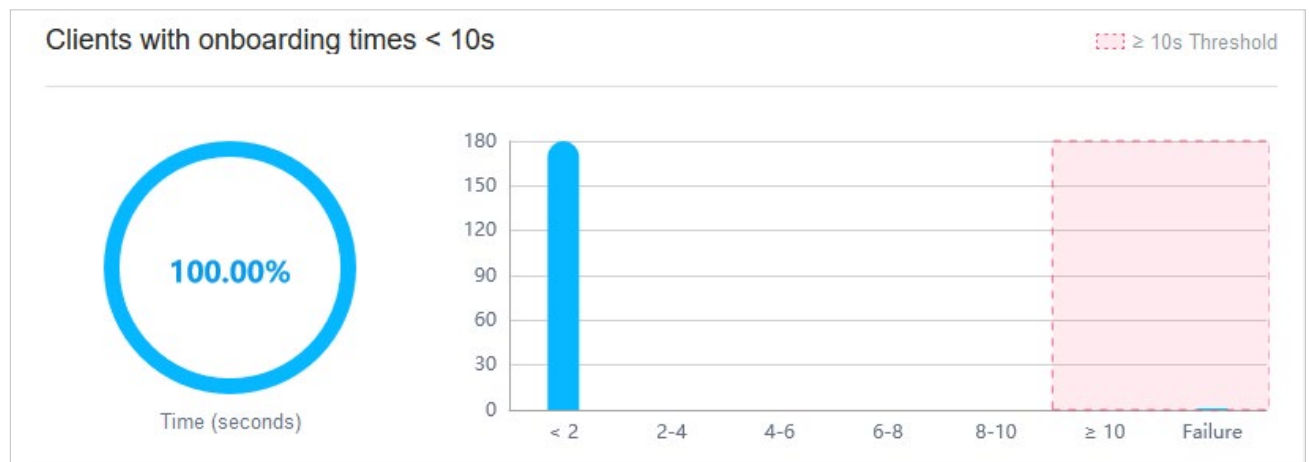
The SSID Distribution widget uses a sunburst chart to display the distribution of wireless clients connected to the different SSIDs in the site. The chart has two levels. The inner circle is divided by the EAP's SSID that the clients connected to, and the outer is by the frequency band. You can hover

the cursor over the slice to view the number of clients connected to the SSID in 2.4 GHz or 5 GHz band. Click a certain SSID to further display the statistics of its band frequency distribution.



■ **Clients with on Boarding Times**

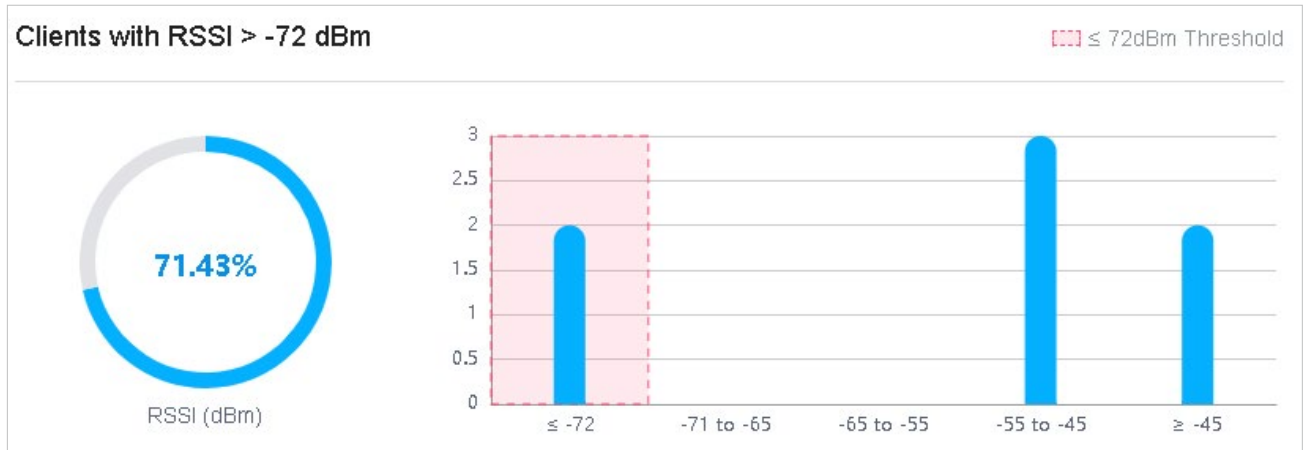
The Clients with on Boarding Times widget describes the time wireless clients uses when connecting to a certain SSID. The donut chart on the left shows the proportion of clients that uses less than 10 seconds to connect to the devices. The line graph on the right displays the number of clients according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



♥ 8.2 View the Statistics of the Network

Statistics provides a visual representation of device data in the SDN Controller. You can easily monitor the network traffic and performance under the following tabs, Performance, Switch Statistics, and Speed Test Statistics.

8.2.1 Performance

In Performance, you can view the device performance in a specified period by graphs, such as user counts, CPU and memory usage, and transmitted and received packets. The graphs vary due to the device type and status.

Tab Bar

The tabs and calendar on the top are used to specify the displayed statistics, and the legends on the right account for elements in the graphs.



| | |
|--|--|
| | Click to select a device from the drop-down list to view its statistics. The tabs vary due to the type of the selected device. |
| | Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right. The available time range is restricted by the time interval. Before selecting a long time range, select Hourly or Daily as the time interval. |
| | Select 5 minutes , Hourly , or Daily to specify the time interval of the data. When selecting a long time range, a longer time interval is recommended for a better view. |
| | (For gateway) Click to select the port of gateway on the tab to view the statistics. |
| | (For AP) Click to select the band of the AP to view the statistics. |

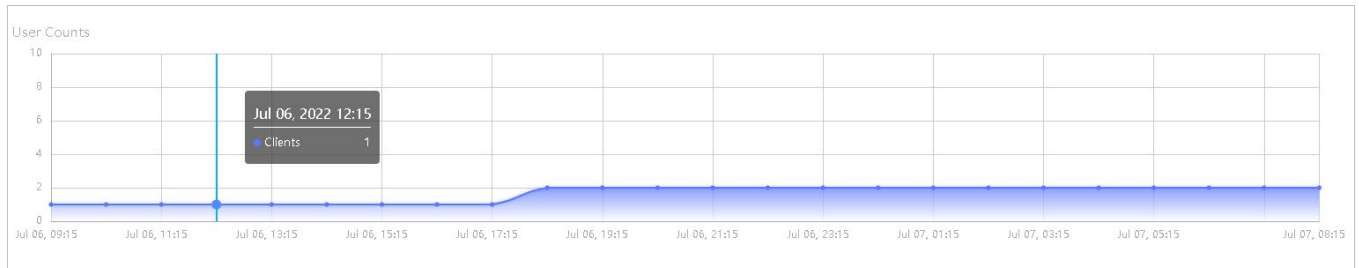
Statistical Graphs

Statistical graphs vary according to the type of devices. The chart below shows the statistical graphs which correspond to the gateway, switch, and AP.

| | |
|---------|--|
| Gateway | User Counts, Usage, Traffic, Packets |
| Switch | User counts, Usage |
| AP | User Counts, Usage, Traffic, Packets, Dropped, Errors, Retries |

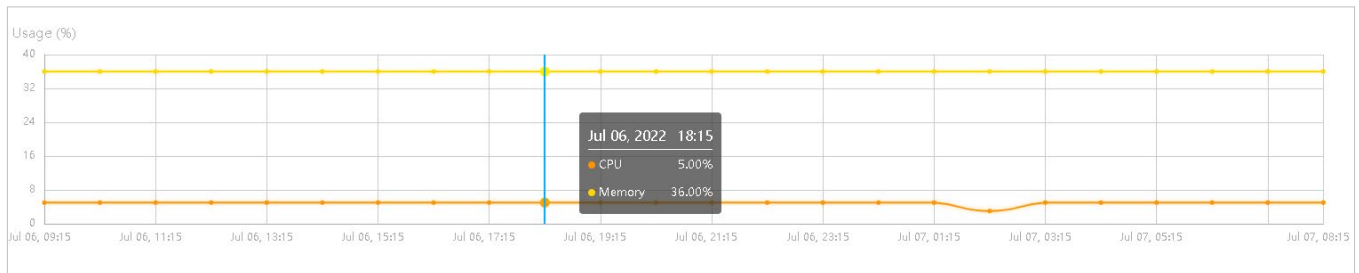
■ User Counts

The User Counts graph displays the number of users connected to the devices during the selected time range. Hover the cursor over the line to display the specific values.



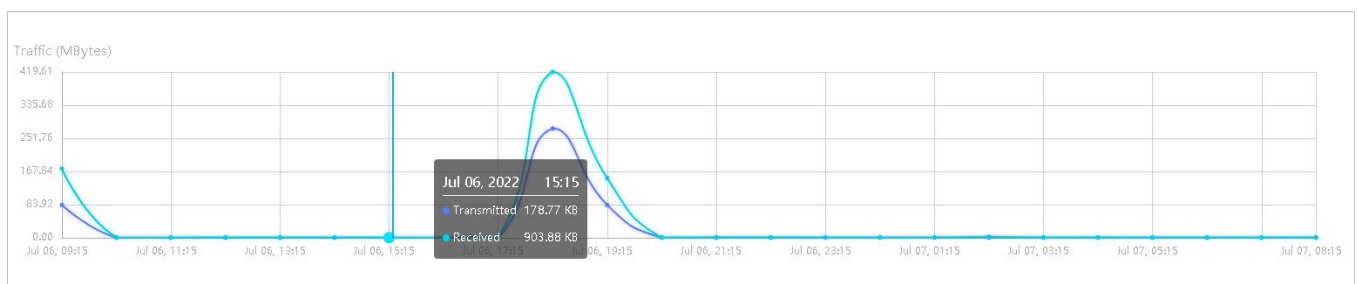
■ Usage

The Usage graph uses the orange line and yellow line to display the percentage of CPU usage and used memory during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



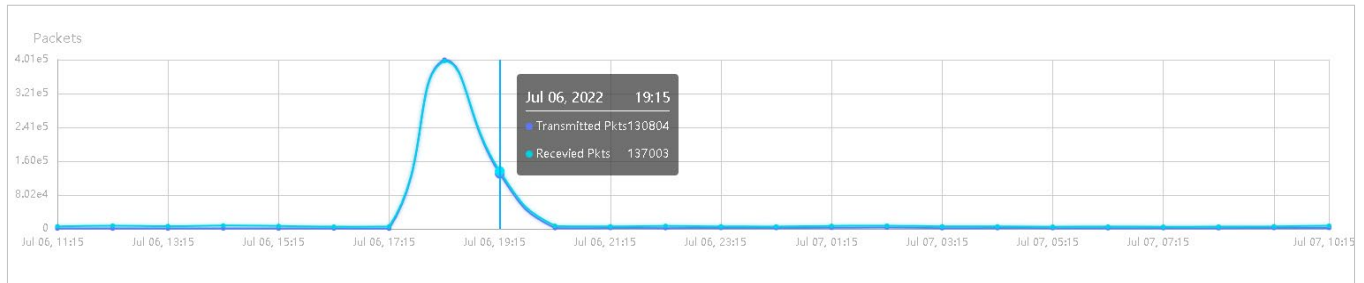
■ Traffic

The Traffic graph uses the dark blue line and light blue line to display the bytes of data transmitted and received during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



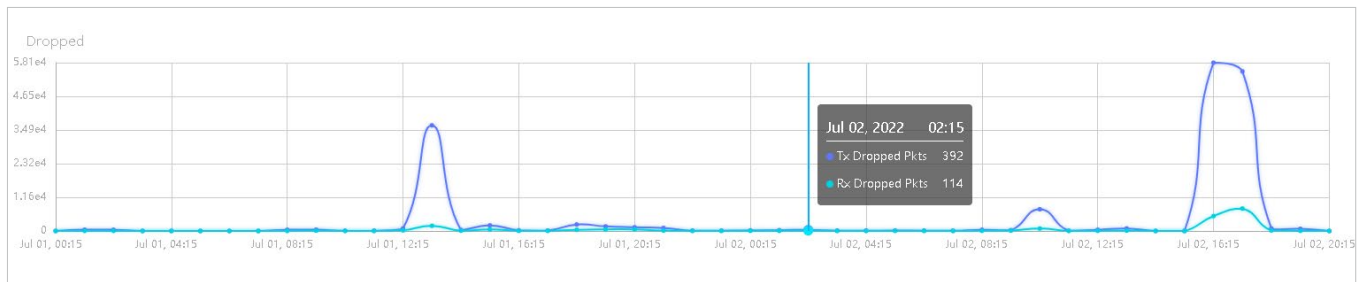
■ Packets

The Packets graph uses the dark blue line and light blue line to display the number of packets transmitted and received during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



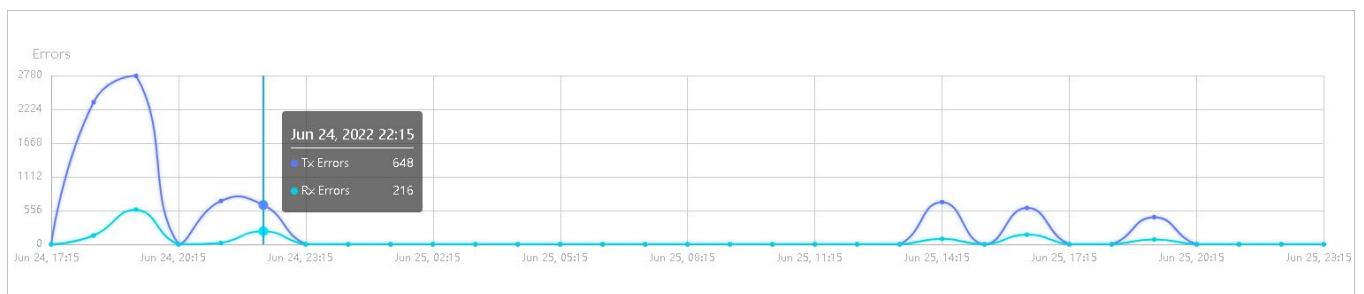
■ Dropped

The Dropped graph uses the dark blue line and light blue line to display the number of dropped Tx packets and Rx packets during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



■ Errors

The Errors graph uses the dark blue line and light blue line to display the number of error packets sent to AP and received by AP during the selected time range, respectively. Hover the cursor over the line to display the specific values.



■ Retries

The Retries graph uses the dark blue line and light blue line to display the number of times that the data packets are transmitted again and received again during the selected period, respectively. Hover the cursor over the lines to display the specific values.



8.2.2 Switch Statistics

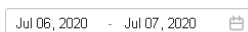
In Switch Statistics, you can view the current status of ports and their traffic statistics of the selected switch in the specified time range via a monitor panel and graphs.

Tab Bar

The tabs and calendar on the top are used to specify the displayed statistics, and the legends on the right account for elements in the graphs.



Click to select a switch from the drop-down list to view its statistics.



Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right.

The available time range is restricted by the time interval. Before selecting a long time range, select Hourly or Daily as the time interval.



Select **5 minutes**, **Hourly**, or **Daily** to specify the time interval of the data. When selecting a long time range, a longer time interval is recommended for a better view.



Select Natural, Transmitted, Received, or All to specify the graph order of ports.

Natural: Displays the line graphs in ascending order of the port number.

Transmitted: Displays the line graphs in descending order based on the traffic volume of transmitted packets.

Received: Displays the line graphs in descending order based on the traffic volume of received packets.

All: Displays the line graphs in descending order based on the total traffic volume of transmitted and received packets.

bps Bytes Packets

Select bps, Bytes or Packets to specify the data type and measuring unit.

bps: Displays the traffic rate in bps.

Bytes: Displays the traffic statistics in Bytes.

Packets: Displays the total number of packets.



If you select **Packet**, click the tab to specify which type of packet statistics to be displayed.

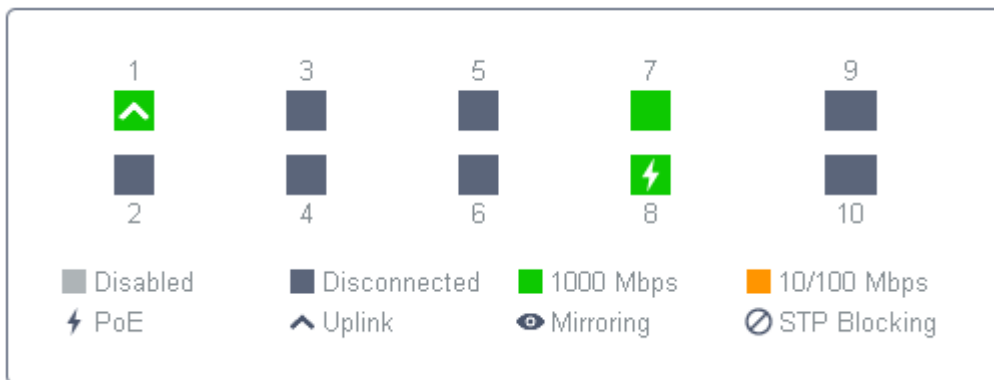
All: Displays statistics of all packets, including broadcast and multicast packets.

Broadcast: Displays statistics of broadcast packets only.

Multicast: Displays statistics of multicast packets only.

Monitor Panel

The monitor panel below the tab bar displays the current status of the ports on the selected switch.



Disabled The port profile is Disable. To enable it, refer to [6.3 Configure and Monitor Switches](#).

Disconnected The port is enabled but connects to no devices or clients.

1000 Mbps The port is running at 1000 Mbps.

10/100 Mbps The port is running at 10/100 Mbps.

PoE A PoE port connected to a powered device (PD).

Uplink An uplink port connected to WAN.

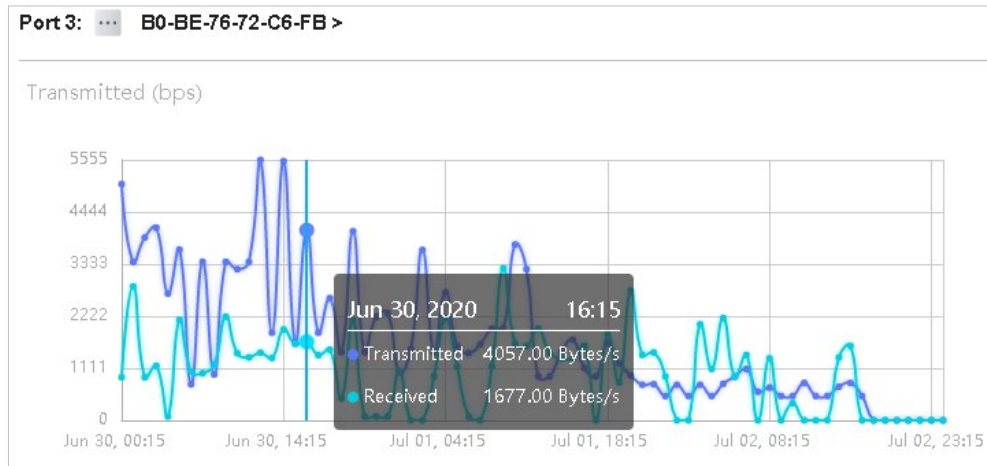
Mirroring A mirroring port that is mirroring another switch port.

STP Blocking A port in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocol Data Unit) packets to maintain the spanning tree. Other packets are dropped.

Statistical Graphs

Statistical graphs below the monitor panel display the traffic statistics of active ports.

You can specify the data type and measuring unit by clicking the **bps** Bytes Packets tab. The dark blue and light blue are used to indicate the transmitted and received statistics, respectively. Hover the cursor over the lines to display the specific values. To view and configure the device connected to the port, click the device name beside the port number.

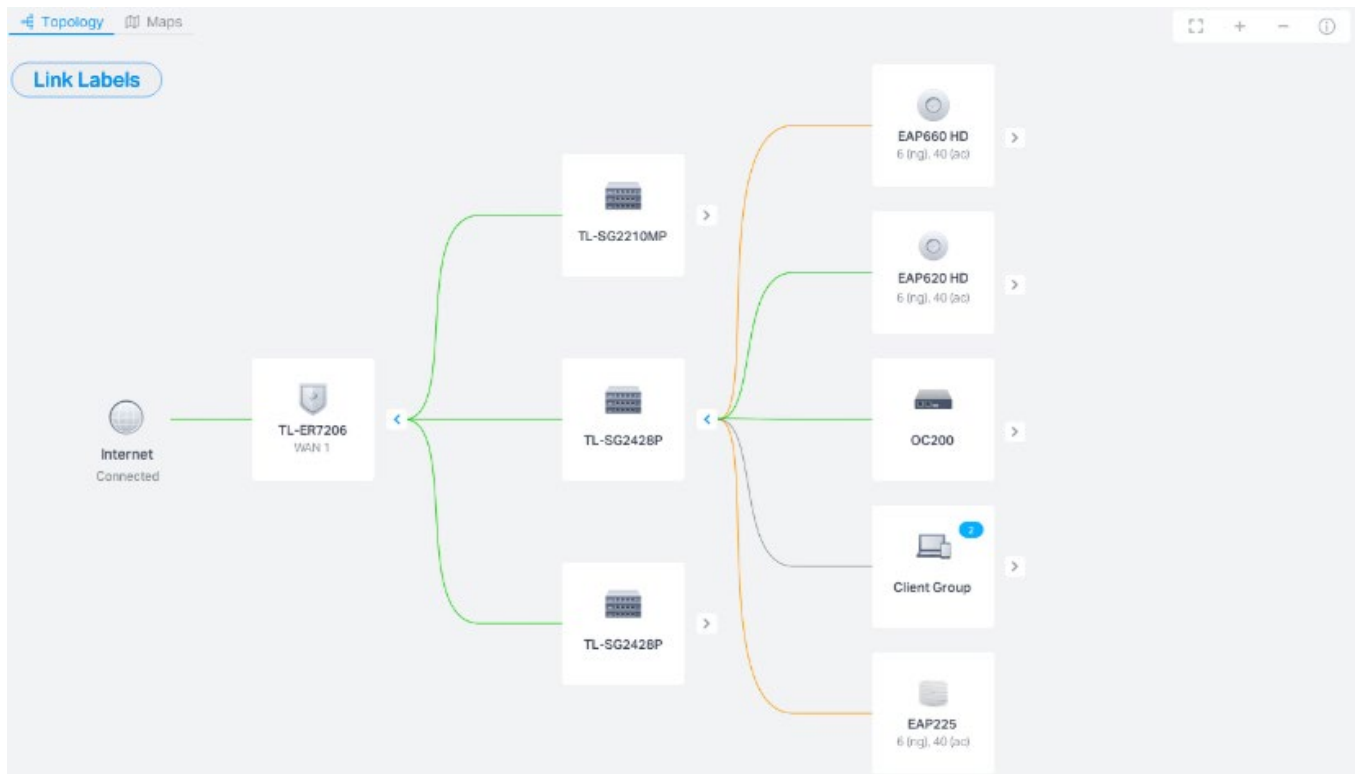


♥ 8.3 Monitor the Network with Map

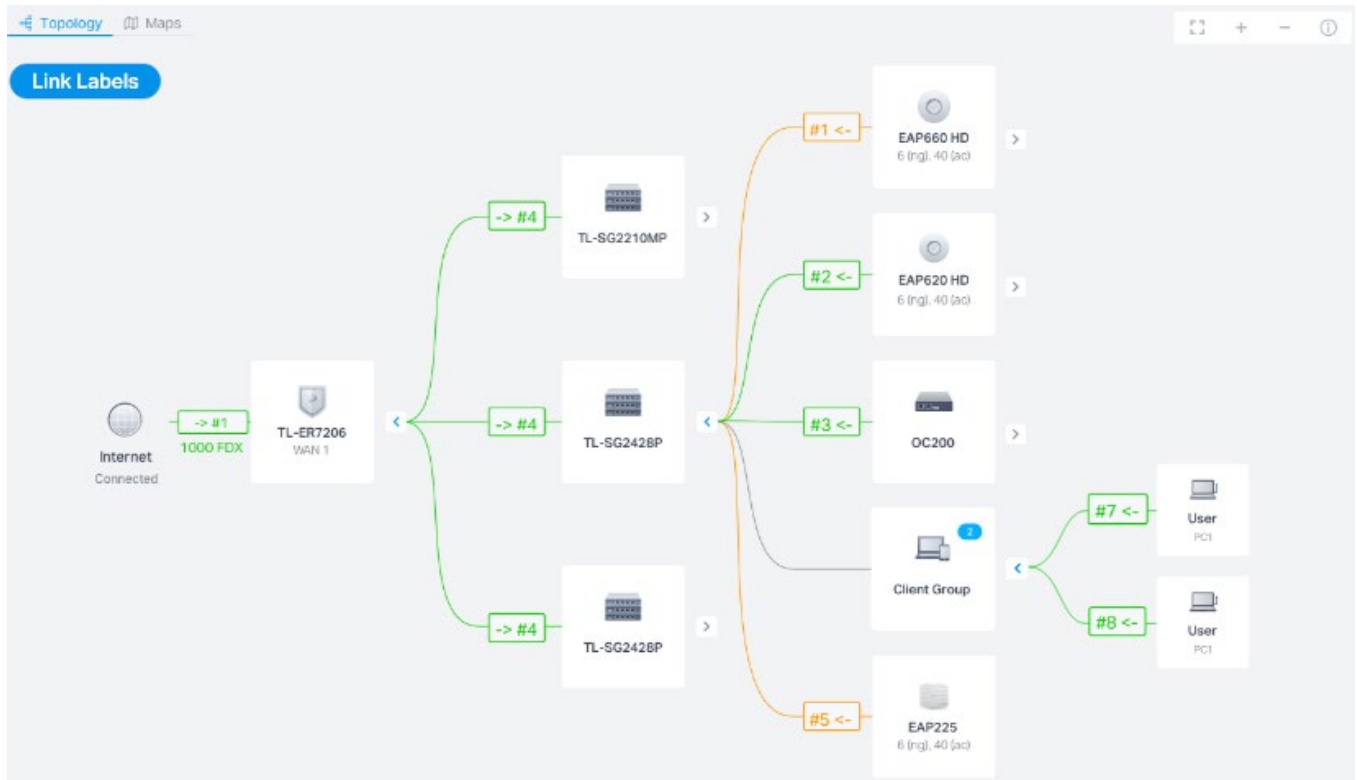
With the Map function, you can look over the topology and device provisioning of network in [Topology](#), customizes a visual representation of your network in [Heat Map](#), and visually display the geographic location of each device and site in [Device Map](#) and [Site Map](#).

8.3.1 Topology

Go to [Map > Topology](#), and you can view the topology generated by the controller automatically. You can click the icon of devices to open the Properties window. For detailed configuration and monitoring in the Properties window, refer to [6 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 nodes \oplus to unfold or \ominus to fold the branches.



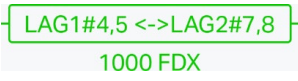
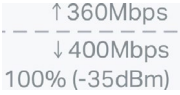
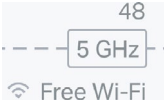
■ Diagram Size

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. |

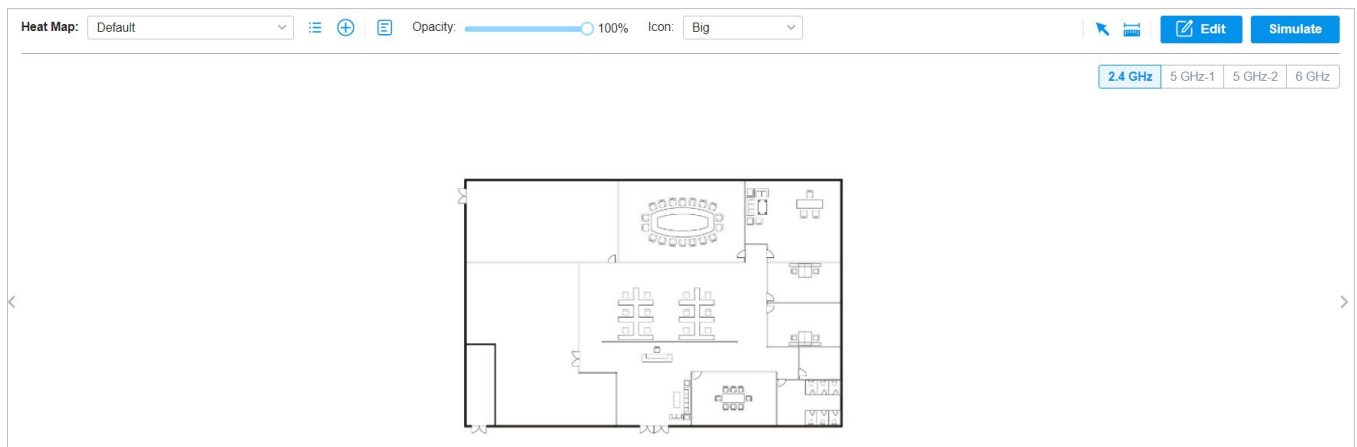
■ Link Labels

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.

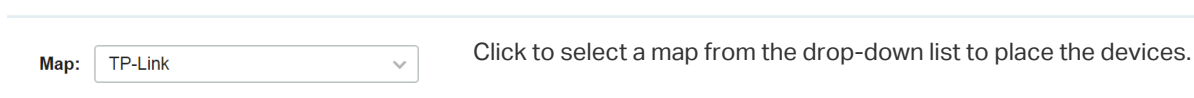
| | |
|---|--|
|  | (For the WAN port of router connected to the internet) Displays the port name, link speed and duplex type. |
|  | (For simple wired connections) Displays the connected port number, link speed, and duplex type. Note that only the switch's port number can be displayed in the label. |
|  | (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. |















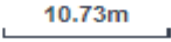


8.3.2 Heat Map

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.



| | |
|---|---|
|  | Click to edit maps in the pop-up window. |
|  | Click  to edit the description and layout of the map. |
|  | Click  to delete the map. |
|  | Click to add a map. In the pop-up window, enter the description, select the layout, and upload an image in the .jpg, .jpeg, .gif, .png, .bmp, .tiff format. |
| Opacity:  100% | Adjust the opacity of the map. |
| Icon: <input type="text" value="Small"/> | 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.

Add Map

Add Devices and Walls

View and Export Results

1. Go to [Map](#) > [Heat Map](#) and click  to add a new map. Then click [Add](#).

Add Map
×

i 1. Provide a description for the map and browse for an image on your computer.
2. The imported image should be less than 8M.

Description:

Layout: Indoors
 Outdoors

Open-Plan Space (Office, Factor ▾)

Upload an image: [Browse](#)

[Add](#) [Cancel](#)

Description

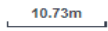
Enter a description for the map.


Layout

Select the general layout of the map, which will make the simulation more accurate.

Upload an image

Upload the map in the .jpg, .jpeg, .gif, .png, .bmp, .tiff, .dxf format.

2. Click  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  to set the default height of the added devices and the information displayed on the map. Then click [Confirm](#).

Settings ✕

[Default Height](#) [Display Information](#)

Ceiling Mounting: m (0-50, default 2.8)

Desktop: m (0-50, default 1)

Wall Plate Mounting: m (0-50, default 0.3)

Wall Mounting: m (0-50, default 2.6)

Outdoors: m (0-200, default 10)

Confirm

Cancel

Settings ✕

[Default Height](#) [Display Information](#)

Display Information:

- Devices Name
- MAC
- IP
- Status
- Model
- Version
- Uptime
- Clients
- Traffic
- Channel
- Transmission Power
- Height

Confirm

Cancel

Default Height

Specify the default height for devices. You can change the height for individual device later.



Display Information

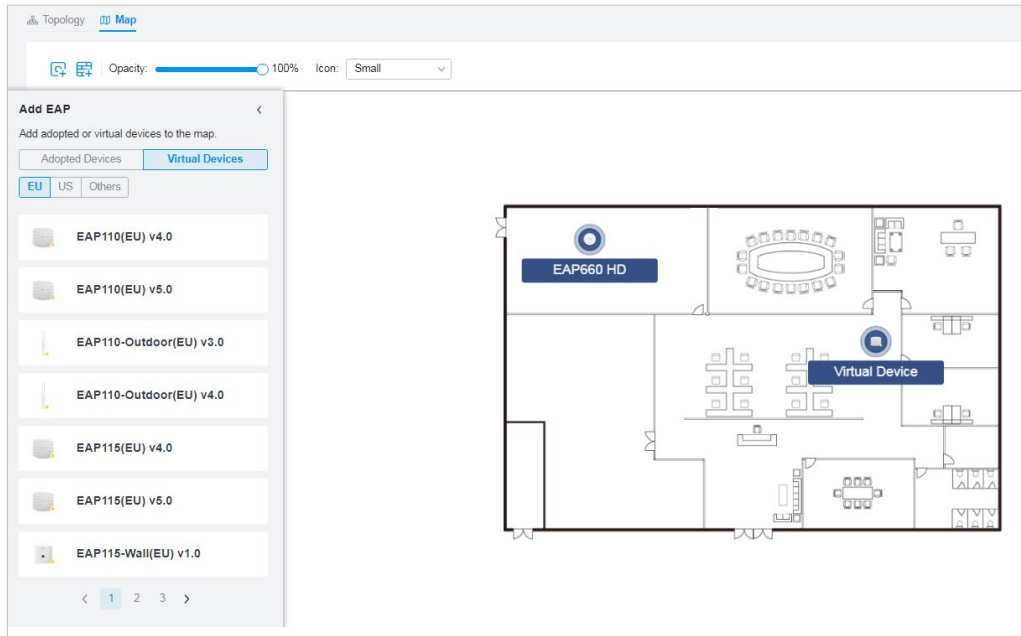
Select the information you want to see on the map.


Add Map

Add Devices and Walls

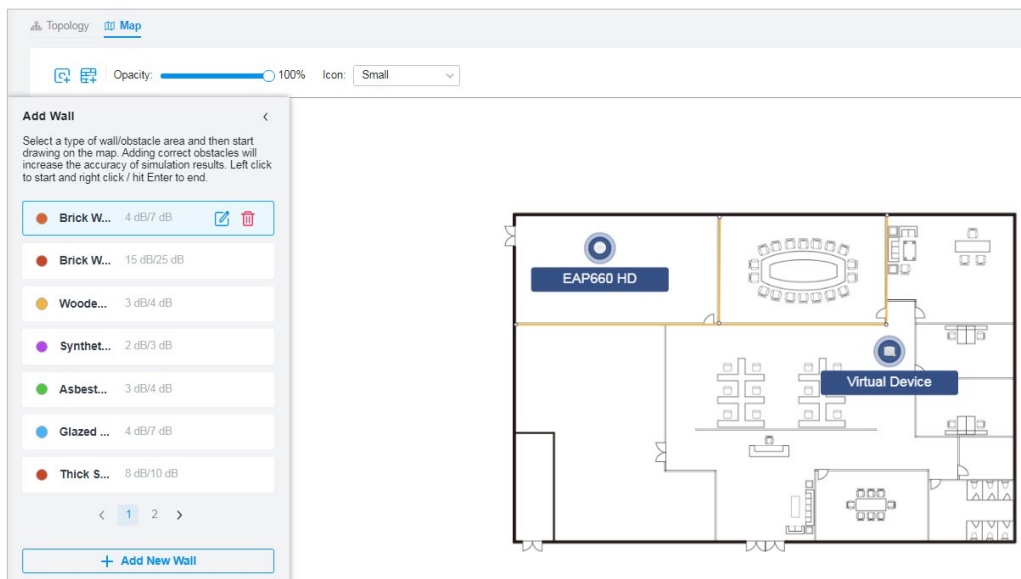
View and Export Results


1. Click  to enter the editing status of the map.
2. Click  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  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  to exit the editing status of the map.

Add Map

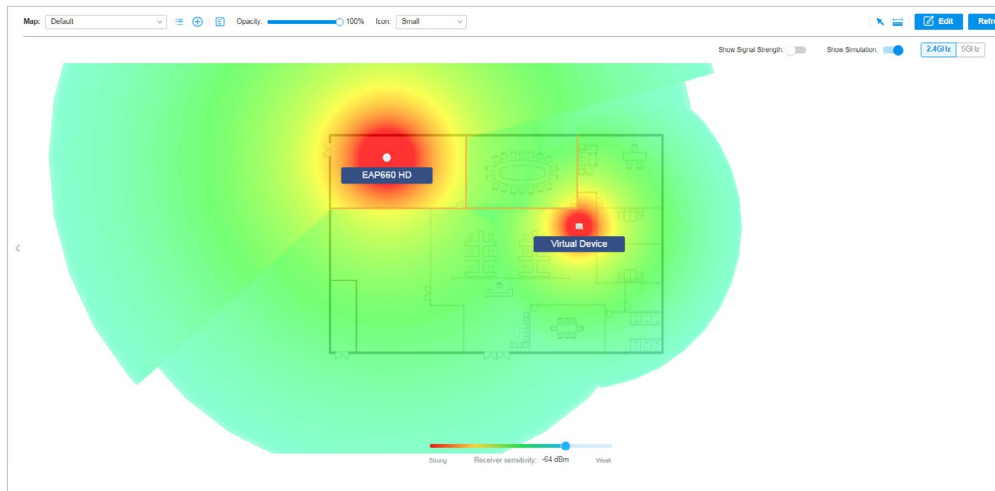
Add Devices and Walls

View and Export Results

Note:

It is required to click [Simulate](#) to generate a new heat map after editing elements on the map.

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



Show Signal Strength:

Enable the feature, and you can move the cursor to view the signal strength of a specific location.

Show Simulation:

Enable or disable the display of simulation results on the map.

2.4GHz 5GHz

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.

Receiver sensitivity: -60 dBm

Adjust the receiver sensitivity, and the new settings will take effect after refreshing the simulation.

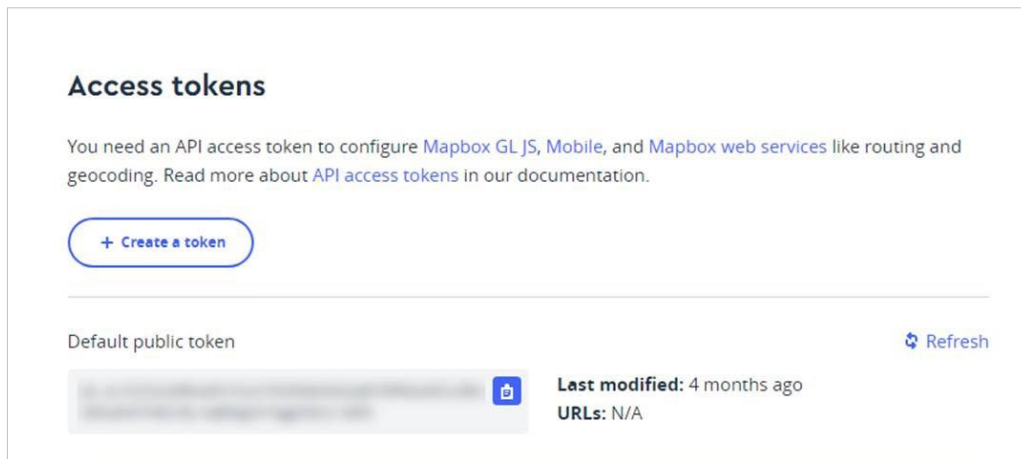
2. (Optional) If you want to export a network coverage report, click [Export](#) on the upper right to export a report in .docx format.

8.3.3 Device Map

Prerequisite

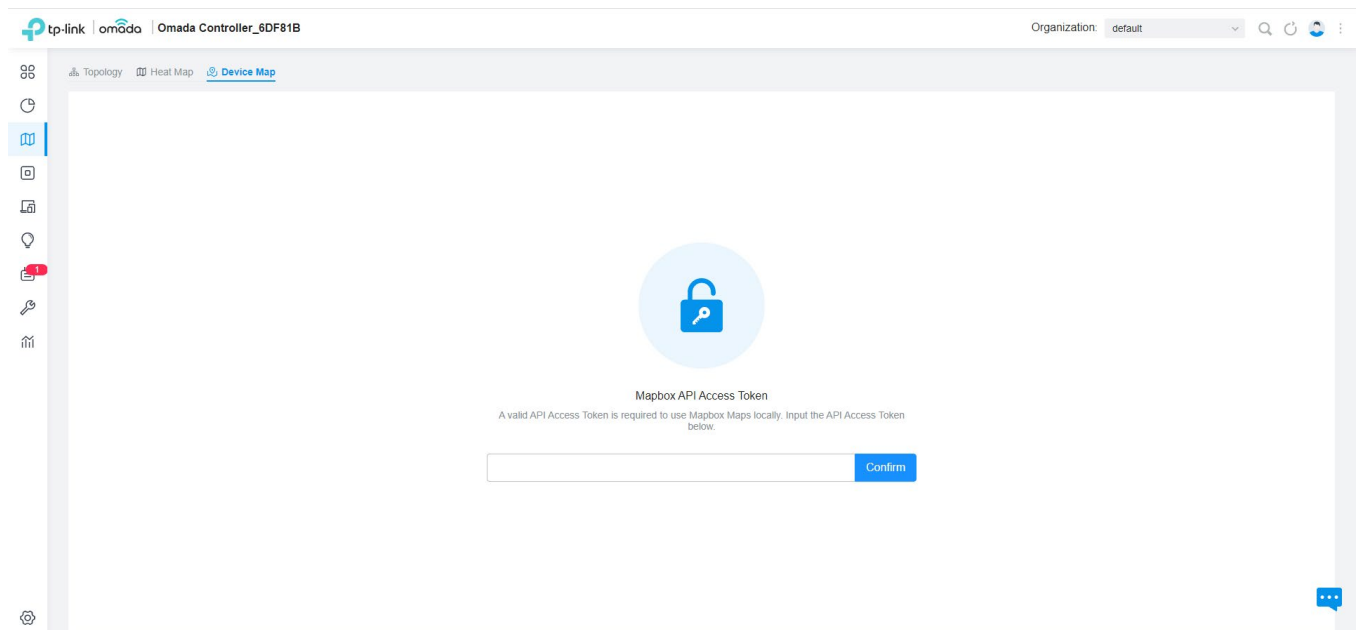
A valid Mapbox API Access Token is required to use the Device Map function.

Visit <https://www.mapbox.com>, register an account, and obtain the default token on the account page.

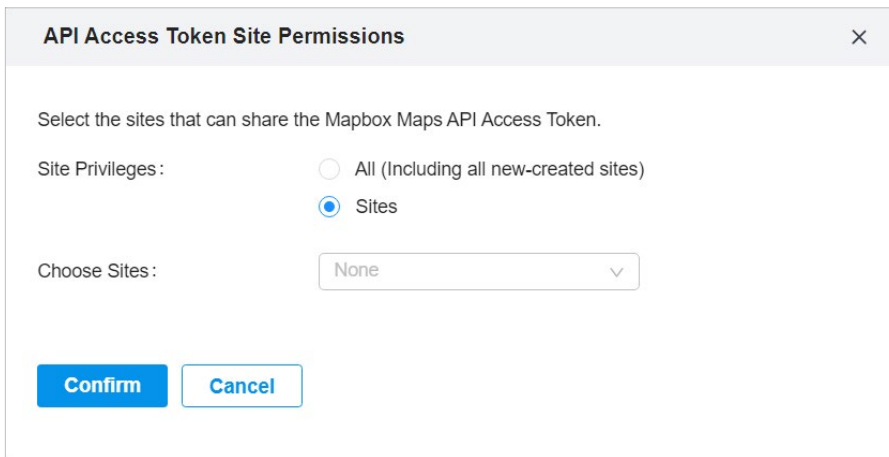


Configuration

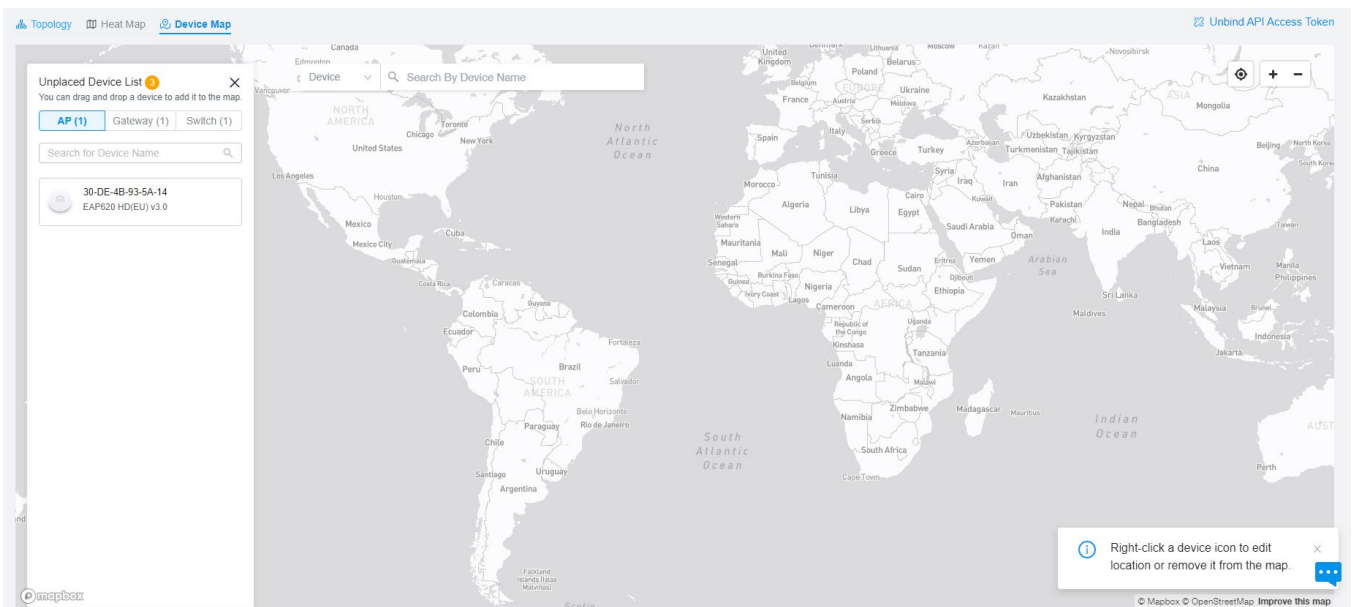
1. Select a site from the drop down list of **Organization** in the top-right corner. Go to **Map > Device Map**.
2. Enter the Mapbox API Access Token you obtained, then click **Confirm**.



3. Select the sites that can share the token, then click **Confirm**.



4. Use the map to manage your devices.



Unplaced Device List

Display a list of sites that are not marked on the map. You can drag and drop a site to add it to the map.

Search bar

Select a category and enter the keyword to search for a site or address.

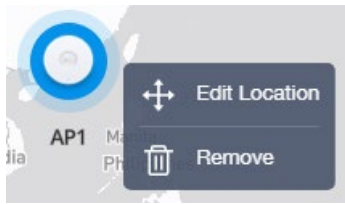


Locate to current location.

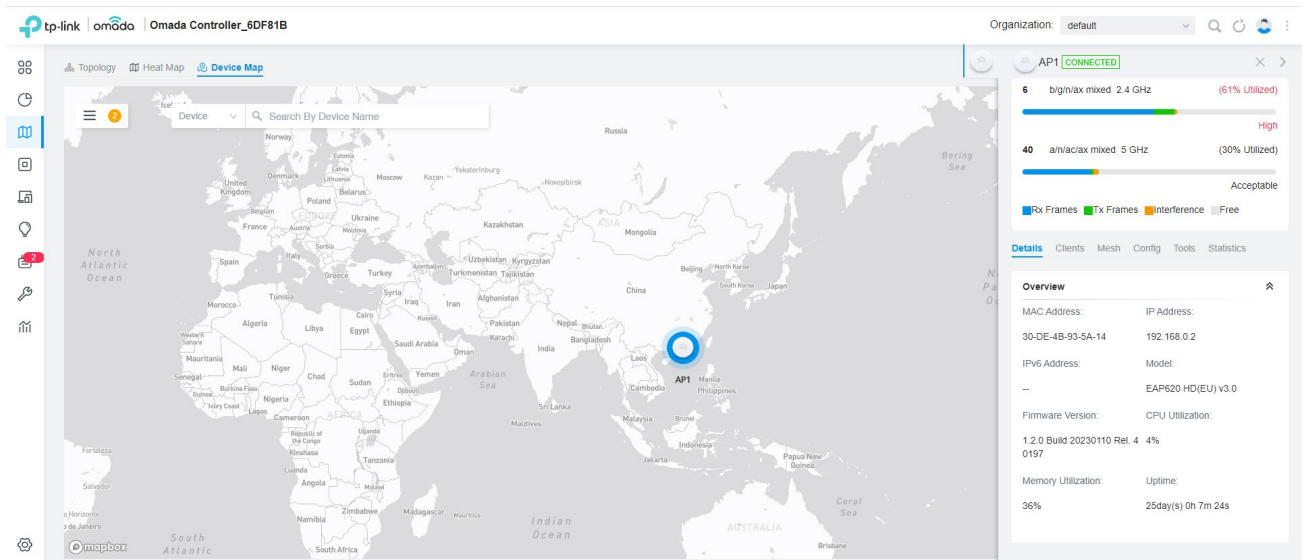


Zoom in and zoom out the map.

Right-click a device icon to edit location or remove it from the map.



Click a device icon to view device info and edit settings.



8.3.4 Site Map

Prerequisite

A valid Mapbox API Access Token is required to use the Site Map function.

Visit <https://www.mapbox.com>, register an account, and obtain the default token on the account page.

Access tokens

You need an API access token to configure [Mapbox GL JS](#), [Mobile](#), and [Mapbox web services](#) like routing and geocoding. Read more about [API access tokens](#) in our documentation.

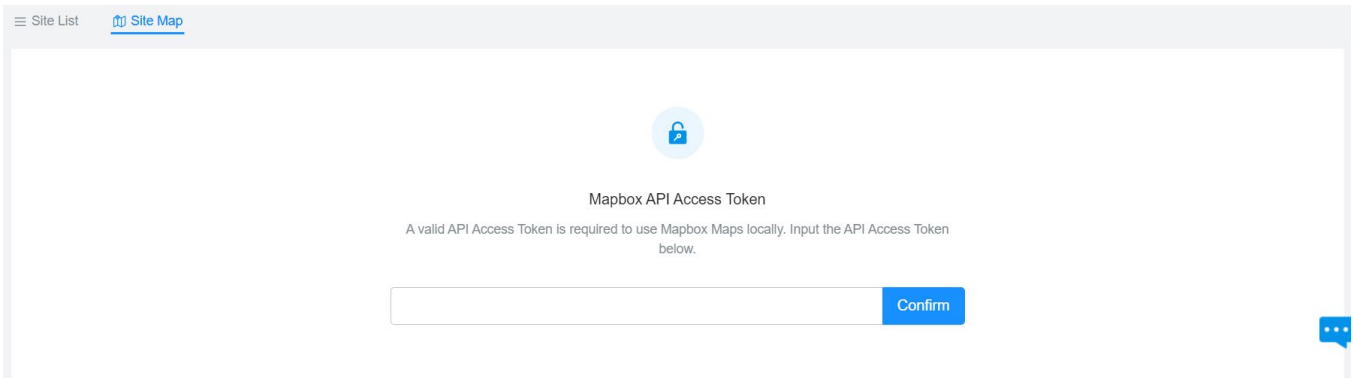
[+ Create a token](#)

Default public token [Refresh](#)

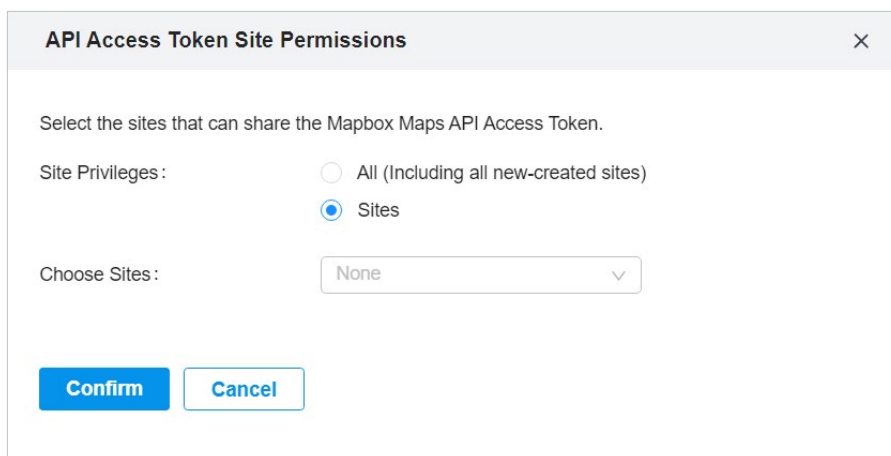
Last modified: 4 months ago
URLs: N/A

Configuration

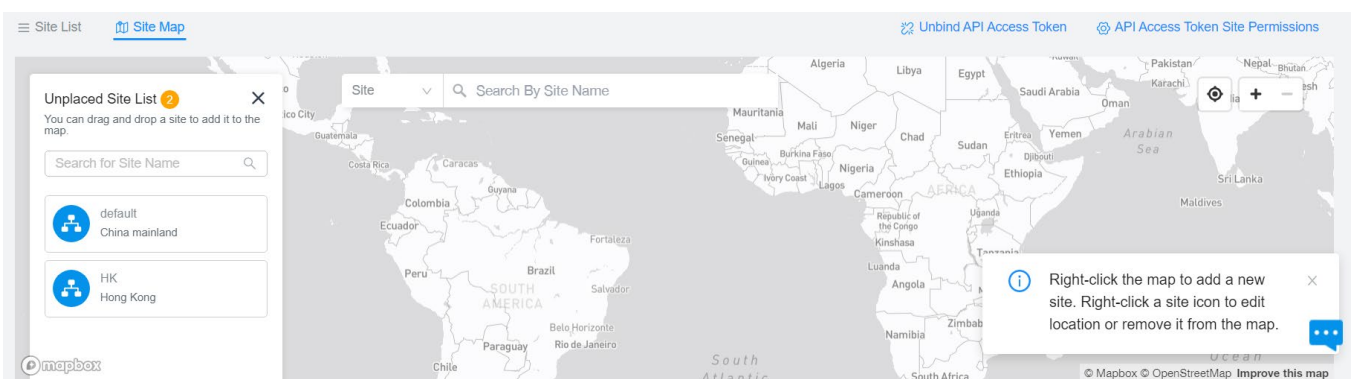
1. Select **Global** from the drop down list of **Organization** in the top-right corner. Go to **Dashboard > Site Map**.
2. Enter the Mapbox API Access Token you obtained, then click **Confirm**.



3. Select the sites that can share the token, then click **Confirm**.



4. Use the map to manage your sites.



Unplaced Site List

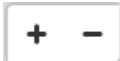
Display a list of sites that are not marked on the map. You can drag and drop a site to add it to the map.

Search bar

Select a category and enter the keyword to search for a site or address.



Locate to current location.

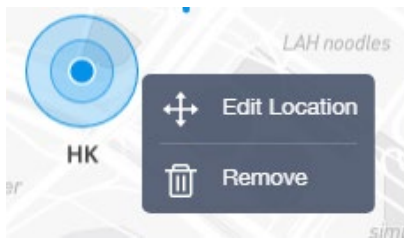


Zoom in and zoom out the map.

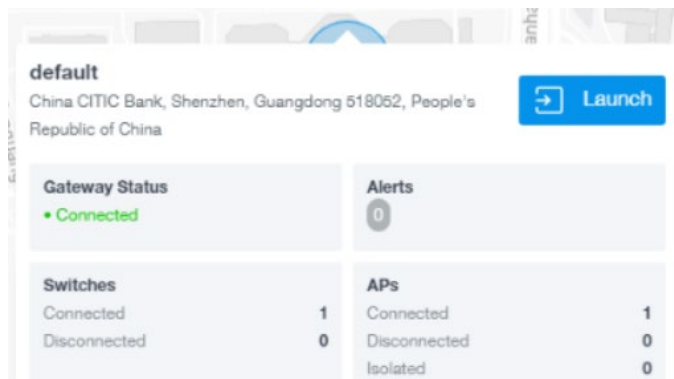
Right-click the map to add a new site.



Right-click a site icon to edit location or remove it from the map.



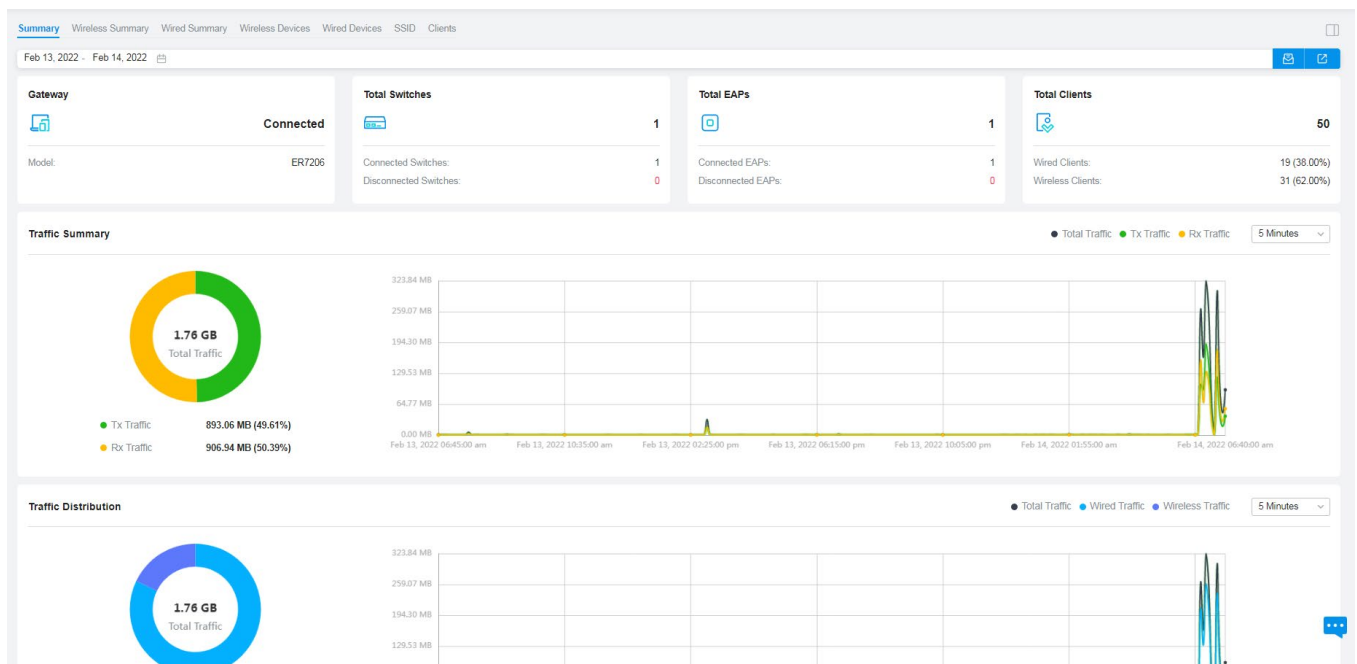
Click a site to view site info, and click Launch to access the site.



♥ 8.4 Monitor the Network with Reports

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

Go to [Reports](#), and you can view the connection data of the devices in the topology and the statistics of various network indicators and their changes over time. Click the tabs on the top to view the statistics of specific section of the network.



Summary Display the statistics summary of the whole network.

Wireless Summary Display the wireless statistics summary of the whole network, including data related to APs, wireless clients, and wireless traffic.

Wired Summary Display the wired statistics summary of the whole network, including data related to gateway, switches, wired clients, and wired traffic.

Wireless Devices Display details of APs in the network, including AP Traffic, CPU Utilization, Memory Utilization, Total Clients, Alerts, and Reboot Times.

Wired Devices Display details of gateway and switches in the network, including Traffic, CPU Utilization, Memory Utilization, Total Clients, Alerts, and Reboot Times.

SSID Display the statistics of SSIDs in the network, including Traffic, Total Clients, and Activities.

Clients Display the statistics of Clients in the network, including Distribution, Client Activities, and Client Numbers.

When you are accessing the controller locally, you can export the network report or send the report via email by clicking the icons on the upper right.



Click to send the report via email. Both Send Now and Send Schedule are available.



Click to export and the network report locally.

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

♥ 8.5 View the Statistics During Specified Period with Insight

In the Insight page, you can monitor the site history of connected clients, portal authorizations, and rouge APs. For a better monitoring, you can specify the time period and classify the clients and APs.

8.5.1 Known Clients

In Known Clients, a table lists all clients that connected to the network before in the site.

In the table, you can view the client's basic information, role and connection statistics, including download and upload traffics, connection duration, and the last time it connected to the network.

| NAME | MAC ADDRESS | USER/GUEST | DOWNLOAD | UPLOAD | DURATION | LAST SEEN | ACTION |
|-------------------|-------------------|------------|----------|----------|-----------------|-----------------------------|--------|
| 00-BE-3B-A5-CC-0F | 00-BE-3B-A5-CC-0F | User | 0 Bytes | 0 Bytes | 7m 25s | Jun 06, 2020 09:02:35 am | |
| 04-D3-B5-29-38-B7 | 04-D3-B5-29-38-B7 | User | 0 Bytes | 0 Bytes | 8m 2s | Jun 02, 2020 11:52:41 am | |
| 06-4D-02-2B-4D-8E | 06-4D-02-2B-4D-8E | User | 0 Bytes | 0 Bytes | 7m 42s | Jun 03, 2020 11:07:47 am | |
| 08-F4-AB-7C-6C-7E | 08-F4-AB-7C-6C-7E | User | 0 Bytes | 0 Bytes | 1h 4m 45s | May 25, 2020 09:21:50 am | |
| 0A-46-58-83-45-43 | 0A-46-58-83-45-43 | User | 430.5 MB | 109.4 MB | 14day(s) 1h 28m | May 29, 2020 02:18:08 pm | |
| 0C-B5-27-6F-83-86 | 0C-B5-27-6F-83-86 | User | 59.1 MB | 27.0 MB | 1day(s) 3h 10m | Jun 05, 2020 01:15:31 pm | |
| 5E-E7-AD-BB-30-49 | 5E-E7-AD-BB-30-49 | User | 0 Bytes | 0 Bytes | 12m 40s | Jun 02, 2020 03:43:41 pm | |

Showing 1-25 of 153 records < 1 2 3 4 5 7 > 25 /page Go To page: **GO**

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

| | |
|---|--|
| <input type="text" value="Search Name or MAC Address"/> | Enter the client name or MAC address to search the clients. |
| <input type="text" value="Start date - End date"/> | Filter the clients based on Last Seen. |
| | Click the selector to open the calendar. Click a specific date twice in the calendar to display the records on the day. To display the records of a time range, click the start date and end date in the calendar. |




Click the tabs to filter the clients listed in the table. The three tabs can take effect simultaneously.



All/Wireless/Wired: Click **All** to display both wireless and wired clients. Click **Wireless** or **Wired** to display wireless or wired clients only.



All/Users/Guests: Click **All** to display both users and guests. Click **Users** or **Guests** to display users or guests only. Guests are users connected to the wireless guest network. To configure guest network, refer to [4.4 Configure Wireless Networks](#).

All/Rate Limited/Blocked: Click **All** to display both rate limited and blocked clients. Click **Rate Limited** or **Blocked** to display rate limited or blocked clients only. To configure Rate Limit, refer to [4.8.3 Rate Limit](#). To block the clients, click the  icon in the table.

You can also take actions to block or forget the client. For detailed monitor and management, click the entry in the table to open the Properties window of the client. For more details, refer to [7.1.2 Using the Clients Table to Monitor and Manage the Clients](#).



(For unblocked clients) Click to block the client in the site. Once blocked, the client is banned from connecting to the network in the site.



(For blocked clients) Click to unblock the client in the site.



Click to forget the client. Once forget, all statistics and history of the client in the site are dropped.

8.5.2 Past Connections

In Past Connections, a table displays information about previous client connection sessions.

In the table, you can view the client's name, MAC address, association time and duration, download and upload traffic, IP address, and the network/port it connected to.

Known Clients [Past Connections](#) Past Portal Authorizations Rogue APs

Search Name, SSID, or MAC Address Start date - End date Association Success (37) Association Failure (0) All (37) Users (37) Guests (0)

| NAME | MAC ADDRESS | USER/GUEST | ASSOCIATION TIME | ASSOCIATED | DOWNLOAD | UPLOAD | DURATION | IP ADDRESS | AP/PORT |
|-------------------|-------------------|------------|------------------|--------------------------|------------|------------|----------|--------------|---------|
| 3C-84-6A-AF-96-50 | 3C-84-6A-AF-96-50 | User | -- | Nov 06, 2020 11:17:32 am | 808 Bytes | 1000 Bytes | 4m 31s | 192.168.0.50 | -- |
| 3C-84-6A-AF-96-50 | 3C-84-6A-AF-96-50 | User | -- | Nov 06, 2020 11:32:36 am | 1023 Bytes | 1.17 KB | 4m 30s | 192.168.0.50 | -- |
| 3C-84-6A-AF-96-50 | 3C-84-6A-AF-96-50 | User | -- | Nov 06, 2020 11:47:42 am | 1.05 KB | 1.22 KB | 4m 29s | 192.168.0.50 | -- |
| 3C-84-6A-AF-96-50 | 3C-84-6A-AF-96-50 | User | -- | Nov 06, 2020 12:02:47 pm | 541 Bytes | 750 Bytes | 4m 28s | 192.168.0.50 | -- |
| 3C-84-6A-AF-96-50 | 3C-84-6A-AF-96-50 | User | -- | Nov 06, 2020 12:17:52 pm | 1.26 KB | 1.41 KB | 4m 59s | 192.168.0.50 | -- |
| 3C-84-6A-AF-96-50 | 3C-84-6A-AF-96-50 | User | -- | Nov 06, 2020 12:32:58 pm | 0 Bytes | 0 Bytes | 2m 26s | 192.168.0.50 | -- |
| 3C-84-6A-AF-96-50 | 3C-84-6A-AF-96-50 | User | -- | Nov 06, 2020 12:48:02 pm | 593 Bytes | 750 Bytes | 3m 26s | 192.168.0.50 | -- |

Showing 1-25 of 37 records < 1 2 > 25 /page Go To page: GO

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

| | |
|--|--|
| Search Name, SSID, or MAC Address <input type="text"/> | Enter the client name, SSID or MAC address to search the clients. |
| Start date - End date <input type="text"/> | Filter the clients based on Start Time. |
| | Click the selector to open the calendar. Click a specific date twice in the calendar to display client connection sessions on the day. To display the client connection sessions during a time range, click the start date and end date in the calendar. |

8.5.3 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 [7.2 Manage Client Authentication in Hotspot Manager](#).

| NAME | MAC ADDRESS | AUTHORIZED BY | START TIME | DOWNLOAD | UPLOAD | DURATION | IP ADDRESS | AP/PORT |
|-----------------|-------------------|---------------------|--------------------------|----------|----------|------------|--------------|---------------|
| DESKTOP-G2N0O3C | F8-63-3F-A8-F7-96 | Local User - tplink | May 29, 2020 02:28:55 pm | 2.1 MB | 449.2 KB | 1m 25s | 192.168.0.27 | EAP225(Hotel) |
| DESKTOP-G2N0O3C | F8-63-3F-A8-F7-96 | Local User - tplink | May 29, 2020 02:31:22 pm | 9.4 MB | 229.1 KB | 41s | 192.168.0.27 | EAP225(Hotel) |
| DESKTOP-G2N0O3C | F8-63-3F-A8-F7-96 | Voucher - 146564 | May 29, 2020 02:33:22 pm | 5.0 MB | 123.3 MB | 1h 20m 48s | 192.168.0.27 | EAP225(Hotel) |

Showing 1-3 of 3 records < 1 > 25 /page Go To page: **GO**

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

Enter the client name or MAC address 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.

8.5.4 Switch Status

In Switch Status, a table displays information about the status of the switches managed by the controller. In the table, you can view the ports, PoE status, mode, and traffic activity of the switches.

| PORT | SWITCH | NAME | POE | MODE | PROFILE | LINK STATUS | STP | TX SUM | RX SUM | TX THROUGHPUT | RX THROUGHPUT | ACTION |
|------|-------------------|--------|------|-----------|---------|-------------------|------------|-----------|----------|---------------|---------------|--------|
| 15 | E4-C3-2A-57-71-AC | Port15 | 0.5W | switching | All | 1000M Full | Forwarding | 6.78 GB | 1.12 GB | 876 bps | 336 bps | |
| 16 | E4-C3-2A-57-71-AC | Port16 | -- | switching | All | -- | -- | 0 Bytes | 0 Bytes | 0 | 0 | |
| 17 | E4-C3-2A-57-71-AC | Port17 | -- | switching | All | 1000M Full Uplink | Forwarding | 2.48 GB | 20.36 GB | 4.81 Kbps | 3.95 Kbps | |
| 18 | E4-C3-2A-57-71-AC | Port18 | -- | switching | All | -- | -- | 0 Bytes | 0 Bytes | 0 | 0 | |
| 19 | E4-C3-2A-57-71-AC | Port19 | -- | switching | All | -- | -- | 237.39 KB | 21.24 KB | 0 | 0 | |
| 20 | E4-C3-2A-57-71-AC | Port20 | -- | switching | All | -- | -- | 0 Bytes | 0 Bytes | 0 | 0 | |

Showing 1-25 of 28 records < 1 2 > 25 /page Go To page: **GO**

A search bar and two tabs are above the table for searching and filtering. You can also click the icons in the Action column for quick operation.

Search Switch or Name

Enter the switch or name to search.


Overview
PoE
Counters

All
Connected
Disconnected


Click the tabs to filter the switch ports listed in the table. The two tabs can take effect simultaneously.

Overview/PoE/Counters: Click [Overview](#) to display the general status of each port. Click [PoE](#) to display the PoE configurations and status of each port. Click [Counters](#) to display TX and RX rates for each port.

All/Connected/Disconnected: Filter the ports by their link status. Click [All](#) to display information of all ports. Click [Connected](#) or [Disconnected](#) to display all connected or disconnected ports.



Click to edit the configurations of the port.













(Only for the PoE port that is connected to a PD) Click the button and the port will stop to supply power to the connected PD momentarily in order to reboot the PD.

The listed information when you select [Overview](#) on the first tab is explained as follows.

| | |
|------------------------|---|
| Port | <p>Display the port number and status of the port .</p> <ul style="list-style-type: none"> ■ 10/100 Mbps: The port is running at 10/100 Mbps. ■ 1000 Mbps: The port is running at 1000 Mbps. ■ 2.5 Gbps: The port is running at 2.5 Gbps. ■ 10 Gbps: The port is running at 10 Gbps. ■ Disabled: The port is disabled. ■ Disconnected: The port is enabled but connects to no devices or clients. ⚡ PoE: The PoE port is connected to a powered device (PD). ^ Uplink: The port is an uplink port connected to WAN. 👁 Mirroring: The port is a mirroring port that is mirroring another switch port. 🚫 STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocol Data Unit) packets to maintain the spanning tree. Other packets are dropped. |
| Switch | Display the MAC address or the alias of the switch. |
| Name | Display the name of the port. |
| PoE | <p>Display the PoE status of the port.</p> <ul style="list-style-type: none"> --: PoE is disabled _W: Display the power output of the port in watts. |











| | |
|----------------------|--|
| Mode | <p>Display the operation mode of the port.</p> <p>Switching: The default mode.</p> <p>Mirroring: The network traffic of this port will receive the mirrored traffic from its mirrored port.</p> <p>Aggregating: The port is a part of an aggregate link</p> |
| Profile | Display the switch port profile that takes effect on the port. |
| Link Status | Display the connection speed and duplex mode of the port. |
| STP | Display the Spanning Tree Protocol (STP) mode. |
| TX Sum | Display the amount of transmitted data. |
| RX Sum | Display the amount of received data. |
| TX Throughput | Display the transmit throughput rate. |
| RX Throughput | Display the receive throughput rate. |

The listed information when you select **PoE** on the first tab is explained as follows.

| | |
|---------------|---|
| Port | <p>Display the port number and status of the port .</p> <p> 10/100 Mbps: The port is running at 10/100 Mbps.</p> <p> 1000 Mbps: The port is running at 1000 Mbps.</p> <p> 2.5 Gbps: The port is running at 2.5 Gbps.</p> <p> 10 Gbps: The port is running at 10 Gbps.</p> <p> Disabled: The port is disabled.</p> <p> Disconnected: The port is enabled but connects to no devices or clients.</p> <p> PoE: The PoE port is connected to a powered device (PD).</p> <p> Uplink: The port is an uplink port connected to WAN.</p> <p> Mirroring: The port is a mirroring port that is mirroring another switch port.</p> <p> STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocol Data Unit) packets to maintain the spanning tree. Other packets are dropped.</p> |
| Switch | Display the MAC address or the alias of the switch. |
| Name | Display the name of the port. |

| | |
|----------|--|
| PoE | Display the PoE status of the port. --: PoE is disabled _W: Display the power output of the port in watts. |
| PD Class | Display the power requirement of the PD connected to the PoE port. |
| Power | Display the power output of the port in watts. |
| Voltage | Display the voltage output in volts. |
| Current | Display the current output in amperes. |

The listed information when you select **Counters** on the first tab is explained as follows.

| | |
|--------------|--|
| Port | <p>Display the port number and status of the port .</p> <ul style="list-style-type: none">  10/100 Mbps: The port is running at 10/100 Mbps.  1000 Mbps: The port is running at 1000 Mbps.  2.5 Gbps: The port is running at 2.5 Gbps.  10 Gbps: The port is running at 10 Gbps.  Disabled: The port is disabled.  Disconnected: The port is enabled but connects to no devices or clients.  PoE: The PoE port is connected to a powered device (PD).  Uplink: The port is an uplink port connected to WAN.  Mirroring: The port is a mirroring port that is mirroring another switch port.  STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocol Data Unit) packets to maintain the spanning tree. Other packets are dropped. |
| Switch | Display the MAC address or the alias of the switch. |
| TX Bytes | Display the number of transmitted bytes. |
| TX Frames | Display the number of transmitted frames. |
| TX Multicast | Display the number of transmitted multicast packets. |
| TX Broadcast | Display the number of transmitted broadcast packets. |
| TX Errors | Display the number of transmitted error packets. |
| RX Bytes | Display the number of received bytes. |
| RX Frames | Display the number of received frames. |




RX Multicast Display the number of received multicast packets.

RX Broadcast Display the number of received broadcast packets.

RX Errors Display the number of received error packets.

8.5.5 Port Forwarding Status

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

| NAME | INTERFACE | SOURCE IP | SOURCE PORT | DESTINATION IP | DESTINATION PORT | PROTOCOL | PACKETS | BYTES | ACTION |
|-------|-----------|----------------|-------------|----------------|------------------|----------|---------|---------|---|
| Lab | | 172.31.53.2/24 | 8043 | 192.168.0.16 | 8043 | TCP&UDP | 0 | 0 Bytes |  |
| TestA | | 0.0.0.0/0 | 443 | 192.168.0.22 | 443 | UDP | 0 | 0 Bytes |  |
| TestB | | 10.0.0.16/24 | 8080 | 192.168.0.16 | 8080 | TCP | 0 | 0 Bytes |  |

Showing 1-3 of 3 records < 1 > 25 /page Go To page: **GO**

A tab is above the table for filtering. You can also click the icons in the Action column for quick operation.



Click the tab to filter the port forwarding entries listed in the table.

User-defined/UPnP: Click **User Defined** to display the port forwarding entries created by the user. Click **UPnP** to display the UPnP port forwarding entries.



Click to edit the configurations of the port forwarding entry.

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. |
| Lease Duration | (Only for UPnP port forwarding) Display the uptime of the port forwarding entry. |

8.5.6 VPN Status

In VPN Status, a table displays the existing VPN tunnels and corresponding information.

| IPsec VPN OpenVPN/PPTP/L2TP SSL VPN | | | | | | | | | |
|---|------------|-----------|--------------------------------|--------------------------------------|----------|--------------------|---------------------|----------------|--------|
| NAME | SPI | DIRECTION | TUNNEL ID | DATA FLOW | PROTOCOL | AH AUTHENTICAT ION | ESP AUTHENTICAT ION | ESP ENCRYPTION | ACTION |
| Ipsec_VPN | 3247465960 | in | 192.168.0.1 ↻ 192.168.0.2 ↻ | 192.168.2.0/24 ↻ 192.168.1.0/24 ↻ | ESP | MD5 | MD5 | 3DES | |

Showing 1-1 of 1 records < 1 > 25 / page Go To page:

A tab is above the table for filtering. You can also click the icons for quick operation.

| | |
|--|--|
| | Click the tab to filter the routing information listed in the table. |
| | When you select OpenVPN/PPTP/L2TP, you can further choose Server or Client. |
| | Click to configure the entry. |
| | (Only for OpenVPN/PPTP/L2TP) Filter the entries. |
| | (Only for OpenVPN/PPTP/L2TP) Click to terminate the VPN tunnel. |
| | (Only for OpenVPN/PPTP/L2TP) Click to choose more listed information to be displayed in the table. |
| | (Only for SSL VPN) Click to lock out the user. You can click View Locked Out Users to manage the locked out users. |
| | (Only for SSL VPN) Click to disconnect the user. |

The listed information of IPsec VPN table is explained as follows.

| | |
|-----------|--|
| Name | Display the name of the IPsec VPN entry. |
| SPI | Display the Security Parameter Index of VPN. |
| Direction | Display the direction of the VPN process. |
| Tunnel ID | Display the local and remote IP address/name. The arrow indicates the traffic direction. |

| | |
|--------------------|---|
| Data Flow | Display local and remote subnet. The arrow indicates the direction. |
| Protocol | Display the authentication and encryption protocol of the entry. |
| AH Authentication | Display checksum algorithms of the entry. |
| ESP Authentication | Display the algorithms for ESP authentication. |
| ESP Encryption | Display the algorithms for ESP encryption. |

| IPsec VPN | OpenVPN/PPTP/L2TP | SSL VPN | Server | Client | | | |
|--|-------------------|----------------------|--------------|-----------------|---------|--------|--------|
| USER | INTERFACE | TYPE | LOCAL IP | REMOTE LOCAL IP | DNS | UPTIME | ACTION |
| l2tpServer | WAN | L2TP Server (Client) | 192.168.11.1 | 192.168.11.2 | 8.8.8.8 | 3 h | |
| pptpServer | WAN | PPTP Server (Client) | 192.168.10.1 | 192.168.10.2 | 8.8.8.8 | 3 h | |
| Showing 1-2 of 2 records < 1 > 25 / page Go To page: <input type="text"/> Go | | | | | | | |

The listed information of OpenVPN/PPTP/L2TP (Server) table is explained as follows (some information listed below is hidden by default). You can further filter the entries based on their type.

| | |
|-----------------|--|
| User | Display the username of the remote user. |
| Interface | Display the interface that the traffic goes through. |
| Type | Display the connection type. |
| Local IP | Display the local IP address of the VPN tunnel. |
| Remote Local IP | Display the IP address of the remote user of the VPN tunnel. |
| DNS | Display the DNS address of the VPN tunnel. |
| Download Pkts | Display the amount of data downloaded as packets. |
| Download Bytes | Display the amount of data downloaded as bytes. |
| Upload Pkts | Display the amount of data uploaded as bytes. |
| Upload Bytes | Display the amount of data uploaded as bytes. |

Uptime

Display the time duration that the VPN tunnel has been active.

| INTERFACE | TYPE | Tunnel | REMOTE LOCAL IP | DNS | UPTIME | ACTION |
|-----------|-------------|--------|-----------------|---------|--------|--------|
| WAN | L2TP Client | -- | 192.168.11.2 | 8.8.8.8 | 3 h | |
| WAN | PPTP Client | -- | 192.168.10.2 | 8.8.8.8 | 3 h | |

Showing 1-2 of 2 records < 1 > 25 / page Go To page: Go

The listed information of OpenVPN/PPTP/L2TP (Client) table is explained as follows (some information listed below is hidden by default). You can further filter the entries based on their type.

Interface

Display the interface that the traffic goes through.

Tunnel

Display the name of the VPN client.

Type

Display the connection type.

Remote Local IP

Display the IP address of the remote user of the VPN tunnel.

DNS

Display the DNS address of the VPN tunnel.

Download Pkts

Display the amount of data downloaded as packets.

Download Bytes

Display the amount of data downloaded as bytes.

Upload Pkts

Display the amount of data uploaded as bytes.

Upload Bytes

Display the amount of data uploaded as bytes.

Uptime

Display the time duration that the VPN tunnel has been active.

| USERNAME | LOGIN IP | VIRTUAL IP | LOGIN TIME | STATISTICS | ACTION |
|----------|-------------|-------------|--------------------------|-----------------------|--------|
| user1 | 192.168.0.1 | 192.168.0.2 | May 08, 2022 07:24:42 pm | ↑ 2.48 KB ↓ 120.76 KB | |

Showing 1-2 of 2 records < 1 > 25 / page Go To page: Go [View Locked Out Users >](#)

The listed information of SSL VPN table is explained as follows.

Username

Display the username of the remote user.



| | |
|------------|---|
| Login IP | Display the login IP address of the remote user. |
| Virtual IP | Display the virtual IP address of the remote user. |
| Login Time | Display the login time of the remote user. |
| Statistics | Display the upload and download traffic of the remote user. |

8.5.7 Routing Table

Routing Table displays information of routing entries that have taken effect.

| ID | DESTINATION IP/SUBNETS | NEXT HOP | INTERFACE | METRIC |
|----|------------------------|----------|--------------|--------|
| 1 | 0.0.0.0/0 | 10.0.0.1 | WAN1 | 0 |
| 2 | 10.0.0.0/22 | 0.0.0.0 | WAN1 | 0 |
| 3 | 10.0.0.1 | 0.0.0.0 | WAN1 | 0 |
| 4 | 127.0.0.0/8 | 0.0.0.0 | lo | 0 |
| 5 | 10.10.10.0/24 | 0.0.0.0 | LAN329457056 | 0 |
| 6 | 192.168.0.0/24 | 0.0.0.0 | LAN1 | 0 |

Showing 1-6 of 6 records < 1 > 25/page Go To page: GO

| NAME | DESTINATION IP/SUBNETS | NEXT HOP | DISTANCE | ACTION |
|-------------------|------------------------|--------------|----------|---|
| E4-C3-2A-57-71-AC | 0.0.0.0/0 | 192.168.0.1 | 254 |  |
| E4-C3-2A-57-71-AC | 192.168.0.0/24 | 192.168.0.11 | 0 |  |

Showing 1-2 of 2 records < 1 > 25/page Go To page: GO

A tab is above the table for filtering. You can also click the icons in the Action column for quick operation.



Click the tab to filter the routing information listed in the table.

Gateway/Switch: Click to display the routing information of the gateway or the switch.




(Only for switch) Click to configure the static routes.

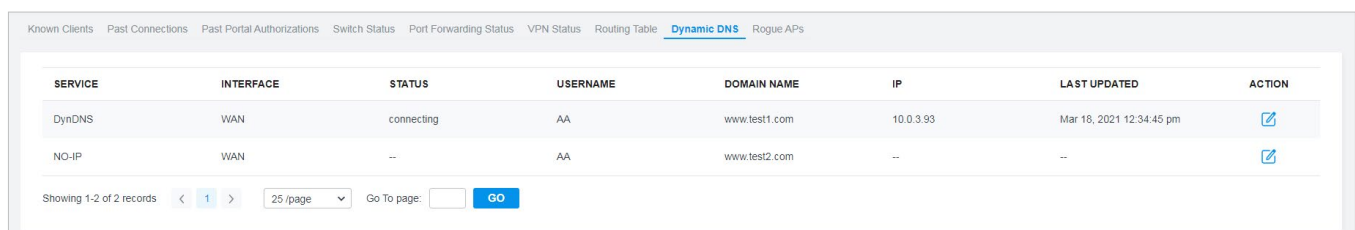
The listed information is explained as follows.



| | |
|------------------------|--|
| Destination IP/Subnets | Display the destination IP addresses of the routing entry.. |
| Next Hop | Display the IP address of the next hop. |
| Interface | (Only for Gateway) Display the interface that the traffic of the entry goes through. |

| | |
|-----------------|--|
| Metric | (Only for Gateway) Display the number of hops before reaching the destination. Generally, if there are a few routing entries with the same destination, the routing with the lowest metric will be used. |
| Distance | (Only for Switch) Display the administrative distance of the routing entry. 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 used. |

8.5.8 Dynamic DNS

In Dynamic DNS, a table displays information about the uses of the dynamic DNS services. You can click  in the Action column to edit the entry.



| SERVICE | INTERFACE | STATUS | USERNAME | DOMAIN NAME | IP | LAST UPDATED | ACTION |
|---------|-----------|------------|----------|---------------|-----------|--------------------------|---|
| DynDNS | WAN | connecting | AA | www.test1.com | 10.0.3.93 | Mar 18, 2021 12:34:45 pm |  |
| NO-IP | WAN | -- | AA | www.test2.com | -- | -- |  |

Showing 1-2 of 2 records < 1 > 25 /page Go To page: GO

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

8.5.9 Rogue APs

A rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. In Rogue APs, you can scan rogue APs and view the rogue APs scanned before.

| NAME/SSID | BSSID | CHANNEL | SECURITY | BEACON | LOCATION | SIGNAL | LAST SEEN |
|---------------|-------------------|-----------|--------------|--------|---|---------------|--------------------------|
| ChinaNet-gcvZ | 48-A7-4E-88-8B-C8 | 11 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 100% (-14dBm) | May 27, 2020 02:01:20 pm |
| yangxinxin2 | 00-0A-EB-13-7A-FF | 9 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 100% (-15dBm) | May 27, 2020 02:01:20 pm |
| mmmmmmmm | 54-A7-03-57-C4-E5 | 6 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 100% (-34dBm) | May 27, 2020 02:01:20 pm |
| Xiaomi_14CD | EC-41-18-E6-14-CE | 1 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 100% (-43dBm) | May 27, 2020 02:01:20 pm |
| nxclly | 8C-AB-8E-99-76-B0 | 13 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 100% (-50dBm) | May 27, 2020 02:01:20 pm |
| midea_e2_2087 | 3C-2C-94-20-C9-52 | 6 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 98% (-51dBm) | May 27, 2020 02:01:20 pm |
| ChinaNet-eGaN | 80-41-26-05-15-64 | 10 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 83% (-57dBm) | May 27, 2020 02:01:20 pm |
| ChinaNet-y7Fk | DC-A3-33-B0-C2-12 | 1 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 80% (-58dBm) | May 27, 2020 02:01:20 pm |
| ChinaNet-azsL | 94-BF-80-88-33-C0 | 7 (11ng) | WPA-Personal | 100 | Nearest B0-95-75-E6-48-C2 | 20% (-82dBm) | May 27, 2020 02:01:20 pm |

Showing 1-25 of 75 records < 1 2 3 > 25 /page Go To page: **GO**

Enter the client name or MAC address to search the clients.

 -

Filter the rogue APs based on Last Seen.

Click the selector to open the calendar. Click a specific date twice in the calendar to display the rogue APs scanned on the day. To display the scanned AP during a time range, click the start date and end date in the calendar.

Click the tab to filter the rogue APs listed in the table based on the frequency band.

Click to scan rogue APs. It may take several minutes, and the wireless service may be influenced during scanning.

BSSID

A string with a similar form as MAC address to recognize access points.

Channel

Displays the operation channel and standard of the rogue AP.

Security

Displays the security strategy of the rogue AP.

Beacon

Displays the beacon interval of the rogue AP.

Beacons are transmitted periodically by the EAP to announce the presence of a wireless network for the clients, and the interval means how often the AP send a beacon to clients.

Location

Displays the managed AP nearest to the rogue AP. You can click the nearest AP to open its Properties window.

Signal

Displays the signal strength in percentage and dBm).

Last Seen

Display the last time that the rogue AP was scanned by the controller.

▼ 8.6 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 [8.6.1 Alerts](#) and [8.6.2 Events](#), and configure their notification levels in [8.6.3 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

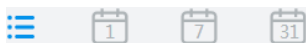
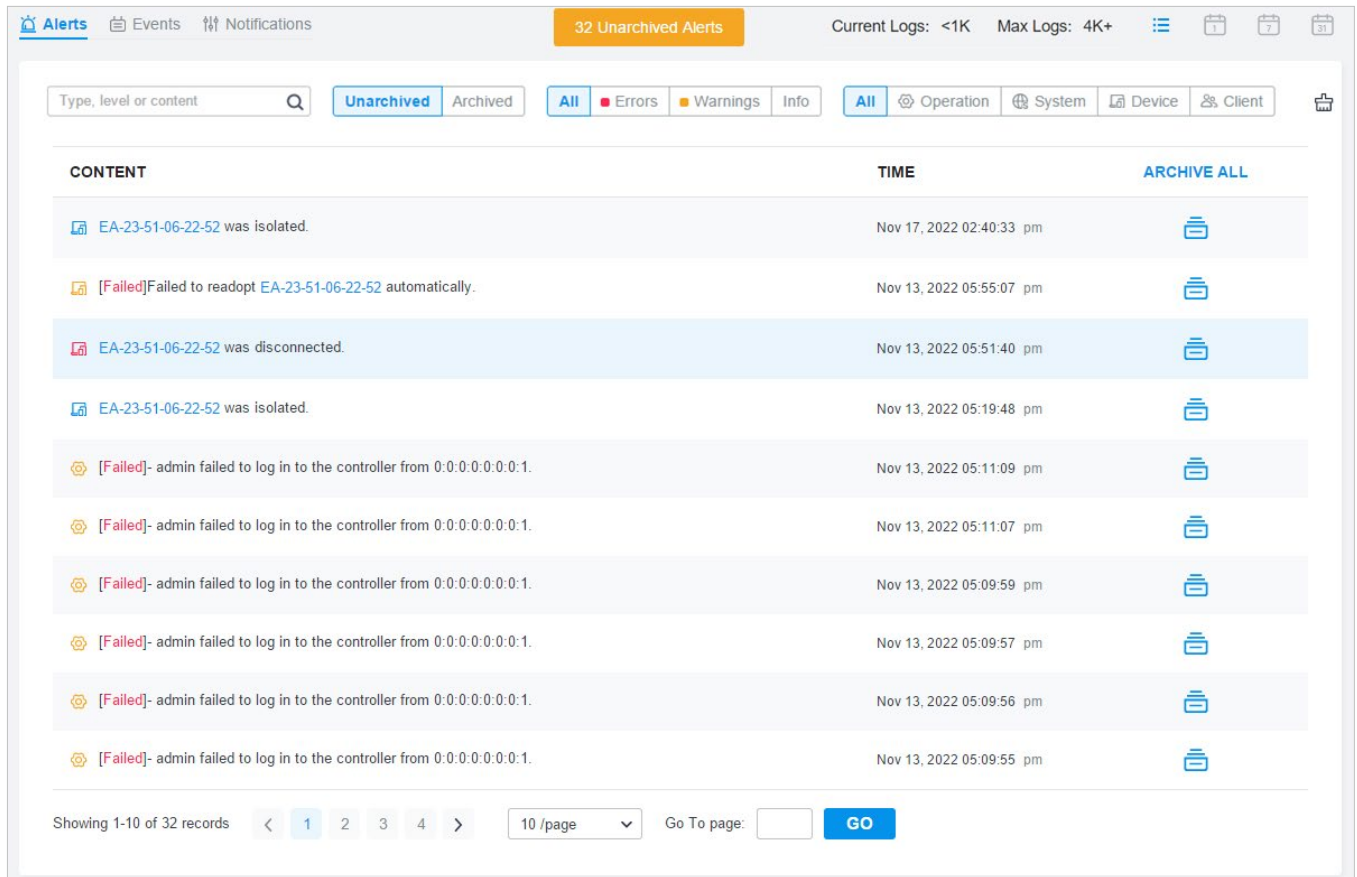
Three levels in severities are Error, Warning, and Info, whose influences are ranked from high to low.

■ Contents

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

8.6.1 Alerts

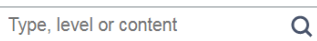
Alerts are the logs that need to be noticed and archived specially. You can configure the logs as Alerts in Notifications, and all the logs configured as Alerts are listed under the Alerts tab for you to search, filter, and archive.



Click to change the view mode for a better overview.

: Displays the logs in a table.

: Displays the logs in a day/week/month. To change the time, click < or >. To jump back to the current one, click [Today/This Week/This Month](#).



Enter the content types, severity levels, or key words to search the logs.



Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously.







Unarchived/Archived: Click the tab to filter the unarchived and archived logs. You can click and **Archive All** to archive a single log and all, respectively.

All/Errors/Warnings: Click **All** to display logs in both Error, Warning, and Info levels. Click **Errors** or **Warnings** to display logs in Error or Warning levels only.

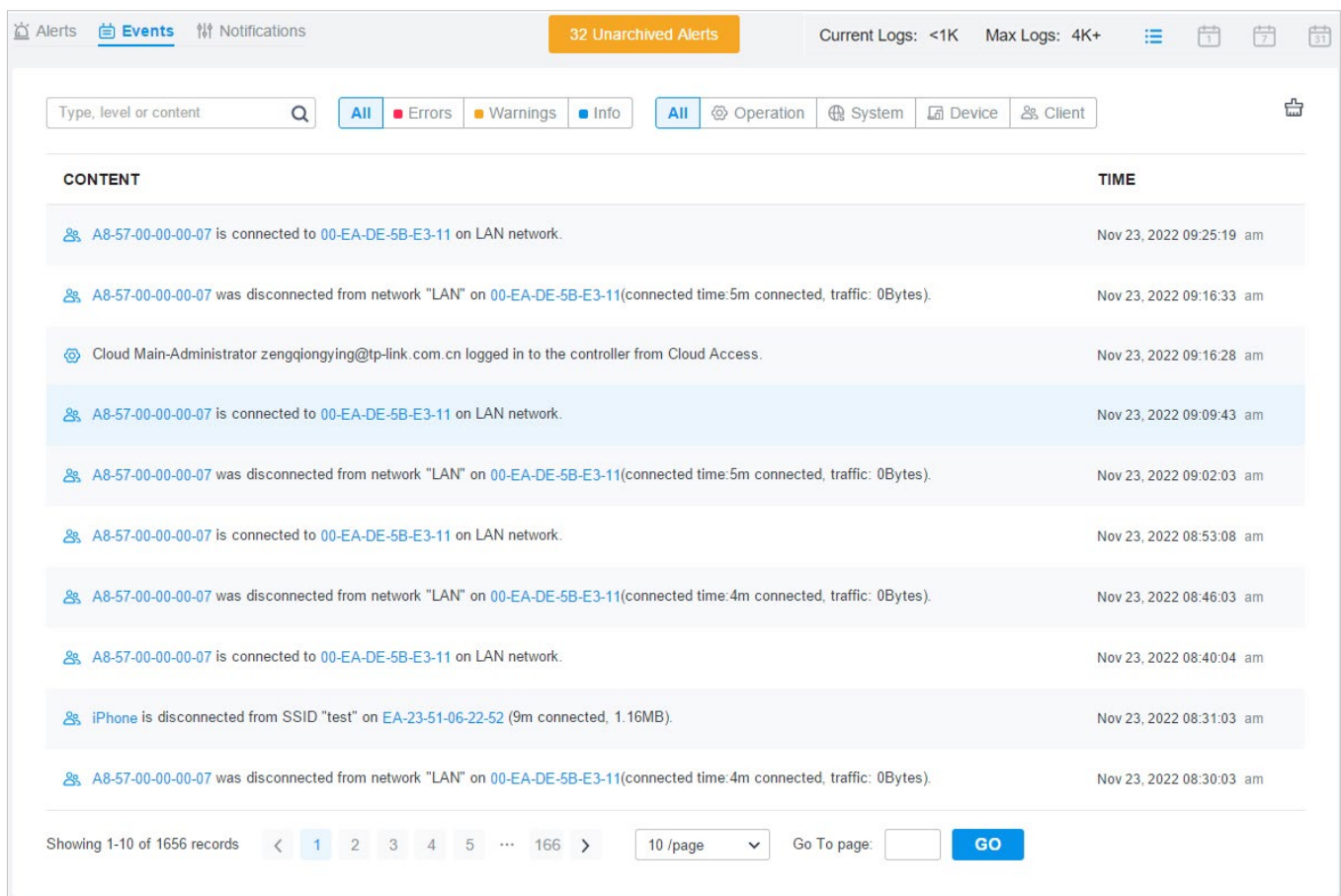
Content

Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.


| | |
|---|---|
|  | Displays when the activity happened. |
|  | Click to archive all unarchived logs. |
|  | Click to archive the log entry. |
|  | Click and select the log types to delete the corresponding alert logs. Once deleted the archived alerts cannot be recovered. The unarchived alerts cannot be deleted. |











8.6.2 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.

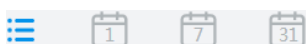


Alerts **Events** Notifications 32 Unarchived Alerts Current Logs: <1K Max Logs: 4K+

Type, level or content 






| CONTENT | TIME |
|--|--------------------------|
|  A8-57-00-00-00-07 is connected to 00-EA-DE-5B-E3-11 on LAN network. | Nov 23, 2022 09:25:19 am |
|  A8-57-00-00-00-07 was disconnected from network "LAN" on 00-EA-DE-5B-E3-11 (connected time:5m connected, traffic: 0Bytes). | Nov 23, 2022 09:16:33 am |
|  Cloud Main-Administrator zengqiongying@tp-link.com.cn logged in to the controller from Cloud Access. | Nov 23, 2022 09:16:28 am |
|  A8-57-00-00-00-07 is connected to 00-EA-DE-5B-E3-11 on LAN network. | Nov 23, 2022 09:09:43 am |
|  A8-57-00-00-00-07 was disconnected from network "LAN" on 00-EA-DE-5B-E3-11 (connected time:5m connected, traffic: 0Bytes). | Nov 23, 2022 09:02:03 am |
|  A8-57-00-00-00-07 is connected to 00-EA-DE-5B-E3-11 on LAN network. | Nov 23, 2022 08:53:08 am |
|  A8-57-00-00-00-07 was disconnected from network "LAN" on 00-EA-DE-5B-E3-11 (connected time:4m connected, traffic: 0Bytes). | Nov 23, 2022 08:46:03 am |
|  A8-57-00-00-00-07 is connected to 00-EA-DE-5B-E3-11 on LAN network. | Nov 23, 2022 08:40:04 am |
|  iPhone is disconnected from SSID "test" on EA-23-51-06-22-52 (9m connected, 1.16MB). | Nov 23, 2022 08:31:03 am |
|  A8-57-00-00-00-07 was disconnected from network "LAN" on 00-EA-DE-5B-E3-11 (connected time:4m connected, traffic: 0Bytes). | Nov 23, 2022 08:30:03 am |



Showing 1-10 of 1656 records ... Go To page:



Click to change the view mode.

 Displays the logs in a table.

  : Displays the logs in a day/week/month. To change the time, click  or . To jump back to the current one, click [Today/This Week/This Month](#).

| | |
|---|--|
| <input type="text" value="Type, level or content"/>  | Enter the content types, severity levels, or key words to search the logs. |
|  | Click and select the log types to delete the corresponding event logs. |
| <input type="button" value="All"/> <input type="button" value="Errors"/> <input type="button" value="Warnings"/> <input type="button" value="Info"/> | Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously. |
| <input type="button" value="All"/> <input type="button" value="Operation"/> <input type="button" value="System"/> <input type="button" value="Device"/> <input type="button" value="Client"/> | <p>All/Errors/Warnings/Info: Click All to display logs in both Error and Warning levels. Click Errors, Warnings or Info to display logs in the corresponding level only.</p> <p>All/Operation/System/Device/Client: Click All to display all types of logs. Click Operation or System or Device or Client to display the corresponding type of logs only.</p> |
| Content | Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information. |
| Time | Displays when the activity happened. |

8.6.3 Notifications

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

With proper configurations, the controller will send emails to the administrators when it records the logs.

| Operation | System | Device | Client |
|---------------------------|---|---|--------------------------------|
| Advanced Features Enabled | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Management VLAN Changed | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Voucher Created | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Voucher Deleted | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Rolling Upgrade Triggered | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Device Adopted | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Device Adoption Failed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Device Adoption in Batch | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Device Rebooted | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email |
| Device Reboot Failed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input type="checkbox"/> Email |

To specify the logs as Alert/Event, click the corresponding checkboxes of logs and click [Apply](#). The following icons and tab are provided as auxiliaries.

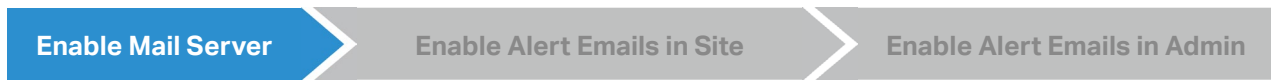
| | |
|---|--|
| Reset to Default | Click to reset all notification configurations in the current site to the default. |
| Operation System Device Client | Click the tabs to display the configurations of corresponding log types. |
| <input type="checkbox"/> Event <input type="checkbox"/> Alert | Enable the checkboxes to specify the activity logs as Events/Alerts, and then the recorded logs will be displayed under the Events/Alerts tab. If both of them are disabled, the controller will not record the activity logs. |
| <input type="checkbox"/> Email | Enable the checkboxes to specify the activity logs as alert logs. With proper settings in Site and Admin, the controller can send emails to notify the administrators and viewers of the site's alert logs once generated. |
| | This icon appears when the configuration of a log is changed but has not been applied. Click it to reset the configuration of the log to the default. |

The Email checkboxes are used to enable Alert Emails for the logs. To make sure the administrators and viewers can receive alert emails of the site, follow the following steps:

- 1) Enable Mail Server
- 2) Enable Alert Emails in Site

3) Enable Alert Emails in Admin

4) Enable Alert Emails in Logs



Go to [Settings](#) > [Controller](#). In the [Mail Server](#) section, enable SMTP Server and configure the parameters. Then click [Save](#).

Mail Server

i With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. For security reasons, we recommend that you configure Mail Server carefully.

SMTP Server: Enable

SMTP:

Port: (1-65535)

SSL: Enable

Authentication: Enable

Sender Address: (Optional)

Test SMTP Server: Send Test Email to

| | |
|--------------------------------|--|
| SMTP | Enter the URL or IP address of the SMTP server according to the instructions of the email service provider. |
| Port | Configure the port used by the SMTP server according to the instructions of the email service provider. |
| SSL | Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between the controller and the SMTP server. |
| Authentication | Enable or disable Authentication according to the instructions of the email service provider. If Authentication is enabled, the SMTP server requires the username and password for authentication. |
| Username | Enter the username for your email account if Authentication is enabled. |
| Password | Enter the password for your email account if Authentication is enabled. |
| Sender Address | (Optional) Specify the sender address of the email. |

Test SMTP Server

Test the Mail Server configuration by sending a test email to an email address that you specify.

Enable Mail Server

Enable Alert Emails in Site

Enable Alert Emails in Admin

5. Go to [Settings](#) > [Site](#) and enable [Alert Emails](#) in the [Services](#) section.

Services

LED: Enable

Automatic Upgrades: Enable

Channel Limit: Enable [i](#)

Mesh: Enable [i](#)

Auto Failover: Enable [i](#)

Connectivity Detection: [v](#)

Full-Sector DFS: Enable [i](#)

Periodic Speed Test: Enable [Speed Test History](#)

Speed Test Interval: hours (10-999)

Alert Emails: Enable alert emails [i](#)

Send similar alerts within seconds in one email. [i](#)

Remote Logging: Enable [i](#)

Syslog Server IP/Hostname:

Syslog Server Port: (1-65535)

Client Detail Logs: Enable [i](#)

Advanced Features: Enable

6. (Optional) On the same page, enable [Send similar alerts within seconds in one email](#) and specify the time interval. When enabled, the similar alerts generated in each time period are collected and sent to administrators and viewers in one email.

Alert Emails: Enable alert emails [i](#)

Send similar alerts within seconds in one email. [i](#)

7. Click [Apply](#).



Go to [Admin](#) and configure Alert Emails for the administrators and viewers to receive the emails. Click [+ Add New Admin Account](#) to create an account or click [🔗](#) to edit an account. Enter the email address in [Email](#) and enable [Alert Emails](#). Click [Create](#) or [Apply](#).

Edit Account

Username:

Change Password: Enable

Role: ▾

Site Privileges: All (Including all new-created sites)
 Sites

Device Permissions: Adopt Devices
 Manage Devices (Move to Site, Restart, Upgrade and Forget)

Email:

Alert Emails: Enable ⓘ

[Save](#) [Cancel](#)

Enable Alert Emails in Site

Enable Alert Emails in Admin

Enable Alert Emails in Logs

Go to [Logs](#) and click [Notifications](#). Click a tab of content types and enable [Email](#) for the activity logs that the controller emails administrators. Click [Save](#).

Alerts
Events
Notifications
Reset to Default

Operation
System
Device
Client

| | | | | |
|-----------------------------------|---|---|---|--|
| Reboot Schedule Executed | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| Reboot Schedule Execution Failed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| PoE Schedule Executed | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email | |
| PoE Schedule Execution Failed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| Logs Mailed Automatically | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| Automatic Logs Mail Failed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| Logs Sent to Log Server | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| Sending Logs to Log Server Failed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| Auto Backup Executed | <input checked="" type="checkbox"/> Event | <input type="checkbox"/> Alert | <input type="checkbox"/> Email | |
| Auto Backup Failed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| Controller Access Port Changed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |
| Portal Port Changed | <input checked="" type="checkbox"/> Event | <input checked="" type="checkbox"/> Alert | <input checked="" type="checkbox"/> Email | |

Save
Cancel

♥ 8.7 Monitor the Network with Tools

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

- **Network Check**
Test the device connectivity via ping or traceroute.
- **Packet Capture**
Capture packets for network troubleshooting.
- **Terminal**
Open Terminal to execute CLI or Shell commands.

ⓘ Note:

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

8.7.1 Network Check

1. In the Site view, go to [Tools > Network Check](#).
2. Configure the test parameters.

Network Check

Device Type: Sources:

Test: Destination Type:

Domain/IP Address:

Advanced Test Settings

Packet Size: (10-2000) Count: (1-100)

ⓘ Devices which are already running commands shall not execute newly added commands. Output history of device with buffer space issues shall be automatically cleared

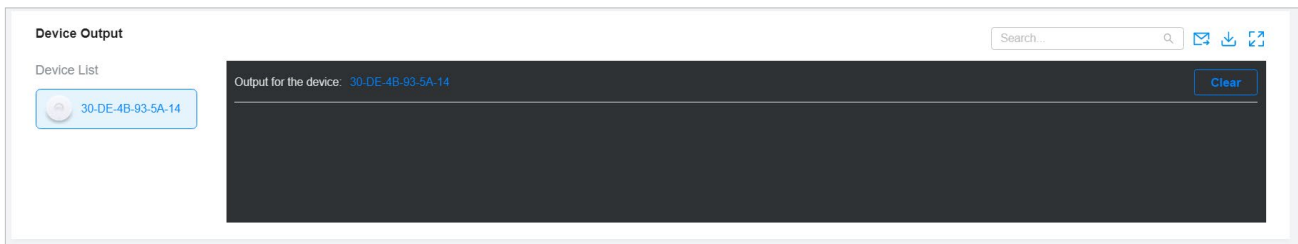
[Run](#)

| | |
|-------------------------|--|
| Device Type | Select the type of device(s) to perform a test: EAP, Switch, or Gateway. |
| Sources | Select one or multiple devices to perform a test. |
| Test | <p>Choose the Ping or Traceroute tool to test the device connectivity.</p> <p>Ping: Test the connectivity between the specified sources and destination, and measure the round-trip time.</p> <p>Traceroute: Display the route (path) the specified sources have passed to reach the specified destination, and measure transit delays of packets across an Internet Protocol network.</p> |
| Destination Type | Select the destination type and specify the Domain/IP Address or Client to ping. Client is unavailable in the traceroute test or when multiple AP devices perform the ping test. |
| Packet Size | When Test Type is Ping , specify the size of ping packets. |

CountWhen **Test Type** is **Ping**, specify the number of ping packets.**Note:**

- Devices which are already running commands shall not execute newly added commands.
- Output history of device with buffer space issues shall be automatically cleared.

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



Click to email the test logs to a mailbox.



Click to download the test logs locally.



Zoom out and zoom in the display area.

8.7.2 Packet Capture

1. In the Site view, go to **Tools > Packet Capture**.
2. Configure the parameters for packet capture.

Packet Capture

Sources: 30-DE-4B-93-5A-14

Interface Type: Wired Wireless

Select Port: ETH0

Duration: 100 seconds (1-300)

Single Packet Size: 1000 Bytes

Packet Capture Filters: (src 192.168.0.1 and tcp port 80) or (src 192.168.0.1 and tcp port 90)
(Optional)

Supported filters:
host, src, dst, tcp port, tcp src port, tcp dst port, udp port, udp src port, udp dst port, ether host, ether src, ether dst

Combination of operators "and", "or", "(" and ")" is supported between multiple filter items. For example:
(src 192.168.0.1 and tcp port 80) or (src 192.168.0.1 and tcp port 90)
(src 192.168.0.1 and tcp src port 80) or (dst 192.168.0.1 and tcp dst port 90)
ether src A0:00:00:04:C5:84 and ether dst A0:00:00:04:C5:85

Note:
host: host address, src: source, dst: destination, ether: ethernet address (MAC address)

1. Packet size cannot exceed 1 MB.
2. The file will be kept for 10 minutes only and can only be downloaded three times.

Start Packet Capture
Download .pcap Files

Sources

Select the source device to capture packets.

| | |
|-------------------------------|--|
| Interface Type | Select the Wired interface type and specify the Port , or select the Wireless interface type and specify the Band and SSID / Interface . |
| Duration | Specify the duration for packet capture. |
| Single Packet Size | Specify the size of a single captured packet. It cannot exceed 1 MB. |
| Packet Capture Filters | <p>Enter the filters to capture packets. Supported filters include: host, src, dst, tcp port, tcp src port, tcp dst port, udp port, udp src port, udp dst port, ether host, ether src, ether dst</p> <p>Combination of operators "and", "or", "(" and ")" is supported between multiple filter items. For example: (src 192.168.0.1 and tcp port 80) or (src 192.168.0.1 and tcp port 90)</p> <p>Note: host: host address, src: source, dst: destination, ether: ethernet address (MAC address)</p> |

3. Click [Start Packet Capture](#) to capture packets. After packets are captured, you can click [Download .pcap Files](#) to download them.

ⓘ **Note:**

The file will be kept for 10 minutes only and can only be downloaded three times.

8.7.3 Terminal

1. In the Site view, go to [Tools > Terminal](#).
2. Configure the parameters.

Remote Control Terminal Session

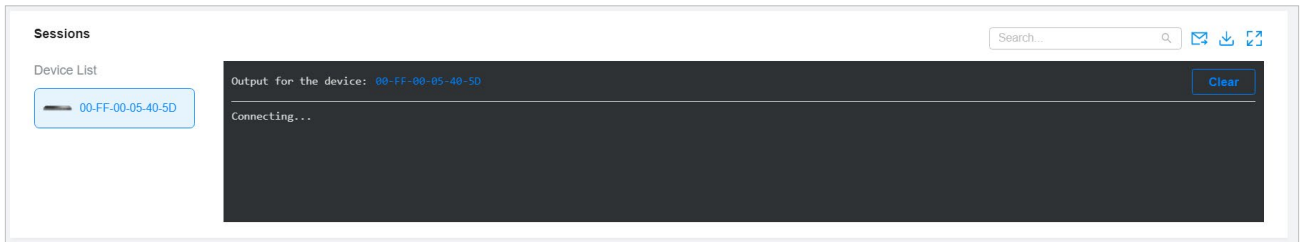
Device Type:

Sources:

[Open Terminal](#)

| | |
|--------------------|--|
| Device Type | Select the type of device(s) to test: EAP, Switch, or Gateway. |
| Sources | Select one or multiple devices to test. |

3. Click [Open Terminal](#). Now you can run CLI or Shell commands.



Click to email the test logs to a mailbox.



Click to download the test logs locally.



Zoom out and zoom in the display area.

9

Manage Accounts of the SDN Controller

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

- [9.1 Introduction to User Accounts](#)
- [9.2 Create and Manage Custom Account Roles](#)
- [9.3 Manage and Create Local User Accounts](#)
- [9.4 Manage and Create Cloud User Accounts](#)

♥ 9.1 Introduction to User Accounts

The SDN Controller offers three levels of access available for users: **main administrator**, **administrator**, and **viewer**. You can also create new account roles and customize their permissions to access different features.

Since the controller can be accessed both locally and via cloud access, users can be further grouped into local users and cloud users.

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

Moreover, in the user accounts list of the main administrator, all accounts created by the main administrator will be displayed. The accounts created by each administrator will be hidden by default, making the interface more systematic and to the point.

■ Main Administrator

The main administrator has access to all features.

The account who first launches the controller will be the main administrator. It cannot be changed and deleted.

■ 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 main 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 main administrator and administrators.

■ Custom roles

Custom roles can be configured to access different features.

They can be created or deleted only by the main administrator.

ⓘ Note:

Please upgrade Omada APP to version 4.6 or later, otherwise you may not be able to log in with the accounts bound with customized roles.

♥ 9.2 Create and Manage Custom Account Roles

1. Select [Global](#) from the drop-down list of [Organization](#) in the top-right corner. Go to [Account > Role](#).

2. Click **Add New Role**. Specify the role type name and customize the permissions for the role.

Add New Role

Role Type Name:

Global

Dashboard

Dashboard Manager: Modify View Only Block

Device

Device Manager: Modify View Only Block

Adopt Device Manager: Access Block

Log

Log Manager: Modify View Only Block

Account

Users Manager: Modify View Only Block

Roles Manager: Modify View Only Block

Settings

Other: Modify View Only Block

Export Data: Access Block

Export Global Log List: Access Block

Site

Dashboard

Dashboard Manager: Modify View Only Block

Hotspot Manager

Hotspot Manager: Modify View Only Block

Statics

Statics Manager: Access Block

Device

Device Manager: Modify View Only Block

Adopt Device Manager: Access Block

Log

Log Manager: Modify View Only Block

Map

Map Manager: Modify View Only Block

Clients

Clients Manager: Modify View Only Block

Insight

Insight Manager: Modify View Only Block

Network Analyze

Network Analyze manager: Modify View Only Block

Network Report

Network Report Manager: Modify View Only Block

Settings

Site Settings Manager: Modify View Only Block

Device Account Manager: Access Block

Export Data: Access Block

3. Click **Create**. The new role will be displayed in the role list.

| ROLE | SOURCE | ACTION |
|--------------------|------------|--------|
| Main Administrator | Default | |
| Administrator | Default | |
| Viewer | Default | |
| 123 | Controller | |

Showing 1-4 of 4 records < 1 > 10 / page Go To page:


To edit/delete a custom role, click the icon in the ACTION Column.

♥ 9.3 Manage and Create Local User Accounts

By default, the SDN Controller automatically sets up a local user with the role called main administrator as the primary administrator. The username and password of the main administrator are the same as that of the controller account by default. The main administrator cannot be deleted, and it can create, edit, and delete other levels of user accounts.

9.3.1 Edit the Main Administrator Account

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

1. Select [Global](#) from the drop-down list of [Organization](#) in the top-right corner. Go to [Account > User](#).
2. Click  in the Action column. Check and edit the account information. Click [Save](#).

Basic Information

Role: Main Administrator Permission Transfer

TP-Link ID:

Site Privileges: All Sites

Edit User

Alert Emails: Enable (i)

Save
Cancel

Permission Transfer

Click the button and select a new main administrator to transfer the Cloud Main Administrator permissions of the current account to the new account. The current account will be downgraded as Administrator.

Alert Emails

Check the box if you want the current user to receive emails about alerts of the privileged sites.

9.3.2 Create and Manage Other Local Accounts

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


1. Select [Global](#) from the drop-down list of [Organization](#) in the top-right corner. Go to [Account > User](#).
2. Click [Add New User](#).


3. Select **Local User** for the administrator type in the pop-out window. Specify the parameters and click **Create**.

Add New User

Administrator Type : Local User
 Cloud User


Username :

Password : 

Role : 

Site Privileges : All (Including all new-created sites)
 Sites

Email : (Optional)

Alert Emails : Enable 

Create **Cancel**

Username Specify the username. The username should be different from the existing ones.

Password Specify the password.

Role Select a role for the created user account.

Administrator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete main administrator.

Viewer: This role can view the information of the sites chosen in the site privileges. It can only edit itself.

Custom roles: If you have created custom roles, they will be displayed in the list. To create custom roles, refer to [9.2 Create and Manage Custom Account Roles](#).

| | |
|-----------------|--|
| Site Privileges | Assign the site permissions to the created local user. |
| | All: The created user has device permissions in all sites, including all new-created sites. |
| | Sites: The created user has device permission in the sites that are selected. Select the sites by checking the box before them. |

| | |
|------------------|--|
| Email (optional) | Enter an email address for receiving alert emails. |
|------------------|--|

| | |
|--------------|---|
| Alert Emails | Check the box if you want the created user to receive emails about alerts of the privileged sites. For detailed configurations, refer to 4. 2. 2 Services . |
|--------------|---|

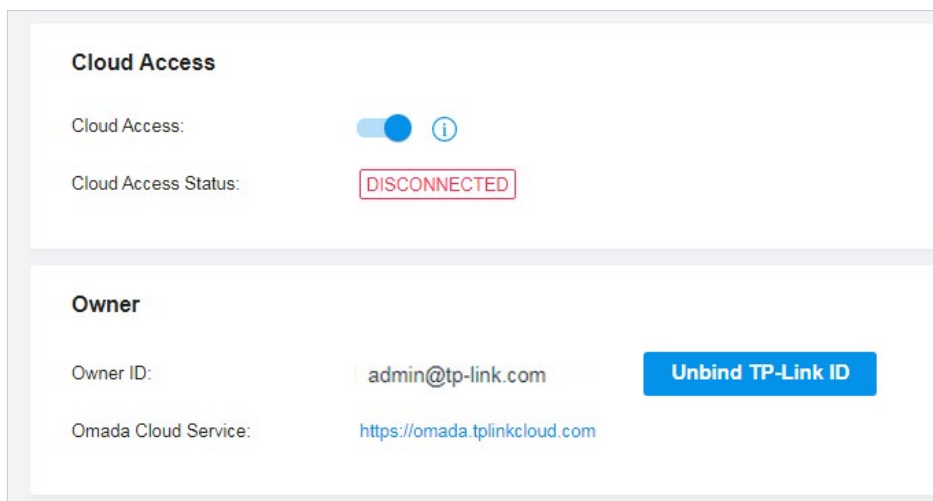
♥ 9.4 Manage and Create Cloud User Accounts

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

9.4.1 Set Up the Cloud Main Administrator

For software and hardware controller, if you have not enabled the cloud access and bound the controller with a TP-Link ID in quick setup, to set up the cloud main administrator, follow these steps:

1. Select [Global](#) from the drop-down list of [Organization](#) in the top-right corner. Go to [Settings](#) > [Cloud Access](#) to enable Cloud Access and bind your TP-Link ID.



2. Go to [Account](#) > [User](#). A cloud main administrator with the same username as the TP-Link ID will be automatically created. The Cloud Main Administrator cannot be deleted. You can log in with the cloud main administrator when the cloud access is enabled.

9.4.2 Create and Manage Other Cloud Accounts

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

1. Select [Global](#) from the drop-down list of [Organization](#) in the top-right corner. Go to [Account](#) > [User](#).
2. Click [Add New User](#).

3. Select **Cloud User** for the administrator type in the pop-out window. Specify the parameters and click **Invite**.

Add New User

Administrator Type : Local User
 Cloud User

TP-Link ID : ⓘ

Role : ▾

Site Privileges : All (Including all new-created sites)
 Sites

Alert Emails : Enable ⓘ

TP-Link ID

Enter an email address of the created cloud user, and then an invitation email will be sent to the email address.

If the email address has already been registered as a TP-Link ID, it will become a valid cloud user after accepting the invitation.

If the email address has not been registered, it will receive an invitation email for registration. After finishing registration, it will automatically becomes a valid cloud user.

Role

Select a role for the created cloud user.

Administrator: This role has permissions to adopt and/or manage devices of the sites chosen in the site privileges, edit itself, create/edit/delete viewer accounts in its privileged sites. However, it cannot delete itself or edit/delete 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.

Custom roles: If you have created custom roles, they will be displayed in the list. To create custom roles, refer to [9.2 Create and Manage Custom Account Roles](#).

Site Privileges

Assign the site permission to the created cloud user.

All: The created user has permission in all sites, including all new-created sites.

Sites: The created user has permission in the sites that are selected. Select the sites by checking the box before them.

Alert Emails

Check the box if you want the created user to receive emails about alerts of the privileged sites. For detailed configurations, refer to [4. 2. 2 Services](#).



Manage Customer Networks in MSP Mode

MSP (Managed Service Provider) mode allows you to know the status of your customers at a glance, and manage customers in the Omada platform.


- **Customer Monitoring**
Keep you informed of accurate, real-time status of every customer.
- **Customer Management**
Manage all customers to deploy the whole network.
- **Account Settings**
Manage all administrative accounts.

This chapter will introduce how to enable MSP mode and manage customer networks in MSP view.

- [10.1 Quick Start](#)
- [10.2 Add and Manage Accounts](#)
- [10.3 Manage System Settings](#)

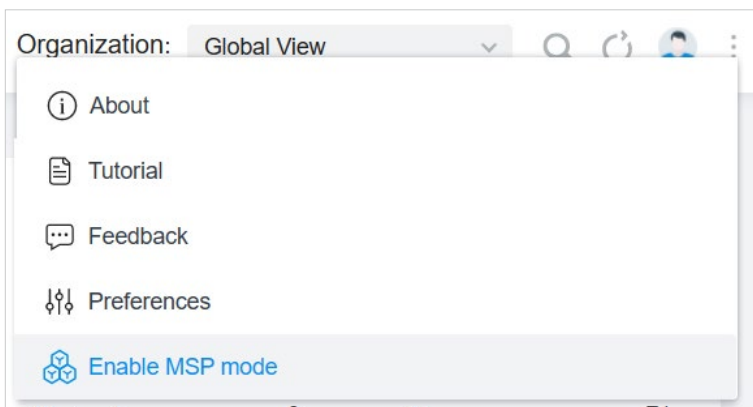
♥ 10.1 Quick Start

10.1.1 Enable the MSP Mode

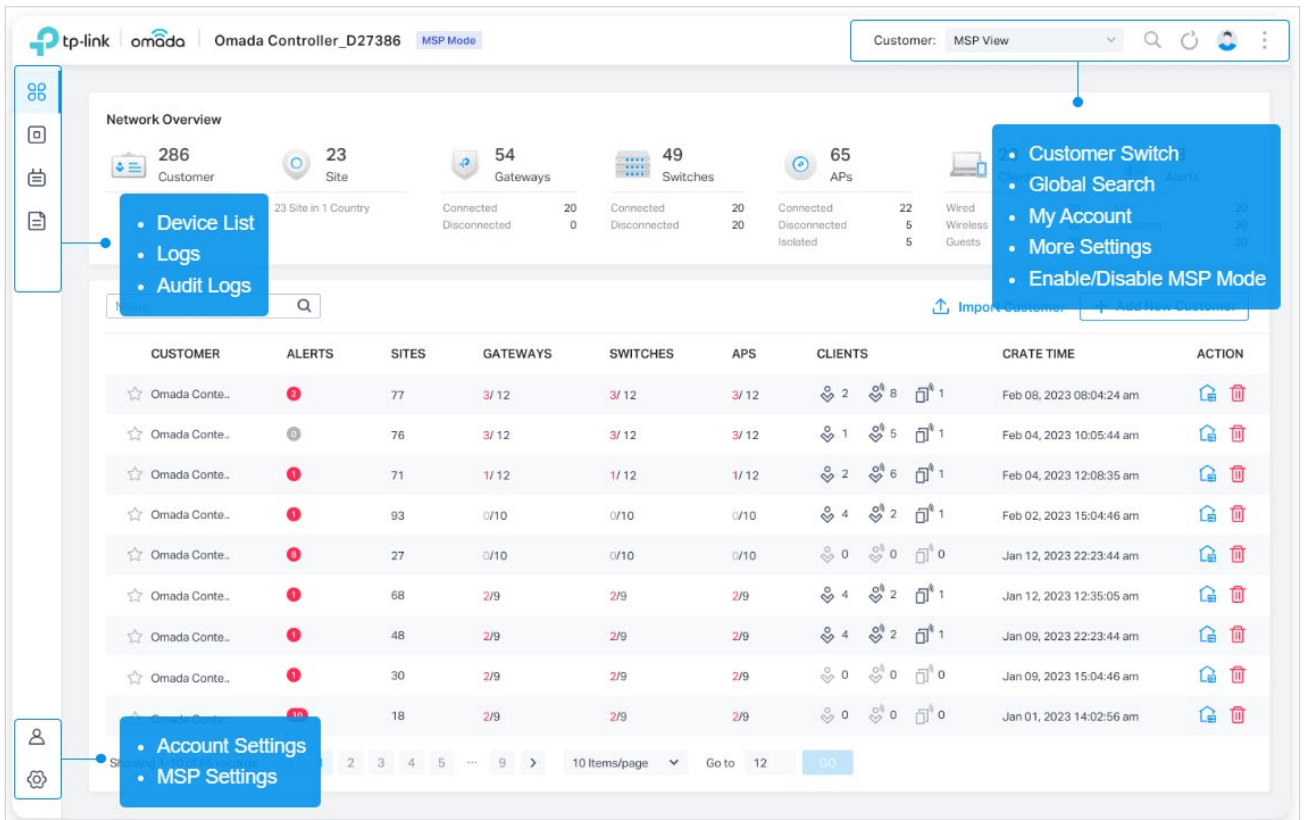
1. Launch your controller.
2. In Global View, click  in the top-right corner and click [Enable MSP mode](#). In the dialog box that pops up, confirm the operation.

 **Note:**

Enabling or disabling MSP mode may cause problems on the connected Cloud access page. In this case, re-enter the web page.



You will enter the MSP view.

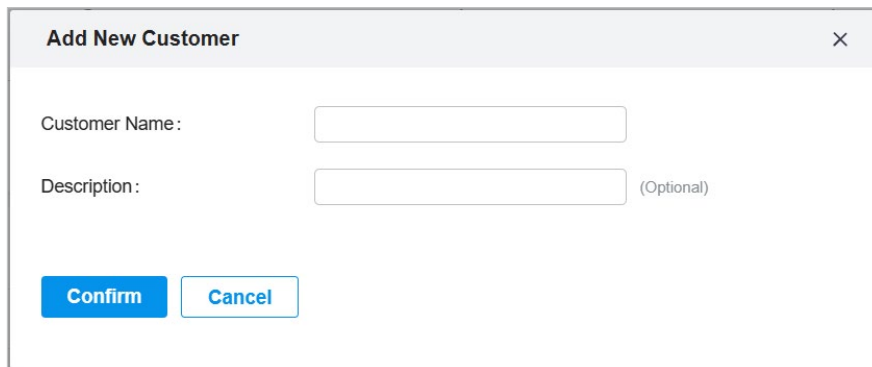


10.1.2 Add and Manage Customers

1. In MSP View, go to the [Customer](#) page.
2. Add customers by using one of the following methods:


- **Add a new customer**

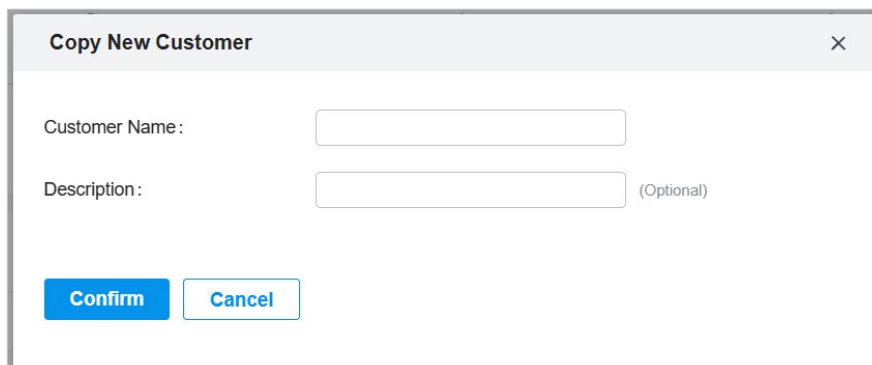
Click [Add New Customer](#) above the customer list. Specify the customer name and enter a description. Then save the settings.



The screenshot shows a dialog box titled "Add New Customer" with a close button (X) in the top right corner. It contains two input fields: "Customer Name:" and "Description:". The "Description:" field is followed by the text "(Optional)". At the bottom of the dialog, there are two buttons: "Confirm" (highlighted in blue) and "Cancel".

- **Copy an existing site**

Click the  icon of a customer entry. Specify the customer name and enter a description. Then save the settings.



The screenshot shows a dialog box titled "Copy New Customer" with a close button (X) in the top right corner. It contains two input fields: "Customer Name:" and "Description:". The "Description:" field is followed by the text "(Optional)". At the bottom of the dialog, there are two buttons: "Confirm" (highlighted in blue) and "Cancel".

- **Import customers from another controller**

Click [Import Customer](#) above the customer list. Specify the customer name and enter a description. Determine whether to retain device info according to your needs. Then import customer from a local file or from a file server.

Import Customer [X]

Name:

Description: (Optional)

Import: Import from Local File
 Import from File Server

Choose File:

3. The new customers will be added to the customer list and the drop-down list of [Customers](#).

In the customer list, you can view the customer information, and click the icons in the ACTION column to manage customer entries and launch the controller of each customer.

| CUSTOMER | SITES | GATEWAYS | SWITCHES | APS | CREATE TIME | ACTION |
|--------------|-------|----------|----------|-------|--------------------------|----------------------------------|
| ☆ Customer 1 | 1 | 0 / 0 | 1 / 0 | 0 / 0 | May 10, 2023 01:28:43 am | [Edit] [Refresh] [Delete] [Home] |
| ☆ Customer 2 | 0 | 0 / 0 | 0 / 0 | 0 / 0 | May 22, 2023 03:53:43 am | [Edit] [Refresh] [Delete] [Home] |
| ☆ Customer 3 | 0 | 0 / 0 | 0 / 0 | 0 / 0 | May 22, 2023 03:53:53 am | [Edit] [Refresh] [Delete] [Home] |

Showing 1-3 of 3 records | 10 / page | Go To page:

10.1.3 Assign and Manage Licenses

1. Launch the Cloud-Based Controller. In MSP View, go to the [License](#) page.
2. Go to [License > Licenses](#). Enable [Auto-Active](#) and [Auto-Renewal](#) if needed.

[Auto-Active](#) will automatically apply device license to a device as soon as it is adopted by your controller. After Auto-Active is enabled on the controller, all its customers will enable Auto-Active by default.

When [Auto-Renewal](#) is enabled for a customer, the licenses for active devices of the customer will be automatically renewed when they expire.

Auto-Active

Auto-Active will automatically apply device license to a device as soon as it is adopted by your controller. After Auto-Active is enabled on the controller, all its customers will enable Auto-Active by default.

Auto-Renewal

Enable this option for a customer, the licenses for active devices of the customer will be automatically renewed when they expire.

| CUSTOMER | Auto-Renewal |
|------------|-------------------------------------|
| Customer 1 | <input checked="" type="checkbox"/> |
| Customer 2 | <input checked="" type="checkbox"/> |
| Customer 3 | <input checked="" type="checkbox"/> |

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

- Go to [License > License Assignment](#), and click [Assign Licenses](#). Select the customer and assign licenses.

Assign Licenses

Remaining Licenses

| TYPE | PRO AP | PRO L2 SWITCH | PRO L3 SWITCH | PRO GATEWAY |
|--------|--------|---------------|---------------|-------------|
| 1-Year | 3 | 1 | 3 | 3 |

1. Select the Customer to assign licenses.

Select Customer:

2. Specify the quantity of licenses to assign.

| TYPE | PRO AP | PRO L2 SWITCH | PRO L3 SWITCH | PRO GATEWAY |
|--------|----------------------|----------------------|----------------------|----------------------|
| 1-Year | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

After license assignment, you can click [Revoke Licenses](#) and select a customer to revoke licenses in case needed.

10.1.4 Add Sites and Devices

- Select a customer from the drop-down list of [Customers](#) in the top-right corner.
- Add sites and adopt devices by referring to [3 Manage Omada Pro Managed Devices and Sites](#).

You can also add devices on the [Devices](#) page in MSP View.

♥ 10.2 Add and Manage Accounts

10.2.1 Configure Role Settings

The system offers two types of roles:

- **MSP Role:** for manage settings in MSP view.
- **Customer Role:** for manage settings in global and site views.

Each role type has three default levels of access permissions: **Main Administrator**, **Administrator**, and **Viewer**. You can also create new account roles and customize their permissions to access different features.

- **Main Administrator**

The Main Administrator has access to all features in the corresponding view.

The account who first launches the controller will be the Main Administrator.

- **Administrator**

Administrators have access to most features in the corresponding view except for some modules. For example, they have no permission to system migration and data auto-backup and have view-only permission to system license management and custom account roles.

- **Viewer**

Viewers can view the status and settings of some features in the corresponding view.

- **Custom roles**

Custom roles can be configured to access different features in the corresponding view.

ⓘ Note:

Please upgrade Omada APP to version 4.6 or later, otherwise you may not be able to log in with the accounts bound with customized roles.

To add a custom role, follow the steps below:

1. In MSP View, go to [Account](#) > [Role](#).

| ROLE | ACTION |
|------------------------|--------|
| MSP Main Administrator | |
| MSP Administrator | |
| MSP Viewer | |

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

+ Add New MSP Role

- 2. MSP roles are used for manage settings in MSP view. On the [MSP Role](#) page, click [Add New MSP Role](#). Specify the role type name and customize the permissions for the role. Parameters may vary by controller type.

Add New Role

Role Type Name:

Customer

Customer Manager: Modify View Only Block

Device

Device Manager: Modify View Only Block

Adopt Device Manager: Access Block

Add Device Manager: Access Block

Bind/Unbind License Manager: Modify View Only Block

License

License Manager: Modify View Only Block

Log & Audit Log

Log & Audit Log Manager: Modify View Only Block

Account

Users Manager: Modify View Only Block

Roles Manager: Modify View Only Block

Saml Roles Manager: Modify View Only Block

Saml Users Manager: Modify View Only Block

Settings

Other: Modify View Only Block

Saml SSO Manager: Modify View Only Block

Webhook Manager: Modify View Only Block

Export Data: Access Block

- Customer roles are used for manage settings in global view and site view. On the [Customer Role](#) page, click [Add New Customer Role](#). Specify the role type name and customize the permissions for the role. Parameters may vary by controller type.

10.2.2 Manage the Main Administrator Account

The account who first launches the controller will be the MSP Main Administrator (for managing settings in MSP View) and Main Administrator (for managing settings in Global View and Site View).

To edit the account settings, follow the steps below:

- In MSP View, go to [Account > User](#).

| USERNAME | MSP ROLE | CUSTOMER ROLE | EMAIL | VERIFIED | CUSTOMER PRIVILEGES | ACTION |
|----------|------------------------|--------------------|-------|----------|---------------------|--------|
| | MSP Main Administrator | Main Administrator | | ✓ | All Customers | |

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

[+ Add New User](#)

2. Click the Edit icon to change settings. You can enable Alert Emails if you want this account to receive emails about alerts.

The screenshot shows a user edit form with two sections: 'Basic Information' and 'Edit User'.
Basic Information:
Role: MSP Main Administrator (with a blue 'Permission Transfer' button)
Customer Role: Main Administrator
TP-Link ID: (empty text field)
Customer Privileges: All Customers
Edit User:
Alert Emails: Enable (with an information icon)

3. If you want to transfer the permissions to another account, click [Permission Transfer](#) and specify the new account.

The screenshot shows a 'Permission Transfer' dialog box with a close button (X) in the top right corner.
Select new main administrator: (dropdown menu)
An information box contains the text: "This operation will transfer the Cloud Main Administrator permissions of the current account to the new account, and the current account will be downgraded as Cloud Administrator."
Buttons: Apply, Cancel

10.2.3 Add New MSP User Accounts

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

1. In MSP View, go to [Account](#) > [User](#).

2. Click [Add New User](#). Specify the parameters and click [Invite](#).

Add New User

Administrator Type: Local User ⚠ Not supported by Cloud-Based Controller
 Cloud User

TP-Link ID: ⓘ

Role: ▾

Customer Privileges: All (Including all new-created Customer)
 Customer

Customer Role: ▾

Alert Emails: Enable ⓘ

Administrator Type

Specify whether to add a local user or cloud user.

Local user is not supported by the cloud-based controller.

TP-Link ID

Enter an email address to send the invitation email.

If the email address is already registered with a TP-Link ID, it will become a valid cloud user account after accepting the invitation.

If not, it will be invited for registration, and automatically becomes a valid cloud user account after finishing the registration.

Role

Select a role for the user account.

MSP Administrator: This role has access to most features in MSP View except for some modules.

MSP Viewer: This role can view the status and settings of some features.

Custom MSP roles: If you have created custom MSP roles, they will be displayed in the list.

Customer Privileges

Assign the customer permissions to the user account.

All: The created user has device permissions of all customers, including all newly created ones.

Customer: The created user has device permissions of only the customers you specify.

Customer Role

Administrator: Compared with the Customer Main Administrator, Customer Administrators have no permission to some modules in Global View and Site View, mainly including cloud access, migration, auto-backup and global view logs. They have read-only permission to some modules in Global View and Site View, such as license management and custom account roles.

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

Custom Customer roles: If you have created custom Customer roles, they will be displayed in the list.

Alert Emails

Check the box if you want the created user to receive emails about alerts of the privileged customers.

♥ 10.3 Manage System Settings

10.3.1 Configure MSP Settings

General Settings

1. In MSP View, go to [Settings > MSP Settings](#).
2. In [General Settings](#), configure the parameters and save the settings.

General Settings

MSP Name:

Time Zone: ⓘ

Daylight Saving Time: Enable

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

Time Offset:

Starts On:

| | | | |
|----------------------------------|-------------------------------------|--------------------------------------|------------------------------------|
| Week | Day | Month | Time |
| <input type="text" value="1st"/> | <input type="text" value="Sunday"/> | <input type="text" value="January"/> | <input type="text" value="00:00"/> |

Ends On:

| | | | |
|----------------------------------|-------------------------------------|--------------------------------------|------------------------------------|
| Week | Day | Month | Time |
| <input type="text" value="1st"/> | <input type="text" value="Sunday"/> | <input type="text" value="January"/> | <input type="text" value="00:00"/> |

| | |
|-----------------------------|--|
| MSP Name | Specify a name to identify the controller. |
| Time Zone | Select the time zone of the controller according to your region. The time of the controller settings and statistics is displayed based on the time zone. |
| Daylight Saving Time | <p>Enable the feature and configure the parameters if your country/region implement DST.</p> <p>Time Offset: Specify the time added in minutes when Daylight Saving Time starts.</p> <p>Starts On: Specify the time when the DST starts. The clock will be set forward by the time offset you specify.</p> <p>Ends On: Specify the time when the DST ends. The clock will be set back by the time offset you specify.</p> |

User Interface

You can customize the User Interface settings of the controller according to your preferences.

1. In MSP View, go to [Settings > MSP Settings](#).

2. In [User Interface](#), configure the parameters and save the settings.

User Interface

Language:

Use 24-Hour Time:

Fixed Menu:

Dark Settings:

Show Pending Devices: ⓘ

Refresh Button:

Refresh Interval:

Enable WebSocket Connection:

Custom Labeling of Controller:

Labeling Image:

Labeling Redirection: (Optional)

Language

Select the language to display the user interface.

Use 24-Hour Time

With Use 24-Hour Time enabled, time is displayed in a 24-hour format. With Use 24-Hour Time disabled, time is displayed in a 12-hour format.

Fixed Menu

With Fixed Menu enabled, the menu icons are fixed and do not prompt menu texts when your mouse hovers on them.

Dark Settings

When enabled, the system will switch to a dark theme.

Show Pending Devices

With this option enabled, the devices in Pending status will be shown, and you can determine whether to adopt them. With this option disabled, they will not be shown, thus you cannot adopt any new devices.

Refresh Button

Enable or disable Refresh Button in the upper right corner of the configuration page.

Refresh Interval

Select how often the controller automatically refreshes the data displayed on the page.

Enable WebSocket Connection

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

| | |
|--|---|
| Custom Labeling of Controller | This option is available on the Cloud-Based Controller. With this function enabled, you can upload your controller labeling and define the redirection URL. |
| Controller Update Notification | This option is available on the local controller. With this feature enabled, you will receive an update notification when a new controller version is available. |

Configure Remote Logging

With Remote Logging configured, the controller will send generated system logs to a log server.

1. In MSP View, go to [Settings > MSP Settings](#).
2. In [Services](#), enable [Remote Logging](#), configure the parameters and save the settings.

Services

Remote Logging: Enable ⓘ

Syslog Server IP/Hostname:

Syslog Server Port: (1-65535)

| | |
|---|--|
| Syslog Server IP/Hostname | Enter the IP address or hostname of the syslog server. |
|---|--|

| | |
|------------------------------------|--------------------------------------|
| Syslog Server Port | Enter the port of the syslog server. |
|------------------------------------|--------------------------------------|

Configure the Mail Server

With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. The Mail Server feature works with the SMTP (Simple Mail Transfer Protocol) service provided by an email service provider.

1. Log in to your email account and enable the SMTP (Simple Mail Transfer Protocol) Service. For details, refer to the instructions of your email service provider.
2. In MSP View, go to [Settings > Server Settings](#).

3. In **Mail Server**, enable **SMTP Server** and configure the parameters. Then save the settings.

Mail Server

i With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. For security reasons, we recommend that you configure Mail Server carefully.

SMTP Server: Enable


SMTP:

Port: (1-65535)

SSL: Enable

Authentication: Enable

Username:

Password: 

Sender Address: (Optional)

Test SMTP Server: Send Test Email to

| | |
|-----------------------|--|
| SMTP | Enter the URL or IP address of the SMTP server according to the instructions of the email service provider. |
| Port | Configure the port used by the SMTP server according to the instructions of the email service provider. |
| SSL | Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between the controller and the SMTP server. |
| Authentication | <p>Enable or disable Authentication according to the instructions of the email service provider.</p> <p>If Authentication is enabled, the SMTP server requires the username and password for authentication.</p> <p>Username: Enter your email address as the username.</p> <p>Password: Enter the authentication code as the password, which is provided by the email service provider when you enable the SMTP service.</p> |
| Sender Address | Specify the sender address of the email. If you leave it blank, the controller uses your email address as the Sender Address. |

Test SMTP Server

Test the Mail Server configuration by sending a test email to an email address that you specify.

History Data Retention

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

1. In MSP View, go to [Settings](#) > [MSP Settings](#).
2. In [History Data Retention](#), configure the parameters and save the settings.

History Data Retention

Clients' History Data: Enable

! When enabled, known clients, client history and client logs will be recorded. This will occupy much storage space.

Known Client:

Time-Based Settings

i The settings below will affect the graphical display of Statistics and Network Report.

Time Series with 5 Minutes Granularity: 2 Days

Time Series with Hourly Granularity: 7 Days

Time Series with Daily Granularity: 1 Year

Time Series with Weekly Granularity:

Others

Portal Authentication Records:

Wireless IDS:

Rogue AP:

Clients' History Data

When enabled, known clients, client history and client logs will be recorded. This will occupy much storage space.

Known Client

Specify the retention time of known client data.

Time Series with 5 Minutes Granularity

Displays the retention time of AP, switch, gateway, and client data. Corresponding to 5-minute statistics.

Time Series with Hourly Granularity

Displays the retention time of AP, switch, gateway, and client data. Corresponding to hourly statistics.

Time Series with Daily Granularity

Specify the retention time of AP, switch, gateway, and client data. Corresponding to daily statistics.

Time Series with Weekly Granularity

Specify the retention time of client data. Corresponding to weekly statistics.

| | |
|---|---|
| Portal Authentication Records | Specify the retention time of portal authorization records. Corresponding to Insight-Past Portal Authorization. |
| Wireless IDS | Specify the retention time of wireless IDS data. |
| Rogue AP | Specify the retention time of scanned Rogue APs. Corresponding to Insight-Rogue APs. |

App-Side Device Notifications (for Cloud-Based Controller)

With App-Side Device Notifications enabled, the Controller will send notifications to the app when your devices go online or offline.

1. Launch the Cloud-Based Controller. In MSP View, go to [Settings](#) > [MSP Settings](#).
2. In [App-Side Device Notifications](#), enable the feature and save the settings.

App-Side Device Notifications

With this function enabled, the Controller will send notifications to the app when your devices go online or offline.

10.3.2 Export for Support

You can export configuration data for technical support to diagnose network problems. The exported data will not contain users' personal information.

1. In MSP View, go to [Settings](#) > [Maintenance](#).
2. Click [Export Configuration Data](#) to save the data file, then you can send it for technical support.

Export for Support

Export configuration data and running logs for technical support to diagnose network problems. The exported data will not contain users' personal information.

[Export Running Logs](#)

[Export Configuration Data](#)

| | |
|---|---|
| Export Running Logs | This option is available for local controller. Click to export running logs. |
| Export Configuration Data | Click to export configuration data. |

10.3.3 Export Data

You can export data to monitor or debug your devices.

1. In MSP View, go to [Settings > Export Data](#).
2. Configure the parameters and click [Export](#).

Export Data

Export List:

Format:

[Export](#)

Export List

[Log List](#): Export the logs generated by the controller.

[Audit Log List](#): Export the audit logs generated by the controller.

Format

The data can be exported to the file in the format of .CSV or .XLSX.

Appendix 1: Omada APP

Omada app is a mobile application designed for Omada and Omada Pro products. It allows you to conveniently monitor and manage your network. The Omada app can be used for Standalone and Controller mode. This appendix introduces how to use Omada app to manage your network. It includes the following sections:

- [Install Omada App on the Mobile Device](#)
- [Manage Your Network in Standalone Mode](#)
- [Manage Your Network in Controller Mode](#)

♥ 1 Install Omada App on the Mobile Device

Omada app runs on iOS and Android devices, such as smart phones and tablets. Launch the Apple App Store (iOS) or Google Play store (Android) and search "TP-Link Omada" or simply scan the QR code to download and install the app.

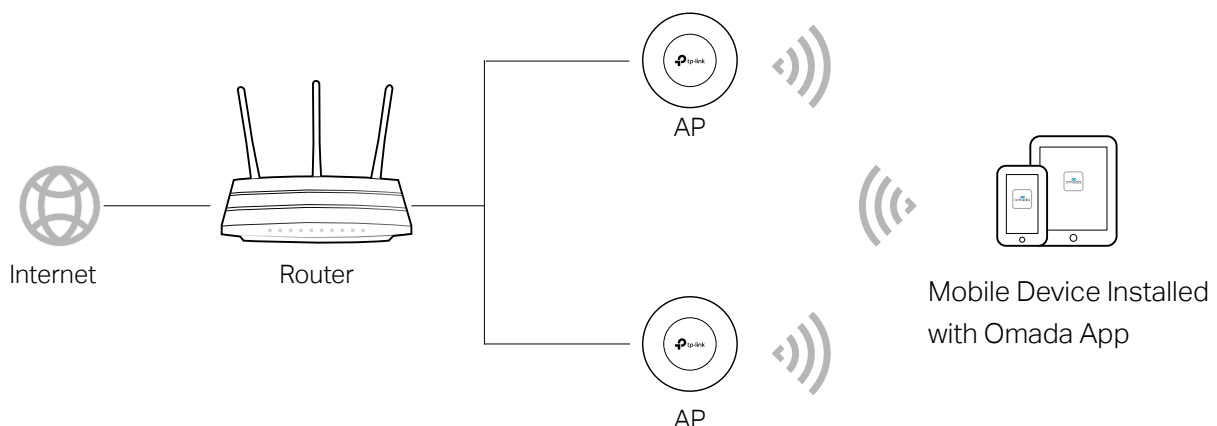


♥ 2 Manage Your Network in Standalone Mode

For a relatively small-scale network which has a few APs (usually less than three) and only basic functions are required, standalone mode is recommended. You can use a mobile device to configure each AP individually for basic functionality without configuring an SDN Controller. Note that the AP which is managed by the SDN Controller is inaccessible in standalone mode.

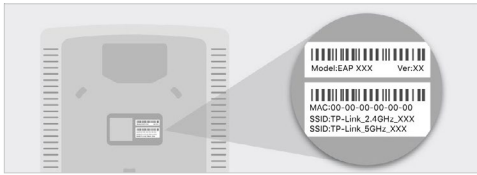
Refer to the topology below, make sure that the following requirements have been met:

- An Ethernet connection from your AP to the LAN with a DHCP server.
- The supported firmware version of the AP. To check the firmware versions of the supported APs, please refer to www.tp-link.com/omada_compatibility_list.
- A compatible iOS or Android device with Omada app.

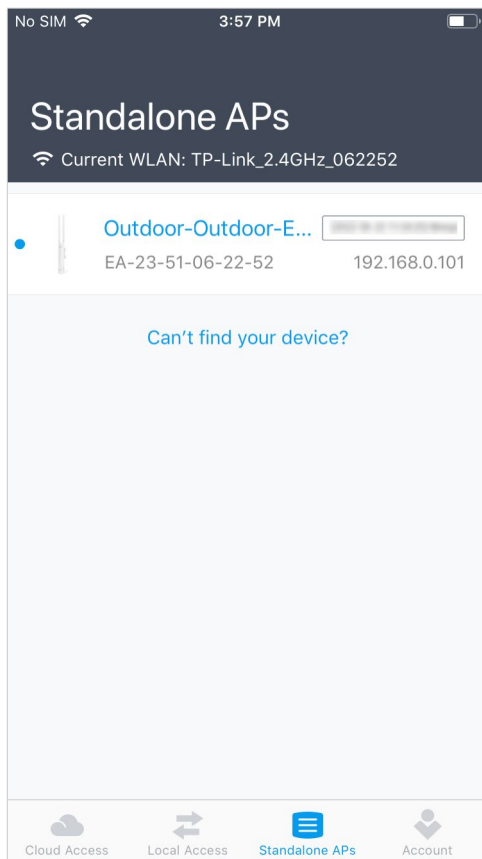


Follow the steps below to manage your network via Omada app in standalone mode. The following page is exemplified with the iOS version of the app. The Android version is similar.

1. Connect your mobile device to the AP by using the default SSID (format: **TP-Link 2.4GHz/5GHz_XXXXXX**) printed on the label.



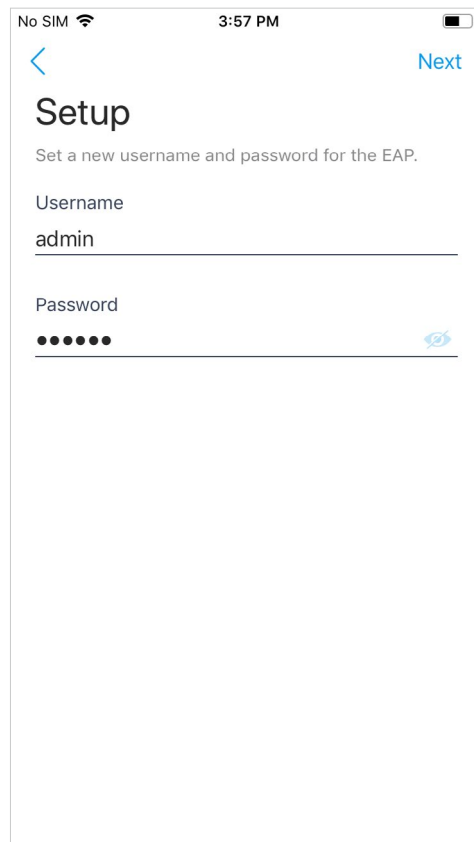
2. Launch the Omada app, tap **Standalone APs** and wait for the AP device to be discovered. Pull down to refresh if your devices do not appear.



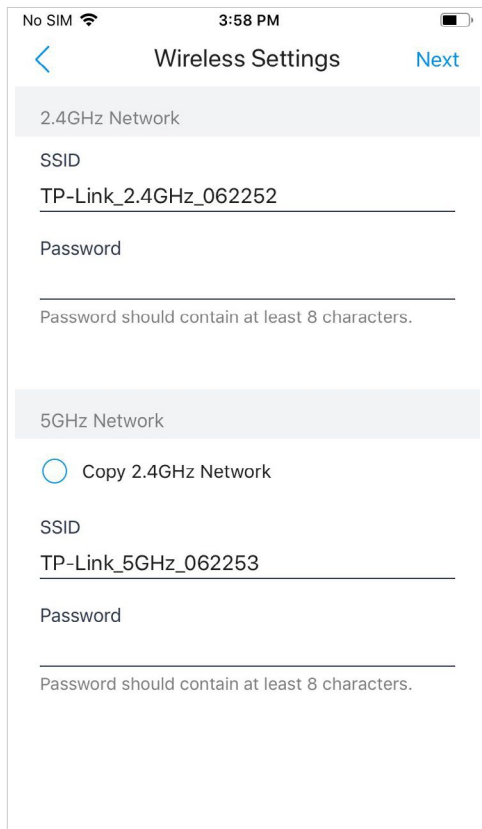
ⓘ Note:

All the AP devices in the same subnet will be discovered by Omada app and shown on the page. You can tap the discovered AP device to configure directly.

3. Tap on the AP device appearing on the page. Set a new username and password for your login account of the AP.




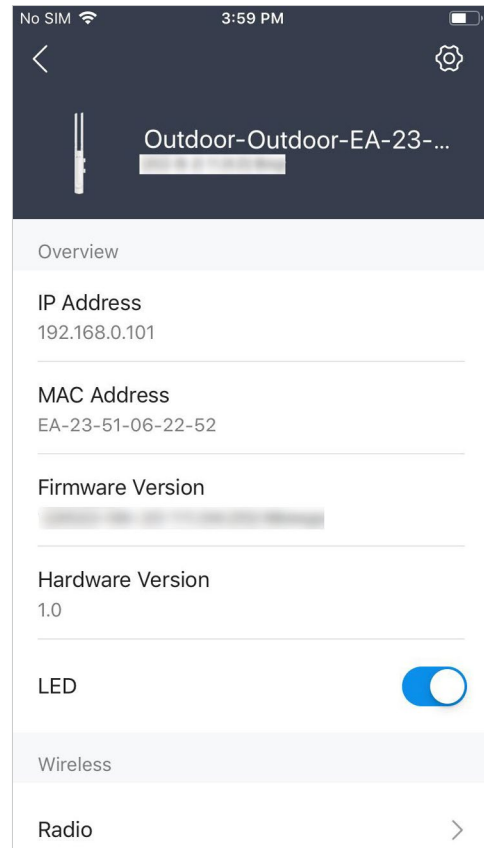
4. Edit the default SSID and password to keep your wireless network secure. Tap **Next**.



Note:

The settings will take effect after several minutes. For operation system differences, the wireless network connection will be different. When the default SSID of the AP device is changed, normally mobile device join the new wireless network automatically. For the unsupported operation system, you should manually connect to the new SSID.

5. You can view the name of the AP device and other information including wireless parameters and clients. You can tap  to change the settings of radio, SSID and device account.



Note:

- Omada app is designed to help you quickly configure some basic settings. For advanced configuration, you can use controller mode. And when your AP is managed by the controller, you can not use standalone mode.
- In standalone mode, only one user is allowed to log in to the management page of the AP at the same time. Thus the management web page of the AP cannot be logged in to when using the Omada app and vice versa. Also, only one user can log in to the AP via Omada app.

♥ 3 Manage Your Network in Controller Mode

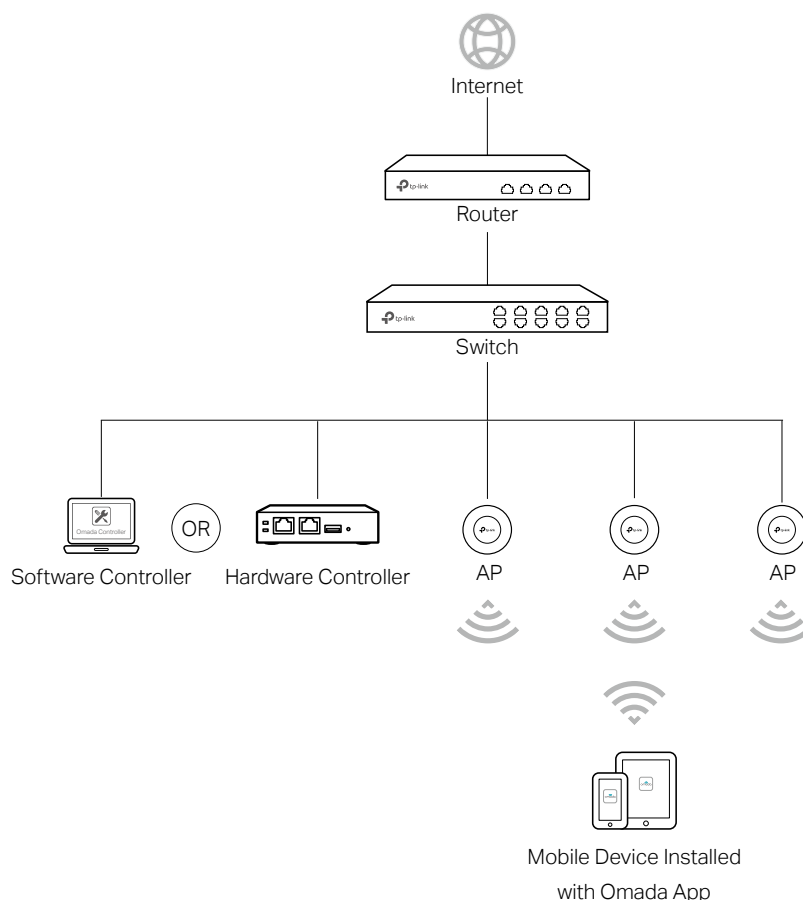
For a large-scale network which has routers, switches and mass APs, advanced functions are required, and controller mode is recommended. Controller mode allows you to configure and manage the devices and network in a straightforward and efficient way.

Omada app offers a convenient way to access the SDN Controller and adopt devices. With Local Access and Cloud Access function on the Omada app, you can manage the devices both locally and remotely while the controller is running.

3.1 Locally Manage Your Devices Using the Omada App

Local Access function on Omada app is designed for accessing the hardware/software controller which is in the same subnet with your mobile devices. Refer to the topology below, make sure that the following requirements have been met:

- An Ethernet connection from your AP to the LAN with a DHCP server.
- The version of the SDN Controller is 4.1.5 or above.
- A compatible iOS or Android device with Omada app (iOS: 3.0.28 and above, Android: 3.0.10 and above).

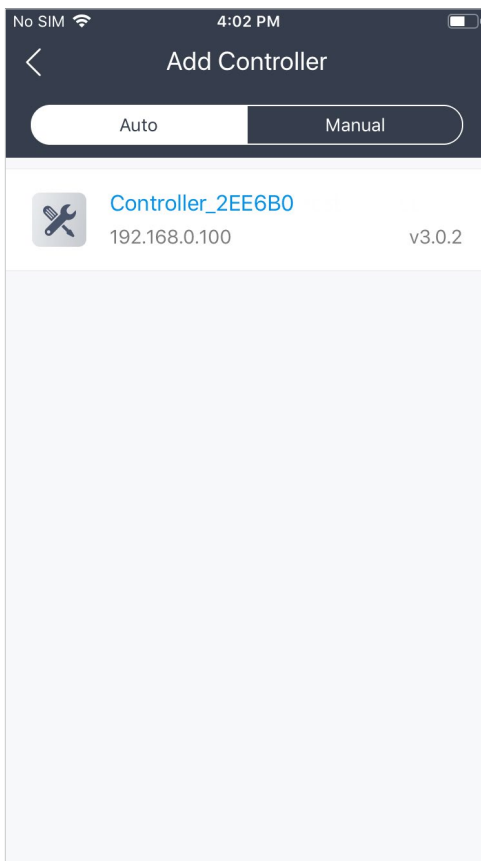


Follow the steps below to manage your network via Omada app in controller mode locally. The following page is exemplified with the iOS version of the app. The Android version is similar.

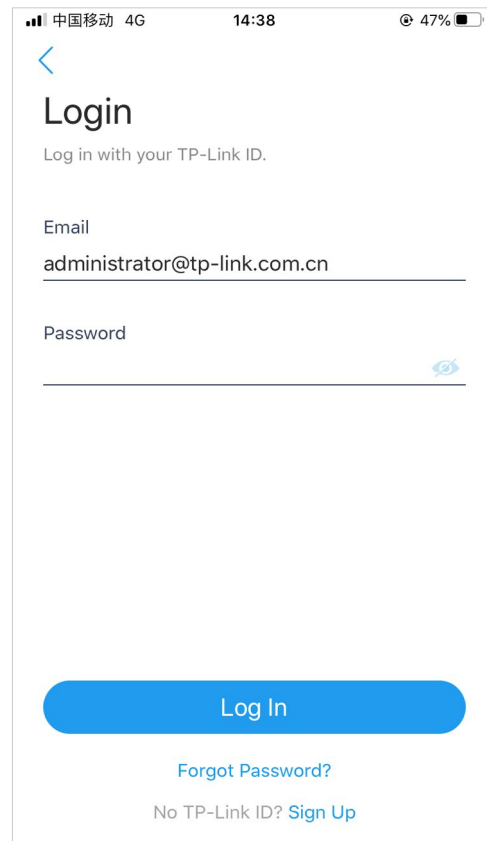
1. Connect your mobile device to the AP by using the default SSID (format: **TP-Link 2.4GHz/5GHz_XXXXXX**) printed on the label. Note that the AP should be in the same subnet with the controller.



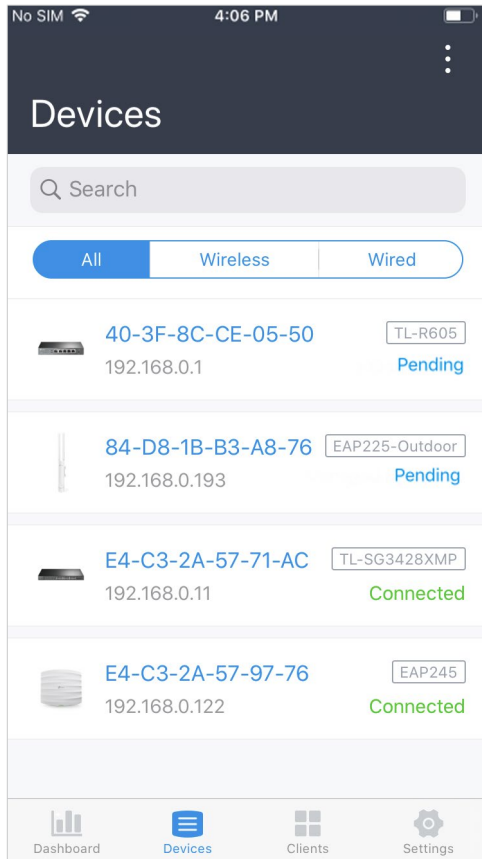
2. Launch the Omada app, go to **Local Access**, tap the **+** button on the upper-right corner to add the controller. Normally Omada app will discover the controller which is in the same subnet. If the controller cannot be found, you can add the controller by entering the IP address and port of the controller host in the manual column.



3. Tap the Controller, the controller login page will show. Enter the username and password of the controller, then tap **Log In** to launch the controller.



4. On the **Devices** screen, tap the Device that is pending for the adoption. And you can use the functions at the bottom to navigate various screens of the Controller including the wireless statistics, clients information and basic settings.



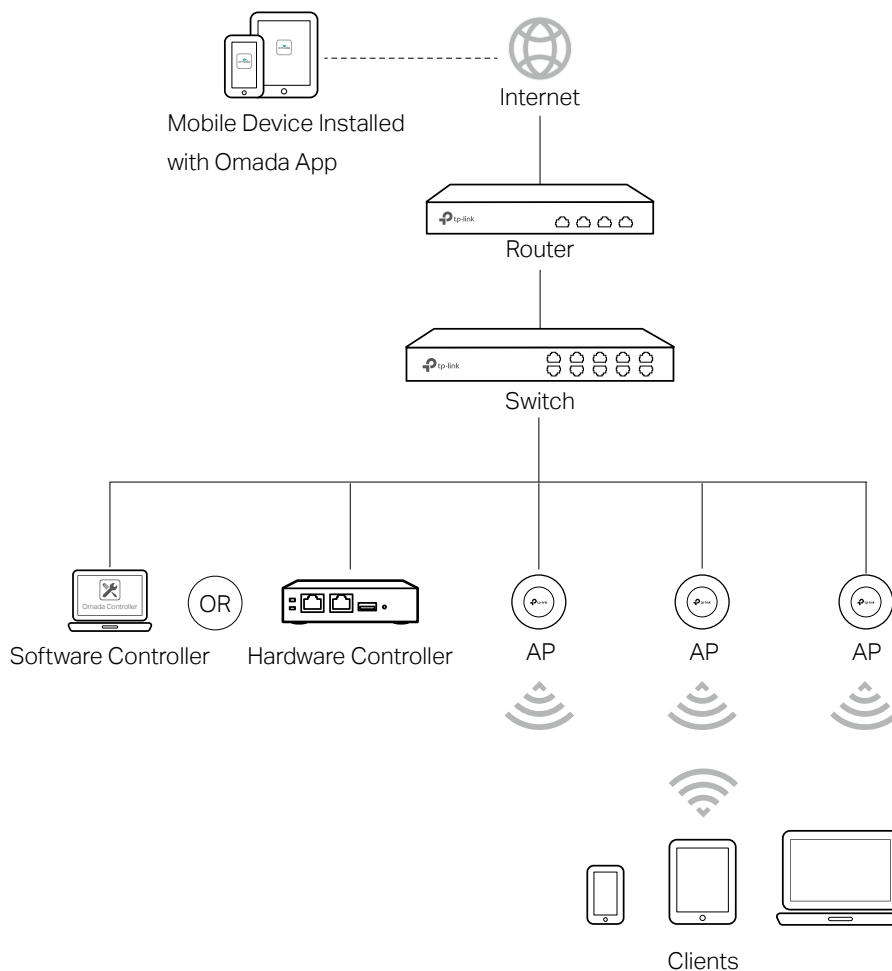
3.2 Remotely Manage Your Devices Using the Omada App

Cloud Access function on Omada app is designed for accessing the controller via Cloud Service. Thus, you can configure your controller and manage APs at any time, from anywhere.

Hardware/Software Controller

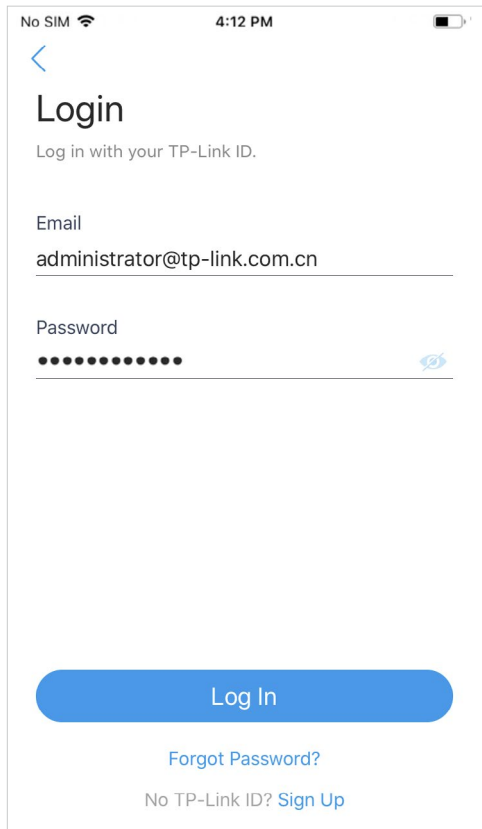
Refer to the topology for hardware/software controller below, make sure that the following requirements have been met:

- Both your hardware controller/controller host and mobile device have internet access.
- The version of the Controller is 4.1.5 or above.
- A compatible iOS or Android device with Omada app (iOS: 3.0.28 and above, Android: 3.0.10 and above).
- Cloud Access is enabled on the controller. The controller has been bound with a TP-Link ID.



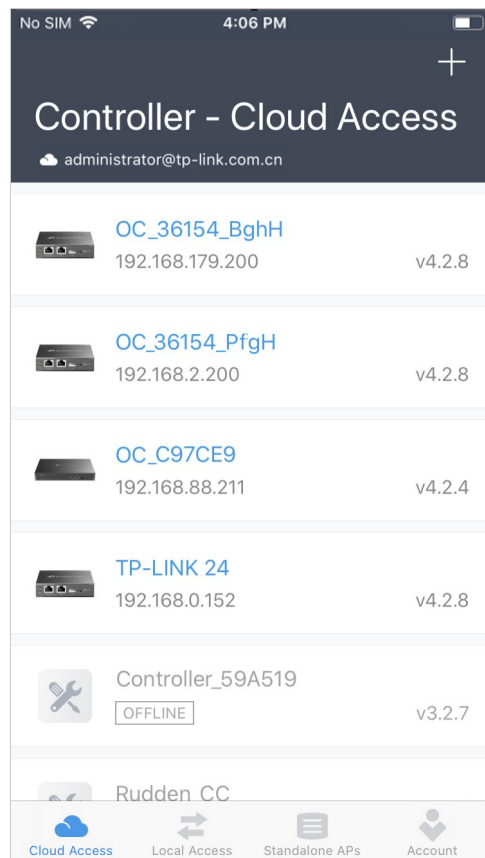
Follow the steps below to manage your network via Omada app in controller mode remotely. The following page is exemplified with the iOS version of the app. The Android version is similar.

1. Launch the Omada app, go to **Cloud Access** and tap **Go to Log In** to log in with your TP-Link ID.

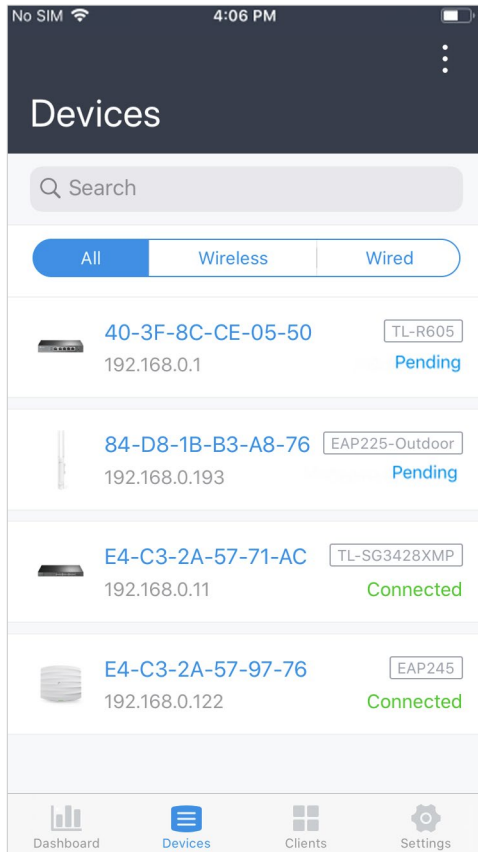


2. All the controllers which are bound with your TP-Link ID will appear on the page.

- If you want to add a hardware controller, tap + on the upper right, scan its QR code and follow the instructions to add a hardware controller.
- If you want to add devices to an existing hardware/software controller, tap the controller to launch the controller.



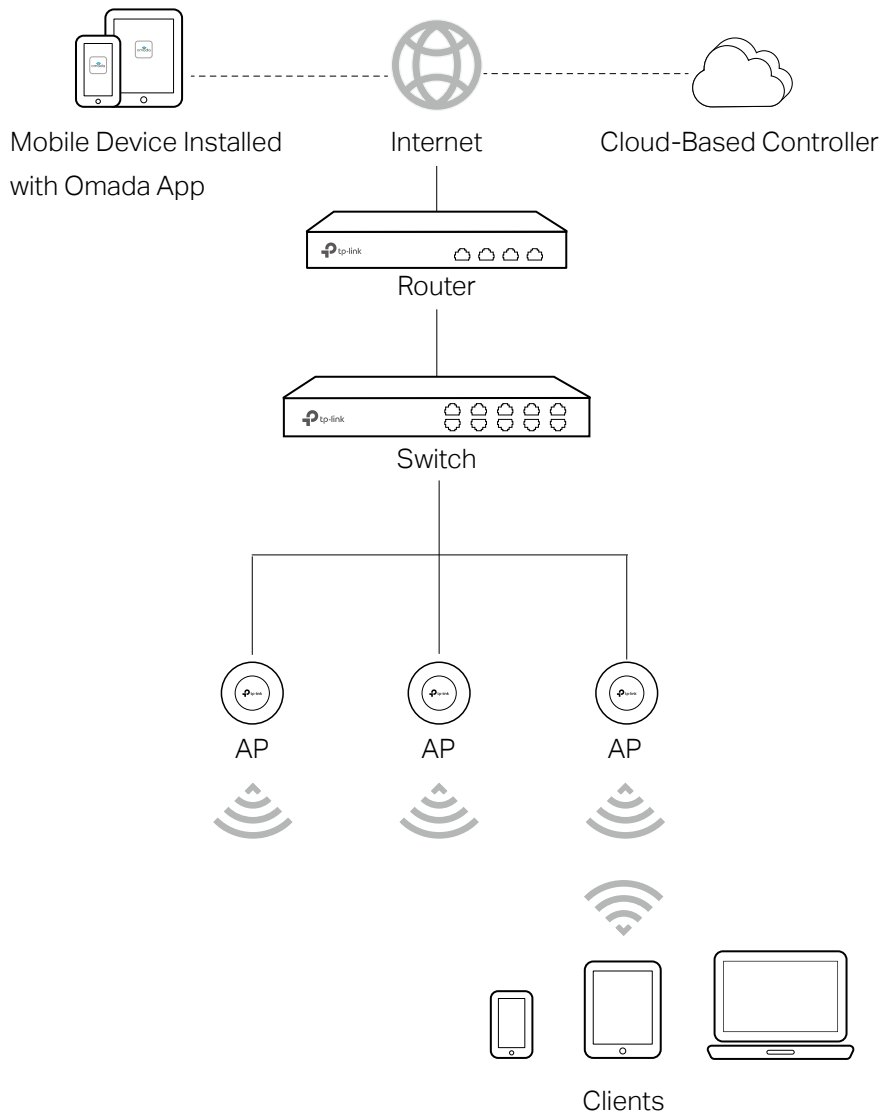
3. On the **Devices** screen, tap the device that is pending for the adoption. And you can use the functions at the bottom to navigate various screens of the the Controller including the wireless statistics, clients information and basic settings.



Cloud-Based Controller

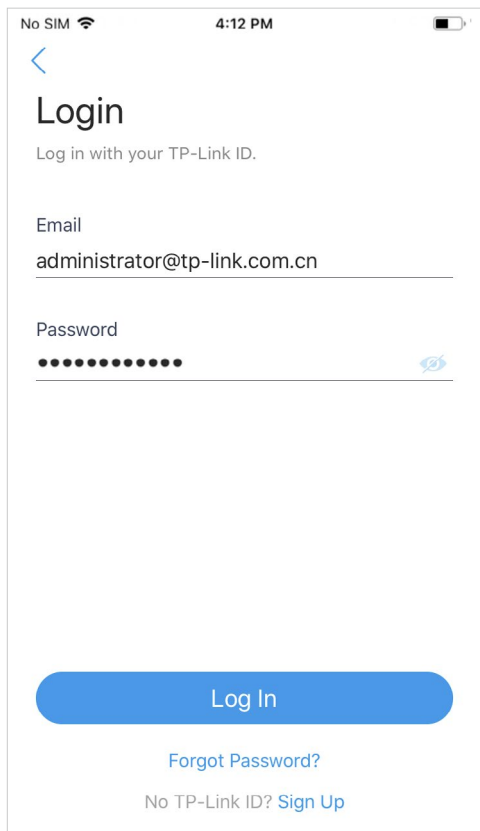
Refer to the topology for cloud-based controller below, make sure that the following requirements have been met:

- Your mobile device has internet access.
- A compatible iOS or Android device with Omada app.
- The supported firmware version of the router/switch/AP.

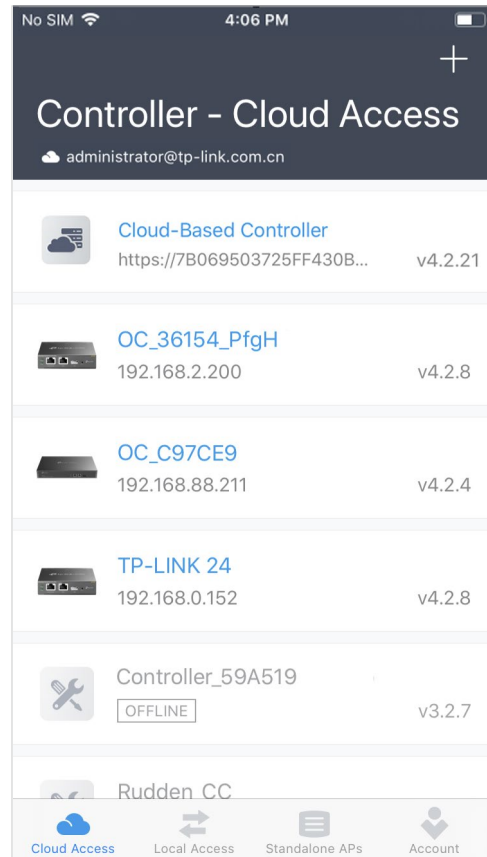


Follow the steps below to manage your network via Omada app in controller mode remotely. The following page is exemplified with the iOS version of the app. The Android version is similar.

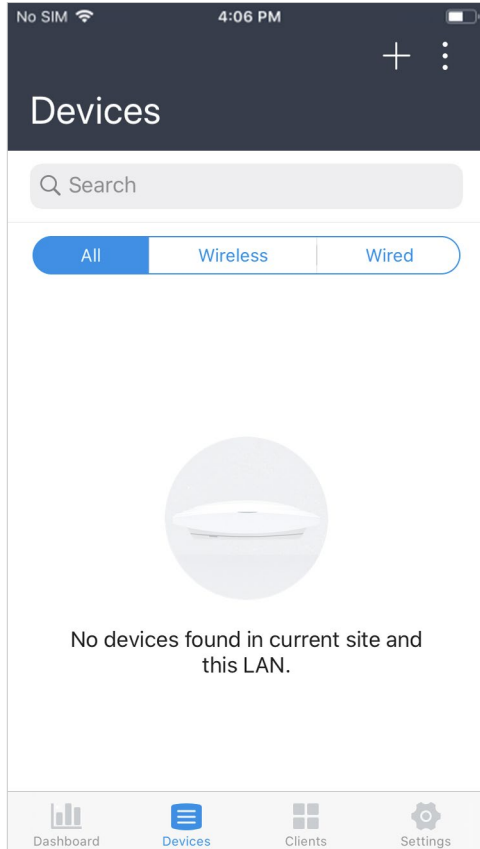
1. Launch the Omada app, go to **Cloud Access** and tap **Go to Log In** to log in with your TP-Link ID.



2. All the online controller which are bound with your TP-Link ID will appear on the page. Tap the cloud-based controller to launch and configure the controller.



3. On the **Devices** screen, tap the + on the upper right to add devices to your cloud-based controller. You can scan the barcode of the serial number of the device or enter the serial number manually.

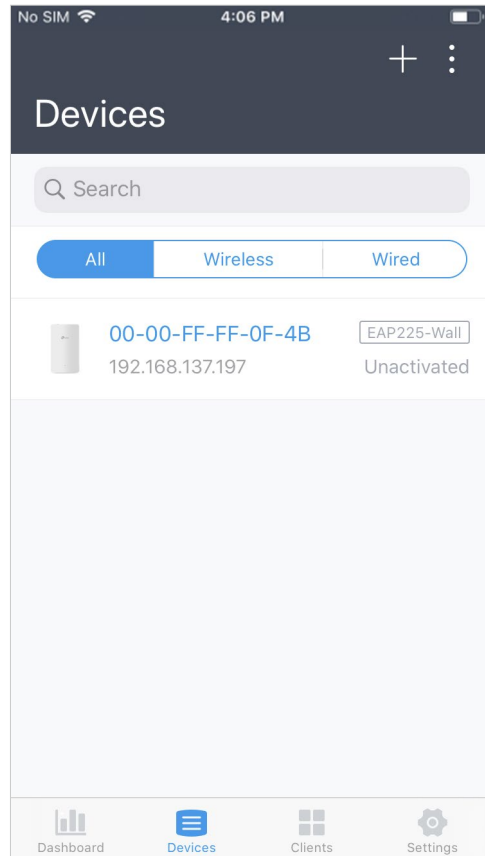


Note:

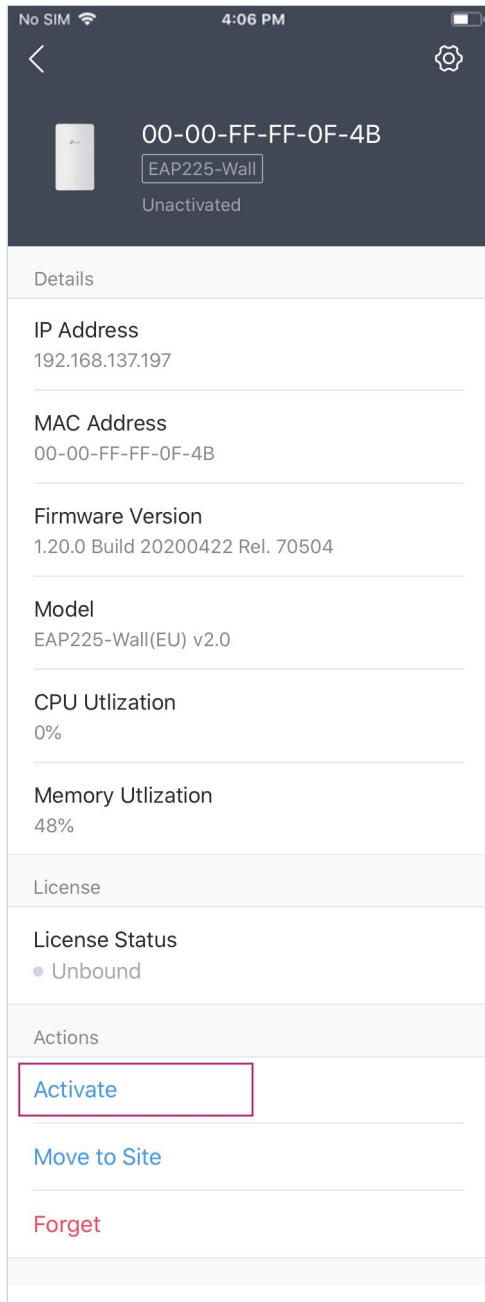
To successfully add a device to your cloud-based controller, make sure the following requirements are met:

- Your device is powered on and connected to the internet.
- If the device has been managed by another controller, please forget it on the previous controller and reset it to factory default.

4. On the **Devices** screen, the newly added device will appear. To manage and configure devices on the cloud-based controller, you need to activate them by assigning available licenses. Tap the device to load the page for device details.



5. Tab **Activate** and follow the instructions to assign licenses to the devices.



6. After binding with licenses, the devices can be managed and configured. You can use the functions at the bottom to navigate various screens of the Controller including the wireless statistics, clients information and basic settings.

