



In-Wall Access Point

User Guide

© 2025 TP-Link 1900000312 REV1.0.0

Note: Features available in the EAP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual product experience.

CONTENTS

About This Guide	1
Overview	3
1 Quick Start	4
1.1 Determine the Management Method	5
1.2 Set Up the EAP	5
1.2.1 AP Mode	5
1.2.2 Router Mode	8
2 System Overview	10
3 Configure the Network (for Router Mode)	14
3.1 Configure WAN Parameters	15
3.2 Configure LAN Parameters	17
3.3 Configure the LAN Port	19
3.3.1 Configure IPv6 Pass	19
3.3.2 Configure the Port VLAN	20
3.4 Configure Static Routing	20
3.5 Configure IP & MAC Binding	21
3.6 Configure the Forwarding Feature	22
3.7 Configure DHCP Reservation	24
3.8 Configure Security Features	24
3.9 Configure Access Control	26
4 Configure Wireless Settings	28
4.1 Configure Wireless Parameters	29
4.1.1 Configure SSIDs	29
4.1.2 Configure Wireless Advanced Settings	33
4.1.3 Configure the MLO Network (Only for Wi-Fi 7 Devices)	37
4.2 Configure Portal Authentication	39

4.2.1	Configure the Portal.....	40
4.2.2	Configure Free Authentication Policy.....	43
4.3	Configure the VLAN	45
4.4	Configure MAC Filtering.....	46
4.5	Configure Scheduler.....	47
4.6	Configure Band Steering.....	49
4.7	Configure QoS.....	50
4.8	Configure Rogue AP Detection.....	54
4.8.1	Manage the Rogue AP List	54
4.8.2	Manage the Trusted AP List.....	56
4.9	Configure User Isolation.....	57
4.10	Configure Access Control (for AP Mode).....	58
5	Monitor the Network	60
5.1	Monitor the EAP	61
5.2	Monitor the Wireless Status.....	61
5.3	Monitor the Clients.....	62
5.4	Monitor the WAN Status (Only for Router Mode)	64
5.5	Monitor the LAN Status (Only for Router Mode).....	65
5.6	Monitor the ARP Table (Only for Router Mode).....	65
5.7	Monitor the Routes (Only for Router Mode)	66
6	Manage the EAP.....	67
6.1	Manage the IP Address of the EAP (Only for AP Mode)	67
6.2	Manage System Logs	69
6.2.1	View System Logs	70
6.2.2	Configure the Way of Receiving Logs.....	70
6.3	Configure Web Server.....	71
6.4	Configure Management Access	73
6.4.1	Configure Access MAC Management.....	73
6.4.2	Configure Management VLAN (Only for AP Mode)	74

6.5	Configure LED	74
6.6	Configure the LAN Port (for AP Mode)	75
6.6.1	Configure the Port VLAN.....	75
6.7	Configure Wi-Fi Control.....	76
6.8	Configure SSH.....	77
6.9	Configure SNMP	77
7	Manage the System.....	80
7.1	Configure the User Account	81
7.2	Configure Controller Settings (Only for AP Mode)	82
7.2.1	Enable Cloud-Based Controller Management	82
7.2.2	Configure Controller Inform URL	83
7.3	Configure the System Time.....	83
7.3.1	Configure the System Time	83
7.3.2	Configure Daylight Saving Time	85
7.4	Reboot and Reset the EAP.....	86
7.5	Backup and Restore the Configuration.....	87
7.6	Update the Firmware	87
7.7	Perform Network Diagnostic (Only for Router Mode)	89
7.7.1	Run a Ping Test	89
7.7.2	Run a Traceroute Test.....	89
7.7.3	Download Device Info	90

About This Guide

When using this guide, notice that features available in the EAP may vary by model and software version. Availability of the EAP may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit <https://www.omadanetworks.com>.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure the 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 product.

Wireless Speed and Range Disclaimer

Maximum wireless transmission rates are the physical rates derived from IEEE Standard 802.11 specifications. Range and coverage specifications were defined according to test results under normal usage conditions. Actual wireless transmission rate and wireless coverage are not guaranteed, and will vary as a result of 1) environmental factors, including building materials, physical objects and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead and 3) client limitations, including rated performance, location, connection quality, and client condition.

Ethernet Port Limitation Disclaimer

Actual network speed may be limited by the rate of the product's Ethernet WAN or LAN port, the rate supported by the network cable, Internet service provider factors and other environmental conditions.

Wireless Client Capacity Disclaimer

Wireless client capacity specifications were defined according to test results under normal usage conditions. Actual wireless client capacity is not guaranteed, and will vary as a result of 1) environmental factors, including building materials, physical objects and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead and 3) client limitations, including rated performance, location, connection quality, and client condition.

Wi-Fi Feature Disclaimer (for EAPs that support the corresponding features)

Use of Wi-Fi 7 (802.11be), Wi-Fi 6 (802.11ax), and features including Multi-Link Operation (MLO), 320 MHz Bandwidth, 4K-QAM, Multi-RUs, OFDMA, MU-MIMO, and BSS Color require clients to also support the corresponding features.

Seamless Roaming Disclaimer (for EAPs that support Seamless Roaming)

Seamless roaming requires both the access point and client devices to support 802.11k and 802.11v protocols.

More Info

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit <https://www.omadanetworks.com>.

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

The Quick Installation Guide can be found where you find this guide or inside the package of the EAP.

The authentication information can be found where you find this guide.

Specifications can be found on the product page at <https://www.omadanetworks.com>.

Overview

Omada EAPs provide wireless coverage solutions for small-medium business and households. They can either work independently as standalone APs or be centrally managed by an Omada Controller, providing a flexible, richly-functional but easily configured wireless network.

1

Quick Start

This chapter introduces how to build a wireless network using the EAPs and how to complete basic settings. Follow the steps below:

1.1 Determine the Management Method

1.2 Set Up the EAP

1.1 Determine the Management Method

Before building your network, choose a proper method to manage your EAPs. You have the following options:

■ Controller Mode

If you want to manage a large-scale network centrally, choose Controller Mode. In Controller Mode, you can configure and monitor mass EAPs, switches, and gateways via an Omada Controller. For more information, go to <https://www.omadanetworks.com/en/business-networking/omada/controller/>.

■ Standalone Mode

If you want to manage only a few EAPs, choose Standalone Mode. In Standalone Mode, you can singly configure and monitor your EAPs via Omada app or a web browser, and each EAP has its own management page.

This guide introduces how to quickly set up the EAP in Standalone Mode.

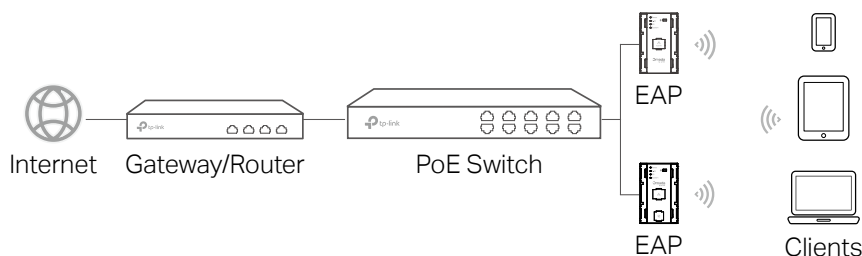
Note:

- Standalone Mode is inaccessible while the EAP is managed by a controller. To turn the EAP back to Standalone Mode, you can forget the EAP on the controller or reset the EAP.
- To make your EAPs discovered by the controller, you need to configure controller settings in certain scenarios. For details, refer to [7.2 Configure Controller Settings \(Only for AP Mode\)](#).

1.2 Set Up the EAP

A standalone EAP can work in AP mode or Router mode. You can choose the working mode according to your needs. The default mode is AP mode.

1.2.1 AP Mode



Note:

- Before you start, be sure to power up and connect your devices according to the topology figure.
- A DHCP server (typically a gateway/router with DHCP function enabled) is required to assign IP addresses to the EAPs and clients in your local network.

- **Method 1: Set Up via the Omada App**

Note:

Omada app is designed to help you quickly configure some basic settings. To configure advanced functions, use the web browser on your PC.

1. Download and install the TP-Link Omada App from the App Store or Google Play.



2. Connect your mobile device to the Wi-Fi of an EAP. The default SSIDs are printed on the EAP.
3. Launch the Omada app and go to **Standalone Mode**. The Omada app will discover and list all the EAPs in the current subnet.
4. Tap on each EAP and follow the app instructions to complete the initial setup.

Generally, you need to set up the username and password for login to the EAP's web management page and configure the SSID and password for Wi-Fi connection.

5. **Enjoy the internet!**

Now you can connect your phones, tablets and laptops to the new WiFi and surf the internet.

Note:

If you cannot access the internet, refer to [Troubleshooting of wireless issues for Omada EAP products](#).

- **Method 2: Set Up via a Web Browser**

1. Connect your device to the EAP by using the default SSID on the product.
2. Launch a web browser and enter **https://omadaeap.net** in the address bar. The EAP web page will be displayed.

3. Set up the username and password for login to the EAP's web management page.

Set up a new account

New Username:

New Password:

Low

Middle

High

Confirm Password:

Automatically check for
firmware upgrades:

☐ Enable

4. Start the initial setup.

Quick Setup

The quick setup will tell you how to configure the basic network parameters.

Let's Get Started

4. Select the AP Mode, and follow web instructions to configure the EAP.

Select an operation mode

The settings will take effect only after the router reboots. Internet access will be disabled temporarily.

☒

AP Mode
In this mode, the AP connects to a router via an Ethernet cable and transforms the wired network into a wireless one.

☐

Router Mode
In this mode, the device enables multiple users to share the internet. The wireless ports share the same IP address as the Ethernet WAN port to connect to the ISP. The wireless port can be regarded as a LAN port while in AP Router mode.

Generally, you need to configure the SSID and password for Wi-Fi connection.

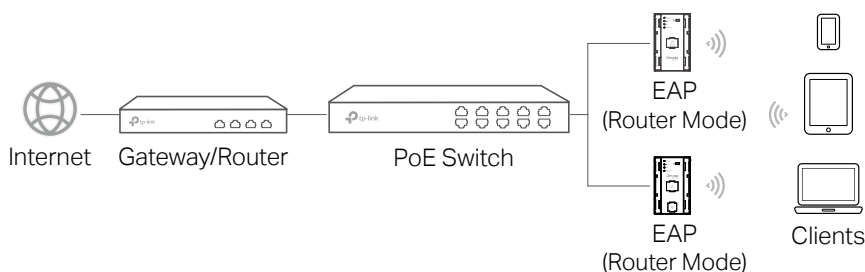
5. Enjoy the internet!

Now you can connect your phones, tablets and laptops to the new WiFi and surf the internet.

Note:

If you cannot access the internet, refer to [Troubleshooting of wireless issues for Omada EAP products](#).

1.2.2 Router Mode

**Note:**

- Before you start, be sure to power up and connect your devices according to the topology figure.
- When the EAP works in Router mode, it cannot be managed by the Omada app and Omada Controller.

1. Connect your device to the EAP by using the default SSID on the product.
2. Launch a web browser and enter **https://omadaeap.net** in the address bar. The EAP web page will be displayed.
3. Set up the username and password for login to the EAP's web management page.

Set up a new account

New Username:

New Password:

Low Middle High

Confirm Password:

Automatically check for firmware upgrades: ☐ Enable

4. Start the initial setup.

Quick Setup

The quick setup will tell you how to configure the basic network parameters.

Let's Get Started

4. Select the Router Mode, and follow web instructions to configure the EAP.

Select an operation mode

The settings will take effect only after the router reboots. Internet access will be disabled temporarily.

☐ **AP Mode**
In this mode, the AP connects to a router via an Ethernet cable and transforms the wired network into a wireless one.

☒ **Router Mode**
In this mode, the device enables multiple users to share the internet. The wireless ports share the same IP address as the Ethernet WAN port to connect to the ISP. The wireless port can be regarded as a LAN port while in AP Router mode.

Generally, you need to configure the WAN connection type, WAN settings, and the SSID and password for Wi-Fi connection.

5. Enjoy the internet!

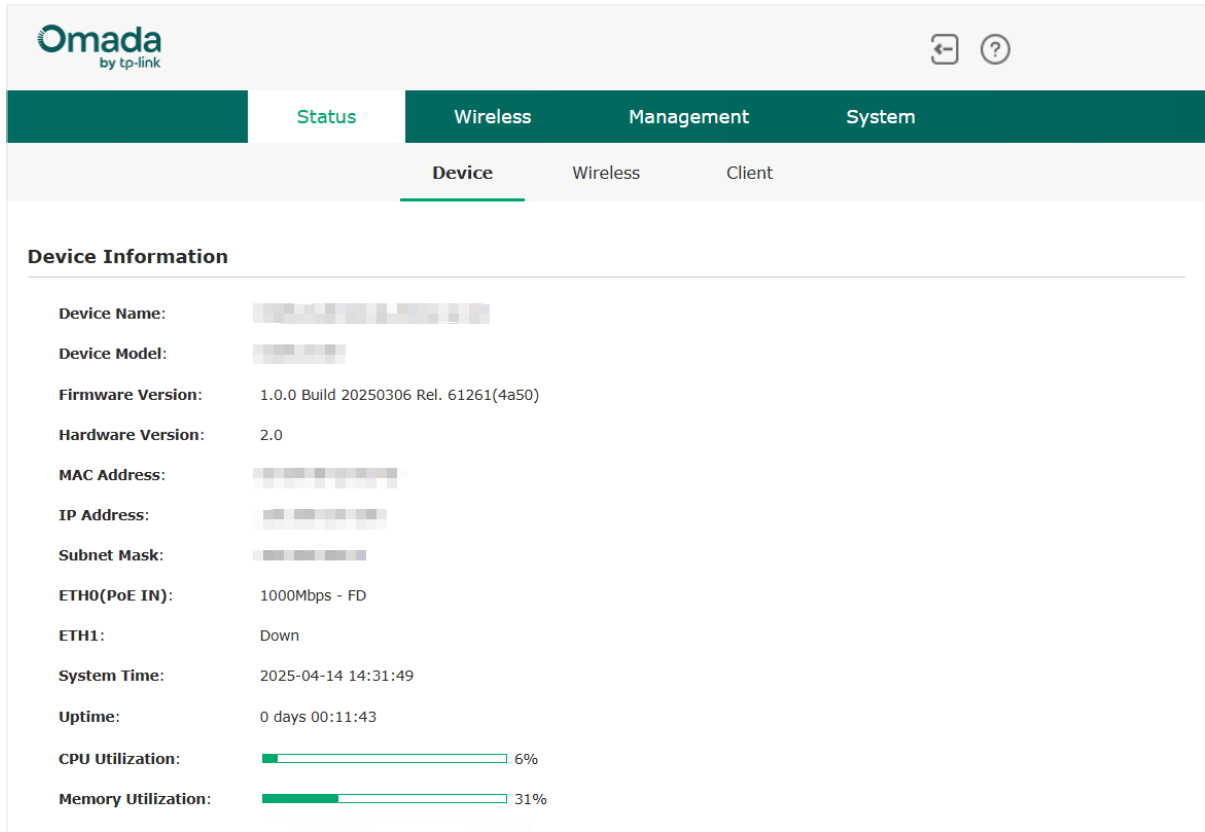
Now you can connect your phones, tablets and laptops to the new WiFi and surf the internet.

2 *System Overview*

This chapter provides a brief introduction to the web management page so you can quickly find the functions you need under the corresponding tabs:

If you use the web browser to configure your EAP, you can configure more advanced functions according to your needs, and manage it conveniently on the web page.

• AP Mode



On the top of the page, you can:

Click the AP Mode/Router Mode drop-down list to change the working mode.

Click  to log out.

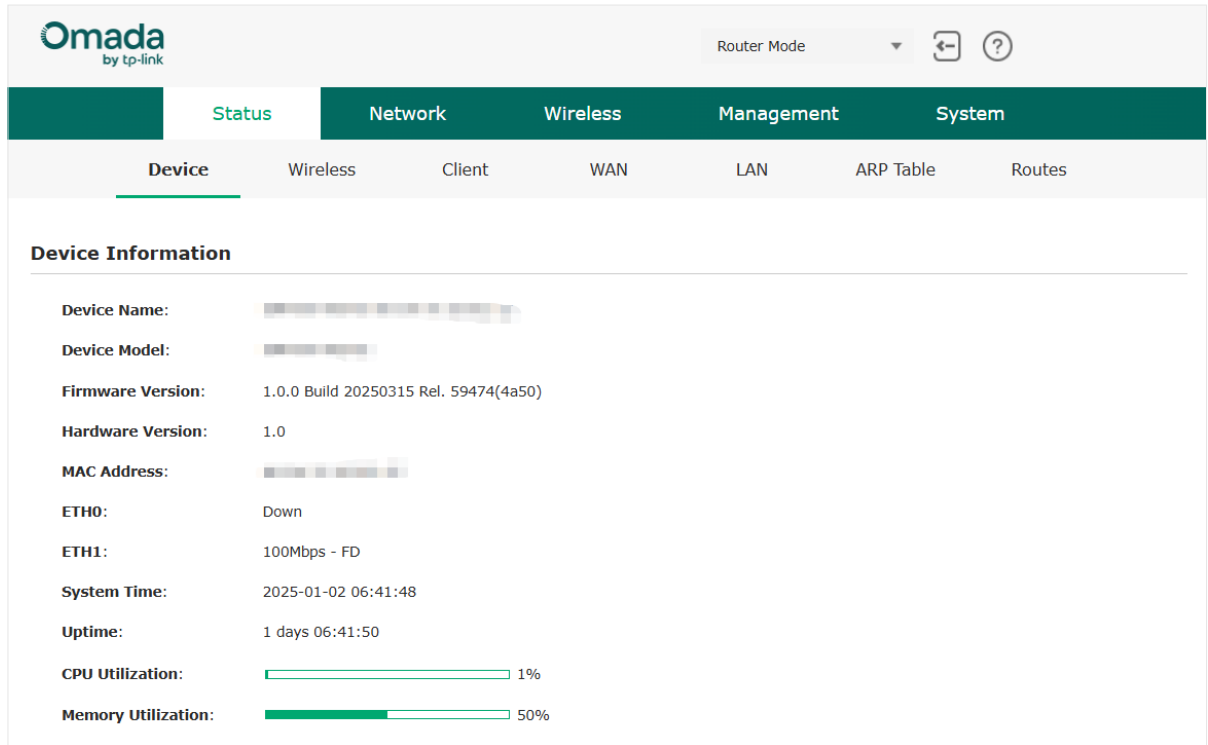
Click  to open the technical support website.

The tabs on the page allow you to access different configurations. The following table introduces what you can configure under each tab, and the following chapters discuss these topics in detail.

Status	You can view the information of the EAP, wireless traffic, and clients.
Wireless	You can configure wireless features, such as wireless radio settings, Portal, VLAN, and more.
Management	You can manage the EAP using the management features, such as Network settings, System Logs, Web Server, and more.

System	You can configure the system parameters, such as the login account, system time, reboot/reset, and more.
--------	--

- Router Mode



On the top of the page, you can:

Click the AP Mode/Router Mode drop-down list to change the working mode.

Click  to log out.

Click  to open the technical support website.

The tabs on the page allow you to access different configurations. The following table introduces what you can configure under each tab, and the following chapters discuss these topics in detail.

Status	You can view the information of the EAP, wireless traffic, clients, and more.
Network	You can configure network settings, such as WAN, LAN, Static Routing, and more.
Wireless	You can configure wireless features, such as wireless radio settings, Portal, VLAN, and more.
Management	You can manage the EAP using the management features, such as System Logs, Web Server, and more.

System

You can configure the system parameters, such as the login account, system time, reboot/reset, and more.

3

Configure the Network (for Router Mode)

This chapter introduces how to configure the network of the EAP in router mode, including:

- *3.1 Configure WAN Parameters*
- *3.2 Configure LAN Parameters*
- *3.3 Configure the LAN Port*
- *3.4 Configure Static Routing*
- *3.5 Configure IP & MAC Binding*
- *3.6 Configure the Forwarding Feature*
- *3.7 Configure DHCP Reservation*
- *3.8 Configure Security Features*
- *3.9 Configure Access Control*

3.1 Configure WAN Parameters

In Router mode, you can create the WAN connection and configure the related advanced parameters.

To configure WAN parameters, go to the **Network > WAN** page.

WAN

Connection Type:

Static IP

IP Address:

192.168.0.254

IP Mask:

255.255.255.0

Gateway:

Primary DNS:

Secondary DNS:

0.0.0.0

(Optional)

IPv6:

☐ Enable

Advanced Settings

MTU Size:

1500

Save

Select the connection type according to your need and configure the parameters.

• PPPoE

If your ISP delivers internet through phone line and provides you with username and password, choose this type and configure the parameters below.

User Name	Enter the User Name that is provided by your ISP.
Password	Enter the Password that is provided by your ISP.
MTU Size	Specify the MTU size. The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually appropriate. For some ISPs, you need modify the MTU. This should not be done unless your ISP told you to. This number should be an integer between 576 and 2026.
Service Name	Specify the Service Name provided by your ISP. Keep it empty if your ISP doesn't provide the name.
AC Name	Specify the AC Name provided by your ISP. Keep it empty if your ISP doesn't provide the name.
Detect Internal	Specify the Detect Interval. The default value is 10. Input the value between 0 and 120. The device will detect Access Concentrator online every interval seconds. If the value is 0, it means not detecting.

Use ISP-specified IP	If your service provider provides you with an IP address along with the user name and password, Enable "Use ISP-specified IP" and enter the IP address.
Use These DNS Servers	If the ISP provides a DNS server IP address for you, Enable Use These DNS Server, and fill the Primary DNS and Secondary DNS fields below. Otherwise, the DNS servers will obtain automatically from ISP.

• Dynamic IP

If your ISP uses a DHCP server to assign your device an IP address for connecting to the internet, choose this type and configure the parameters below.

IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a WAN IPv6 address.
IPv6 Pass	Control whether to pass WAN port IPv6 packets.
IPv6 Address	Set the IPv6 address for the device.
IPv6 Mask	Set the IPv6 mask for the device.
MTU Size	Displays the MTU (Maximum Transmission Unit) size, which is 1500 bytes.
Use These DNS Servers	If the ISP provides a DNS server IP address for you, Enable Use These DNS Server, and fill the Primary DNS and Secondary DNS fields below. Otherwise, the DNS servers will obtain automatically from ISP.

• Static IP

If your ISP provides a permanent, fixed (static) IP address, choose this type and configure the parameters below.




IP address	Enter the IP address provided by your ISP.
Netmask	Enter the netmask provided by your ISP. Normally use 255.255.255.0.
Gateway IP	Enter the gateway IP address provided by your ISP.
Primary DNS	Enter the DNS IP address provided by your ISP.
Secondary DNS	Enter alternative DNS IP address if your ISP provides it.
IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a WAN IPv6 address.
IPv6 Pass	Control whether to pass WAN port IPv6 packets.

IPv6 Address	Set the IPv6 address for the device.
IPv6 Mask	Set the IPv6 mask for the device.
MTU Size	Displays the MTU (Maximum Transmission Unit) size, which is 1500 bytes.



3.2 Configure LAN Parameters

In Router mode, you can configure the LAN parameters for the device and its clients.

To configure LAN parameters, go to the **Network > LAN** page.

Network List							
							 Add
ID	Name	VLAN	IP Address	Subnet Mask	DHCP Server	DHCP Relay	Operation
1	LAN	1	192.168.0.1	255.255.255.0	Enable	Disable	 

Click **Add** to add a LAN network or click the edit icon of a network entry to configure the following parameters.

ID	Name	VLAN	IP Address	Subnet Mask	DHCP Server	DHCP Relay	Operation
1	LAN	1	192.168.0.1	255.255.255.0	Enable	Disable	 

Name: (1-31 characters)

IP Address:

Subnet Mask:

VLAN: (1-4094)

IPv6: ☐ Enable

DHCP Settings

Status: ☒ Enable

DHCP Mode: ☒ DHCP Server ☐ DHCP Relay

Starting IP Address:

Ending IP Address:

Lease Time: min

Default Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Note:
Changing LAN-related configurations will cause client disconnection. Please unplug then reconnect the Ethernet cable of the client to the device or manually configure the correct IP address on the client.

Name	Specify a name for the LAN network.
IP address	Enter the LAN IP address of your device.
Subnet Mask	Enter the subnet mask provided by your ISP. Generally use 255.255.255.0.
VLAN	Specify the VLAN to which the LAN network belongs. The valid value ranges from 1 to 4094. Note: The LAN VLAN here is used to identify LAN subnets, and the packets do not carry the VLAN tag.
IPv6	Enable or disable the IPv6 function. If the IPv6 function is enabled, the device will obtain a LAN IPv6 address.
IPv6 Address	Set the IPv6 address for the device.

IPv6 Netmask	Set the IPv6 netmask for the device.
DHCP Server Status	Enable or disable the DHCP server function. With this function enabled, the build-in DHCP server will assign IP address to the clients connected to the device.
DHCP Mode	<p>Select a mode to assign IP addresses to clients.</p> <p>DHCP Server: In this mode, the device works as a DHCP server to assign IP addresses to clients.</p> <p>DHCP Relay: In this mode, clients obtain IP addresses from an external DHCP server on a different subnet.</p>
Starting IP Address	In DHCP Server mode, specify the first IP address of the IP address pool.
Ending IP Address	In DHCP Server mode, specify the last IP address of the IP address pool.
Lease Time	In DHCP Server mode, specify the amount time of the leased IP address assigned by the DHCP server. When the time expires, the clients will request to renew the lease automatically.
Default Gateway	In DHCP Server mode, specify the gateway IP address for the LAN network. By default, it is 192.168.0.254.
Primary DNS	In DHCP Server mode, specify the DNS IP address for the LAN. By default, it is 0.0.0.0, which means no primary DNS is assigned.
Secondary DNS	In DHCP Server mode, specify the IP address of alternative DNS server if there are two DNS servers. By default, it is 0.0.0.0, which means no secondary DNS is assigned.
Server Address	In DHCP Relay mode, specify the IP address of the external DHCP server.

3.3 Configure the LAN Port

3.3.1 Configure IPv6 Pass

IPv6 Pass is used to control whether to pass LAN port IPv6 packets.

To configure IPv6 Pass, go to the **Network > LAN Port Config** page and enable or disable IPv6 Pass for the LAN port.

IPv6 Pass

ETH1:

☒ Enable

3.3.2 Configure the Port VLAN

Port VLAN is used to set VLANs for the LAN ports. The wired clients in different VLANs cannot directly communicate with each other. Port VLAN is used to identify LAN subnets, and the packets do not carry the VLAN tag.

To configure the port VLAN, go to the **Network > LAN Port Config** page. The port VLAN ID here follows the LAN VLAN ID.

VLAN Config

ETH Port	VLAN ID
ETH1	1 (LAN) ▼

Note:
Changing the VLAN of the LAN port will cause client disconnection. Please unplug then reconnect the Ethernet cable of the client to the device or manually configure the correct IP address on the client.

Save

3.4 Configure Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. If static route is used properly in the network, it can decrease the network overhead and improve the speed of forwarding packets.

Static routing is generally suitable for simple network environment, in which users clearly understand the topology of the network so as to set the routing information correctly. When the network topology is complicated and users are not so familiar with the topology structure, this function should be used with caution or under the guidance of the experienced administrator.

To configure this feature, go to the **Network > Static Routing** page and click Add to add a routing entry.

Static Routing

+

Add

Target Network IP	Netmask	Gateway IP	Modify
--	--	--	--

Target Network IP:

Netmask:

255.255.255.255

Gateway IP:

0.0.0.0

OK

Cancel

Configure the following parameters.

Target Network IP	Enter the Target Network IP, the address of the network or host to be visited. The IP address cannot be on the same network segment with the device's WAN or LAN port.
Netmask	Specify the netmask for the desired entry.
Gateway IP	Enter the Gateway IP, the address of the gateway that allows for contact between the Device and the network or host

3.5 Configure IP & MAC Binding

Enabling the IP & MAC binding can effectively prevent ARP attack and IP embezzlement. Within the local network, the device transmits IP packets to the certain target identified by the MAC address. Therefore, the IP and MAC address should be one-to-one correspondence and their corresponding relations are maintained by the ARP table. ARP attack can use forged information to renewal the ARP table, and destroy the corresponding relations between IP and MAC addresses, which would prevent the communication between the device and the corresponding host. When the IP&MAC Binding function is enabled, the IP and MAC relations in the ARP table won't be expired and renewed automatically, which effectively prevents the ARP attack.

Some functions such as access control and bandwidth control, are based on the IP addresses to identify the access clients. The network administrator can allocate every client a static IP, according to which he makes the access and bandwidth rules to control the clients' online behavior and the bandwidth they've used. Some illegal users may change the IP address in order to get higher internet access. Enabling IP & MAC binding function can effectively prevent the IP embezzlement.

Note:

After IP & MAC binding function is enabled, the IP bound to the MAC cannot be used by other MAC addresses. However this MAC can use other IPs within the same segment, which are not bounded by other MAC addresses, to access the network.

To configure this feature, go to the **Network > IP & MAC Binding** page and add a binding entry.

IP & MAC Binding+ Add

IP	MAC	Modify
--	--	--

IP:

0.0.0.0

MAC:

AA-BB-CC-DD-EE-FF

OK

Cancel

Configure the following parameter.

IP	Enter the IP address that you want to bind with the MAC address.
MAC	Enter the MAC address that you want to bind with the IP address.

3.6 Configure the Forwarding Feature

The IP address used on the internet is public IP address, while IP address used on local area network is private IP address. The hosts using private IP addresses cannot access the internet directly and vice versa.

The hosts using private IP addresses visit internet through NAT (Network Address Translation) technology. NAT can transfer private IP addresses into public IP addresses to realize the communication from internal hosts to external hosts.

The forwarding function, such as DMZ and Virtual server, allows the hosts on the internet to visit the hosts on local area network

To configure this feature, go to the **Network > Forwarding** page.

Forwarding

DMZ:

☐ Enable

i

Virtual Server:

☐ Enable

i

Save

Configure the feature according to your needs.

- **DMZ**

DMZ (Demilitarized Zone) specifically allows one computer/device behind NAT to become “demilitarized”, so all packets from the external network are forwarded to this computer/device. The demilitarized host is exposed to the wide area network, which can realize the unlimited bidirectional communication between internal hosts and external hosts.

DMZ	Enable or disable the DMZ function.
DMZ IP	Specify the IP address of the local host network device. The DMZ host device will be completely exposed to the external network. Any PC that was used for a DMZ must have a static or reserved IP Address because its IP Address may change when using the DHCP function.

- **Virtual Server**

Virtual servers can be used for setting up public services on your local area network, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the internet to this service port will be redirected to the LAN server. Virtual Server function not only makes the users from internet visit the local area network, but also keeps network security within the intranet as other services are still invisible from internet. The LAN server must have a static or reserved IP Address because its IP Address may change when using the DHCP function.

To configure this feature, enable Virtual Server and save the settings. Then click Add to add a server.

Enable	Enable the entry.
IP	Enter the IP Address of the PC providing the service application.
Internal Port	Enter the Internal Port number of the PC running the service application. You can leave it blank if the Internal Port is the same as the Service Port, or enter a specific port number.
Service Port	Enter the numbers of external Service Port. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is the start port, YYY is the end port). Internet users send request to the port for services.
Protocol	Choose the one of the protocols used for this application: TCP, UDP, or TCP/UDP.

3.7 Configure DHCP Reservation

You can reserve an IP address for a local PC or a local server on your network, so it will always obtain the same IP address each time when it starts up.

To reserve an IP address, go to the **Network > DHCP Reservation** page.

DHCP Reservation

Add

ID	Enable	MAC Address	Reserved IP Address	Operation
--	--	--	--	--

Enable:

☐ Enable

MAC Address:

AA-BB-CC-DD-EE-FF

Reserved IP Address:

0.0.0.0

OK

Cancel

Configure the following parameters.

Enable	Enable the entry.
MAC	Enter the MAC address that you want to reserve an IP address.
IP	Enter the IP address to reserve.

3.8 Configure Security Features

The device provides many features to help ensure network security.

To use these features, go to the **Network > Security** page.

Basic

Firewall:

☒ SPI Firewall ⓘ

Disable WAN Ping:

☐ Enable

Advanced Settings

DoS Protection:

☐ Enable

Save

- **SPI Firewall**

Stateful Packet Inspection (SPI) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed to pass through by the firewall and others will be rejected.

SPI Firewall is enabled by factory default.

If forwarding rules are enabled at the same time, the device will give priority to meet forwarding rules.

- **Disable WAN Ping**

With this option enabled, the device will not reply the ping request originates from internet.

By default, it is disabled. You can enable it if needed.

- **DoS Protection**

DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host, which incurs an abnormal service or even breakdown of the network. With DoS Protection function enabled, the device can analyze the specific fields of the IP packets and distinguish the malicious DoS attack packets. Upon detecting the packets, the device will discard the illegal packets directly and limit the transmission rate of the legal packets if the over legal packets may incur a breakdown of the network. The hosts sending these packets will be added into the Blocked DoS Host List. The device can defend a few types of DoS attack such as ICMP_FLOOD, UDP_FLOOD and TCP_SYN_FLOOD.

By default, DoS protection is disabled. If needed, you can enable it and configure the following parameters.

DoS Protection	Enable the DoS Protection.
Packets Statistics Interval	Select a value between 5 and 60 seconds from the drop-down list. The default value is 10. The value indicates the time interval of the packets statistics. The result of the statistic is used for analysis by ICMP-Flood, UDP Flood and TCP-SYN Flood.
ICMP_FLOOD Attack Filter	Enable this option and enter a value between 5 and 3600. The default value is 50. When the current ICMP-FLOOD Packets number is beyond the set value, the device will start up the blocking function immediately.

UDP_FLOOD Attack Filter

Enable this option and enter a value between 5 and 3600. The default value is 500. When the current UDP-FLOOD Packets number is beyond the set value, the device will start up the blocking function immediately.

TCP_SYN_ FLOOD Attack Filter

Enable this option and enter a value between 5 and 3600. The default value is 50. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Device will start up the blocking function immediately.

After completing DoS protection configurations, the Blocked DoS Host List will be displayed. You can click **Refresh** to renewal the table list, or click **Clear All** to release all the blocked hosts. If you want to release one or some of the blocked hosts, select them and click the delete icon.

3.9 Configure Access Control

In Router mode, the ACL (Access Control) function can be used to control the internet activities of hosts in the local area network. For example, the online time limit and the specified web stations to visit can be controlled by the filtering policy.

Note:


In Router mode, Access Control only takes effect on the packets from LAN to WAN.

To configure this feature, follow the steps below:

1. Go to the **Network > ACL** page.

Access Control

Access Control:

☒ Enable 

Filtering Policy:


☐ Allow the packets specified by any enabled access control policy to pass through the device.

☒ Deny the packets specified by any enabled access control policy to pass through the device.

Note:

Access Controller only take effect on the packets from LAN to WAN.

Save

 Add

ID	Enable	Protocol	Host IP	Target IP	Target Port	Days of a week	Time	Operation
--	--	--	--	--	--	--	--	--

2. Enable **Access Control** and select the filtering policy according to your need..

Filtering Policy

Allow the packets specified by any enabled access control policy to pass through the device: When selected, the entries enabled below will be allowed to access the internet, while others are forbidden to access.

Deny the packets specified by any enabled access control policy to pass through the device: When selected, the entries enabled below will be forbidden to access the internet, while others are allowed to access.

3. Save the settings.
4. Click **Add** and create the filtering entries.

Enable	Enable or disable the desired entry.
Protocol	Choose one of the protocols from the drop-down list used for the target, any of IP, TCP, UDP, or ICMP.
Host IP	Enter the IP address or address range of the hosts that you need to control, for example 192.168.0.12-192.168.0.25.
Target IP	Enter the IP address or address range of the targets that you need to control, for example 192.168.3.12-192.168.3.25.
Target Port	Specify the port or port range for the target when protocol is TCP or UDP.
Days of a week	Specify the days in which the rules take effect.
Time	Enter the time rule in HH:MM-HH:MM format, the default value is 00:00-24:00.

5. Save the settings.

4

Configure Wireless Settings

This chapter introduces how to configure the wireless settings of the EAP, including:

- *4.1 Configure Wireless Parameters*
- *4.2 Configure Portal Authentication*
- *4.3 Configure the VLAN*
- *4.4 Configure MAC Filtering*
- *4.5 Configure Scheduler*
- *4.6 Configure Band Steering*
- *4.7 Configure QoS*
- *4.8 Configure Rogue AP Detection*
- *4.9 Configure User Isolation*
- *4.10 Configure Access Control (for AP Mode)*

4.1 Configure Wireless Parameters

To configure the wireless parameters, go to the **Wireless > Wireless Settings** page.

2.4GHz5GHzMLO

2.4GHz Wireless Radio

2.4GHz Wireless Radio: ☒ Enable

Save

2.4GHz SSIDs

+ Add

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
1	test	0	Enable	WPA-Personal	Disable	

2.4GHz Wireless Advanced Settings

Radio Settings | Load Balance | Airtime Fairness | More Settings

Wireless Mode:

802.11b/g/n/ax/be mixed

Channel Width:

Auto

Channel:

Auto

Tx Power(EIRP):

19

dBm(7-19)

Note:
The EIRP transmit power includes the antenna gain.

Save

You can click each band to enable Wireless Radio and configure wireless parameters.

The following sections are demonstrated with 2.4GHz.

4.1.1 Configure SSIDs

SSID (Service Set Identifier) is used as an identifier for a wireless LAN, and is commonly called as the "network name". Clients can find and access the wireless network through the SSID.

Follow the steps below to create an SSID on the EAP:

1. Go to **Wireless > Wireless Settings**. Click a band on which the new SSID will be created.
2. Click **Add** to add a new SSID on the chosen band.

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
--	--	--	--	--	--	--

SSID:

SSID Broadcast: ☒ Enable

Security Mode: WPA-Personal ▾

Version: WPA2-PSK ▾

Encryption: ☐ Auto ☒ AES

Wireless Password:

Group Key Update Period: seconds (30-8640000, 0 means no update.)

Guest Network: ☐ Enable ⓘ

Rate Limit: ☐ Enable

IPv6 Pass: ☒ Enable

OK Cancel

3. Configure the following required parameters for this SSID:

SSID	Specify a name for the wireless network.
SSID Broadcast	With the option enabled, EAP will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP.
Security Mode	<p>Select the security mode of the wireless network.</p> <p>None: Clients can access the wireless network without authentication.</p> <p>WPA-Enterprise / WPA-Personal: Clients need to pass the authentication before accessing the wireless network.</p> <p>For network security, we recommend that you encrypt your wireless network. The following sections will introduce how to configure these security modes.</p>
Guest Network	With this option enabled, guest network will block clients from reaching any private IP subnet.

Rate Limit	<p>(Only for certain models)</p> <p>With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage.</p> <p>You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to View Client Information to get more details.</p> <p>Note that the download and upload rate will be limited to the smaller value if you set the limit value both in SSID and client configuration.</p>
IPv6 Pass	Control whether to pass wireless IPv6 packets.

4. Click **OK** to create the SSID.

Following is the detailed instructions about how to configure [WPA-Enterprise](#) and [WPA-Personal](#).

• WPA-Enterprise

WPA-Enterprise (Wi-Fi Protected Access-Enterprise) is a safer encryption method compared with WEP and WPA-Personal. It requires a RADIUS server to authenticate the clients via 802.1X and EAP (Extensible Authentication Protocol). WPA-Enterprise can generate different passwords for different clients, which ensures higher network security. But it also costs more to maintain the network, so it is more suitable for business networks.

The following table introduces how to configure each item:

Version	Select the version of WPA-Enterprise according to your needs. If you select WPA/WPA2-Enterprise, the EAP automatically decides whether to use WPA-Enterprise or WPA2-Enterprise during the authentication process.
Encryption	<p>Select the Encryption type. Note that some encryption type is only available under certain circumstances.</p> <p>Auto: The default setting is Auto and the EAP will select the encryption method automatically based on the client device's request.</p> <p>AES: Advanced Encryption Standard. It is a secure encryption method.</p>
RADIUS Server IP	Enter the IP address of the RADIUS Server.
RADIUS Port	Enter the port number of the RADIUS Server.
RADIUS Password	Enter the shared secret key of the RADIUS server.

RADIUS Accounting	Enable or disable RADIUS accounting feature.
Accounting Server IP	Enter the IP address of the accounting server.
Accounting Server Port	Enter the port number of the accounting server.
Accounting Server Password	Enter the shared secret key of the accounting server.
Interim Update	With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled. Enter the appropriate duration between updates for EAPs in Interim Update Interval .
Interim Update Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the EAP should change the encryption key. 0 means that the encryption key does not change at anytime.

• WPA-Personal

WPA-Personal is based on a pre-shared key. It is characterized by high safety and simple settings, so it is mostly used by common households and small businesses.

The following table introduces how to configure each item:

Version	Select the version of WPA-Personal according to your needs. If you select WPA/WPA2-PSK, the EAP automatically decides whether to use WPA-PSK or WPA2-PSK during the authentication process.
Encryption	Select the Encryption type. Note that some encryption type is only available under certain circumstances. Auto: The default setting is Auto and the EAP will select the encryption method automatically based on the client device's request. AES: Advanced Encryption Standard. It is a secure encryption method.
Wireless Password	Configure the wireless password with ASCII characters. <ul style="list-style-type: none"> For ASCII, the length should be between 8 and 63 and the valid characters contain numbers, letters (case-sensitive) and common punctuations.
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the EAP should change the encryption key. 0 means that the encryption key does not change at anytime.

4.1.2 Configure Wireless Advanced Settings

Proper wireless advanced parameters can improve the performance of your wireless network.

This section introduces how to configure the advanced wireless parameters of the EAP, including [Radio Settings](#), [Load Balance](#), [Airtime Fairness](#) and [More Settings](#).

- **Radio Settings**

Radio settings directly control the behavior of the radio in the EAP and its interaction with the physical medium; that is, how and what type of signal the EAP emits.

2.4GHz Wireless Advanced Settings

[Radio Settings](#) | [Load Balance](#) | [Airtime Fairness](#) | [More Settings](#)

Wireless Mode:

802.11b/g/n/ax mixed

Channel Width:

Auto

Channel:

Auto

Tx Power:

20

dBm(4-25)

Save

To configure radio settings, follow the steps below:

1. Go to **Wireless > Wireless Settings**, click a band, locate the **Wireless Advanced Settings** section, and go to **Radio Settings**.
2. Configure the following parameters. Click **Save**.

Wireless Mode	<div>Select the IEEE 802.11 mode the radio uses.</div> <ul style="list-style-type: none">• For 2.4GHz: 802.11b/g/n/ax/be mixed is recommended so that all of 802.11b, 802.11g, 802.11n, 802.11ax, and 802.11be clients operating in the 2.4GHz frequency can connect to the AP. Note that some devices may not support 802.11ax and 802.11be; in this case, select the one with most types mixed.• For 5GHz: 802.11a/n/ac/ax/be mixed is recommended so that all of 802.11a, 802.11n, 802.11ac, 802.11ax, and 802.11be clients operating in the 5GHz frequency can connect to the AP. Note that some devices may not support 802.11ax and 802.11be; in this case, select the one with most types mixed.
---------------	--

Channel Width	<p>Select the channel width of the AP. The available options differ among different APs.</p> <p>We recommend you set the channel bandwidth to Auto to improve the transmission speed. However, you may choose a lower bandwidth due to the following reasons:</p> <ul style="list-style-type: none"> • To increase the available number of channels within the limited total bandwidth. • To avoid interference from overlapping channels occupied by other devices in the environment. • Lower bandwidth can concentrate higher transmit power, increasing stability of wireless links over long distances.
Channel Limit	<p>Check the box to enable the Channel Limit function. With this function enabled, the wireless frequency 5150MHz~5350MHz will be disabled. This function can influence the available options in Channel.</p> <p>This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.</p>
Channel	<p>Select the channel used by the EAP. For example, 1/2412MHz means that the channel is 1 and the frequency is 2412MHz.</p> <p>By default, the channel is automatically selected, and we recommend that you keep the default setting.</p>
Tx Power (EIRP)	<p>Specify the transmit power value.</p> <p>If this value is set to be larger than the maximum transmit power that is allowed by the local regulation, the regulated maximum transmit power will be applied in the actual situation.</p> <p>Note: In most cases, it is unnecessary to use the maximum transmit power. Specifying a larger transmit power than needed may cause interference to the neighborhood. Also it consumes more power and reduces longevity of the device.</p>

• Load Balance

With the Load Balance feature, you can limit the maximum number of clients who can access the EAP. In this way, you can achieve rational use of network resources.

2.4GHz Wireless Advanced Settings

[Radio Settings](#) | [Load Balance](#) | [Airtime Fairness](#) | [More Settings](#)

Load Balance:

☐ Enable

Maximum Associated Clients:

(1-63)

Save

To configure Load Balance, follow the steps below:

1. Go to **Wireless > Wireless Settings**, click a band, locate the **Wireless Advanced Settings** section, and go to **Load Balance**.
2. Check the box to enable Load Balance.
3. Specify the maximum number of clients who can connect to the EAP at the same time. While the number of connected clients has reached the limit and there are more clients requesting to access the network, the EAP will disconnect those with weaker signals.
4. Click **Save**.

- **Airtime Fairness**

With Airtime Fairness enabled, each client connected to the EAP can get the same amount of time to transmit data, avoiding low-data-rate clients to occupy too much network bandwidth.

Compared with the relatively new client devices, some legacy client devices support slower wireless rate. If they communicate with the same EAP, the slower clients take more time to transmit and receive data compared with the faster clients. As a result, the overall wireless throughput of the network decreases.

Therefore we recommend you check the box to enable this function under multi-rate wireless networks. In this way, the faster clients can get more time for the data transmission and the network overall throughput can be improved.

2.4GHz Wireless Advanced Settings

[Radio Settings](#) | [Load Balance](#) | [Airtime Fairness](#) | [More Settings](#)

Airtime Fairness:

☐ Enable

Save

Note:

- Airtime Fairness is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.
- With Airtime Fairness enabled, 50 wireless clients at most can connect to the EAP in 2.4GHz band.

To configure Airtime Fairness, follow the steps below:

1. Go to **Wireless > Wireless Settings**, click a band, locate the **Wireless Advanced Settings** section, and go to **Airtime Fairness**.
2. Check the box to enable Airtime Fairness.
3. Click **Save**.

• More Settings

Proper wireless parameters can improve the network's stability, reliability and communication efficiency.

2.4GHz Wireless Advanced Settings

[Radio Settings](#) | [Load Balance](#) | [Airtime Fairness](#) | [More Settings](#)

Beacon Interval:

100

ms (40-100)

DTIM Period:

1

(1-255)

RTS Threshold:

2347

(1-2347)

Fragmentation Threshold:

2346

(256-2346. This works only in 11b/g mode.)

OFDMA:

☐ Enable (This works only in 11ax mode.)

Note:

OFDMA enables multiple users to transmit data simultaneously, and thus greatly improves speed and efficiency. Noted that only when your clients also support OFDMA, can you fully enjoy the benefits.

Save

To configure the following parameters, go to **Wireless > Wireless Settings**, click a band, locate the **Wireless Advanced Settings** section, and go to **More Settings**.

Beacon Interval

Beacons are transmitted periodically by the EAP to announce the presence of a wireless network for the clients. **Beacon Interval** determines the time interval of the beacons sent by the EAP.

You can specify a value between 40 and 100ms. The default is 100ms.

DTIM Period	<p>The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the EAP has buffered data for client devices. The DTIM Period indicates how often the clients served by this EAP should check for buffered data still on the EAP awaiting pickup.</p> <p>You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating that clients check for buffered data at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend you keep the default value.</p>
RTS Threshold	<p>RTS/CTS (Request to Send/Clear to Send) is used to improve the data transmission efficiency of the network with hidden nodes, especially when there are lots of large packets to be transmitted.</p> <p>When the size of a data packet is larger than the RTS Threshold, the RTS/CTS mechanism will be activated. With this mechanism activated, before sending a data packet, the client will send an RTS packet to the EAP to request data transmitting. And then the EAP will send CTS packet to inform other clients to delay their data transmitting. In this way, packet collisions can be avoided.</p> <p>For a busy network with hidden nodes, a low threshold value will help reduce interference and packet collisions. But for a not-so-busy network, a too low threshold value will cause bandwidth wasting and reduce the data throughput. The recommended and default value is 2347 bytes.</p>
Fragmentation Threshold	<p>The fragmentation function can limit the size of packets transmitted over the network. If the size of a packet exceeds the Fragmentation Threshold, the fragmentation function is activated and the packet will be fragmented into several packets.</p> <p>Fragmentation helps improve network performance if properly configured. However, a too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.</p>
OFDMA	<p>OFDMA enables multiple users to transmit data simultaneously, and thus greatly improves speed and efficiency. Only when your clients also support OFDMA, can you fully enjoy the benefits.</p> <p>This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.</p>

4.1.3 Configure the MLO Network (Only for Wi-Fi 7 Devices)

MLO (Multi-Link Operation) enables Wi-Fi 7 devices to simultaneously send and receive data across different bands and channels. This ensures fast and reliable connections even in dense network environments.


To configure an MLO network, go to **Wireless > Wireless Settings > MLO** and click **Add**.

MLO SSIDs

 Add

ID	SSID	Band	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
--	--	--	--	--	--	--	--

SSID:

Band: ☒ 2.4GHz ☒ 5GHz 

SSID Broadcast: ☒ Enable


Security Mode:

Version:

Encryption: ☐ Auto ☒ AES

Wireless Password:

Group Key Update Period: seconds (30-8640000. 0 means no update.)

Guest Network: ☐ Enable 

Rate Limit: ☐ Enable

Note::

MLO (Multi-Link Operation) enables Wi-Fi 7 devices to simultaneously send and receive data across different frequency bands and channels. This ensures fast and reliable connections even in dense network environments.

Configure the parameters and save the settings.

SSID	Specify a name for the MLO network.
Band	Select the bands to form the MLO network. Available band options may vary by model.
SSID Broadcast	With the option enabled, AP will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the AP.
Security Mode/ Version/ Encryption	Configure the security settings of the wireless network. For detailed instructions, refer to 4.1.1 Configure SSIDs .
Guest Network	With this option enabled, guest network will block clients from reaching any private IP subnet.

Rate Limit

With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage.

You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to [View Client Information](#) to get more details.

Note that the download and upload rate will be limited to the smaller value if you set the limit value both in SSID and client configuration.

4.2 Configure Portal Authentication

Portal authentication provides authentication service to the clients that only need temporary access to the wireless 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.

In this module, you can also configure Free Authentication Policy, which allows the specific clients to access the specific network resources without authentication.

To configure portal authentication, go to the **Wireless > Portal** page.

Portal Configuration

SSID:

- Please Select -

Authentication Type:

No Authentication

Authentication Timeout:

1 Hour

D

H

M

Redirect:

☐ Enable

Redirect URL:

Portal Customization:

Local Web Portal

Term of Use:

☐ I accept the Term of Use

Login

Save

4.2.1 Configure the Portal

Three portal authentication types are available: *No Authentication*, *Local Password* and *External RADIUS Server*. The following sections introduce how to configure each authentication type.

• No Authentication

With this authentication type configured, clients can pass the authentication and access the network without providing any login information. They only need to accept the term of use on the authentication page.

Follow the steps below to configure No Authentication as the portal authentication type:

1. Select the SSID on which the portal will take effect.
2. Select **No Authentication** as the authentication type.
3. Configure the relevant parameters as the following table shows:

Authentication Timeout	<p>Specify the value of authentication timeout.</p> <p>A client's authentication will expire after the authentication timeout and the client needs to log in to the authentication page again to access the network.</p> <p>Options include 1 Hour, 8 Hours, 24 Hours, 7 Days, and Custom. With Custom selected, you can customize the time in days, hours, and minutes.</p>
Redirect	<p>With this function configured, the newly authenticated client will be redirected to the specific URL.</p>
Redirect URL	<p>With Redirect enabled, you also need to enter the URL in this field. The newly authenticated client will be redirected to this URL.</p>
Portal Customization	<p>Configure the authentication page. Local Web Portal is the only available option in this authentication type. Enter the title and term of use in the two boxes.</p> <p>The EAP uses its built-in web server to provide this authentication page for clients. To pass the authentication, clients only need to check the box of I accept the Term of Use and click the Login button.</p>

4. Click **Save**.

• Local Password

With this authentication type configured, clients are required to provide the correct password to pass the authentication.

Follow the steps below to configure Local Password as the portal authentication type:

1. Select the SSID on which the portal will take effect.
2. Select **Local Password** as the authentication type.
3. Configure the relevant parameters as the following table shows:

Password	Specify a password for authentication.
Authentication Timeout	<p>Specify the value of authentication timeout.</p> <p>A client's authentication will expire after the authentication timeout and the client needs to log in to the authentication page again to access the network.</p> <p>Options include 1 Hour, 8 Hours, 24 Hours, 7 Days, and Custom. With Custom selected, you can customize the time in days, hours, and minutes.</p>
Redirect	With this function configured, the newly authenticated client will be redirected to the specific URL.
Redirect URL	With Redirect enabled, you also need to enter the URL in this field. The newly authenticated client will be redirected to this URL.
Portal Customization	<p>Configure the authentication page. Local Web Portal is the only available option is this authentication type. Enter the title and term of use in the two boxes.</p> <p>The EAP uses its built-in web server to provide this authentication page for clients. To pass the authentication, clients need to provide the correct password in the Password field, check the box of I accept the Term of Use and click the Login button.</p>

4. Click **Save**.

• External RADIUS Server

If you have a RADIUS server on the network to authenticate the clients, you can select **External Radius Server**. Clients need to provide the correct login information to pass the authentication.

Follow the steps below to configure External Radius Server as the portal authentication type:

1. Select the SSID on which the portal will take effect.
2. Build a RADIUS server on the network and make sure that it is reachable by the EAP.
3. Go to the **Portal** configuration page on the EAP. Select **External Radius Server** as the authentication type.

3. Configure the relevant parameters as the following table shows:

RADIUS Server IP	Enter the IP address of RADIUS server.
RADIUS Port	Enter the port of the RADIUS server.
RADIUS Password	Enter the password of the RADIUS server.
NAS ID	Configure a Network Access Server Identifier (NAS ID) using 1 to 64 characters on the portal. The NAS ID is sent to the RADIUS server by the EAP through an authentication request packet. With the NAS ID which classifies users to different groups, the RADIUS server can send a customized authentication response.
RADIUS Accounting	Enable or disable RADIUS accounting feature.
Accounting Server IP	Enter the IP address of the accounting server.
Accounting Server Port	Enter the port number of the accounting server.
Accounting Server Password	Enter the shared secret key of the accounting server.
Interim Update	<p>With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled.</p> <p>Enter the appropriate duration between updates for EAPs in Interim Update Interval.</p>
Interim Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.
Authentication Timeout	<p>Specify the value of authentication timeout.</p> <p>A client's authentication will expire after the authentication timeout and the client needs to log in to the authentication page again to access the network.</p> <p>Options include 1 Hour, 8 Hours, 24 Hours, 7 Days, and Custom. With Custom selected, you can customize the time in days, hours, and minutes.</p>
Redirect	With this function configured, the newly authenticated client will be redirected to the specific URL.
Redirect URL	With Redirect enabled, you also need to enter the URL in this field. The newly authenticated client will be redirected to this URL.

Portal Customization

Configure the authentication page. There are two options: **Local Web Portal** and **External Web Portal**.

- Local Web Portal

Enter the title and term of use in the two boxes. The EAP uses its built-in web server to provide this authentication page for clients. To pass the authentication, clients need to provide the correct username and password in the **Username** and **Password** fields, check the box of **I accept the Term of Use** and click the **Login** button.

- External Web Portal

With External Web Portal configured, the authentication page will be provided by the web portal server built on the network. To configure External Web Portal, you need to complete the following configurations:

1. Build an external web portal server on your network and make sure that it is reachable by the EAP.
2. On this configuration page, enter the URL of the authentication page provided by the external portal server.
3. Add the external web portal server to the **Free Authentication Policy** list. In this way, clients can access the web portal server before authenticated. For details about how to configure Free Authentication Policy, refer to [4.2.2 Configure Free Authentication Policy](#).

-
4. Click **Save**.

4.2.2 Configure Free Authentication Policy

Free Authentication Policy allows some specific clients to access the specific network resources without authentication. For example, you can set a free authentication policy to allow clients to visit the external web portal server before authenticated. In this way, the clients can visit the login page provided by the web portal server and then pass the subsequent authentication process.

Free Authentication Policy

+

Add

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC Address	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Policy Name:

Source IP Range:

0.0.0.0 / (Optional)

Destination IP Range:

0.0.0.0 / (Optional)

Source MAC Address:

00-00-00-00-00-00 (Optional)

Destination Port:

(Optional)

Status:

☒ Enable

OK

Cancel

Follow the steps below to add free authentication policy.

1. In the **Free Authentication Policy** section, click **Add**.
2. Configure the following parameters. When all the configured conditions are met, the client can access the network without authentication.

Policy Name	Specify a name for the policy.
Source IP Range	<p>Specify an IP range with the subnet and mask length. The clients in this IP range can access the network without authentication.</p> <p>Leaving the field empty means that clients with any IP address can access the specific resources.</p>
Destination IP Range	<p>Specify an IP range with the subnet and mask length. The devices in this IP range can be accessed by the clients without authentication.</p> <p>Leaving the field empty means that all devices in the LAN can be accessed by the specific clients.</p>
Source MAC Address	<p>Specify the MAC address of the client, who can access the specific resources without authentication.</p> <p>Leaving the field empty means that clients with any MAC address can access the specific resources.</p>
Destination Port	<p>Specify the port number of the service. When using this service, the clients can access the specific resources without authentication.</p> <p>Leaving the field empty means that clients can access the specific resources no matter what service they are using.</p>
Status	Check the box to enable the policy.

Tips:

When External Web Portal is configured in the portal configuration, you should set the IP address and subnet mask of the external web server as the **Destination IP Range**. As for **Source IP Range**, **Source MAC Address** and **Destination Port**, you can simply keep them as empty or configure them according to your actual needs.

3. Click **OK** to add the policy.

4.3 Configure the VLAN

Wireless VLAN is used to set VLANs for the wireless networks. With this feature, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks will be added with different VLAN tags according to the VLAN settings of the wireless networks. The wireless clients in different VLANs cannot directly communicate with each other. Note that the traffic from the wired clients will not be added with VLAN tags.

To configure VLAN for the wireless network, go to the **Wireless > VLAN** page.

VLAN configurations vary with the working mode of the device.

• AP Mode

In AP mode, you can follow the steps below to configure VLAN.

VLAN ID				
ID	SSID Name	Band	VLAN	VLAN ID
1	603	2.4GHz	Disable ▼	0
2	6035	5GHz	Disable ▼	0

Save

1. Select the specific SSID in the list to configure the VLAN.
2. In the **VLAN** column, select **Enable** to enable the VLAN function on the SSID.
3. Specify the VLAN ID for the wireless network in the **VLAN ID** column. Every VLAN ID represents a different VLAN. It supports maximum 8 VLANs per frequency band. The VLAN ID range is 0 to 4094. 0 is used to disable VLAN tagging.
4. Click **Save**.

- Router Mode

In Router mode, the SSID VLAN ID follows the LAN VLAN ID.

VLAN Config

ID	SSID Name	Band	VLAN ID
1	test	2.4GHz	2 (LAN) ▼
2	test	5GHz	2 (LAN) ▼

Save

4.4 Configure MAC Filtering

MAC Filtering is used to allow or block the clients with specific MAC addresses to access the network. With this feature you can effectively control clients' access to the wireless network according to your needs.


To configure MAC Filtering, go to the **Wireless > MAC Filtering** page.

Settings

Enable MAC Filtering: ☒ Enable

Save

Station MAC Group

 Create Groups

MAC Filtering Association

ID	SSID	Band	MAC Group Name	Action
1	603	2.4GHz	None ▼	Deny ▼
2	6035	5GHz	None ▼	Deny ▼

Note:
Deny: Block access from the stations in the MAC Group list.
Allow: Only allow access from the stations in the MAC Group list.

Save

Follow the steps below to configure MAC Filtering on this page:

1. In the **Settings** section, check the box to enable **MAC Filtering**, and click **Save**.

2. In the **Station MAC Group** section, click **Create Group** and the following page will appear.

Station MAC Group

+ Add a Group

MAC Group Name	Modify
--	--

➡

+ Add a Group Member

ID	MAC Address	Modify
--	--	--

- 1) Click **Add a Group** and specify a name for the MAC group to be created. Click **OK**.
You can create more MAC groups if needed.
- 2) Select a MAC group in the group list. Click **Add a Group Member** to add group members to the MAC group. Specify the MAC address of the host and click **OK**. In the same way, you can add more MAC addresses to the selected MAC group.
3. In the **MAC Filtering Association** section, configure the filtering rule. For each SSID, you can select a MAC group in the **MAC Group Name** column and select the filtering rule (**Allow/Deny**) in the **Action** column. Click **Save**.

For example, the following configuration means that the hosts in Group2 are denied to access the SSID **SSID-1** on the 2.4GHz band and allowed to access the SSID **SSID-2** on the 5GHz band.

MAC Filtering Association

ID	SSID	Band	MAC Group Name	Action
1	SSID-1	2.4GHz	Group2 ▼	Deny ▼
2	SSID-2	5GHz	Group2 ▼	Allow ▼

Note:

Deny: Block access from the stations in the MAC Group list.

Allow: Only allow access from the stations in the MAC Group list.

Save

4.5 Configure Scheduler

With the Scheduler feature, the EAP or its wireless network can automatically turn on or off at the time you set. For example, you can schedule the radio to operate only during the office working time to reduce power consumption.

To configure Scheduler, go to the **Wireless > Scheduler** page.

Settings

Scheduler:

☒
Enable

Association Mode:

Associated with SSID

Save

Profile

+

Create Profiles

Scheduler Association

ID	SSID	Band	Profile Name	Action
1	603	2.4GHz	None	Radio Off
2	6035	5GHz	None	Radio Off

Save

Follow the steps below to configure Scheduler on this page:

- In the **Settings** section, check the box to enable **Scheduler** and select the **Association Mode**. There are two modes: **Associated with SSID** (the scheduler profile will be applied to the specific SSID) and **Associated with AP** (the profile will be applied to all SSIDs on the EAP). Then click **Save**.
- In the **Scheduler Profile Configuration** section, click **Create Profiles** and the following page will appear.

Profile

+

Add a Profile

Profile Name	Modify
--	--

➡

+

Add an item

ID	Profile Name	Days	Start Time	End Time	Modify
--	--	--	--	--	--

- Click **Add a Profile** and specify a name for the profile to be created. Click **OK**. You can create more profiles if needed.
- Select a profile in the list. Click **Add an item** to add time range items to the profile. Specify the **Day**, **Start Time** and **End Time** of the time range, and click **OK**.

Tips:

You can add multiple time range items for one profile. If there are several time range items in one profile, the time range of this profile is the sum of all of these time ranges.

3. In the **Scheduler Association** section, configure the scheduler rule. There are two association modes: *Association with SSID* and *Association with AP*. The following sections introduce how to configure each mode.

■ Association with SSID

If you select **Association with SSID** in step 1, the Scheduler Association table will display all the SSIDs on the EAP. For each SSID, you can select a profile in the **Profile Name** column and select the scheduler rule (**Radio On/Radio Off**) in the **Action** column. Then click **Save**.

For example, the following configuration means that during the time range defined in Profile-2, the radio of SSID **SSID-1** is on and the radio of SSID **SSID-2** is off.

Scheduler Association

ID	SSID	Band	Profile Name	Action
1	SSID-1	2.4GHz	Profile-2 ▼	Radio On ▼
2	SSID-2	5GHz	Profile-2 ▼	Radio Off ▼

Save

■ Association with AP

If you select **Association with AP** in step 1, the Scheduler Association table will display the name and MAC address of the EAP. Select a profile in the **Profile Name** column and select the scheduler rule (**Radio On/Radio Off**) in the **Action** column. Then click **Save**.

For example, the following configuration means that during the time range defined in Profile2, the radio of all SSIDs on the EAP-1 is on.

Scheduler Association

ID	AP	AP MAC	Profile Name	Action
1	EAP-1	■■■■■■■■■■	Profile-2 ▼	Radio On ▼

Save

4.6 Configure Band Steering

A client device that is capable of communicating on multiple frequency bands will typically connect to the 2.4GHz band. However, if too many client devices are connected to an AP

on the same band, the efficiency of communication will be diminished. Band Steering can steer multi-band clients to different bands to greatly improve the network quality.

To configure Band Steering, go to the **Wireless > Band Steering** page.

Band Steering

Band Steering: Disable

Note:
To run the Band Steering function on an SSID, please create the SSIDs on both of the 2GHz and 5GHz bands and make sure they have the same name, security mode and wireless password.

Save

Band Steering

Configure the Band Steering function.

Disable: The AP will not steer clients.

Prefer 5GHz: The AP will steer clients to the 5GHz in priority.

Balance: The AP will balance client connections among different bands.

4.7 Configure QoS

Quality of service (QoS) is used to optimize the throughput and performance of the EAP when handling differentiated wireless traffic, such as Voice-over-IP (VoIP), other types of audio, video, streaming media, and traditional IP data.

In QoS configuration, you should set parameters on the transmission queues for different types of wireless traffic and specify minimum and maximum wait time for data transmission. In normal use, we recommend that you keep the default values.

To configure QoS, go to the **Wireless > QoS** page.

2.4GHz

5GHz

AP EDCA Parameters

Queue	Arbitration Inter-Frame Spacing	Minimum Contention Window	Maximum Contention Window	Maximum Burst
Data 0 (Voice)	1	3	7	1504
Data 1 (Video)	1	7	15	3008
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Station EDCA Parameters

Queue	Arbitration Inter-Frame Spacing	Minimum Contention Window	Maximum Contention Window	TXOP Limit
Data 0 (Voice)	2	3	7	1504
Data 1 (Video)	2	7	15	3008
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

No Acknowledgement:

☐ Enable

Unscheduled Automatic Power Save Delivery:

☒ Enable

Save

Follow the steps below to configure QoS on this page:

1. Click a band to be configured.
2. In the **AP EDCA Parameters** section, configure the AP EDCA ((Enhanced Distributed Channel Access) parameters. AP EDCA parameters affect traffic flowing from the EAP to the client station. The following table detailedly explains these parameters.

The following table detailedly explains these parameters:

Queue	<p>Displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters.</p> <p>Data 0 (Voice): Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.</p> <p>Data 1 (Video): High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.</p> <p>Data 2 (Best Effort): Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.</p> <p>Data 3 (Background): Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).</p>
Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values are from 0 to 15.
Minimum Contention Window	<p>A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.</p> <p>This value cannot be higher than the value of Maximum Contention Window.</p>
Maximum Contention Window	<p>The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.</p> <p>This value must be higher than the value of Minimum Contention Window.</p>
Maximum Burst	Maximum Burst specifies the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.

3. In the **Station EDCA Parameters** section, configure the station EDCA (Enhanced Distributed Channel Access) parameters. Station EDCA parameters affect traffic flowing from the client station to the EAP.

The following table detailedly explains these parameters:

Queue	<p>Displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters.</p> <p>Data 0 (Voice): Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.</p> <p>Data 1 (Video): High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.</p> <p>Data 2 (Best Effort): Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.</p> <p>Data 3 (Background): Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).</p>
Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values are from 0 to 15.
Minimum Contention Window	<p>A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.</p> <p>This value cannot be higher than the value of Maximum Contention Window.</p>
Maximum Contention Window	<p>The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.</p> <p>This value must be higher than the value of Minimum Contention Window.</p>
TXOP Limit	<p>The TXOP Limit is a station EDCA parameter and only applies to traffic flowing from the client station to the EAP.</p> <p>The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a WME (Wireless Multimedia Extensions) client station has the right to initiate transmissions onto the wireless medium (WM) towards the EAP. The valid values are multiples of 32 between 0 and 8192.</p>
4. Choose whether to enable the following two options according to your need.	
No Acknowledgment	With this option enabled, the EAP would not acknowledge frames with QoSNoAck. No Acknowledgment is recommended if VoIP phones access the network through the EAP.
Unscheduled Automatic Power Save Delivery	As a power management method, it can greatly improve the energy-saving capacity of clients.

5. Click **Save**.

4.8 Configure Rogue AP Detection

A Rogue AP is an access point that is installed on a secure network without explicit authorization from the network administrator. With Rogue AP Detection, the EAP can scan all channels to detect the nearby APs and display the detected APs in the Detected Rogue AP list. If the specific AP is known as safe, you can move it to the Trusted APs list. Also, you can backup and import the Trusted AP list as needed.

Note:

The Rogue AP Detection feature is only used for collecting information of the nearby wireless network and does not impact the detected APs, no matter what operations you have executed in this feature.

To configure Rogue AP Detection, go to the **Wireless > Rogue AP Detection** page.

Settings

Rogue AP Detection: ☐ Enable

Save

Detected Rogue AP List

Scan

MAC	SSID	Band	Channel	Security	Beacon Interval	Signal	Action
--	--	--	--	--	--	--	--

Trusted AP List

MAC	SSID	Band	Channel	Security	Action
--	--	--	--	--	--

Download/Backup Trusted AP List

Save Action: ☒ Download (PC to AP) ☐ Backup (AP to PC)

Source File Name: Browse

File Management: ☒ Replace ☐ Merge









Save

4.8.1 Manage the Rogue AP List

Follow the steps below to detect the nearby APs and move the trusted ones to the Trusted AP list.

1. In the **Settings** section, check the box to enable **Rogue AP Detection**. Click **Save**.
2. In the **Detected Rogue AP List** section, click **Scan**.

- Wait for a few seconds without any operation. After detection is finished, the detected APs will be displayed in the list.

MAC	SSID	Band	Channel	Security	Beacon Interval	Signal	Action
00:0A:EB:13:09:17	C7v3_5G	5.0	36	ON	100		Known
00:0A:EB:13:09:18	C7v3	2.4	11	ON	100		Known
00:0A:EB:13:7A:FD	TP-Link_7B00_5G_1	5.0	36	ON	100		Known
00:0A:EB:13:7A:FE	TP-Link_7B00_5G_2	5.0	36	ON	100		Known
00:0A:EB:13:7A:FF	TP-Link_7B00	2.4	1	ON	100		Known
00:0A:EB:13:7B:01	RvR5	5.0	48	OFF	100		Known
00:1D:0F:E3:33:B1	Camera	2.4	4	ON	100		Known
00:20:02:16:38:22	TP-LINK_2.4G_3822	2.4	1	ON	100		Known
02:71:CC:4C:16:B8	DIRECT-na-BRAVIA	2.4	11	ON	100		Known
06:18:D6:C1:92:23	qwer	2.4	6	OFF	100		Known

The following table introduces the displayed information of the APs:

MAC	Displays the MAC address of the AP.
SSID	Displays the SSID of the AP.
Band	Displays the frequency band the AP is working on.
Channel	Displays the channel the AP is using.
Security	Displays whether the security mode is enabled on the AP.
Beacon Interval	Displays the Beacon Interval value of the EAP. Beacon frames are sent periodically by the AP to announce to the stations the presence of a wireless network. Beacon Interval determines the time interval of the beacon frames sent by the AP device.
Signal	Displays the signal strength of the AP.

- To move the specific AP to the Trusted AP list, click **Known** in the **Action** column. For example, you can move the first two APs in the above Detected Rogue AP list to the Trusted AP list.

5. View the trusted APs in the **Trusted AP List** section. To move the specific AP back to the Rogue AP list, you can click **Unknown** in the **Action** column.

Trusted AP List					
MAC	SSID	Band	Channel	Security	Action
00:0A:EB:13:7A:FD	TP-Link_7B00_5G_1	5.0	36	ON	Unknown
00:0A:EB:13:7A:FE	TP-Link_7B00_5G_2	5.0	36	ON	Unknown

4.8.2 Manage the Trusted AP List

You can download the trusted AP list from your local host to the EAP or backup the current Trusted AP list to your local host.

- **Download the Trusted AP List From the Host**

You can import a trusted AP list which records the MAC addresses of the trusted APs. The AP whose MAC address is in the list will not be detected as a rogue AP.

Download/Backup Trusted AP List

Save Action:

☒ Download (PC to AP) ☐ Backup (AP to PC)

Source File Name:

Browse

File Management:

☒ Replace ☐ Merge

Save

Follow the steps below to import a trusted AP list to the EAP:

1. Acquire the trusted AP list. There are two ways:
 - Backup the list from a EAP. For details, refer to [Backup the Trusted AP List to the Host](#).
 - Manually create a trusted AP list. Create a txt. file, input the MAC addresses of the trusted APs in the format XX:XX:XX:XX:XX:XX and use the Space key to separate each MAC address. Save the file as a **cfg** file.
2. On this page, check the box to choose **Download (PC to AP)**.
3. Click **Browse** and select the trusted AP list from your local host.
4. Select the file management mode. Two modes are available: **Replace** and **Merge**. Replace means that the current trusted AP list will be replaced by the one you import. Merge means that the APs in the imported list will be added to the current list with the original APs remained.

5. Click **Save** to import the trusted AP list.

- **Backup the Trusted AP List to the Host**

You can backup the current trusted AP list and save the backup file to the local host.

Download/Backup Trusted AP List

Save Action: ☐ Download (PC to AP) ☒ Backup (AP to PC)

Save

Follow the steps below to backup the current trusted AP list:

1. On this page, check the box to choose **Backup (AP to PC)**.
2. Click **Save** and the current trusted AP list will be downloaded to your local host as a **cfg** file.

4.9 Configure User Isolation

Wireless user isolation is a security feature that prevents wireless clients from communicating with each other. It adds a level of security to limit attacks and threats between devices connected to the wireless network.

To configure User Isolation, go to the **Wireless > User Isolation** page.

User Isolation

User Isolation: ☒ Enable ⓘ

Inter-SSID: ☒ Enable ⓘ

Intra-SSID: ☒ Enable ⓘ

LAN-WLAN: ☒ Enable ⓘ

Save

User Isolation	Enable or disable user isolation.
Inter-SSID	When enabled, the device isolates all users in different SSIDs.
Intra-SSID	When enabled, the device isolates all users in the same SSID.
LAN-WLAN	When enabled, the device isolates all users between LAN and SSID.

4.10 Configure Access Control (for AP Mode)

In AP mode, the ACL (Access Control) function can be used 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.

Note:

To configure Access Control in Router mode, refer to [3.9 Configure Access Control](#).

To configure Access Control, follow the steps below:

- 1. Go to the **Wireless > ACL** page.

IP Group

Add

Refresh

Name	IP Subnet	Modify
--	--	--

IP-Port Group

Add

Refresh

Name	IP Subnet	Port	Modify
--	--	--	--

ACL

Add

Refresh

Priority	Policy	Protocols	Source	Destination	Set Priority	Modify
--	--	--	--	--	--	--

- 2. In the **IP Group** or **IP-Port Group** section, click **Add** to add a group according to your needs.

IP Group:

Name	Specify the name for the group.
IP Subnet	Specify one or multiple IP subnets.

IP-Port Group:

Name	Specify the name for the group.
IP Subnet	Specify one or multiple IP subnets.
Port	Specify one or multiple ports.

3. In the **ACL** section, click **Add** to add an ACL rule.

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 multiple protocol types to which the rule applies from the drop-down list.
Source	Select the source of the packets to which this rule applies: IP Group: The device will examine whether the source IP address of the packet is in the IP Group you select. IP-Port Group: The device will examine whether the source IP address and port number of the packet are in the IP-Port Group you select. SSID: The device will examine whether the SSID of the packet is the SSID you select.
Destination	Select the destination of the packets to which this rule applies: IP Group: The device will examine whether the destination IP address of the packet is in the IP Group you select. IP-Port Group: The device will examine whether the destination IP address and port number of the packet are in the IP-Port Group you select.

4. Save the settings.

5

Monitor the Network

This chapter introduces how to monitor the running status and statistics of the wireless network, including:

- *5.1 Monitor the EAP*
- *5.2 Monitor the Wireless Status*
- *5.3 Monitor the Clients*
- *5.4 Monitor the WAN Status (Only for Router Mode)*
- *5.5 Monitor the LAN Status (Only for Router Mode)*
- *5.6 Monitor the ARP Table (Only for Router Mode)*
- *5.7 Monitor the Routes (Only for Router Mode)*

5.1 Monitor the EAP

To monitor the EAP information, go to the **Status > Device** page.

The displayed information may vary by model and working mode.

Device Information	
Device Name:	
Device Model:	
Firmware Version:	1.0.0 Build 20250315 Rel. 59474(4a50)
Hardware Version:	1.0
MAC Address:	
IP Address:	192.168.0.254
Subnet Mask:	255.255.255.0
ETH0(PoE IN):	Down
ETH1:	1000Mbps - FD
System Time:	2025-01-01 00:01:53
Uptime:	0 days 00:01:55
CPU Utilization:	<div><div></div></div> 1%
Memory Utilization:	<div><div></div></div> 49%

5.2 Monitor the Wireless Status

You can view the wireless status of the EAP, such as SSID lists, radio settings, radio traffic and more.

Tips:

To change the wireless parameters, you can refer to [4.1 Configure Wireless Parameters](#).

To monitor the wireless status, go to the **Status > Wireless** page.

The displayed information may vary by model and working mode.

SSID List

 Refresh

ID	SSID Name	Clients	Band	Security	Portal	VLAN ID	Guest Network	Down (Byte)	Up (Byte)
1	603	1	2.4GHz	WPA-PSK	Disable	Disable	Disable	0	0
2	6035	0	5GHz	WPA-PSK	Disable	Disable	Disable	0	0

Radio Settings

2.4GHz

5GHz

2.4GHz Wireless Radio:

Channel Frequency:

Channel Width:

IEEE802.11 Mode:

Max TX Rate:

Tx Power:

Radio Traffic

2.4GHz

5GHz

Rx Packets: 0

Tx Packets: 0

Rx Bytes: 0

Tx Bytes: 0

Rx Dropped Packets: 0

Tx Dropped Packets: 0

Rx Errors: 0

Tx Errors: 0

LAN Traffic

Rx Packets: 0

Tx Packets: 151

Rx Bytes: 0

Tx Bytes: 14766

Rx Dropped Packets: 0

Tx Dropped Packets: 0

Rx Errors: 0

Tx Errors: 0

5.3 Monitor the Clients

You can monitor the information of the clients connected to the EAP.

To monitor the client information, go to the **Status > Client** page.

The displayed information may vary by working mode.

• View Client Information

You can view the information of wireless clients.

There are two types of clients: users and portal authenticated guests. Users are the clients that connect to the SSID with portal authentication disabled. Guests are the clients that connect to the SSID with portal authentication enabled.

Wireless Client List											
User Guest											
											Refresh
ID	Hostname	IP Address	MAC Address	Band	SSID	Active Time	Up (Byte)	Down (Byte)	RSSI (dBm)	Rate (Mbps)	Action
1				2.4GHz	!!2g_650v2	0 days 00:00:13	100k	66k	-39	154.0	

Click the **User** or **Guest** tab to select the client types to view the information of the EAP.

You can execute the corresponding operation to the EAP by clicking an icon in the Action column.



Click the icon to configure the rate limit of the client to balance bandwidth usage. Enter the download limit and upload limit and click **OK**.

You can limit the download and upload rate for each clients by which connect to specific SSIDs when configuring SSIDs, refer to [4.1.1 Configure SSIDs](#) to get more details.

Note that the download and upload rate will be limited to the smaller value if you set the limit value both in SSID and client configuration.



Click the icon to block the access of the client to the network.

• View Block Client Information

You can view the information of the clients that have been blocked and resume the client's access.

Block Client List					
					Refresh
ID	Hostname	MAC Address	Up (Byte)	Down (Byte)	Action
1			100k	66k	

You can click the delete icon to remove the client from the block list. This will resume the client's access to the internet.

- **View DHCP Client Information (Only for Router Mode)**

In Router mode, you can view the DHCP client information and DHCP server status.

DHCP Clients				
<div>Refresh</div>				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1			192.168.0.100	0 days 01:58:41

DHCP Server Status		
<div>Refresh</div>		
ID	IP Address Range	Usage
1	192.168.0.100 - 192.168.0.200	0.99% (1 / 101)

5.4 Monitor the WAN Status (Only for Router Mode)

In Router mode, you can view the WAN status, such as IPv4 WAN status, IPv6 WAN status, and WAN traffic.

Tips:

To change the WAN parameters, you can refer to [3.1 Configure WAN Parameters](#).

To monitor the WAN status, go to the **Status > WAN** page.

IPv4 WAN Status

Connection Type:

Static

MAC Address:

IP Address:

192.168.0.254

Subnet Mask:

255.255.255.0

Default Gateway:

Primary DNS:

Secondary DNS:

0.0.0.0

IPv6 WAN Status

IPv6 IP Address:

--

IPv6 IP Prefix:

--

WAN Traffic

Rx Packets:

0

Rx Bytes:

0

Rx Dropped Packets:

0

Rx Errors:

0

Tx Packets:

0

Tx Bytes:

0

Tx Dropped Packets:

0

Tx Errors:

0

Refresh

5.5 Monitor the LAN Status (Only for Router Mode)

In Router mode, you can view the LAN status.

To monitor the WAN parameters, go to the **Status > LAN** page.

LAN Traffic

Rx Packets:

4513

Rx Bytes:

1320386

Rx Dropped Packets:

2

Rx Errors:

0

Tx Packets:

4380

Tx Bytes:

2241985

Tx Dropped Packets:

0



Tx Errors:

0

5.6 Monitor the ARP Table (Only for Router Mode)

In Router mode, you can view the ARP information.





To monitor the ARP information, go to the **Status > ARP Table** page.

ARP Table		
		 Refresh
ID	IP Address	MAC Address
1	192.168.0.143	

5.7 Monitor the Routes (Only for Router Mode)

In Router mode, you can view the route information.

To monitor the route information, go to the **Status > Routes** page.

Routes				
				 Refresh
ID	Destination	Gateway	Subnet Mask	Interface
1	0.0.0.0		0.0.0.0	WAN
2	192.168.0.0		255.255.255.0	BRIDGE
3	192.168.0.0		255.255.255.0	WAN

6

Manage the EAP

The EAP provides powerful functions of device management and maintenance. This chapter introduces how to manage the EAP, including:

- *6.1 Manage the IP Address of the EAP (Only for AP Mode)*
- *6.2 Manage System Logs*
- *6.3 Configure Web Server*
- *6.4 Configure Management Access*
- *6.5 Configure LED*
- *6.6 Configure the LAN Port (for AP Mode)*
- *6.7 Configure Wi-Fi Control*
- *6.8 Configure SSH*
- *6.9 Configure SNMP*

6.1 Manage the IP Address of the EAP (Only for AP Mode)

The IP address of the EAP can be a dynamic IP address assigned by the DHCP server or a static IP address manually specified by yourself. By default, the EAP gets a dynamic IP

address from the DHCP server. You can also specify a static IP address according to your needs.

To configure the IP address of the EAP, go to the **Management > Network** page.

IP Settings

☒ Dynamic ☐ Static

Fallback IP: ☒ Enable

DHCP Fallback IP: 192.168.0.254

DHCP Fallback IP Mask: 255.255.255.0

DHCP Fallback Gateway:

Save

Follow the steps below to configure the IP address of the EAP:

1. Choose your desired IP address mode: **Dynamic** or **Static**.
2. Configure the related parameters according to your selection.

- **Dynamic**

If you choose Dynamic as the IP address mode, make sure that there is a reachable DHCP server on your network and the DHCP sever is properly configured to assign IP address and the other network parameters to the EAP.

For network stability, you can also configure the fallback IP parameters for the EAP:

Fallback IP	With the fallback IP configured, if the EAP fails to get an IP address from a DHCP server within 10 seconds, the fallback IP will work as the IP address of the EAP. After that, however, the EAP will keep trying to obtain an IP address from the DHCP server until it succeeds.
DHCP Fallback IP	Specify a fallback IP address for the EAP. Make sure that this IP address is not being used by any other device in the same LAN. The default DHCP fallback IP is 192.168.0.254.
DHCP Fallback IP MASK	Specify the network mask of the fallback IP. The default DHCP fallback IP mask is 255.255.255.0.
DHCP Fallback Gateway	Specify the network gateway.

- **Static**

If you choose Static as the IP address mode, you need to manually specify an IP address and the related network parameters for the EAP. Make sure that the specified IP address is not being used by any other device in the same LAN.

Configure the IP address and network parameters as the following table shows:

IP Address	Specify a static IP address for the EAP.
IP Mask	Specify the network mask.
Gateway	Specify the network gateway.
Primary DNS	Specify the primary DNS server.
Secondary DNS	Specify the secondary DNS server. (Optional)


3. Click **Save**.

6.2 Manage System Logs

System logs record information about hardware, software as well as system issues and monitors system events. With the help of system log, you can get informed of system running status and detect the reasons for failure.

To manage system logs, go to the **Management > System Log** page.

Log

 Refresh

Index	Time	Type	Level	Log Content
2	2025-01-01 00:00:59	DEV_IP_C	WARNING	[ap:] got IP address 192.168.0.254/255.255.255.0.
1	1970-01-01 00:00:14	OTHER	INFO	System started

Log Settings

Enable Auto Mail:

☐ Enable

Enable Server:

☐ Enable

Save

On this page, you can view the system logs and configure the way of receiving system logs.

6.2.1 View System Logs

In the **Log** section, you can click **Refresh** to refresh the logs and view them in the table.

6.2.2 Configure the Way of Receiving Logs

In the **Log Settings** section, you can configure the ways of receiving system logs.

Log Settings

Enable Auto Mail:

☒ Enable

From:

To:

SMTP Server:

Enable SSL:

☐ Enable

SMTP Port:

25

(1-65535)

Enable Authentication:

☐ Enable

Time:

☒ Fixed Time ☐ Period

Fixed Time:

00

:

00

(HH:MM)

Enable Server:

☒ Enable

System Log Server IP:

0.0.0.0

System Log Server Port:

514

(514, 1025-65535)

More Client Detail Log:

☐ Enable

Save

Follow the steps below to configure this feature:

1. Check the corresponding box to enable one or more ways of receiving system logs, and configure the related parameters. Two ways are available: [Auto Mail](#) and [Server](#).

■ Auto Mail

If Auto Mail is configured, system logs will be sent to a specified mailbox. Check the box to enable the feature and configure the related parameters.

The following table introduces how to configure these parameters:

From	Enter the sender's E-mail address.
To	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address of the sender's SMTP server. Note: At present, the domain name of SMTP server is not supported in this field.

Enable Authentication	If the sender's mailbox is configured with You can check the box to enable mail server authentication. Enter the sender's username and password.
Time Mode	Select Time Mode: Fixed Time or Period Time . Fixed Time means that the system logs will be sent at the specific time every day. Period Time means that the system logs will be sent at the specific time interval.
Fixed Time	If you select Fixed Time , specify a fixed time to send the system log mails. For example, 08:30 indicates that the mail will be sent at 8:30 am everyday.
Period Time	If you select Period Time , specify a period time to regularly send the system log mail. For example, 6 indicates that the mail will be sent every six hours.

■ Server

If Server is configured, system logs will be sent to the specified system log server, and you can use the syslog software to view the logs on the server.

Enable this feature and enter the IP address and port of the system log server.

System Log Server IP	Enter the IP address of the server.
System Log Server Port	Enter the port of the server.
More Client Detail Log	With the option enabled, the logs of clients will be sent to the server.

2. Click **Save**.

6.3 Configure Web Server

With the web server, you can log in to the management web page of the EAP. You can configure the web server parameters of the EAP according to your needs.

To configure Web Server, go to the **Management > Web Server** page.

Web server configurations vary with the working mode of the device.

- AP mode

Web Server

Secure Server Port:

443

Server Port:

80

Session Timeout:

15

minutes

Layer-3 Accessibility:

☐ Enable

TLS Version 1.0/1.1:

☐ Enable ⓘ

Older Security Kits:

☐ Enable ⓘ

HTTP Server:

☐ Enable

Note:

Please enter the EAP's IP address to access the web-based configuration utility via an HTTPS connection.

Save

Secure Server Port	Designate a secure server port for web server in HTTPS mode. By default the port is 443.
---------------------------	--

Server Port	Designate a server port for web server in HTTP mode. By default the port is 80.
--------------------	---

Session Timeout	Set the session timeout. If you do nothing with the web page within the timeout, the system will log out automatically. You can log in again if you want to go back to web page.
------------------------	--

Layer-3 Accessibility	With this feature enabled, devices from a different subnet can access Omada managed devices via the management web page. With this feature disabled, only the devices in the same subnet can access Omada managed devices via the management web page.
------------------------------	--

TLS Version 1.0/1.1	<p>The EAP management page uses TLS v1.2 by default. You can enable the feature if you prefer TLS v1.0/1.1.</p> <p>This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.</p>
----------------------------	--

- Router mode

Web Server

Secure Server Port:

443

Server Port:

80

Session Timeout:

15

minutes

Remote Login IP Address:

0.0.0.0

(Optional)

HTTP Server:

☐ Enable

Note:

Please enter the EAP's IP address to access the web-based configuration utility via an HTTPS connection.

Save

Secure Server Port	Designate a secure server port for web server in HTTPS mode. By default the port is 443.
Server Port	Designate a server port for web server in HTTP mode. By default the port is 80.
Session Timeout	Set the session timeout. If you do nothing with the web page within the timeout, the system will log out automatically. You can log in again if you want to go back to web page.
Remote Login IP Address	Configure an IP address that can access the device remotely.
HTTP Server	Enable this option if you want to log in to the management web page of the EAP via HTTP.

6.4 Configure Management Access

By default, all hosts in the LAN can log in to the management web page of the EAP with the correct username and password. To control the hosts' access to the web page of the EAP, you can specify the MAC addresses and management VLAN (only for AP mode) of the hosts that are allowed to access the web page.

6.4.1 Configure Access MAC Management

Only the hosts with the specific MAC addresses are allowed to access the web page, and other hosts without MAC addresses specified are not allowed to access the web page.

To configure this feature, go to the **Management > Management Access** page.

Access MAC Management

MAC Authentication:
☐ Enable

MAC1:
AA-BB-CC-DD-EE-FF

MAC2:
AA-BB-CC-DD-EE-FF

MAC3:
AA-BB-CC-DD-EE-FF

MAC4:
AA-BB-CC-DD-EE-FF

Add PC's MAC Address

Save

Follow the steps below to configure Management Access on this page:

1. Check the box to enable **MAC Authentication**.
2. Specify one or more MAC addresses in the **MAC1/MAC2/MAC3/MAC4** fields. Up to four MAC addresses can be added.

3. Click **Save**.

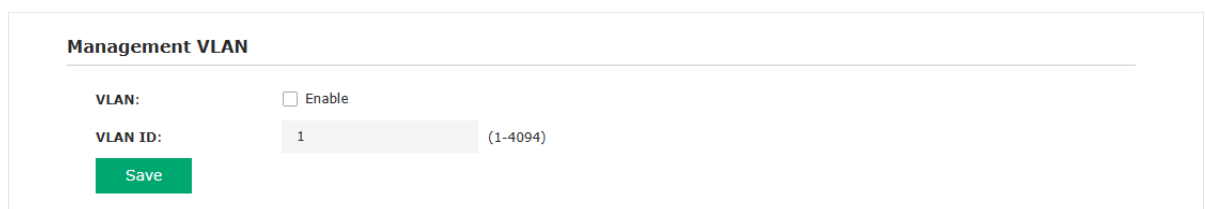
Tips:

- You can click **Add PC's MAC Address** to quickly add the MAC address of your current logged-in host, .
- Verify the MAC addresses carefully. Once the settings are saved, only the hosts in the MAC address list can access the web page of the EAP.
- If you cannot log in to the web page after saving the wrong configuration, you can reset the EAP to the factory defaults and use the default username and password (both admin) to log in.

6.4.2 Configure Management VLAN (Only for AP Mode)

Management VLAN provides a safer method to manage the EAP. With Management VLAN enabled, only the hosts in the Management VLAN can access the web page of the EAP. Since most hosts cannot process VLAN TAGs, you can connect the management host to the network via a switch, and set up correct VLAN settings for the switches on the network to ensure the communication between the host and the EAP in the Management VLAN.

To configure this feature, go to the **Management > Management Access** page and locate the Management VLAN section.



Management VLAN

VLAN: ☐ Enable

VLAN ID: (1-4094)

Save

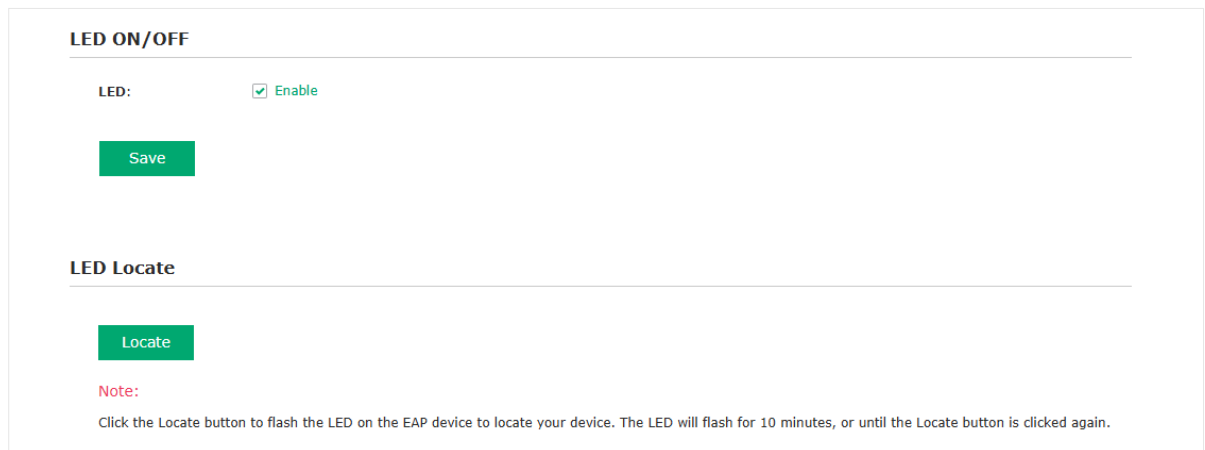
Follow the steps below to configure Management VLAN on this page:

1. Check the box to enable **Management VLAN**.
2. Specify the VLAN ID of the management VLAN. Only the hosts in the Management VLAN can log in to the EAP via the Ethernet port.
3. Click **Save**.

6.5 Configure LED

You can turn on or off the LED light of the EAP and flash the LED to locate your device.

To configure LED, go to the **Management > LED Control** page.



LED ON/OFF

LED: ☒ Enable

Save

LED Locate

Locate

Note:
Click the Locate button to flash the LED on the EAP device to locate your device. The LED will flash for 10 minutes, or until the Locate button is clicked again.

Check the box to turn on or turn off the LED light of the EAP, and click **Save**. To flash the LED, click **Locate**. Then the LED will flash for 10 minutes or until the locate button is clicked again.

6.6 Configure the LAN Port (for AP Mode)

Note:

To configure the LAN port in Router mode, refer to [3.3 Configure the LAN Port](#).

6.6.1 Configure the Port VLAN

Certain devices support VLAN configuration. If you want the EAP's LAN port to forward data with VLAN tags, you can configure the VLAN for it.

Port VLAN is used to set VLANs for the LAN ports. With this feature, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients connected to different LAN ports will be added with different VLAN tags according to the VLAN settings of the ports. The wired clients in different VLANs cannot directly communicate with each other.

To configure VLAN for the LAN port, go to the **Management > LAN Port Config** page. Select your desired port, enable VLAN, and set the VLAN ID according to your needs.

IPv6 Pass

ETH0:

☒ Enable

ETH1:

☒ Enable

VLAN Config

ETH Port	VLAN	VLAN ID
ETH1	Disable ▼	1

Note:

Changing the VLAN of the LAN port will cause client disconnection. Please unplug then reconnect the Ethernet cable of the client to the device or manually configure the correct IP address on the client.

Save

Follow the steps below to configure port VLAN on this page.

1. Select the specific ETH port in the list to configure the VLAN.
2. In the **VLAN** column, select **Enable** to enable the VLAN function on the port.
3. Specify the VLAN ID for the port in the **VLAN ID** column. Every VLAN ID represents a different VLAN.
4. Click **Save**.

6.7 Configure Wi-Fi Control

Note:

Wi-Fi Control is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If Wi-Fi Control is available, there is **Management > Wi-Fi Control** in the menu structure.

Certain devices have an LED/Wi-Fi button on the front panel. With Wi-Fi Control enabled, you can press the button to turn on or off both of the Wi-Fi and LED at the same time.

To configure Wi-Fi Control, go to the **Management > Wi-Fi Control** page.

Wi-Fi Control

With the Wi-Fi Control enabled, you can turn on/off the Wi-Fi and LED simultaneously by pressing the LED button on the product.

Wi-Fi Control:

☐ Enable

Note:

You can enable Wi-Fi Control feature only when the LED ON/OFF is enabled.

Save

Check the box to enable Wi-Fi Control and click **Save**.

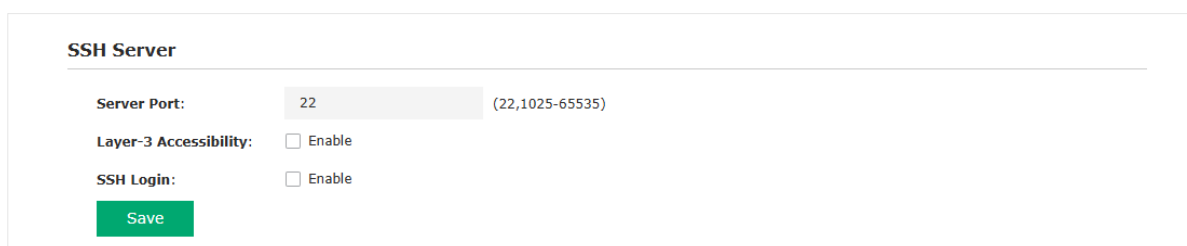
Note:

You can enable Wi-Fi Control only when the option **LED ON/OFF** is enabled.

6.8 Configure SSH

If you want to remotely log in to the EAP via SSH, you can deploy an SSH server on your network and configure the SSH feature on the EAP.

To configure SSH, go to the **Management > SSH** page.



Follow the steps below to configure SSH on this page:

1. Refer to the following table to configure the parameters:

Server Port	Designate a server port for SSH. By default the port is 22.
Layer-3 Accessibility	With this feature enabled, devices from a different subnet can access Omada managed devices via SSH. With this feature disabled, only the devices in the same subnet can access Omada managed devices via SSH.
SSH Login	Enable or disable SSH Login globally.

2. Click **Save**.

6.9 Configure SNMP

The EAP can be configured as an SNMP agent and work together with the SNMP manager. Once the EAP has become an SNMP agent, it is able to receive and process request messages from the SNMP manager. At present, the EAP supports SNMP v1 and v2c.

To configure the EAP as an SNMP agent, go to the **Management > SNMP** page.

SNMP Agent

SNMP Agent:

☐ Enable

SysContact:

SysName:

SysLocation:

Get Community:

Low

Middle

High

Get Source:

0.0.0.0

Set Community:

Low

Middle

High

Set Source:

0.0.0.0

Save

Follow the steps below to complete the configuration on this page:

1. Check the box to enable **SNMP Agent**.
2. Refer to the following table to configure the required parameters:

SysContact	Enter the textual identification of the contact person for this managed node.
SysName	Enter an administratively-assigned name for this managed node.
SysLocation	Enter the physical location of this managed node.
Get Community	Community refers to a host group aiming at network management. Get Community only has the read-only right of the device's SNMP information. The community name can be considered a group password. The default setting is public.
Get Source	Defines the IP address (for example, 10.10.10.1) for management systems that can serve as Get Community to read the SNMP information of this device. The default is 0.0.0.0, which means all hosts can read the SNMP information of this device.
Set Community	Set Community has the read and write right of the device's SNMP information. Enter the community name that allows read/write access to the device's SNMP information. The community name can be considered a group password. The default setting is private.
Set Source	Defines the IP address (for example, 10.10.10.1) for management systems that can serve as Set Community to read and write the SNMP information of this device. The default is 0.0.0.0, which means all hosts can read and write the SNMP information of this device.

3. Click **Save**.

Note:

Defining community can allow management systems in the same community to communicate with the SNMP Agent. The community name can be seen as the shared password of the network hosts group. Thus, for the security, we recommend that modify the default community name before enabling the SNMP Agent service. If the field of community is blank, the SNMP Agent will not respond to any community name.

7

Manage the System

This chapter introduces how to configure the system of the EAP, including:

- *7.1 Configure the User Account*
- *7.2 Configure Controller Settings (Only for AP Mode)*
- *7.3 Configure the System Time*
- *7.4 Reboot and Reset the EAP*
- *7.5 Backup and Restore the Configuration*
- *7.6 Update the Firmware*
- *7.7 Perform Network Diagnostic (Only for Router Mode)*

7.1 Configure the User Account

Every EAP has a user account, which is used to log in to the management page of the EAP. When you start the EAP at the first time, the username and password of the user account are both admin. After the first login, the system will require you to set a new username and a new password for the user account. And then you can use the new user account to log in to the EAP. Also, you can change your user account as needed.

Tips:

Please remember your user account well. If you forget it, reset the EAP to the factory defaults and log in with the default user account (username and password are both admin).

To configure the user account, go to **System > User Account** page.

Account Management

Old User Name:

Old Password:

New User Name:

New Password:

Low

Middle

High

Confirm New Password:

Save

Follow the steps below to change your user account on this page:

1. Enter the old username and old password of your user account.
2. Specify a new username and a new password for your user account. The system will automatically detect the strength of your entered password. For security, we recommend that you set a password with high strength.
3. Retype the new password.
4. Click **Save**.

7.2 Configure Controller Settings (Only for AP Mode)

To make your controller adopt your EAP, make sure the EAP can be discovered by the controller. Controller Settings enable your EAP to be discovered in either of the following scenarios.

Cloud-Based Controller Management

Connection Status: Disabled

Cloud-Based Controller Management: ☐ Enable

Note:

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:

Note:

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.

Save

- If you are using Omada Cloud-Based Controller, refer to [7.2.1 Enable Cloud-Based Controller Management](#).
- If your EAP and controller are located in the same network, LAN and VLAN, the controller can discover and adopt the EAP without any controller settings. Otherwise, you need to inform the EAP of the controller's URL/IP address by referring to [7.2.2 Configure Controller Inform URL](#).

For details about the whole procedure, refer to the User Guide of Omada SDN Controller.

The guide can be found on our Documents page:

<https://support.omadanetworks.com/document>

7.2.1 Enable Cloud-Based Controller Management

Go to the **System > Controller Settings** page. In the Cloud- Based Controller Management section, enable **Cloud-Based Controller Management** and click **Save**. After you add the EAP to your Omada Cloud-Based Controller, you can check the connection status on this page.

7.2.2 Configure Controller Inform URL

Go to the **System > Controller Settings** page. In the Controller Inform URL section, inform the EAP of the controller's URL/IP address, and click **Save**. Then the EAP make contact with the controller so that the controller can discover the EAP.

7.3 Configure the System Time

System time is the standard time for Scheduler and other time-based functions. The EAP supports the basic system time settings and the Daylight Saving Time (DST) feature.

To configure the system time, go to the **System > Time Settings** page.

Time Settings

Time zone:

(GMT-08:00) Pacific Time

Date:

01/01/2025

MM/DD/YYYY

Time:

08

:

02

:

26

(HH/MM/SS)

Primary NTP Server:

(Optional)

Secondary NTP Server:

(Optional)

Get GMT

Synchronize with PC

Save

Daylight Saving

Daylight Saving:

☐ Enable

Mode:

☒ Predefined Mode

☐ Recurring Mode

Predefine Country:

USA

Save

The following two sections introduce how to configure the basic system time settings and the Daylight Saving Time feature.

7.3.1 Configure the System Time

In the **Time Settings** section, you can configure the system time. There are three methods to set the system time: *Set the System Time Manually*, *Acquire the System Time From an NTP Server*, and *Synchronize the System Time with PC's Clock*.

Determine the way of setting the system time and follow the steps below to complete the configurations:

- **Set the System Time Manually**

To set the system time manually, follow the steps below:

1. Configure the following three options on the page: **Time Zone**, **Date** and **Time**.

Time Zone	Select your time zone from the drop-down list. Here GMT means Greenwich Mean Time.
Date	Specify the current date in the format MM/DD/YYYY. MM means month, DD means day and YYYY means year. For example: 06/01/2017.
Time	Specify the current time in the format HH/MM/SS. HH means hour, MM means minute and SS means second. It uses 24-hour system time. For example: 14:36:21.

2. Click **Save**.

Note:

The system time set manually will be lost after the EAP is rebooted.

- **Acquire the System Time From an NTP Server**

To get the system time from an NTP server, follow the steps below:

1. Build an NTP server on your network and make sure that it is reachable by the EAP. Or you can simply find an NTP server on the internet and get its IP address.
2. Specify the NTP server for the EAP. If you have two NTP servers, you can set one of them as the primary NTP server, and the other as the secondary NTP server. Once the primary NTP server is down, the EAP can get the system time from the secondary NTP server.

Primary NTP Server	Enter the IP address of the primary NTP server. Note: If you have only one NTP server on your network, enter the IP address of the NTP server in this field.
Secondary NTP Server	Enter the IP address of the secondary NTP server.

3. Click the button **Get GMT** and the acquired system time will be displayed in the **Date** and **Time** fields.
4. Click **Save**.

- **Synchronize the System Time with PC's Clock**

To synchronize the system time with the clock of your currently logged-in host, follow the steps below:

1. Click the button **Synchronize with PC** and the synchronized system time will be displayed in the **Date** and **Time** fields.
2. Click **Save**.

Note:

The system time synchronized with PC's clock will be lost after the EAP is rebooted.

7.3.2 Configure Daylight Saving Time

Daylight saving time is the practice of advancing clocks during summer months so that evening daylight lasts longer, while sacrificing normal sunrise times. The EAP provides daylight saving time configuration.

Follow the steps below to configure daylight saving time:

1. Check the box to enable **Daylight Saving**.
2. Select the mode of daylight saving time. Three modes are available: **Predefined Mode**, **Recurring Mode** and **Date Mode**.
3. Configure the related parameters of the selected mode.

■ **Predefined Mode**

If you select Predefined Mode, choose your region from the drop-down list and the EAP will use the predefined daylight saving time of the selected region.

There are four regions provided: **USA**, **European**, **Australia** and **New Zealand**. The following table introduces the predefined daylight saving time of each region.

USA	From 2: 00 a.m. on the Second Sunday in March to 2:00 a.m. on the First Sunday in November.
European	From 1: 00 a.m. on the Last Sunday in March to 1:00 a.m. on the Last Sunday in October.
Australia	From 2:00 a.m. on the First Sunday in October to 3:00 a.m. on the First Sunday in April.
New Zealand	From 2: 00 a.m. on the Last Sunday in September to 3:00 a.m. on the First Sunday in April.

■ Recurring Mode

If you select Recurring Mode, manually specify a cycle time range for the daylight saving time of the EAP. This configuration will be used every year.

The following table introduces how to configure the cycle time range.

Time Offset	Specify the time to set the clock forward by.
Start	Specify the start time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).
End	Specify the end time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).

■ Date Mode (Only for certain models)

If you select Date Mode, manually specify an absolute time range for the daylight saving time of the EAP. This configuration will be used only once.

The following table introduces how to configure the absolute time range.

Time Offset	Specify the time to set the clock forward by.
Start	Specify the start time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).
End	Specify the end time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).

4. Click **Save**.

7.4 Reboot and Reset the EAP

You can reboot and reset the EAP according to your need.

To reboot and reset the EAP, go to the **System > Reboot&Reset** page.

Reboot & Reset

Reboot Device:

Reboot

Reset to Factory Defaults:

Reset

- To reboot the EAP, click the **Reboot** button, and the EAP will be rebooted automatically. Please wait without any operation.
- To reset the EAP, click the **Reset** button, and the EAP will be reset to the factory defaults automatically. Please wait without any operation.

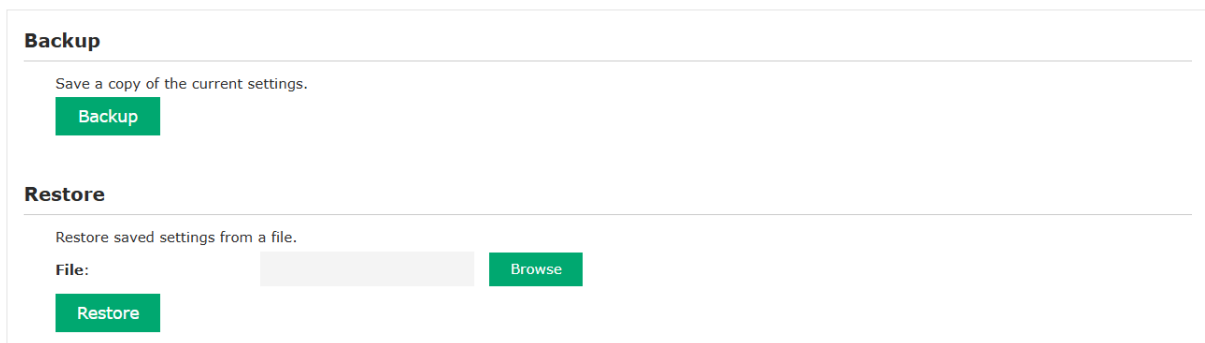
Note:

After reset, all the current configuration of the EAP will be lost. We recommend that you check whether you have any configuration that needs to be backed up before resetting the EAP.

7.5 Backup and Restore the Configuration

You can save the current configuration of the EAP as a backup file and save the file to your host. And if needed, you can use the backup file to restore the configuration. We recommend that you backup the configuration before resetting or upgrading the EAP.

To backup and restore the configuration, go to the **System > Backup&Restore** page.



Backup

Save a copy of the current settings.

Backup

Restore

Restore saved settings from a file.

File: **Browse**

Restore

- To backup the configuration, click the **Backup** button in the Backup section, and the backup file will be saved to the host automatically.
- To restore the configuration, click the **Browse** button in the Restore section and choose the backup file from the host. Then click the **Restore** button to restore the configuration.

7.6 Update the Firmware

We provide the firmware update files for the EAP products on our official website. To get new functions of the EAP, you can check our official website and download the update files to update the firmware of your EAP.

To update the firmware, go to the **System > Firmware Update** page.

Online Firmware Update

Current Firmware version:

1.0.0

Latest Firmware version:

Check

Automatically check for firmware upgrades:

☐ Enable

Save

Local Firmware Update

New Firmware File:

Browse

Warning:

The firmware update process takes a couple of minutes. Please do not power off the device until the process finishes.

Update

- **Online Firmware Update**

Follow the steps below to update the firmware of your EAP online:

1. In the **Online Firmware Update** section, click **Check** to see whether a new firmware is released.
2. If a new firmware is found, click **Update**. You can also check the box to automatically check for firmware updates.

- **Local Firmware Update**

Follow the steps below to update the firmware of your EAP locally:

1. Go to our website <https://www.omadanetworks.com> and search for your EAP model. Download the proper firmware file on the support page of the EAP.
2. Log in to the EAP web page and go to the **System > Firmware Update** page.
3. In the **Local Firmware Update** section, click the **Browse** button, locate and choose the correct firmware file from your host.
4. Click the **Update** button to update the firmware of the EAP. After updated, the EAP will be rebooted automatically.

Note:

The update process takes several minutes. To avoid damage to the EAP, please wait without any operation until the update is finished.

7.7 Perform Network Diagnostic (Only for Router Mode)

7.7.1 Run a Ping Test

The ping test function is used to test the connectivity and reachability between the device and the target host so as to locate the network malfunctions.

To run a ping test, go to the **System > Diagnostic** page and choose the Ping tool.

Diagnostic

Diagnostic Tool:

Ping

Destination IP/Domain:

0.0.0.0

Packet Count:

(1-50)

Ping Timeout:

milliseconds (100-2000)

Packet Size:

bytes (4-1472)

Start

Stop

Result:

Configure the parameters and start the test. The results will be displayed in the **Result** section.

Destination IP/ Domain	Enter the IP address of the destination node for Ping test. The device will send Ping packets to test the network connectivity and reachability of the host.
Packet Count	Enter the number of packets to be sent during the testing. It can be 1 to 50.
Ping Timeout	Enter a time value to wait for a response. If the device doesn't receive any response during the timeout time, the connection will be considered to be failed. It can be 100-2000 milliseconds.
Packet Size	Enter the number of data bytes to be sent. It can be 4-1472 bytes and the default is 64.

7.7.2 Run a Traceroute Test

The traceroute test function is used to tracks the route packets taken from source on their way to a given target host. When malfunctions occur in the network, troubleshoot with traceroute utility.

To run a traceroute test, go to the **System > Diagnostic** page and choose the Traceroute tool.

Diagnostic

Diagnostic Tool:

Traceroute

Destination IP/Domain:

0.0.0.0

Traceroute Max TTL:

(1-30)

Start

Stop

Result:

Configure the parameters and start the test. The results will be displayed in the **Result** section.

Destination IP/ Domain	Enter the IP address of the destination node for Traceroute test. The device will send Traceroute packets to test the network connectivity and reachability of the host.
Traceroute Max TTL	Specify the traceroute max TTL (Time To Live) during the traceroute process. It is the maximum number of the route hops the test packets can pass through.

7.7.3 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.

To download the device info, go to the **System > Diagnostic** page.

Download Device Info

Download

Note:

If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem.