

User Guide

Access Point

CONTENTS

About This User Guide.....	1
Overview	3
1 Quick Start.....	4
1.1 Determine the Management Method.....	5
1.2 Connect Network Devices.....	6
1.3 Log in to the EAP and Change the SSID.....	8
1.4 Configure and Manage the EAP	23
2 Configure the Network.....	24
2.1 Configure the Wireless Parameters.....	25
2.1.1 Configure SSIDs	26
2.1.2 Configure Wireless Advanced Settings	33
Radio Setting.....	33
Load Balance.....	35
Airtime Fairness	35
More Settings	36
2.1.3 Configure the MLO Network (Only for Wi-Fi 7 Devices).....	38
2.2 Configure Portal Authentication	40
Configure Portal.....	41
Configure Free Authentication Policy	47
2.3 Configure VLAN.....	50
2.4 Configure MAC Filtering	51
2.5 Configure Scheduler.....	54
2.6 Configure Band Steering.....	57
2.7 Configure QoS.....	58
2.8 Configure Rogue AP Detection.....	62
Detect Rogue APs and Move the Rogue APs to the Trusted AP List.....	63

Manage the Trusted AP List.....	64
2.9 Configure Smart Antenna (Only for Certain Devices).....	66
3 Monitor the Network	67
3.1 Monitor the EAP	68
3.2 Monitor the Wireless Parameters.....	70
Monitor the SSIDs.....	71
Monitor the Radio Settings.....	72
Monitor Radio Traffic	72
Monitor LAN Traffic	73
3.3 Monitor the Clients	75
View Client Information.....	75
View Block Client Information	77
4 Manage the EAP	78
4.1 Manage Bridge APs (Only for a Bridge Main AP).....	79
4.2 Manage the IP Address of the EAP	80
4.3 Manage System Logs	83
View System Logs	83
Configure the Way of Receiving Logs.....	84
4.4 Configure Web Server.....	86
4.5 Configure Management Access	87
Configure Access MAC Management.....	87
Configure Management VLAN	88
4.6 Configure Trunk (Only for Certain Devices).....	89
4.7 Configure LED	90
4.8 Configure Wi-Fi Control (Only for Certain Devices).....	91
4.9 Configure PoE Out (Only for Certain Devices)	92
4.10 Configure SSH.....	93
4.11 Configure SNMP	94
4.12 Configure Power Saving (Only for Certain Devices)	96

5	Configure the System.....	97
5.1	Configure the User Account	98
5.2	Controller Settings	99
	Enable Cloud-Based Controller Management	99
	Configure Controller Inform URL	101
5.3	Configure the System Time.....	102
	Configure the System Time	103
	Configure Daylight Saving Time	105
5.4	Reboot and Reset the EAP.....	107
5.5	Backup and Restore the Configuration.....	108
5.6	Update the Firmware	109
6	Application Example	110
6.1	Determine the Network Requirements	111
6.2	Build the Network Topology.....	112
6.3	Log in to the EAP	113
6.4	Configure the EAP	114
	Configure SSIDs	114
	Configure Portal Authentication.....	115
	Configure Scheduler	117
6.5	Test the Network.....	119

About This User 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.tp-link.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.

MU-MIMO Disclaimer (for EAPs that support MU-MIMO)

MU-MIMO capability requires client devices that also support MU-MIMO.

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.

Lightning and Electro-Static Discharge Protection Disclaimer (for Outdoor EAPs)

Protection against lightning and electro-static discharge may be achieved through proper product setup, grounding and cable shielding. Refer to the instruction manual and consult an IT professional to assist with setting up this product.

More Info

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

For technical support, latest software, and management app, visit <https://www.tp-link.com/support>.

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.tp-link.com>.

To ask questions, find answers, and communicate with TP-Link users or engineers, please visit <https://community.tp-link.com> to join TP-Link Community.

Overview

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

1

Quick Start

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

1.1 Determine the Management Method

1.2 Connect Network Devices

1.3 Log in to the EAP and Change the SSID

1.4 Configure and Manage the EAP

1.1 Determine the Management Method

Before building your network, choose a proper method to manage your EAPs. You have the following two 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 Omada SDN Controller. For detailed instructions, go to the [Support Page of Omada Controller](#) and download the User Guide.

■ 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.

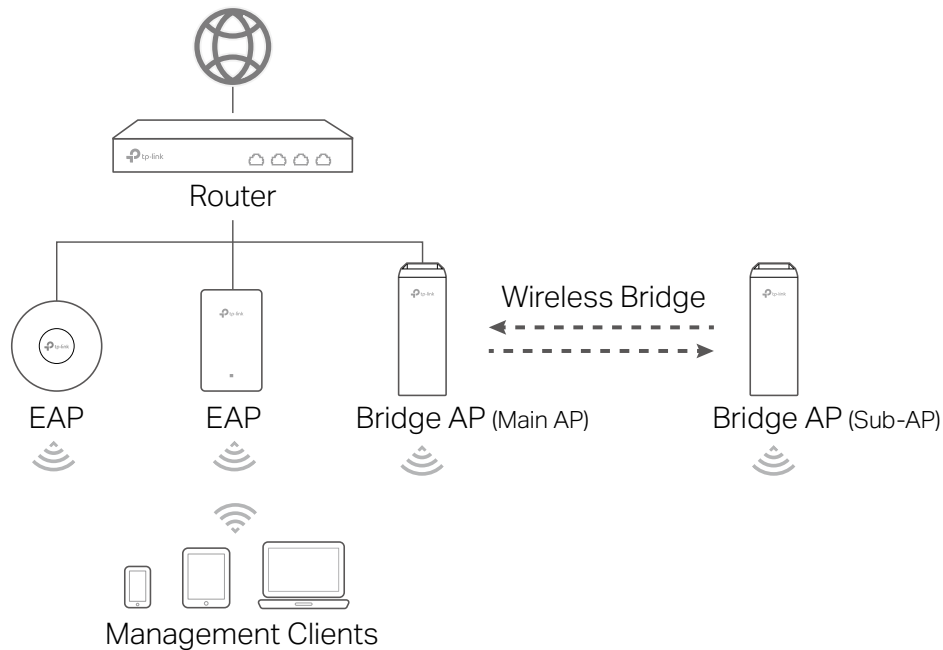
This chapter introduces how to start configuring the EAP in Standalone Mode.

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 [5.2 Controller Settings](#) in certain scenarios.

1.2 Connect Network Devices

To connect your EAPs to the local network, refer to the following topology.



1. Connect your router to the internet.
2. Connect your EAPs to the LAN ports of your router.

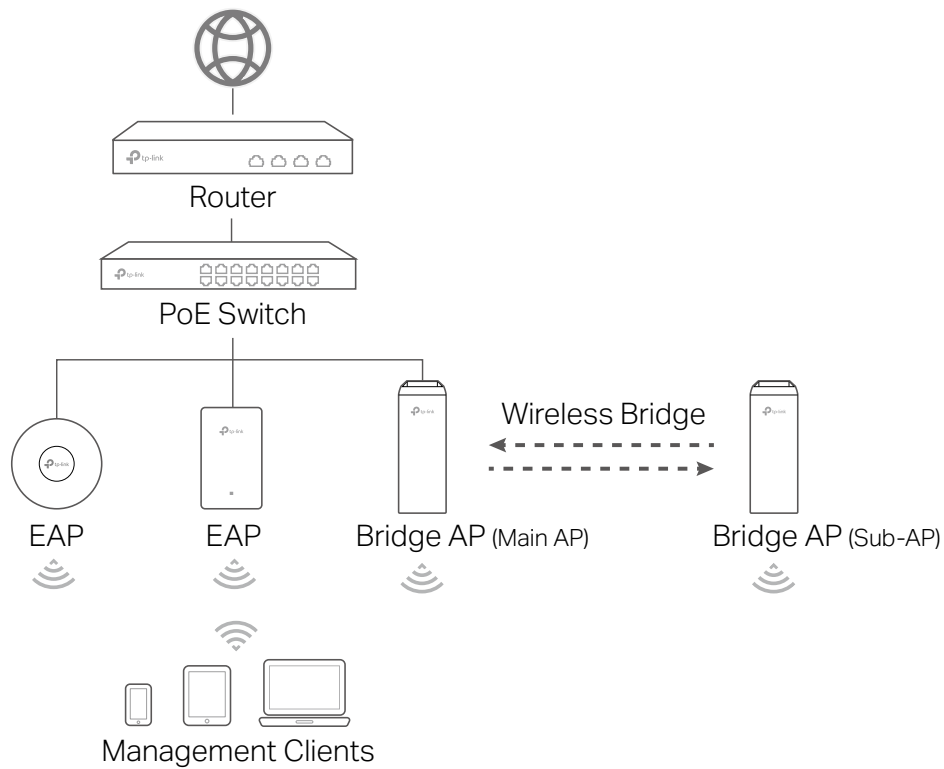
For a Bridge kit product, connect one EAP to your router. This EAP will work as the **Main AP**. The other EAP(s) in the kit will automatically connect to the Main AP via wireless bridge and work as the **Sub-AP(s)**.

3. Connect your wireless clients such as phones, tablets and laptops to the WiFi of an EAP. The default SSIDs are printed on the EAP.

Now you can surf the internet on your phones, tablets and laptops. If you cannot access the internet, follow the [FAQ](#) to troubleshoot the problem.

Tips:

- If you want to power your EAPs using a PoE switch, refer to the following topology.



- The router is the gateway of the network, and devices in the LAN surf the internet via the router. At the same time, the router acts as a DHCP server to assign dynamic IP addresses to the EAPs and clients.

1.3 Log in to the EAP and Change the SSID

By default, anyone can connect to the WiFi of EAP without authentication, because the default SSID has no password. For security purposes, we recommend changing the default SSID.

Log in to the EAP before changing the default SSID. You can use either Omada App on your mobile device or the web browser on your PC. Choose a method from the following sections and follow the instructions.

Tips:

- Only one user is allowed to log in to the EAP at one time.
- Omada app is designed to help you quickly configure some basic settings. To configure advanced functions, use the web browser on your PC.
- Omada app is only compatible with certain firmware versions of the EAP. To check the firmware versions of the supported EAPs, please refer to https://www.tp-link.com/omada_compatibility_list.

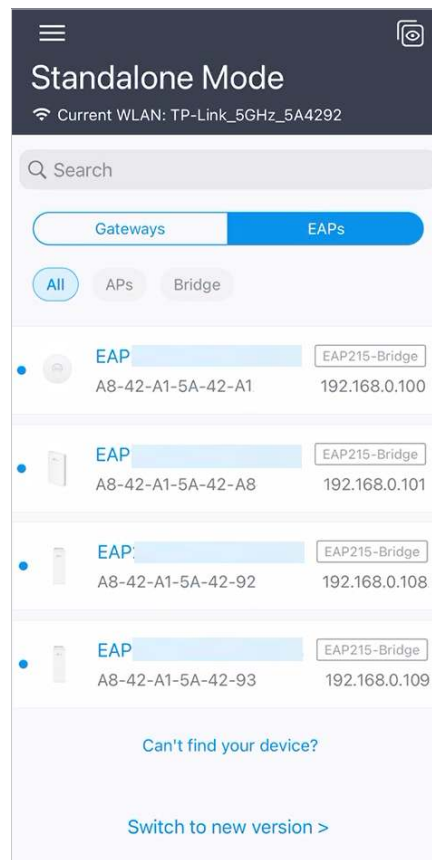
■ Using Omada App on Your Mobile Device

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

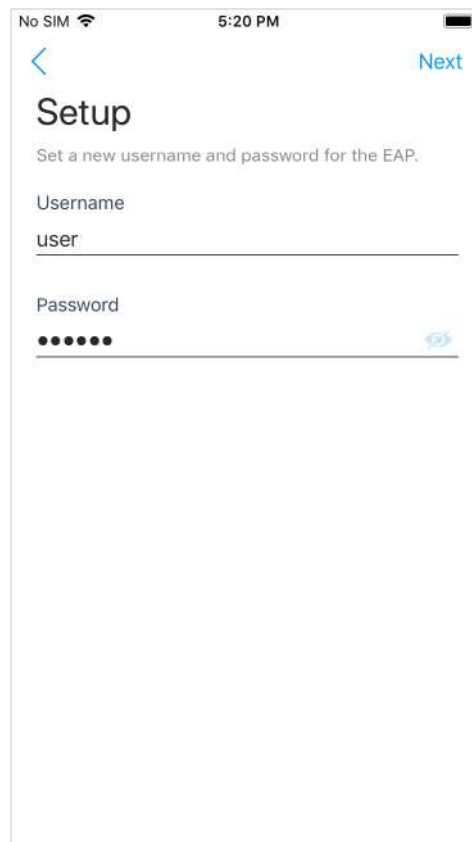


2. Connect your mobile device to the WiFi of an EAP. The default SSIDs are printed on the EAP.

3. Launch the Omada app and go to **Standalone Devices > EAPs**. 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 configure it. Set a new username and password for your login account of the EAP.



No SIM 5:20 PM

< Next

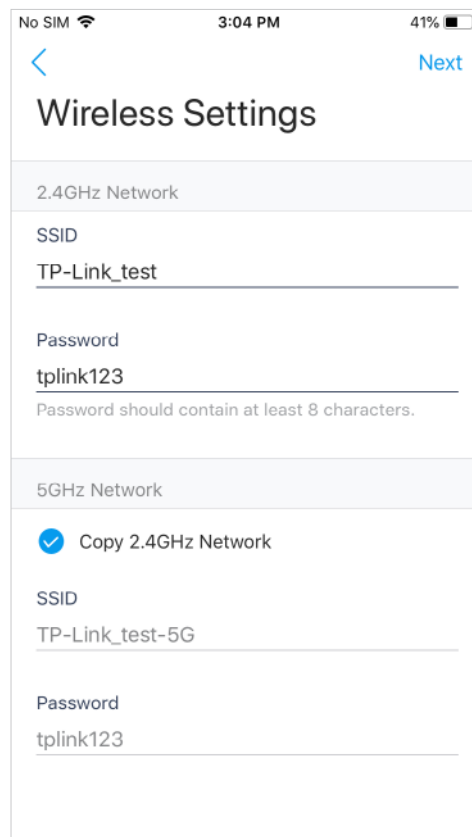
Setup

Set a new username and password for the EAP.

Username
user

Password
•••••

5. Change the SSID and password to keep your wireless network secure. Tap **Next**.



No SIM 3:04 PM 41%

< Next

Wireless Settings

2.4GHz Network

SSID
TP-Link_test

Password
tplink123
Password should contain at least 8 characters.

5GHz Network

☒ Copy 2.4GHz Network

SSID
TP-Link_test-5G

Password
tplink123

6. Confirm the settings in the summary page. Tap Next, and the settings will take effect in several minutes.

No SIM 3:04 PM 41%

< Next

Summary

Device Account

Username
admin

Password
tplink123

2.4GHz Network

SSID
TP-Link_test

Password
tplink123

5GHz Network

SSID
TP-Link_test-5G

Password
tplink123

7. To join your new wireless network, select the SSID and tap **Join**.

No SIM 3:05 PM 41%

Now join your new wireless network.

2.4GHz Network

SSID
TP-Link_test Join

Password
tplink123

5GHz Network

SSID
TP-Link_test-5G Join

Password
tplink123

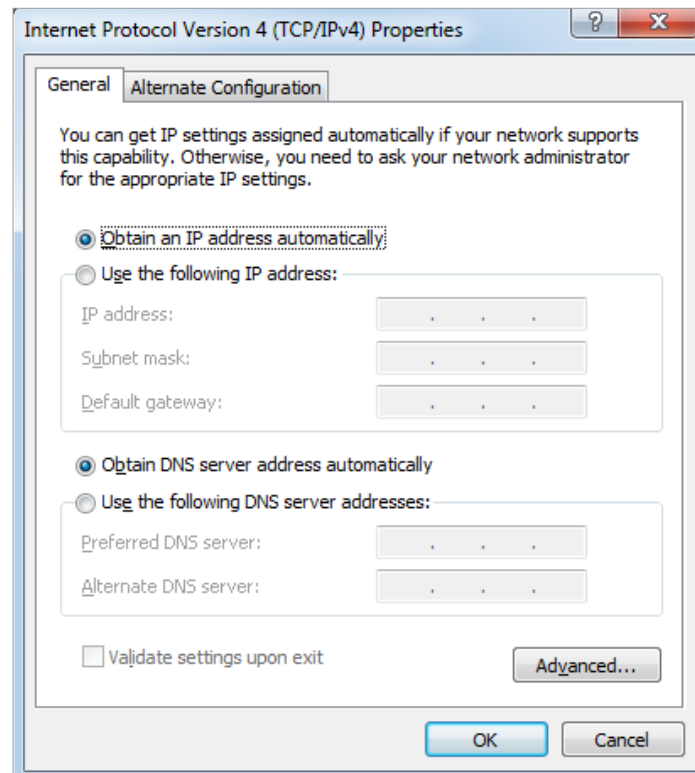
8. Tap **Continue** to go to the management page. In this page, you can view the information and settings of the EAP. If you want to change the settings including radio, SSID and device account, tap .



Now you can connect your phones, tablets and laptops to the new WiFi. If you cannot access the internet, follow the [FAQ](#) to troubleshoot the problem.

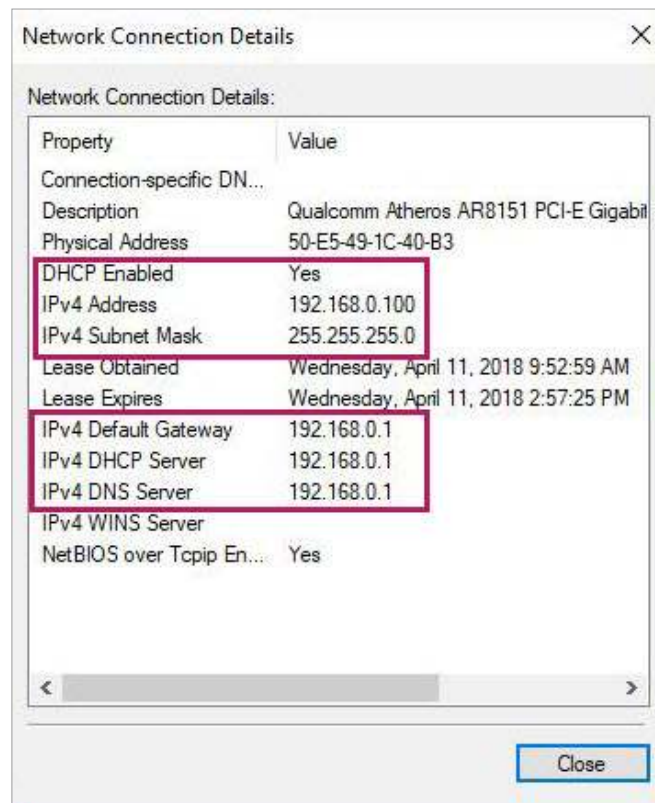
■ Using Web Browser on Your PC and Connecting to the WiFi

1. Set your PC to obtain an IP address automatically.

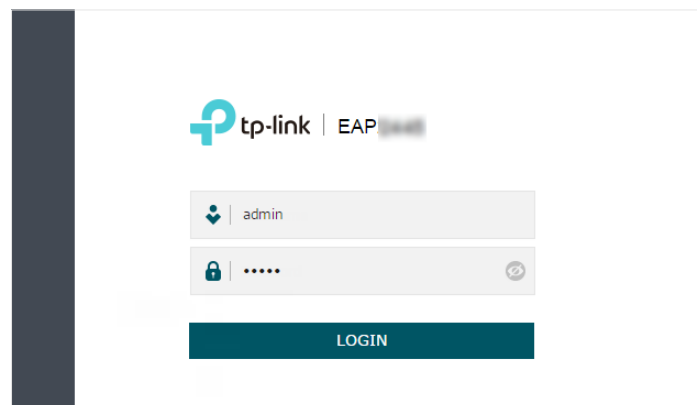


2. Connect your PC to the WiFi of an EAP. The default SSIDs are printed on the EAP.

3. Make sure that your PC has got the IP address, default gateway, and DNS server from the DHCP server.

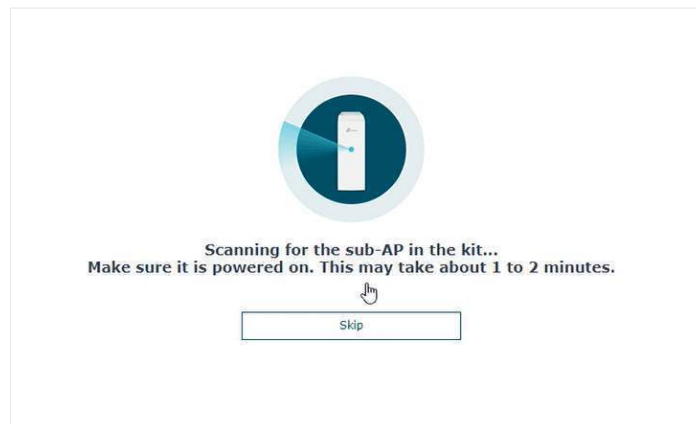


4. To log in to the EAP, launch a web browser and enter **http://tplinkeap.net** in the address bar. The login page will appear. By default, both the username and password are **admin**.

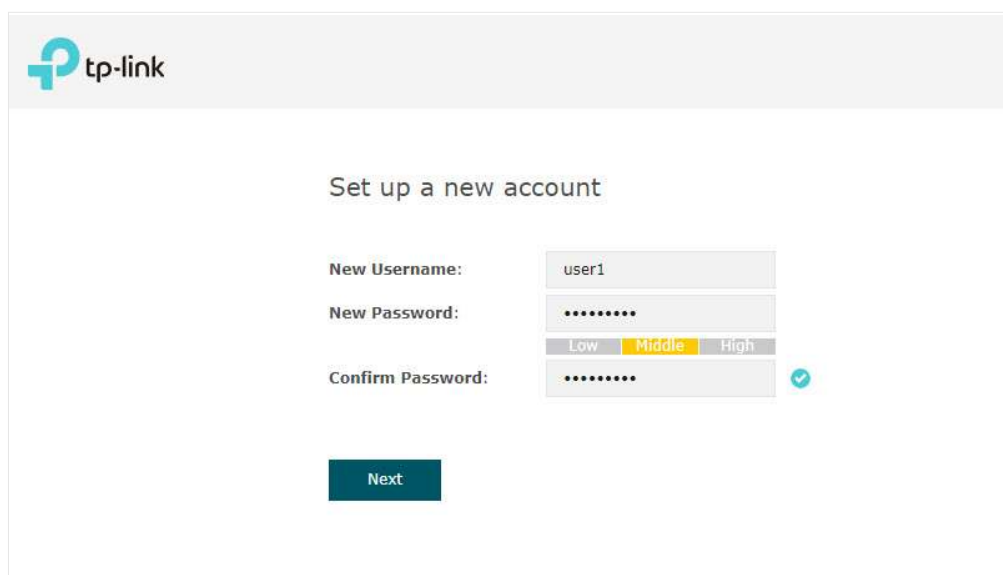


5. After logging in to the EAP, follow the step-by-step instructions to complete the basic configurations.

If you connect to the Main AP (the one connected to your router) of a Bridge kit product, the system will automatically scan for the Sub-AP(s) in the kit and connect it/them to the network.



6. In the pop-up window, configure a new username and a new password for your user account, then click **Next**.

A screenshot of the TP-Link web interface for setting up a new account. The header shows the TP-Link logo. The main heading is "Set up a new account". Below this, there are three input fields: "New Username:" with the value "user1", "New Password:" with a masked password ".....", and "Confirm Password:" with a masked password ".....". A strength indicator bar is shown below the password fields, with "Low" in grey, "Middle" in yellow, and "High" in grey. A green checkmark is visible next to the "Confirm Password:" field. At the bottom, there is a dark blue "Next" button.

7. Configure the SSID and password. Click **Save**.



Wireless Basic Settings

2.4GHz Wireless Radio: ☒ Enable

SSID:

Password:

5GHz Wireless Radio: ☒ Enable

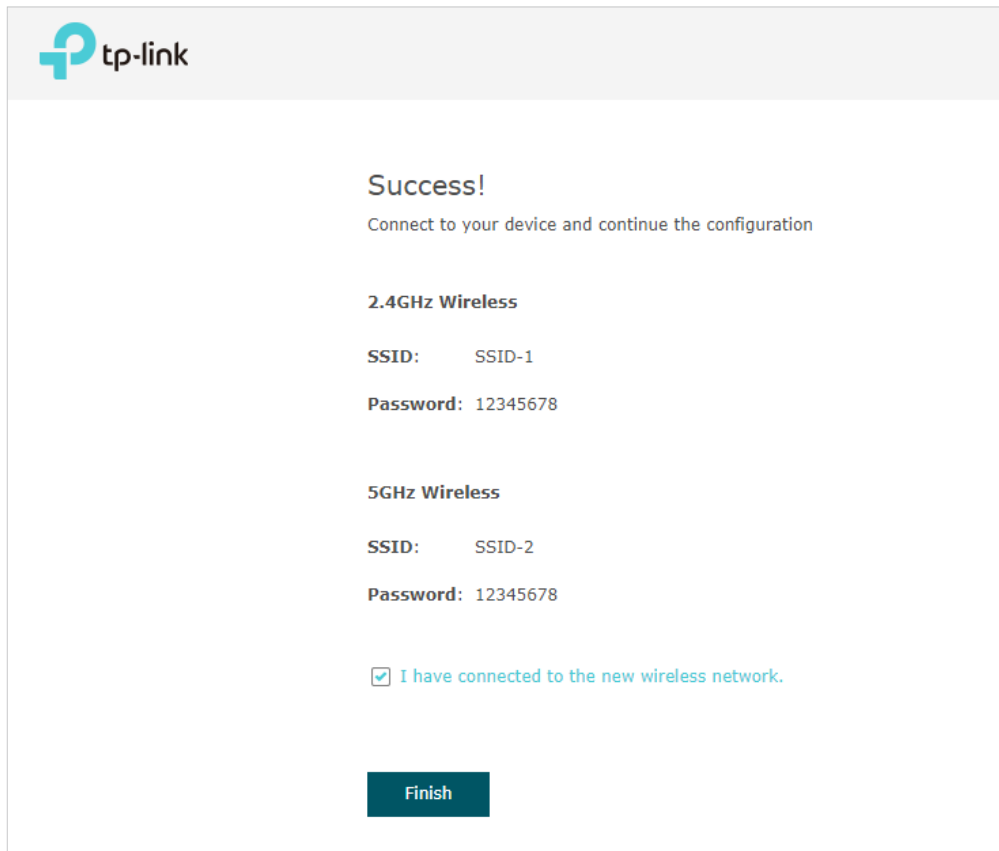
SSID:

Password:

Tips:

You can skip this step and configure wireless settings later on the management page. If needed, you can also create more SSIDs. For detailed instructions, refer to [2.1 Configure the Wireless Parameters](#).

8. The following page will appear. Make sure that your device has connected to the new wireless network and tick the check box. Then click **Finish**.

The image shows a screenshot of a TP-Link router's web interface. At the top left is the TP-Link logo. The main heading is "Success!" followed by the instruction "Connect to your device and continue the configuration". Below this, there are two sections for wireless settings. The first section is "2.4GHz Wireless" with "SSID: SSID-1" and "Password: 12345678". The second section is "5GHz Wireless" with "SSID: SSID-2" and "Password: 12345678". At the bottom, there is a checkbox that is checked, with the text "I have connected to the new wireless network." next to it. Below the checkbox is a dark blue button labeled "Finish".

Success!
Connect to your device and continue the configuration

2.4GHz Wireless
SSID: SSID-1
Password: 12345678

5GHz Wireless
SSID: SSID-2
Password: 12345678

☒ I have connected to the new wireless network.

Finish

Now you can connect your phones, tablets and laptops to the new WiFi. If you cannot access the internet, follow the [FAQ](#) to troubleshoot the problem.

■ Using Web Browser on Your PC and Connecting to the Ethernet

1. Get the IP address of the EAP. There are two methods.

- Using DHCP Client List of the Router

Log in to the router which acts as the DHCP server. In the DHCP client list, find the IP address of your EAP according to its MAC address. The MAC address can be found at

the bottom of the EAP. In the following figure, for example, the IP address of the EAP is **192.168.0.118**.

The screenshot shows the TP-Link Advanced Settings page. The left sidebar contains navigation options: Status, Network (selected), Operation Mode, Wireless, Guest Network, USB Settings, Parental Controls, QoS, and Security. The main content area is titled 'Settings' and includes a 'DHCP Server' section with the following configuration:

- DHCP Server: ☒ Enable DHCP Server
- IP Address Pool: 192.168.0.100 - 192.168.0.199
- Address Lease Time: 120 minutes. (2-2880. The default value is 120.)
- Default Gateway: 192.168.0.1 (Optional)
- Primary DNS: 192.168.0.1 (Optional)
- Secondary DNS: 192.168.0.1 (Optional)

A 'Save' button is located at the bottom right of the DHCP Server section. Below this is the 'Address Reservation' section, which is currently empty. At the bottom is the 'DHCP Client List' section, showing a total of 1 client. The client list table is as follows:

ID	Client Name	MAC Address	Assigned IP Address	Lease Time
1	EAP [redacted]	B0-4E-26-B4-A7-42	192.168.0.118	01:59:30

Tips:

When the DHCP server is not available in your network, the EAP has the DHCP fallback IP address, which is **192.168.0.254** by default.

- Using EAP Discovery Utility

Go to https://www.tp-link.com/download/EAP-Controller.html#EAP_Discovery_Tool to download, install and launch EAP Discovery Utility on your PC. EAP Discovery Utility can

scan all EAPs in the same network segment, and find the IP address of the EAP. In the following figure, for example, the IP address of the EAP is **192.168.0.5**.

Select	MAC Address	IP Address	Model	Version	Status	Action
☒	50:c7:bf:17:a6:e2	192.168.0.5	EAP-650	1.0.1 Build 20170414 R...	Pending	<button>Manage</button>

Displayed EAP : 1

Select All
Batch Setting

Tips:

Some EAP models only works with certain software version of Discovery Utility. If your Discovery Utility can't discover your EAP anyway, try a different software version.

2. To log in to the EAP, launch a web browser and enter the IP address of the EAP in the address bar. The login page will appear. By default, both the username and password are **admin**.

A screenshot of the TP-Link EAP login page. The page has a dark blue header with the TP-Link logo and the text "tp-link | EAP". Below the header, there are two input fields. The first field contains the username "admin" and has a user icon on the left. The second field contains masked characters "*****" and has a lock icon on the left and a circular refresh icon on the right. At the bottom of the page, there is a large blue button labeled "LOGIN".

Tips:

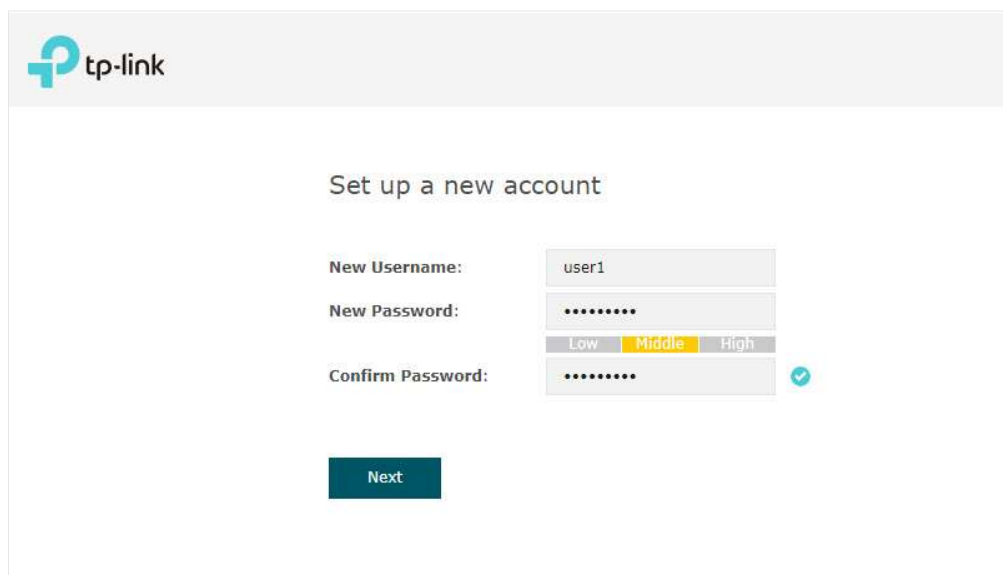
To facilitate access to the EAP, you can set a static IP address for the EAP and remember it well or write it down. But make sure that this IP address is not being used by other devices in the same LAN. For detailed instructions about how to set a static IP address for the EAP, refer to [4.2 Manage the IP Address of the EAP](#).

3. After logging in to the EAP, follow the step-by-step instructions to complete the basic configurations.

If you connect to the Main AP (the one connected to your router) of a Bridge kit product, the system will automatically scan for the Sub-AP(s) in the kit and connect it/them to the network.



4. In the pop-up window, configure a new username and a new password for your user account, then click **Next**.

A screenshot of the TP-Link web interface for setting up a new account. The header shows the TP-Link logo. The main heading is "Set up a new account". Below this, there are three input fields: "New Username:" with the value "user1", "New Password:" with a masked password "....." and a strength indicator showing "Low", "Middle" (highlighted in yellow), and "High", and "Confirm Password:" with a masked password "....." and a green checkmark icon. A "Next" button is at the bottom.

5. Configure the SSID and password. Click **Save**.



Wireless Basic Settings

2.4GHz Wireless Radio: ☒ Enable

SSID:

Password:

5GHz Wireless Radio: ☒ Enable

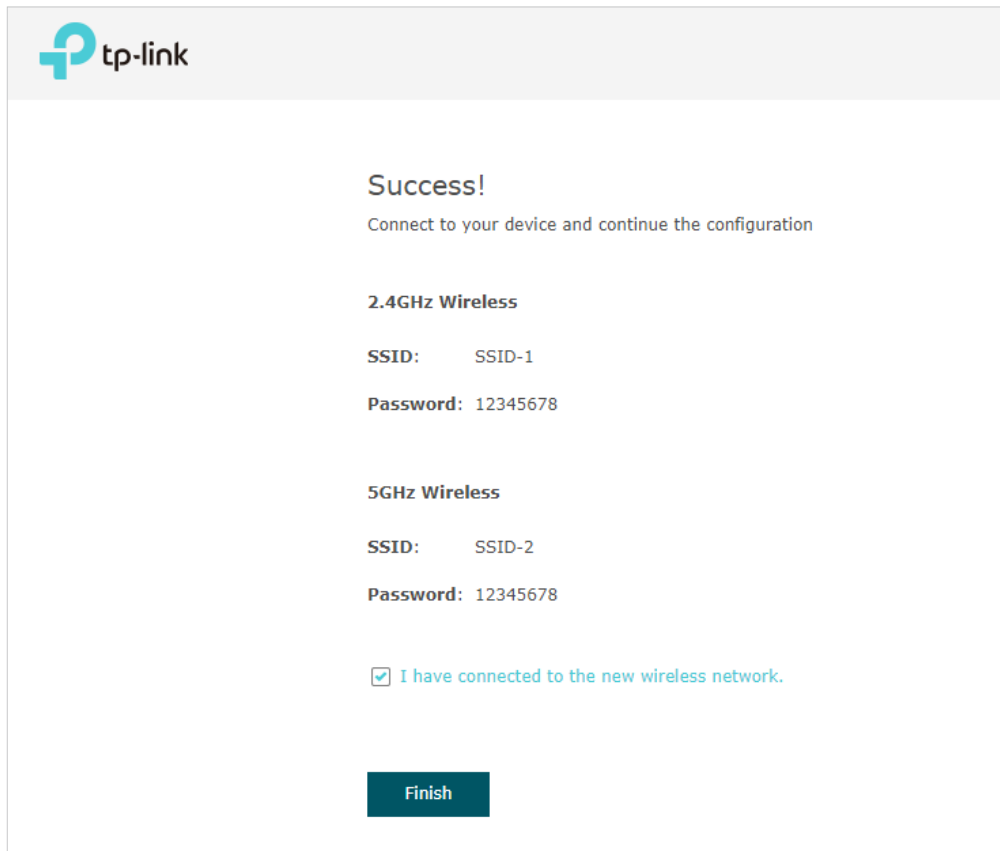
SSID:

Password:

Tips:

You can skip this step and configure wireless settings later on the management page. If needed, you can also create more SSIDs. For detailed instructions, refer to [2.1 Configure the Wireless Parameters](#).

6. The following page will appear. Make sure that your device has connected to the new wireless network and tick the check box. Then click **Finish**.

The image shows a TP-Link web interface for a successful configuration. At the top left is the TP-Link logo. The main heading is "Success!" followed by the instruction "Connect to your device and continue the configuration". Below this, there are two sections for wireless settings. The first section is "2.4GHz Wireless" with "SSID: SSID-1" and "Password: 12345678". The second section is "5GHz Wireless" with "SSID: SSID-2" and "Password: 12345678". At the bottom, there is a checked checkbox with the text "I have connected to the new wireless network." and a dark teal "Finish" button.



Success!
Connect to your device and continue the configuration

2.4GHz Wireless

SSID: SSID-1

Password: 12345678

5GHz Wireless

SSID: SSID-2

Password: 12345678

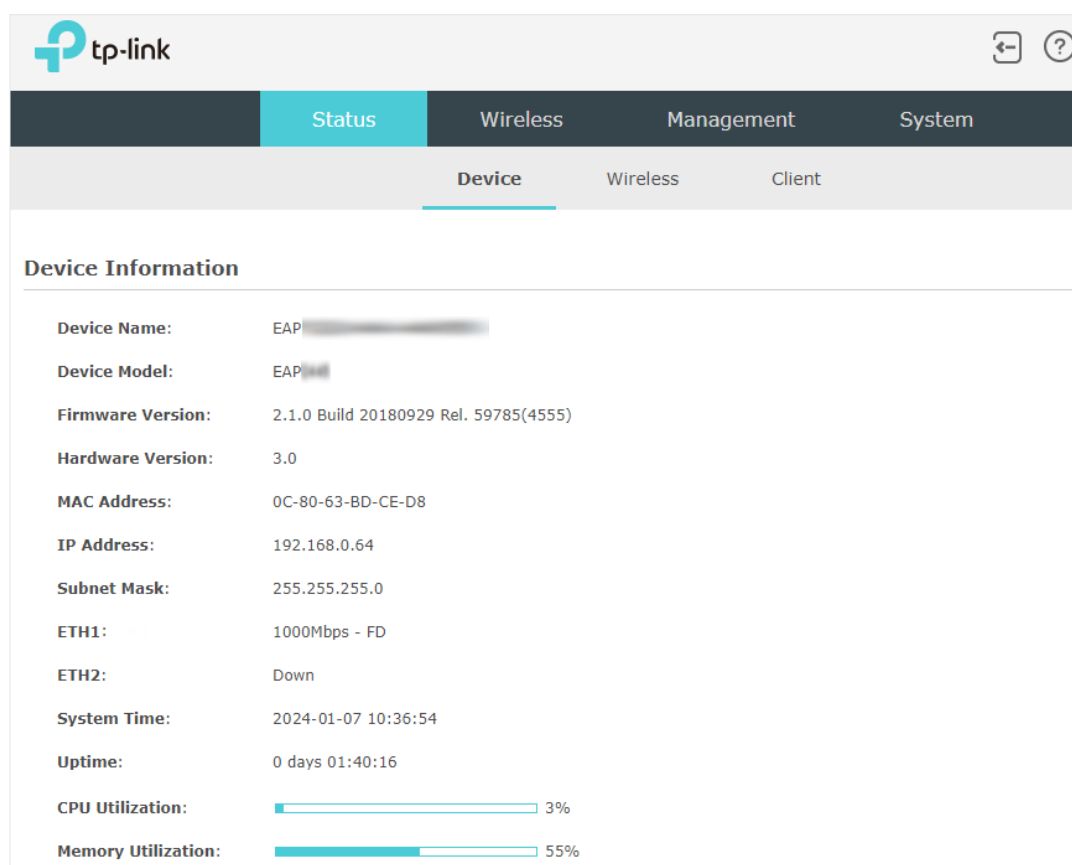
☒ I have connected to the new wireless network.

Finish

Now you can connect your phones, tablets and laptops to the new WiFi. If you cannot access the internet, follow the [FAQ](#) to troubleshoot the problem.

1.4 Configure and Manage the EAP

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.



On the top of the page, you can click  to log out and click  to open the technical support website.

There are four tabs: **Status**, **Wireless**, **Management** and **System**. 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 the wireless parameters and advanced features, such as Portal, VLAN, MAC Filtering, Scheduler, Band Steering, QoS and Rogue AP Detection.
Management	You can manage the EAP using the management features, such as System Logs, Web Server, Management Access, LED Control, SSH and SNMP.
System	You can configure the system parameters, including the login account and the system time. In addition, you can reboot and reset the EAP, backup and restore the configuration, and upgrade the EAP using the new firmware file.

2 *Configure the Network*

This chapter introduces how to configure the network parameters and the advanced features of the EAP, including:

- *2.1 Configure the Wireless Parameters*
- *2.2 Configure Portal Authentication*
- *2.3 Configure VLAN*
- *2.4 Configure MAC Filtering*
- *2.5 Configure Scheduler*
- *2.6 Configure Band Steering*
- *2.7 Configure QoS*
- *2.8 Configure Rogue AP Detection*
- *2.9 Configure Smart Antenna (Only for Certain Devices)*

2.1 Configure the Wireless Parameters

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

tp-link

←

?

Status

Wireless

Management

System

Wireless Settings

Portal

VLAN

MAC Filtering

Scheduler

Band Steering

QoS

Rogue AP Detection

2.4GHz

5GHz

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	SSID-1	0	Enable	WPA-PSK	Disable	

2.4GHz Wireless Advanced Settings

Radio Settings | Load Balance | Airtime Fairness | More Settings

Wireless Mode:

802.11b/g/n mixed

Channel Width:

20/40MHz

Channel:

Auto

Tx Power(EIRP):

20

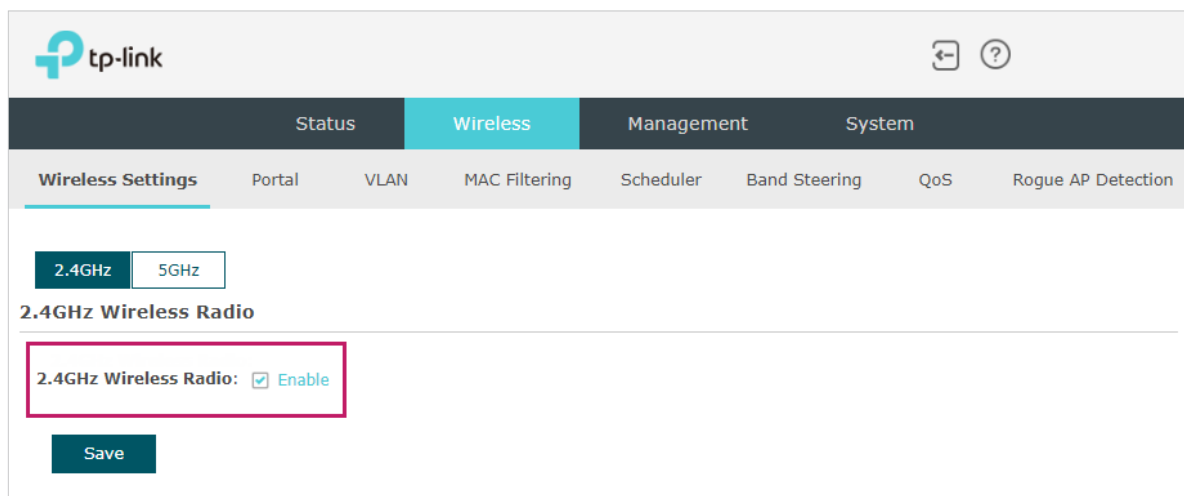
dBm(9-20)

Note:

The EIRP transmit power includes the antenna gain.

Save

For a multi-band EAP, you can click each band to enable Wireless Radio and configure wireless parameters.

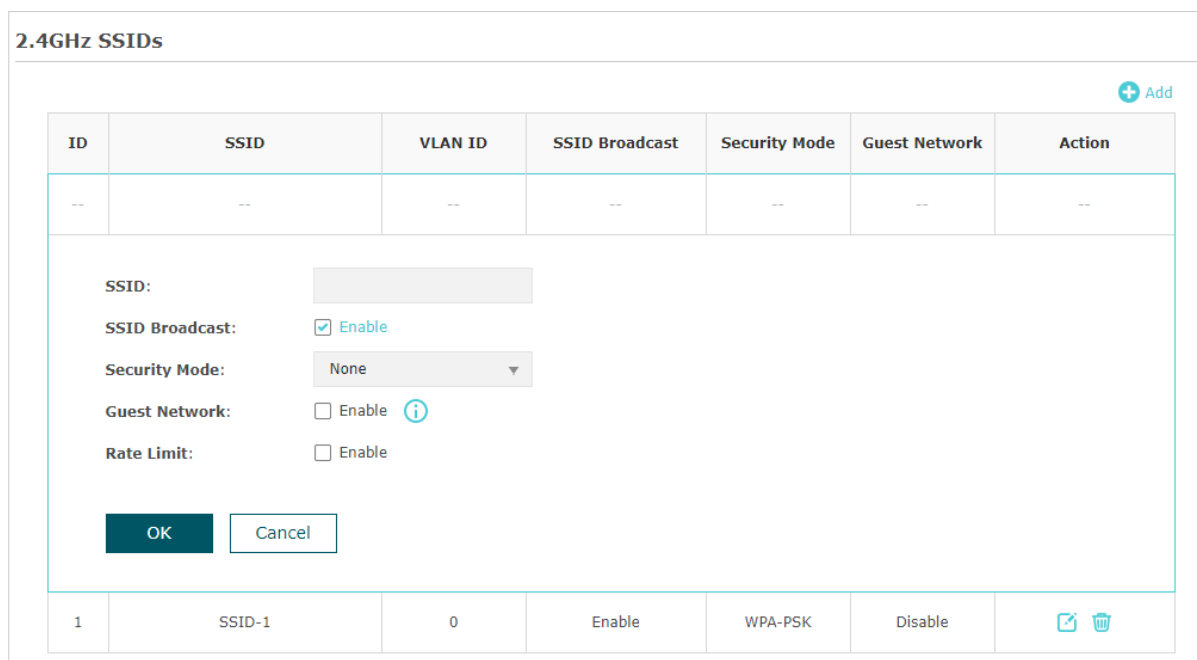


The screenshot shows the TP-Link web interface. At the top, there's a navigation bar with 'Status', 'Wireless' (highlighted), 'Management', and 'System'. Below this is a sub-menu bar with 'Wireless Settings' (highlighted), 'Portal', 'VLAN', 'MAC Filtering', 'Scheduler', 'Band Steering', 'QoS', and 'Rogue AP Detection'. In the 'Wireless Settings' section, there are two tabs: '2.4GHz' and '5GHz'. Under the '2.4GHz Wireless Radio' section, there is a checkbox labeled '2.4GHz Wireless Radio:' which is checked and has the word 'Enable' next to it. Below this is a 'Save' button.

Demonstrated with 2.4GHz, the following sections introduce these contents: [2.1.1 Configure SSIDs](#) and [2.1.2 Configure Wireless Advanced Settings](#).

2.1.1 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. For one EAP, you can build up to eight SSIDs per frequency band.



The screenshot shows the '2.4GHz SSIDs' configuration page. At the top right, there is an 'Add' button. Below it is a table with the following columns: ID, SSID, VLAN ID, SSID Broadcast, Security Mode, Guest Network, and Action. The table has one row with dashes in all cells. A modal form is open for creating a new SSID. The form contains the following fields: 'SSID:' with a text input field; 'SSID Broadcast:' with a checked checkbox and the word 'Enable'; 'Security Mode:' with a dropdown menu showing 'None'; 'Guest Network:' with an unchecked checkbox and an information icon; 'Rate Limit:' with an unchecked checkbox and the word 'Enable'. At the bottom of the modal are 'OK' and 'Cancel' buttons. Below the modal, the table has one row with the following values: ID: 1, SSID: SSID-1, VLAN ID: 0, SSID Broadcast: Enable, Security Mode: WPA-PSK, Guest Network: Disable, and Action: Edit/Delete icons.

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

1. If your EAP is a dual-band device, click [2.4GHz](#) [5GHz](#) to choose a frequency band on which the new SSID will be created.

2. Click  **Add** to add a new SSID on the chosen band.

Tips:

You can also click  to edit the specific SSID which already exists in the list. And you can click  to delete the SSID in the list.

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	Select the security mode of the wireless network. There are four options: None: Clients can access the wireless network without authentication. WEP / WPA-Enterprise / WAP-Personal: Clients need to pass the authentication before accessing the wireless network. For 6GHz: Enhanced Open: Enhanced Open is a Wi-Fi Alliance certification that preserves the convenience open networks offer while reducing some of the risks associated with accessing an unsecured network. WPA3-Enterprise / WAP3-Personal: Clients need to pass the authentication before accessing the wireless network. For network security, we recommend that you encrypt your wireless network. The following sections will introduce how to configure these security modes.
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. Click **OK** to create the SSID.

Following is the detailed instructions about how to configure [WEP](#), [WPA-Enterprise](#), [WPA-Personal](#), [WPA3-Enterprise](#), and [WAP3-Personal](#)

- **WEP (for certain models)**

WEP (Wired Equivalent Privacy) is a traditional encryption method. It has been proved that WEP has security flaws and can easily be cracked, so WEP cannot provide effective protection for wireless networks. Since WPA-Personal and WPA-Enterprise are much safer than WEP, we recommend that you choose WPA-Personal or WPA-Enterprise if your clients also support them.

Note:

WEP is not supported in 802.11n mode or 802.11ac mode. If WEP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network. If WEP is applied in 802.11b/g/n mode (2.4GHz) or 802.11a/n (5GHz), the EAP may work at a low transmission rate.

The screenshot shows a configuration interface for WEP. It includes the following fields and options:

- Security Mode:** A dropdown menu set to "WEP".
- Type:** Three radio buttons: "Auto" (selected), "Open System", and "Shared Key".
- Key Selected:** A dropdown menu set to "Key1".
- Wep Key Format:** Two radio buttons: "ASCII" (selected) and "Hexadecimal".
- Key Type:** Three radio buttons: "64-bit" (selected), "128-bit", and "152-bit".
- Key Value:** A text input field containing the value "weppw".

The following table detailedly introduces how to configure each item:

Type	Select the authentication type for WEP. Auto: The EAP can select Open System or Shared Key automatically based on the wireless capability and request of the clients. Open System: Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission. Shared Key: Clients have to input the correct password to pass the authentication, otherwise the clients cannot associate with the wireless network or transmit data.
Key Selected	Select one key to specify. You can configure four keys at most.
WEP Key Format	Select ASCII or Hexadecimal as the WEP key format. ASCII: With this format selected, the WEP key can be any combination of keyboard characters of the specified length. Hexadecimal: With this format selected, the WEP key can be any combination of hexadecimal digits (0-9, a-f, A-F) with the specified length.

Key Type	Select the WEP key length for encryption. 64Bit: Enter 10 hexadecimal digits or 5 ASCII characters. 128Bit: Enter 26 hexadecimal digits or 13 ASCII characters. 152Bit: Enter 32 hexadecimal digits or 16 ASCII characters.
Key Value	Enter the WEP keys. The length and valid characters are determined by the key format and key type.

- **WPA-Enterprise (for certain models)**

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.

Security Mode:	WPA-Enterprise ▼	
Version:	WPA/WPA2 - Enterpris ▼	
Encryption:	☒ Auto ☐ TKIP ☐ AES	
RADIUS Server IP:	0.0.0.0	
RADIUS Port:	0	(1-65535, 0 means the default port, which is 1812.)
RADIUS Password:		
RADIUS Accounting:	☒ Enable	
Accounting Server IP:	0.0.0.0	
Accounting Server Port:	0	(1-65535, 0 means the default port, which is 1813.)
Accounting Server Password:		
Interim Update:	☐ Enable	
Group Key Update Period:	0	seconds (30-8640000, 0 means no update.)
Guest Network:	☐ Enable 	
Rate Limit:	☐ Enable	
OK Cancel		

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	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 TKIP or AES automatically based on the client device's request. TKIP: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. AES: Advanced Encryption Standard. It is securer than TKIP.
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 (for certain models)**

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 screenshot shows a configuration window for WPA-Personal. It includes fields for Security Mode (WPA-Personal), Version (WPA/WPA2-PSK), Encryption (Auto, TKIP, AES), Wireless Password (12345678), Group Key Update Period (0 seconds), Guest Network (disabled), and Rate Limit (disabled). There are OK and Cancel buttons at the bottom.

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 TKIP or AES automatically based on the client device's request. TKIP: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. AES: Advanced Encryption Standard. It is securer than TKIP.
Wireless Password	Configure the wireless password with ASCII characters. • 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.

- **WPA3-Enterprise (for certain models)**

WPA3-Enterprise is a safer encryption method compared with WPA3-Personal. It requires a RADIUS server to authenticate the clients via 802.1X and AP (Extensible Authentication

Protocol). WPA3-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.

Security Mode:	WPA3-Enterprise ▼	
Encryption:	☒ AES-GCM 256 ☐ AES-CCMP	
RADIUS Server IP:	0.0.0.0	
RADIUS Port:	0	(1-65535. 0 means the default port, which is 1812.)
RADIUS Password:		
RADIUS Accounting:	☐ Enable	
Group Key Update Period:	0	seconds (30-8640000. 0 means no update.)

The following table introduces how to configure each item:

Encryption	Select the Encryption type: AES-GCM 256 or AES-CCMP.
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 APs in Interim Update Interval .
Interim Update Interval	With Interim Update enabled, specify the appropriate duration between updates for APs. 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 AP should change the encryption key. 0 means that the encryption key does not change at anytime.

- **WPA3-Personal (for certain models)**

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.

Security Mode:	WPA3-Personal ▼	
Wireless Password:	wpapass1	
Group Key Update Period:	0	seconds (30-8640000. 0 means no update.)

The following table introduces how to configure each item:

Wireless Password	Configure the wireless password with ASCII characters. • 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 AP should change the encryption key. 0 means that the encryption key does not change at anytime.

2.1.2 Configure Wireless Advanced Settings

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

Radio Setting

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.

Note: For Sub-APs, the Wireless Mode, Channel Width, and Channel will follow the settings of their Main AP and cannot be edited.

2.4GHz Wireless Advanced Settings

Radio Settings

Load Balance | Airtime Fairness | More Settings

Wireless Mode:	802.11b/g/n mixed ▼	
Channel Width:	20/40MHz ▼	
Channel:	Auto ▼	
Tx Power(EIRP):	20	dBm(6-20)

Note:
The EIRP transmit power includes the antenna gain.

Save

Select the frequency band and configure the following parameters.

Wireless Mode	Select the IEEE 802.11 mode the radio uses. • 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. • For 6GHz: 802.11ax/be mixed is recommended so that all of 802.11ax and 802.11be clients operating in the 6GHz frequency can connect to the AP. Note that Wi-Fi 6E devices support 802.11ax only.
Channel Width	Select the channel width of the AP. The available options differ among different APs. 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: • 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	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. This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.
Channel	Select the channel used by the EAP. For example, 1/2412MHz means that the channel is 1 and the frequency is 2412MHz. By default, the channel is automatically selected, and we recommend that you keep the default setting.

Tx Power (EIRP)

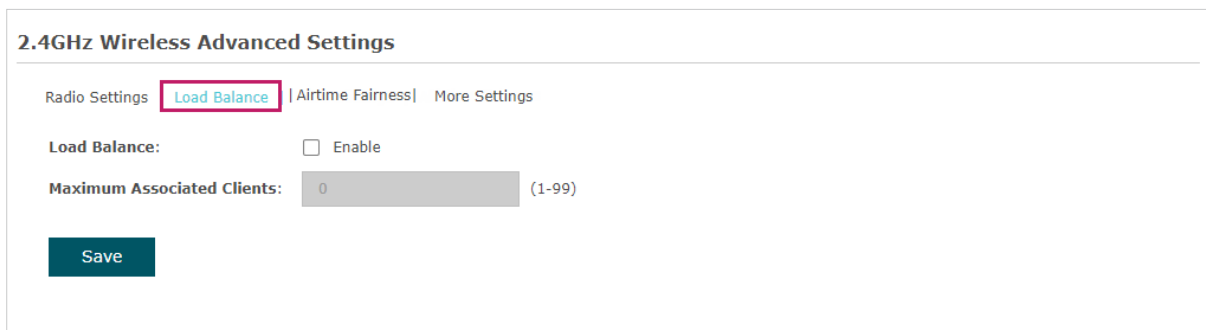
Specify the transmit power value.

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.

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.

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.



The screenshot shows the '2.4GHz Wireless Advanced Settings' page. At the top, there are tabs for 'Radio Settings', 'Load Balance' (which is highlighted with a red box), 'Airtime Fairness', and 'More Settings'. Below the tabs, the 'Load Balance' section is visible. It includes a 'Load Balance:' label followed by an unchecked checkbox and the word 'Enable'. Below that, there is a 'Maximum Associated Clients:' label followed by a text input field containing the number '0' and a range indicator '(1-99)'. At the bottom left of the settings area is a dark blue 'Save' button.

Follow the steps below to configure Load Balance:

1. Click 2.4GHz 5GHz to choose a frequency band on which the load balance feature will take effect.
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

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, 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:

With Airtime Fairness enabled, 50 wireless clients at most can connect to the EAP in 2.4GHz band.

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: ms (40-100)

DTIM Period: (1-255)

RTS Threshold: (1-2347)

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

OFDMA: ☐ Enable

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

The following table introduces how to configure each item:

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	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. 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.
RTS Threshold	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. 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. 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.
Fragmentation Threshold	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. 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.
OFDMA	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. This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.
Non-PSC Channel	Preferred Scanning Channels (PSCs) are channels that are prioritized within the 6 GHz WiFi band for efficient connectivity. Some clients may not discover 6GHz networks using non-PSC channels. This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

2.1.3 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

</

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.

2.2 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.

The image shows the TP-Link Web Management Interface. The top navigation bar includes the TP-Link logo, a home icon, and a help icon. Below this is a main menu with 'Status', 'Wireless' (highlighted in red), 'Management', and 'System'. Under 'Wireless', there is a sub-menu with 'Wireless Settings', 'Portal' (highlighted in red), 'VLAN', 'MAC Filtering', 'Scheduler', 'Band Steering', 'QoS', and 'Rogue AP Detection'.

The 'Portal Configuration' section contains the following fields:

- SSID: - Please Select -
- Authentication Type: No Authentication
- Authentication Timeout: 1 Hour
- Redirect: ☐ Enable
- Redirect URL:
- Portal Customization: Local Web Portal

Below these fields is a preview of the authentication page, which includes a 'Term of Use' section with a checkbox 'I accept the Term of Use' (checked) and a 'Login' button.

A 'Save' button is located at the bottom of the 'Portal Configuration' section.

The 'Free Authentication Policy' section features a table with the following columns: ID, Policy Name, Source IP Range, Destination IP Range, Source MAC Address, Destination Port, Status, and Settings. An 'Add' button is located to the right of the table.

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

Configure 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.

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

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	Specify the value of authentication timeout. 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. 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.
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. Local Web Portal is the only available option in this authentication type. 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 only need to check the box of I accept the Term of Use and click the Login button.

4. Click **Save**.

- **Local Password**

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

Portal Configuration

SSID:

- Please Select -

Authentication Type:

Local Password

Password:

Authentication Timeout:

1 Hour

D

H

M

Redirect:

☐ Enable

Redirect URL:

Portal Customization:

Local Web Portal

Password:

Term of Use:

☒ I accept the Term of Use

Login

Save

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	Specify the value of authentication timeout. 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. 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.
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. Local Web Portal is the only available option is this authentication type. 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 password in the Password field, check the box of I accept the Term of Use and click the Login button.

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.

Portal Configuration

SSID:

- Please Select -

Authentication Type:

External Radius Server

RADIUS Server IP:

RADIUS Port:

1812

(1-65535)

RADIUS Password:

NAS ID:

RADIUS Accounting:

☒ Enable

Accounting Server IP:

Accounting Server Port:

1813

(1-65535)

Accounting Server Password:

Interim Update:

☐ Enable

Interim Interval:

600

seconds (60-86400)

Authentication Timeout:

1 Hour

D

H

M

Redirect:

☐ Enable

Redirect URL:

Portal Customization:

Local Web Portal

Username:

Password:

Term of Use:

☒ I accept the Term of Use

Login

Save

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	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 Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.
Authentication Timeout	Specify the value of authentication timeout. 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. 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.

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: - Build an external web portal server on your network and make sure that it is reachable by the EAP. - On this configuration page, enter the URL of the authentication page provided by the external portal server. Portal Customization: External Web Portal ▼ External Web Portal URL: - 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 Configure Free Authentication Policy.

4. Click **Save**.

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
--	--	--	--	--	--	--	--

Follow the steps below to add free authentication policy.

1. In the **Free Authentication Policy** section, click [+ Add](#) to load the following page.

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

Policy Name:

Source IP Range: / (Optional)

Destination IP Range: / (Optional)

Source MAC Address: (Optional)

Destination Port: (Optional)

Status: ☐ Enable

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	Specify an IP range with the subnet and mask length. The clients in this IP range can access the network without authentication. Leaving the field empty means that clients with any IP address can access the specific resources.
Destination IP Range	Specify an IP range with the subnet and mask length. The devices in this IP range can be accessed by the clients without authentication. Leaving the field empty means that all devices in the LAN can be accessed by the specific clients.
Source MAC Address	Specify the MAC address of the client, who can access the specific resources without authentication. Leaving the field empty means that clients with any MAC address can access the specific resources.

Destination Port	Specify the port number of the service. When using this service, the clients can access the specific resources without authentication. Leaving the field empty means that clients can access the specific resources no matter what service they are using.
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.

2.3 Configure 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 is added with different VLAN tags according to the VLAN settings of the wireless networks. Then 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.

ID	SSID Name	Band	VLAN	VLAN ID
1	SSID-1	2.4GHz	Disable	0
2	SSID-2	5GHz	Disable	0

Save

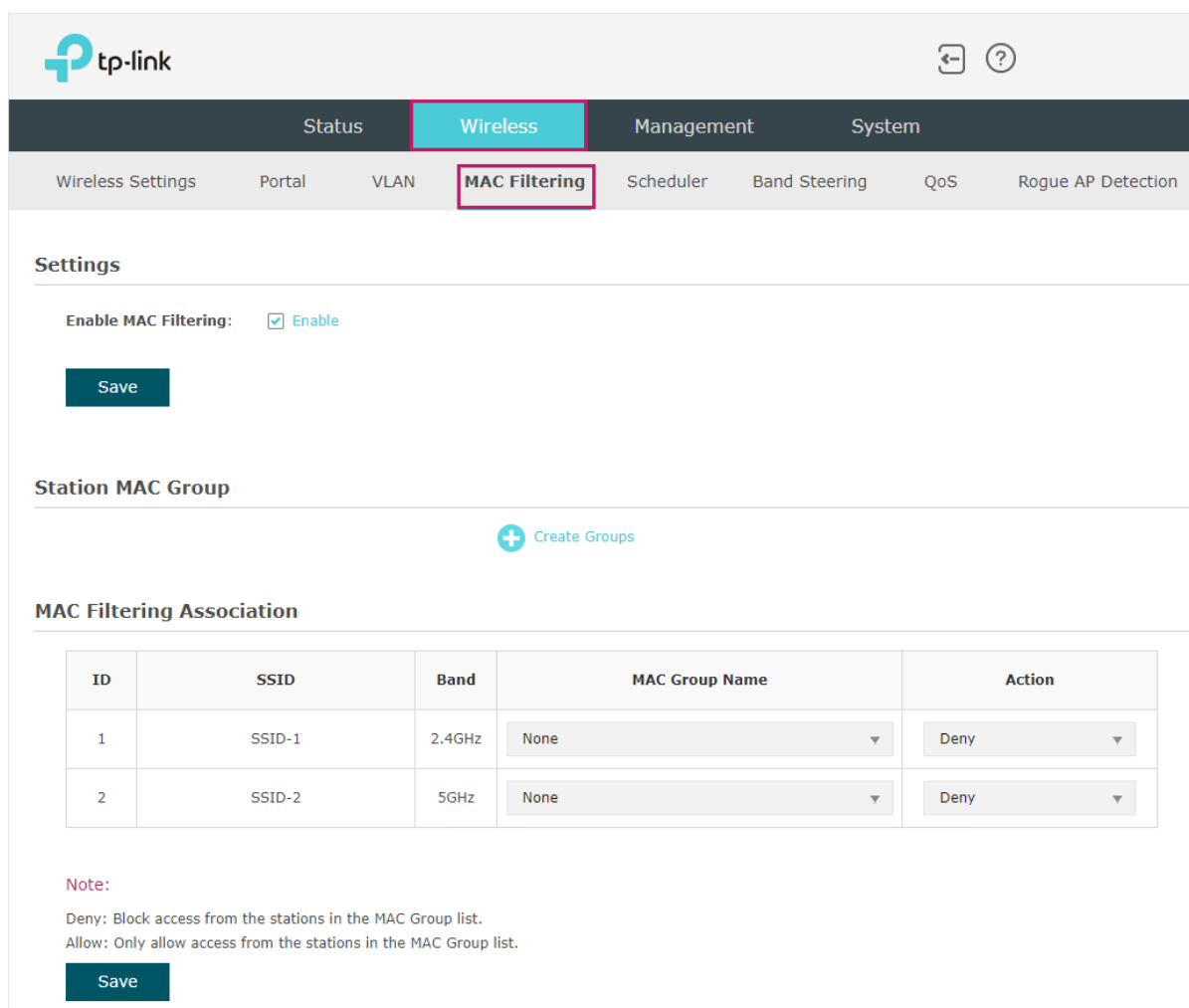
Follow the steps below to configure VLAN on this page.

1. Select the specific SSID in the list to configure the VLAN.
2. In the **VLAN** column and 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**.

2.4 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.



tp-link

Status **Wireless** Management System

Wireless Settings Portal VLAN **MAC Filtering** Scheduler Band Steering QoS Rogue AP Detection

Settings

Enable MAC Filtering: ☒ Enable

Save

Station MAC Group

+ Create Groups

MAC Filtering Association

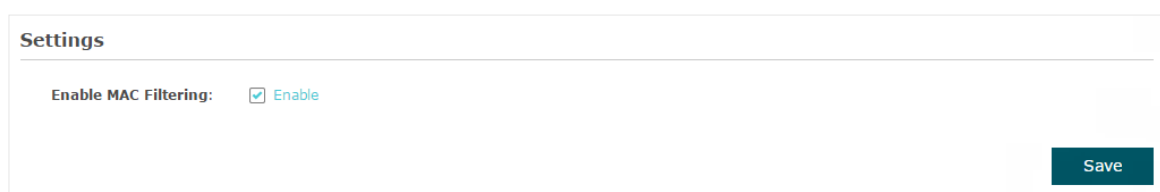
ID	SSID	Band	MAC Group Name	Action
1	SSID-1	2.4GHz	None	Deny
2	SSID-2	5GHz	None	Deny

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**.



Settings

Enable MAC Filtering: ☒ Enable

Save

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

Station MAC Group

 Add a Group

 Add a Group Member

MAC Group Name	Modify
--	--

➔

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 up to eight MAC groups.

Station MAC Group

 Add a Group

 Add a Group Member

MAC Group Name	Modify
--	--

➔

ID	MAC Address	Modify
--	--	--

MAC Group:

Cancel
OK

- 2) Select a MAC group in the group list (the color of the selected one will change to blue). 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.

Station MAC Group

 Add a Group

 Add a Group Member

MAC Group Name	Modify
Group 1	 
Group 2	 

➔

MAC Address:

Cancel
OK

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 Group 2 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.

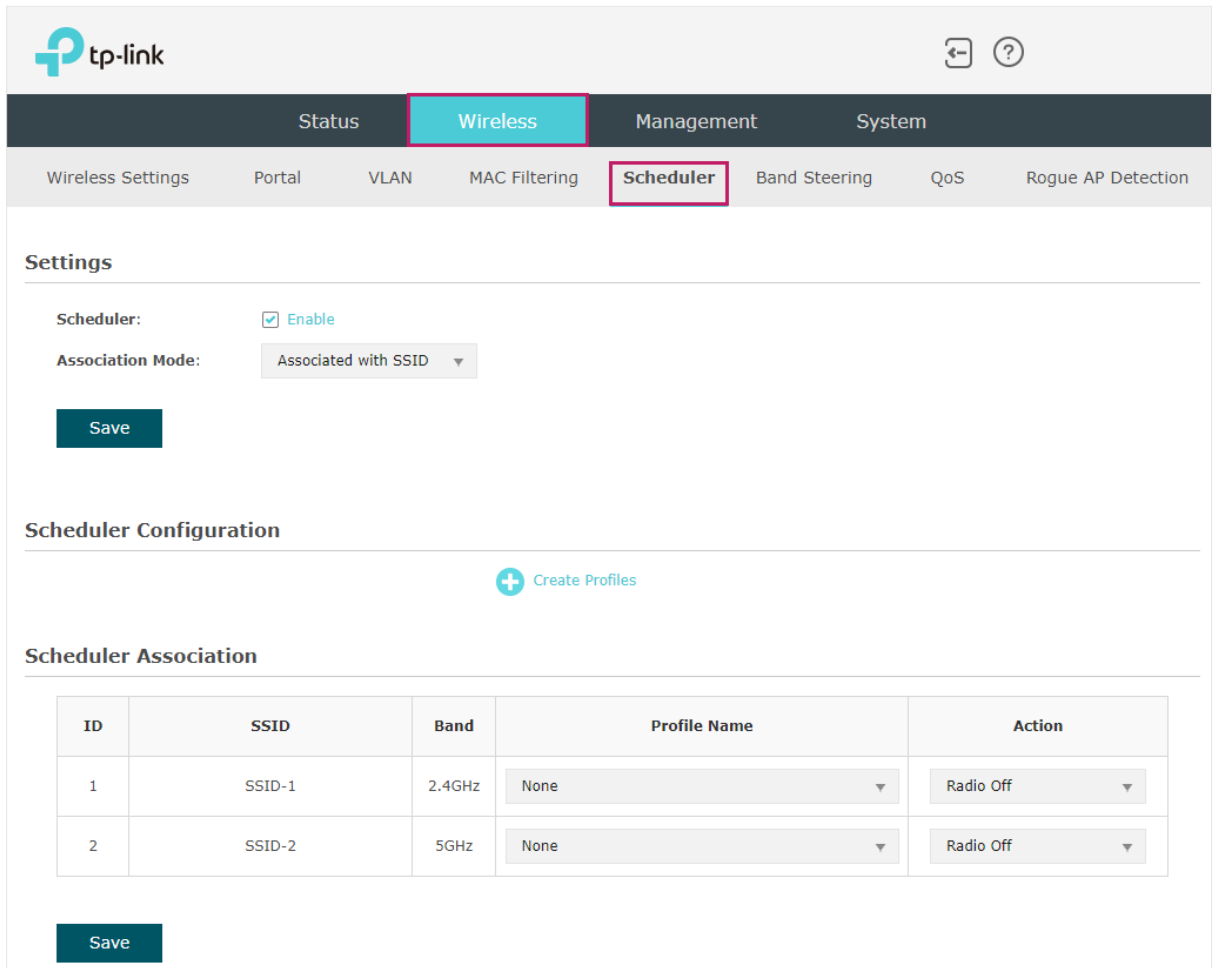
Allow: Only allow access from the stations in the MAC Group list.

Save

2.5 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.



tp-link

Status **Wireless** Management System

Wireless Settings Portal VLAN MAC Filtering **Scheduler** Band Steering QoS Rogue AP Detection

Settings

Scheduler: ☒ Enable

Association Mode: Associated with SSID ▼

Save

Scheduler Configuration

+ Create Profiles

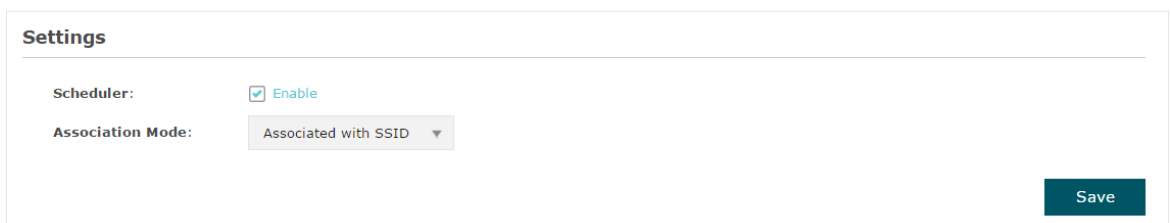
Scheduler Association

ID	SSID	Band	Profile Name	Action
1	SSID-1	2.4GHz	None ▼	Radio Off ▼
2	SSID-2	5GHz	None ▼	Radio Off ▼

Save

Follow the steps below to configure Scheduler on this page:

1. 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**.



Settings

Scheduler: ☒ Enable

Association Mode: Associated with SSID ▼

Save

2. In the **Scheduler Profile Configuration** section, click  **Create Profiles** and the following page will appear.

+

Add a Profile

Profile Name	Modify
--	--

+

Add an item

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

- 1) Click  **Add a Profile** and specify a name for the profile to be created. Click **OK**. You can create up to eight profiles.

+

Add a Profile

Profile Name	Modify
--	--

+

Add an item

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

Profile:

Profile 1

Cancel

OK

- 2) Select a profile in the list (the color of the selected one will change to blue). 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**.

+

Add a Profile

Profile Name	Modify
Profile 1	 
Profile 2	 

+

Add an item

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

Day:

☒ Weekday
 ☐ Weekend
 ☐ Every Day
 ☐ Custom

☒ Mon
 ☒ Tue
 ☒ Wed
 ☒ Thu
 ☒ Fri
 ☐ Sat
 ☐ Sun

Time:

☐ 24 hours

Start Time:

09

:

00

End Time:

18

:

00

Cancel

OK

Tips:

You can add up to eight 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 Profile2, 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	profile2 ▼	Radio On ▼
2	SSID-2	5GHz	profile2 ▼	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 is on.

Scheduler Association				
ID	AP	AP MAC	Profile Name	Action
1	EAP245-50-c7-bf-17-a6-e2	50-C7-BF-17-A6-E2	Profile 2 ▼	Radio On ▼

Save

2.6 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 SSID with the same wireless password on the 2GHz, 5GHz, and 6GHz bands.

Save

Band Steering

Configure the Band Steering function.

Disable: The AP will not steer clients.

Prefer 5GHz/6GHz: The AP will steer clients to the 5GHz and 6GHz in priority.

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

2.7 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.





StatusWirelessManagementSystem

Wireless SettingsPortalVLANMAC FilteringSchedulerBand SteeringQoSRogue AP Detection

2.4GHz5GHz

Wi-Fi Multimedia (WMM): ☒ Enable

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

2.4GHz5GHz

 to choose a frequency band to be configured.

2. Check the box to enable **Wi-Fi Multimedia (WMM)**. With WMM enabled, the EAP uses the QoS function to guarantee the high priority of the transmission of audio and video packets.

Wi-Fi Multimedia (WMM): ☒ Enable

Note:

If **802.11n only** mode is selected in 2.4GHz (or **802.11n only**, **802.11ac only**, or **802.11 n/ac mixed** mode selected in 5GHz), the WMM should be enabled. If WMM is disabled, the **802.11n only** mode cannot be selected in 2.4GHz (or **802.11n only**, **802.11ac only**, or **802.11 n/ac mixed** mode in 5GHz).

3. 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.

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

The following table detailedly explains these parameters:

Queue	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. Data 0 (Voice): Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. Data 1 (Video): High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. Data 2 (Best Effort): Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. 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).
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	A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value cannot be higher than the value of Maximum Contention Window.
Maximum Contention Window	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. This value must be higher than the value of Minimum Contention Window.
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.

- 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.

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

The following table detailedly explains these parameters:

Queue	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. Data 0 (Voice): Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. Data 1 (Video): High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. Data 2 (Best Effort): Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. 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).
--------------	--

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	A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value cannot be higher than the value of Maximum Contention Window.
Maximum Contention Window	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. This value must be higher than the value of Minimum Contention Window.
TXOP Limit	The TXOP Limit is a station EDCA parameter and only applies to traffic flowing from the client station to the EAP. 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.

5. Choose whether to enable the following two options according to your need.

No Acknowledgement: ☐ Enable

Unscheduled Automatic Power Save Delivery: ☒ Enable

The following table detailedly explains these options:

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.

6. Click **Save**.

2.8 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.

The screenshot shows the TP-Link web interface for configuring Rogue AP Detection. The top navigation bar includes the TP-Link logo and a search icon. Below it, a dark blue menu bar contains 'Status', 'Wireless' (highlighted with a red box), 'Management', and 'System'. Under the 'Wireless' menu, a sub-menu bar lists 'Wireless Settings', 'Portal', 'VLAN', 'MAC Filtering', 'Scheduler', 'Band Steering', 'QoS', and 'Rogue AP Detection' (highlighted with a red box).

The main content area is divided into three sections:

- Settings:** Contains a 'Rogue AP Detection' section with an 'Enable' checkbox (unchecked) and a 'Save' button.
- Detected Rogue AP List:** Features a 'Scan' button (magnifying glass icon) and a table with the following columns: MAC, SSID, Band, Channel, Security, Beacon Interval, Signal, and Action. The table currently shows one row with dashes ('--') in all columns.
- Trusted AP List:** Contains a table with the following columns: MAC, SSID, Band, Channel, Security, and Action. The table currently shows one row with dashes ('--') in all columns.

Below these sections is the **Download/Backup Trusted AP List** section, which includes:

- Save Action:** Two radio buttons: 'Download (PC to AP)' (selected) and 'Backup (AP to PC)'.
- Source File Name:** A text input field followed by a 'Browse' button.
- File Management:** Two radio buttons: 'Replace' (selected) and 'Merge'.
- A 'Save' button at the bottom.

Detect Rogue APs and Move the Rogue APs to the Trusted 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**.

Settings

Rogue AP Detection: ☒ Enable

Save

2. In the **Detected Rogue AP List** section, click  **Scan**.
3. Wait for a few seconds without any operation. After detection is finished, the detected APs will be displayed in the list.

Detected Rogue AP 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
 1 2 3 4 5 ... 8 							

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, we move the first two APs in the above Detected Rogue AP list to the Trusted AP list.
- 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

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:

File Management: ☒ Replace ☐ Merge

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

- 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.

2.9 Configure Smart Antenna (Only for Certain Devices)

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

To enable or disable Smart Antenna, go to the **Wireless > Smart Antenna** page.

Smart Antenna

Smart Antenna: ☒ Enable

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

Save

3

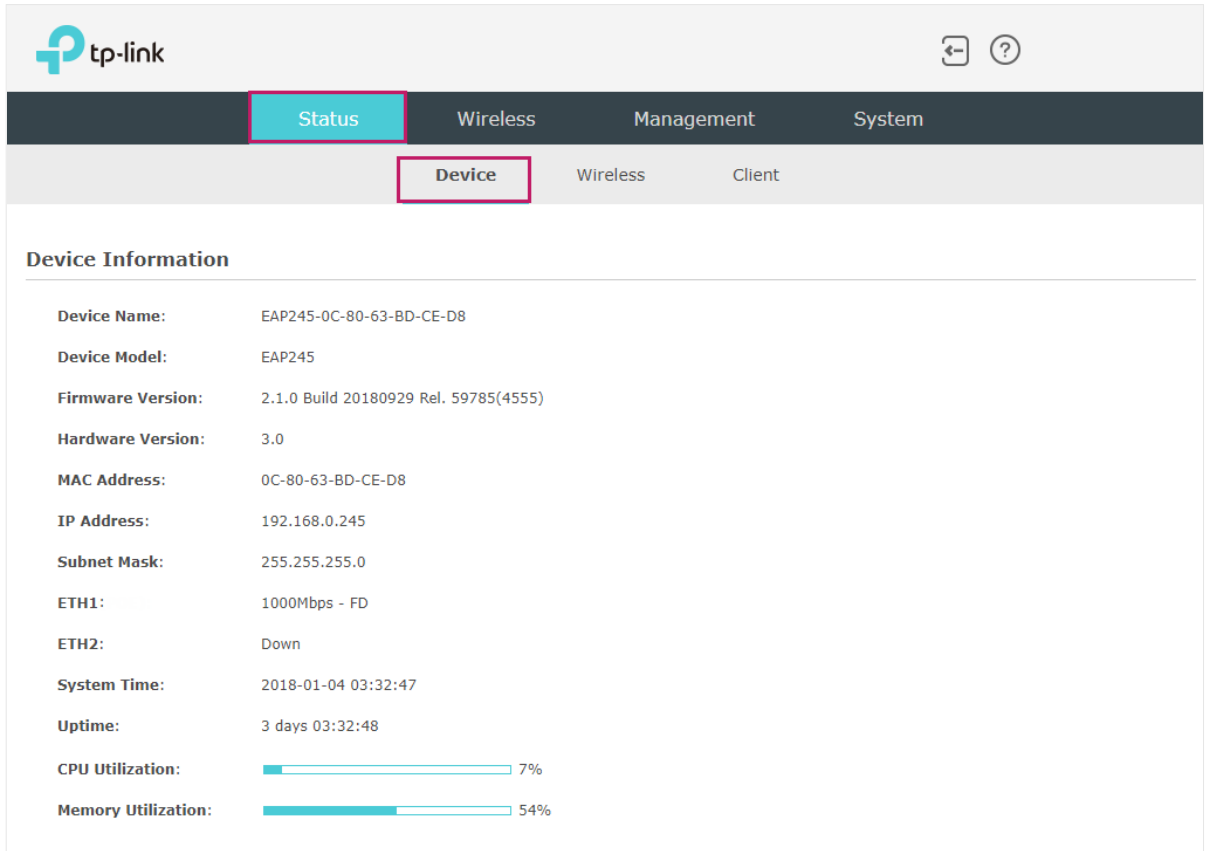
Monitor the Network

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

- *3.1 Monitor the EAP*
- *3.2 Monitor the Wireless Parameters*
- *3.3 Monitor the Clients*

3.1 Monitor the EAP

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



The screenshot shows the TP-Link web interface. The top navigation bar has 'Status' highlighted. Below it, the 'Device' sub-tab is selected. The 'Device Information' section displays the following details:

Device Name:	EAP245-0C-80-63-BD-CE-D8
Device Model:	EAP245
Firmware Version:	2.1.0 Build 20180929 Rel. 59785(4555)
Hardware Version:	3.0
MAC Address:	0C-80-63-BD-CE-D8
IP Address:	192.168.0.245
Subnet Mask:	255.255.255.0
ETH1:	1000Mbps - FD
ETH2:	Down
System Time:	2018-01-04 03:32:47
Uptime:	3 days 03:32:48
CPU Utilization:	7%
Memory Utilization:	54%

The following device information is displayed:

Device Name	Displays the name of the EAP. The name consists of the product model followed with the MAC address of the EAP by default.
Device Model	Displays the product model of the EAP.
Firmware Version	Displays the current firmware version the EAP. To update the firmware, you can refer to 5.6 Update the Firmware .
Hardware Version	Displays the hardware version the EAP.
MAC Address	Displays the MAC address of the EAP.
IP Address	Displays the IP address of the EAP.
Subnet Mask	Displays the subnet mask of the EAP.
System Time	Displays the current system time. To configure the system time, you can refer to 5.3 Configure the System Time .
Uptime	Displays how long the EAP has been working since it starts up.

CPU Utilization	Displays the CPU occupancy. If this value is too high, the EAP may work abnormally.
Memory Utilization	Displays the memory occupancy.

If your product is a Bridge kit:

On the Main AP's Device page, you can view the Sub-AP list. For a Sub-AP entry, you can click  to launch its web page.

Sub-APs				
ID	MAC Address	IP Address	Signal Strength	Action
1	A8-42-A1-5A-42-93	192.168.0.105	 -51dbm	

On the Sub-AP's Device page, you can view its Main AP.

Main AP	
MAC Address:	A8-42-A1-5A-42-92

3.2 Monitor the Wireless Parameters

You can view the wireless parameters of the EAP, including SSID lists, radio settings, radio traffic and LAN traffic.

Tips:

To change the wireless parameters, you can refer to [2.1 Configure the Wireless Parameters](#).

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



StatusWirelessManagementSystem

DeviceWirelessClient

SSID List

 Refresh

ID	SSID Name	Clients	Band	Security	Portal	VLAN ID	Guest Network	Down (Byte)	Up (Byte)
1	SSID-1	0	2.4GHz	WPA-PSK	Disable	Disable	Disable	922k	82k
2	SSID-2	0	5GHz	None	Disable	Disable	Disable	12k	2k

Radio Settings

2.4GHz5GHz

2.4GHz Wireless Radio: Enable

Channel Frequency: 6 / 2437MHz

Channel Width: 20/40MHz

IEEE802.11 Mode: b/g/n mixed

Max TX Rate: 300.0Mbps

Tx Power: 20dBm

Radio Traffic

2.4GHz5GHz

Rx Packets: 66730494

Rx Bytes: 16998586607

Rx Dropped Packets: 0

Rx Errors: 0

Tx Packets: 7099989

Tx Bytes: 1610535114

Tx Dropped Packets: 0

Tx Errors: 65

LAN Traffic

Rx Packets: 455929

Rx Bytes: 259238847

Rx Dropped Packets: 0

Rx Errors: 0

Tx Packets: 169208

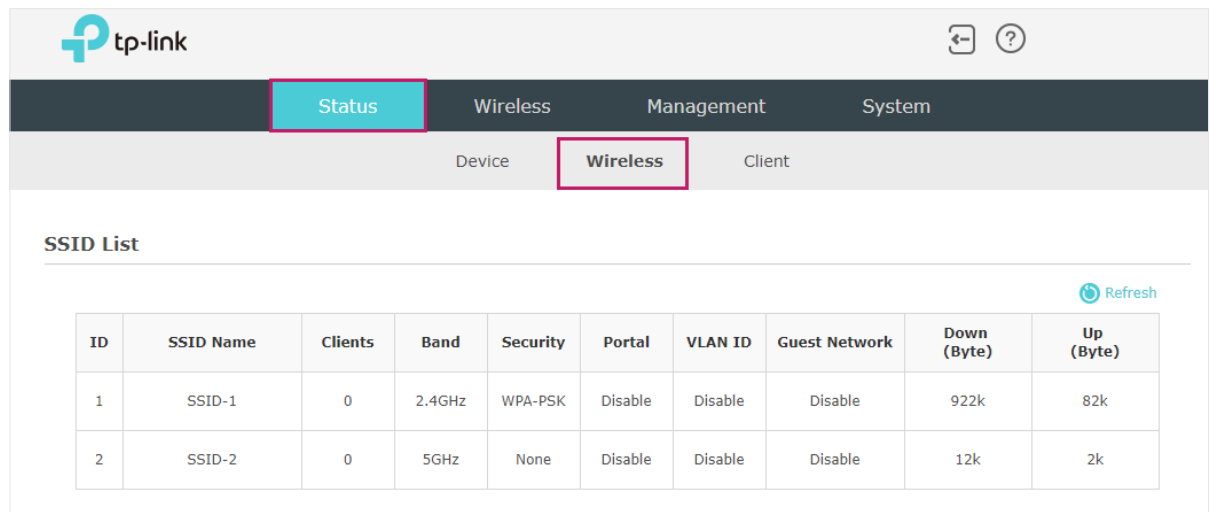
Tx Bytes: 167366153

Tx Dropped Packets: 0

Tx Errors: 0

Monitor the SSIDs

You can monitor the SSID information of the EAP.



The screenshot shows the TP-Link web interface. At the top, there's a navigation bar with 'tp-link' logo and icons for back and help. Below it, a dark blue menu bar contains 'Status' (highlighted with a red box), 'Wireless', 'Management', and 'System'. Under 'Wireless', there's a sub-menu bar with 'Device', 'Wireless' (highlighted with a red box), and 'Client'. The main content area is titled 'SSID List' and features a table with 10 columns: ID, SSID Name, Clients, Band, Security, Portal, VLAN ID, Guest Network, Down (Byte), and Up (Byte). A 'Refresh' button is located to the right of the table. The table contains two rows of data.

ID	SSID Name	Clients	Band	Security	Portal	VLAN ID	Guest Network	Down (Byte)	Up (Byte)
1	SSID-1	0	2.4GHz	WPA-PSK	Disable	Disable	Disable	922k	82k
2	SSID-2	0	5GHz	None	Disable	Disable	Disable	12k	2k

The following table introduces the displayed information of the SSID:

SSID Name	Displays the SSID name.
Clients	Displays the number of clients currently connected to the SSID.
Band	Displays the frequency band the SSID is currently using.
Security	Displays the security mode of the SSID.
Portal	Displays whether portal function is enabled on the SSID.
VLAN ID	Displays the VLAN ID of the SSID.
Guest Network	Display guest network is enabled on the SSID.
Down (Byte)	Displays the total download traffic since the SSID starts working.
Up (Byte)	Displays the total upload traffic since the SSID starts working.

Monitor the Radio Settings

You can monitor the radio settings of the EAP. The following figure posted in the introduction takes 2.4GHz as an example.

Radio Settings	
2.4GHz	5GHz
2.4GHz Wireless Radio:	Enable
Channel Frequency:	6 / 2437MHz
Channel Width:	20/40MHz
IEEE802.11 Mode:	b/g/n mixed
Max TX Rate:	300.0Mbps
Tx Power:	20dBm

The following table introduces the displayed information of the EAP.

Wireless Radio	Displays whether wireless function is enabled on the radio band.
Channel Frequency	Displays the channel and frequency which are currently used by the EAP.
Channel Width	Displays the channel width which is currently used by the EAP.
IEEE802.11 Mode	Displays the IEEE802.11 protocol currently used by the EAP.
Max TX Rate	Displays the maximum physical rate of the EAP.
Tx Power	Displays the transmit power of the EAP.

Monitor Radio Traffic

You can monitor the radio traffic of the EAP. The following figure posted in the introduction takes 2.4GHz of a dual-band device as an example.

Radio Traffic			
2.4GHz	5GHz		
Rx Packets:	82874437	Tx Packets:	8800930
Rx Bytes:	20906526476	Tx Bytes:	1990845129
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	65

The following traffic information of the radio is displayed:

Rx Packets	Displays the total number of the received packets on the current band since the EAP starts up.
------------	--

Tx Packets	Displays the total number of the sent packets on the current band since the EAP starts up.
Rx Bytes	Displays the total received traffic on the current band since the EAP starts up.
Tx Bytes	Displays the total sent traffic on the current band since the EAP starts up.
Rx Dropped Packets	Displays the total number of the dropped packets which are received on the current band since the EAP starts up.
Tx Dropped Packets	Displays the total number of the dropped packets which are sent on the current band since the EAP starts up.
Rx Errors	Displays the total number of error packets which are received on the current band since the EAP starts up.
Tx Errors	Displays the total number of error packets which are sent on the current band since the EAP starts up.

Monitor LAN Traffic

You can view the LAN traffic of EAP.

LAN Traffic			
Rx Packets:	559223	Tx Packets:	206607
Rx Bytes:	320073875	Tx Bytes:	204207153
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

The following traffic information of the LAN is displayed:

Rx Packets	Displays the total number of received packets in the LAN since the EAP starts up.
Tx Packets	Displays the total number of sent packets in the LAN since the EAP starts up.
Rx Bytes	Displays the total received traffic in the LAN since the EAP starts up.
Tx Bytes	Displays the total sent traffic in the LAN since the EAP starts up.
Rx Dropped Packets	Displays the total number of the dropped packets which are received by the EAP since it starts up.
Tx Dropped Packets	Displays the total number of the dropped packets which are sent by the EAP since it starts up.

Rx Errors	Displays the total number of the received error packets since the EAP starts up.
Tx Errors	Displays the total number of the sent error packets since the EAP starts up.

3.3 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.

tp-link

Status

Wireless

Management

System

Device

Wireless

Client

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	iPhone	192.168.1.100	D0-A6-37-83-DA-99	5GHz	SSID-2	0 days 00:01:24	39k	20k	-83	263.0	

Block Client List

Refresh

ID	Hostname	MAC Address	Up (Byte)	Down (Byte)	Action
1	android-6532c20e9aa005cc	1C-77-F6-91-C7-B8	3k	1k	

View Client Information

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.

Click the

User

Guest

 to select the client types to view the information of the EAP. The following figure posted in the introduction takes user as an example.

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	iPhone	192.168.1.100	D0-A6-37-83-DA-99	5GHz	SSID-2	0 days 00:00:07	4k	1k	-80	175.0	

The following client information is displayed:

Hostname	Displays the hostname of the user.
IP Address	Displays the IP address of the user.

MAC Address	Displays the MAC address of the user.
Band	Displays the frequency band the user is working on.
SSID	Displays the SSID the user is connecting to.
Active Time	Displays how long the user has been connected to the SSID.
Up (Byte)	Displays the user's total uploaded traffic to the EAP since the last connection.
Down (Byte)	Displays the user's total downloaded traffic from the EAP since the last connection.
RSSI (dBm)	Displays the RSSI(Received Signal Strength Indication) of the user.
Rate (Mbps)	Displays the wireless transmission rate of the user.

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 [2.1.1 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.

Rate Limit:

☒ Enable
 ?

Download Limit:

Kbps

(1-10240000)

Upload Limit:

Kbps

(1-10240000)

OK



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	android-6532c20e9aa005cc	1C-77-F6-91-C7-B8	3k	1k	

The following information of the blocked client is displayed:

Hostname	Displays the hostname of the user.
MAC Address	Displays the MAC address of the user.
Up (Byte)	Displays the user's total uploaded traffic to the EAP since the last connection.
Down (Byte)	Displays the user's total downloaded traffic from the EAP since the last connection.
Action	You can click the  to resume the client's access to the internet.

4 *Manage the EAP*

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

- 4.1 *Manage Bridge APs (Only for a Bridge Main AP)*
- 4.2 *Manage the IP Address of the EAP*
- 4.3 *Manage System Logs*
- 4.4 *Configure Web Server*
- 4.5 *Configure Management Access*
- 4.6 *Configure Trunk (Only for Certain Devices)*
- 4.7 *Configure LED*
- 4.8 *Configure Wi-Fi Control (Only for Certain Devices)*
- 4.9 *Configure PoE Out (Only for Certain Devices)*
- 4.10 *Configure SSH*
- 4.11 *Configure SNMP*
- 4.12 *Configure Power Saving (Only for Certain Devices)*

4.1 Manage Bridge APs (Only for a Bridge Main AP)

If your product is a Bridge kit, you can view and manage Bridge APs centrally on the Main AP's web page.

Go to the **Management > Wireless Bridge APs** page. The system automatically displays the Main AP and Sub-AP(s) in the kit.

StatusWirelessManagementSystem

Wireless Bridge APsNetworkSystem LogWeb ServerManagement AccessLED ControlSSHSNMP

Wireless Bridge APs (2/5)

Refresh

ID	Type	Mac Address	IP Address	Signal Quality	Action
1	Main AP (Current AP)	A8-42-A1-5A-42-92	192.168.0.101		
2	Sub-AP (Kit AP)	A8-42-A1-5A-42-93	192.168.0.105	-51dbm	

Add Sub-AP

Note:

To delete a sub-AP, launch it to open its management interface and reset the device. (KIT APs will still automatically form a network after resetting.)

For a Sub-AP entry, you can click  to launch its web page.

If you want to add other APs, click the **Add Sub-AP** button and follow the web instructions to add them.

4.2 Manage the IP Address of the EAP

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.

Tips:

For detailed introduction about how to find the dynamic IP address of the EAP, refer to [Using Web Browser on Your PC and Connecting to the Ethernet](#).

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

The screenshot shows the TP-Link web interface. At the top, there's a navigation bar with 'Status', 'Wireless', 'Management' (highlighted), and 'System'. Below this, a sub-navigation bar shows 'Network' (highlighted), 'System Log', 'Web Server', 'Management Access', 'LED Control', 'SSH', and 'SNMP'. The main content area is titled 'LAN IP Settings'. It features two radio buttons: 'Dynamic' (selected) and 'Static'. Below this, there's a 'Fallback IP' section with a checkbox labeled 'Enable' which is checked. Underneath, there are three input fields: 'DHCP Fallback IP' with the value '192.168.0.245', 'DHCP Fallback Mask' with the value '255.255.255.0', and 'DHCP Fallback Gateway' which is empty. A 'Save' button is located at the bottom left of the settings area.

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.

Dynamic Static

Fallback IP: ☒ Enable

DHCP Fallback IP: 192.168.0.245

DHCP Fallback Mask: 255.255.255.0

DHCP Fallback Gateway:

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.

Dynamic Static

IP Address: 192.168.0.245

IP Mask: 255.255.255.0

Gateway: 0.0.0.0

Primary DNS: 192.168.0.1

Secondary DNS: 0.0.0.0 (Optional)

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

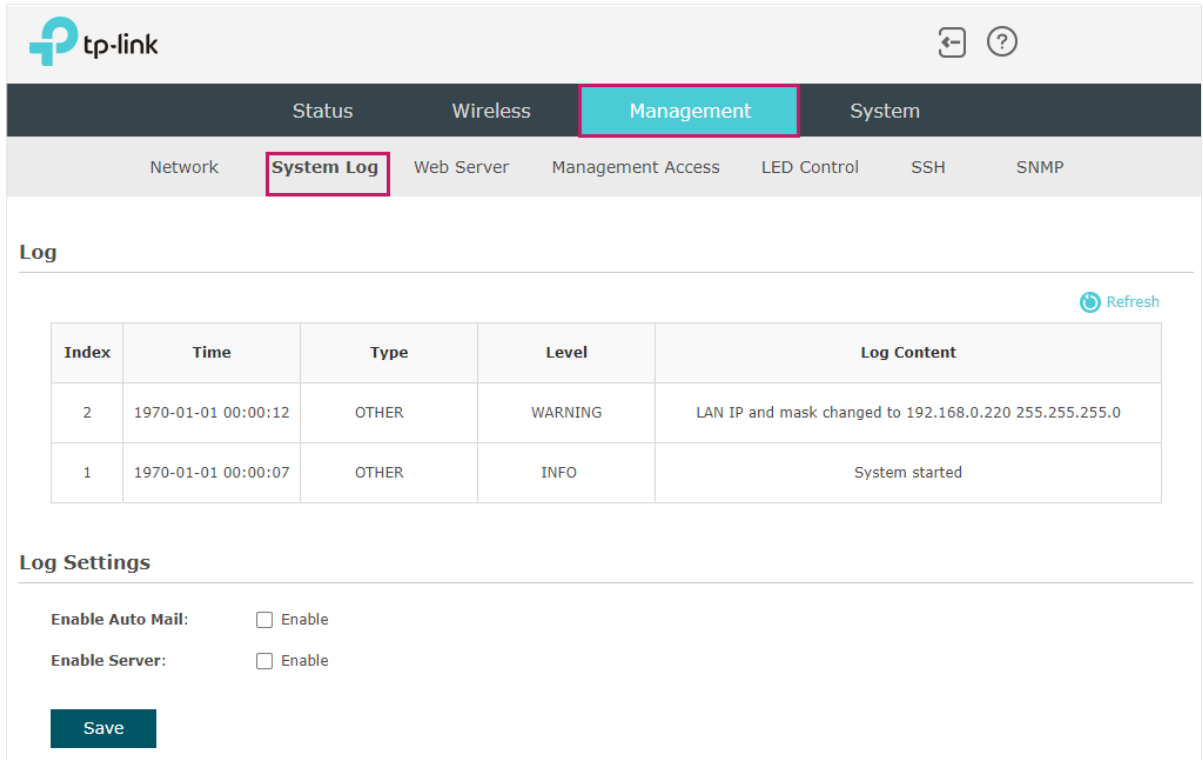
IP Address	Specify a static IP address for the EAP.
IP Mask	Specify the network mask.
Gateway	Specify the network gateway.
Primary DNS	Specify the primary DNS server.
Secondary DNS	Specify the secondary DNS server. (Optional)

3. Click **Save**.

4.3 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	1970-01-01 00:00:12	OTHER	WARNING	LAN IP and mask changed to 192.168.0.220 255.255.255.0
1	1970-01-01 00:00:07	OTHER	INFO	System started

Log Settings

Enable Auto Mail: ☐ Enable

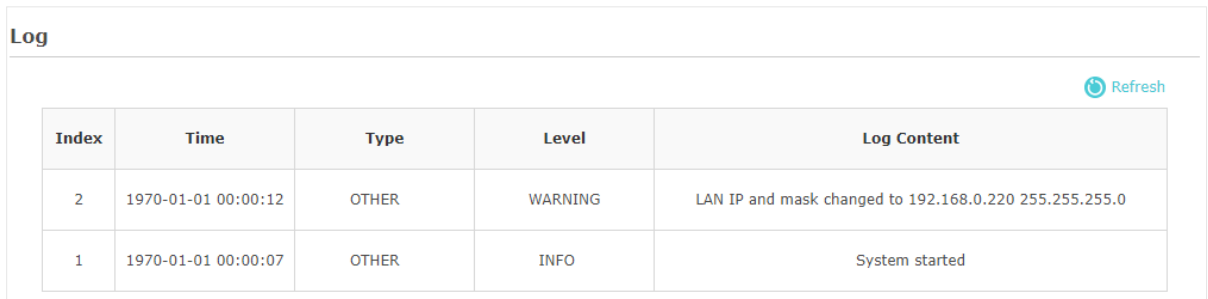
Enable Server: ☐ Enable

[Save](#)

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

View System Logs

In the **Log** section, you can click [Refresh](#) to refresh the logs and view them in the table.



Log

[Refresh](#)

Index	Time	Type	Level	Log Content
2	1970-01-01 00:00:12	OTHER	WARNING	LAN IP and mask changed to 192.168.0.220 255.255.255.0
1	1970-01-01 00:00:07	OTHER	INFO	System started

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

Enable Server:

☐ 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.

Note:

SSL encryption is not currently supported.

Enable Auto Mail:

☒ Enable

From:

To:

SMTP Server:

Enable Authentication:

☐ Enable

Time:

☒ Fixed Time ☐ Period

Fixed Time:

00

:

00

(HH:MM)

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.

Enable Server:	☒ Enable
System Log Server IP:	0.0.0.0
System Log Server Port:	514
More Client Detail Log:	☐ Enable

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**.

4.4 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

Secure Server Port:	443
Server Port:	80
Session Timeout:	15 minutes
Layer-3 Accessibility:	☐ Enable
TLS Version 1.0/1.1:	☐ Enable 

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

Save

Follow the steps below to configure Web Server:

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

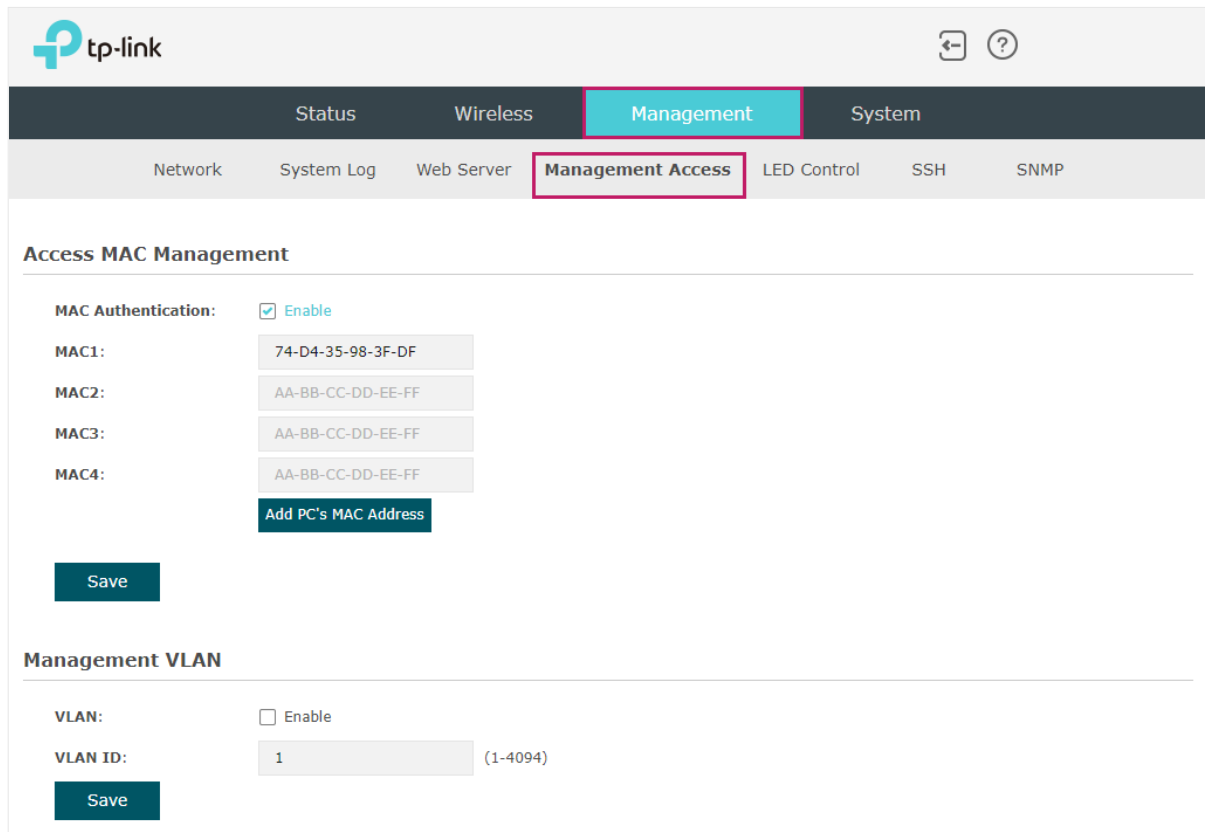
Secure Server Port	Designate a secure server port for web server in HTTPS mode. By default the port is 443.
Server Port	Designate a server port for web server in HTTP mode. By default the port is 80.
Session Timeout	Set the session timeout. If you do nothing with the web page within the timeout, the 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	The EAP management page uses TLS v1.2 by default. You can enable the feature if you prefer TLS v1.0/1.1. This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

2. Click **Save**.

4.5 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 of the hosts that are allowed to access the web page.

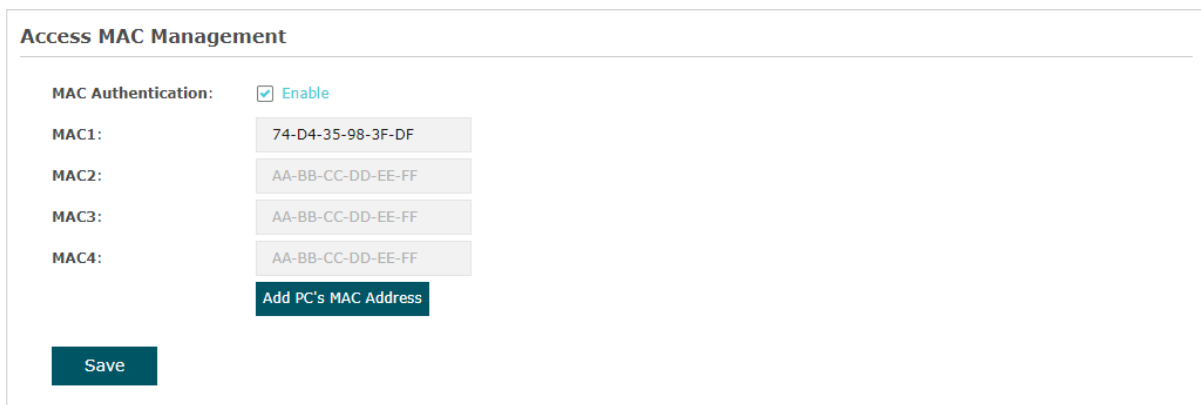
To configure Management Access, go to the **Management > Management Access** page.



The screenshot shows the TP-Link web interface. The top navigation bar includes 'Status', 'Wireless', 'Management' (highlighted in blue), and 'System'. Below this, a sub-navigation bar shows 'Network', 'System Log', 'Web Server', 'Management Access' (highlighted with a red box), 'LED Control', 'SSH', and 'SNMP'. The main content area is titled 'Access MAC Management'. It features a 'MAC Authentication' section with a checked 'Enable' checkbox. Below this are four MAC address input fields labeled 'MAC1:', 'MAC2:', 'MAC3:', and 'MAC4:', each containing the placeholder text 'AA-BB-CC-DD-EE-FF'. A button labeled 'Add PC's MAC Address' is positioned below the 'MAC4' field. A 'Save' button is located at the bottom of this section. The 'Management VLAN' section below it has an unchecked 'VLAN' checkbox and a 'VLAN ID' input field with the value '1' and a range '(1-4094)' to its right. A 'Save' button is also present at the bottom of this section.

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.



This screenshot shows the 'Access MAC Management' configuration page, which is identical to the one above. It displays the 'MAC Authentication' section with 'Enable' checked, four MAC address input fields (MAC1-MAC4) with placeholder text, an 'Add PC's MAC Address' button, and a 'Save' button. Below it is the 'Management VLAN' section with an unchecked 'VLAN' checkbox, a 'VLAN ID' input field set to '1', and a range '(1-4094)', followed by another 'Save' button.

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.

Configure Management VLAN

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.

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**.

4.6 Configure Trunk (Only for Certain Devices)

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

To configure the trunk function, go to the Management > Trunk page.

Trunk Settings

Enable:

☐ Enable

Mode:

SRC MAC+DST MAC ▼

Save

Enable

Check the box to enable the function.

Mode

Select the trunk algorithm mode. Based on the selected algorithm mode, the AP determines which physical port is used to send out the received packet.

SRC MAC+DST MAC: The AP determines the outgoing port based on both the source and destination MAC addresses of the packet.

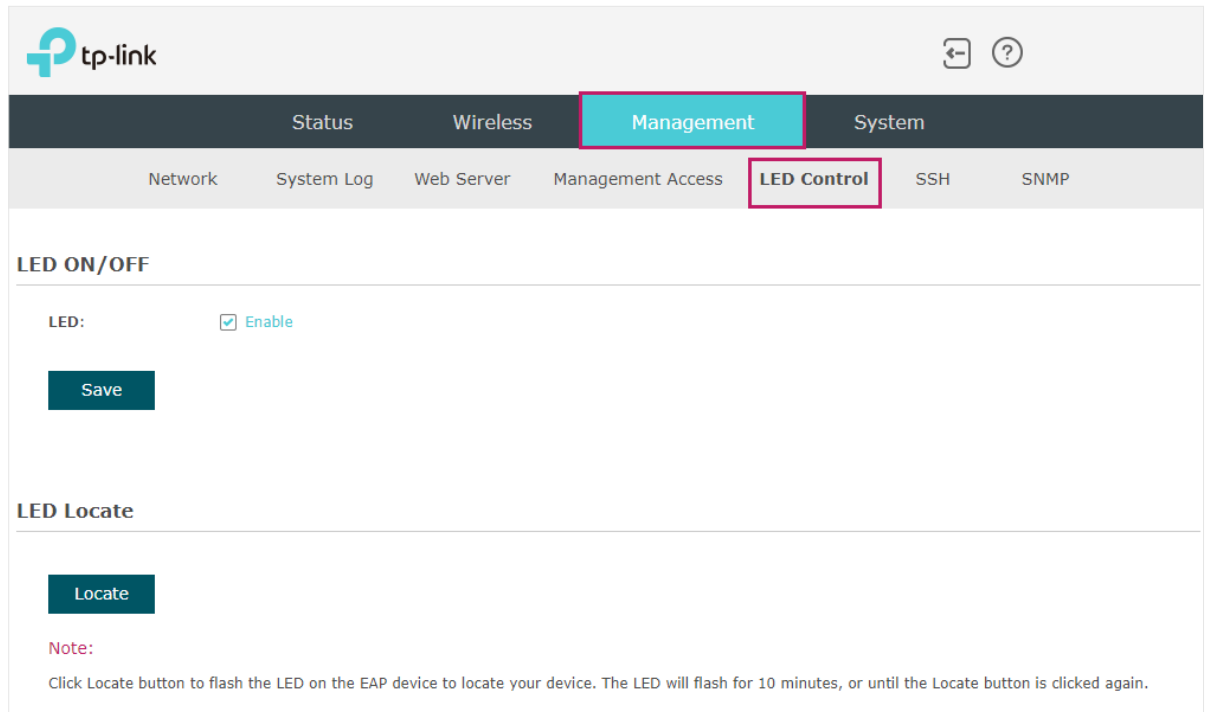
DST MAC: The AP determines the outgoing port based on the destination MAC address of the packet.

SRC MAC: The AP determines the outgoing port based on the source MAC address of the packet.

4.7 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.



The screenshot shows the TP-Link web interface. At the top, there is a navigation bar with the TP-Link logo on the left and two icons (a square with an arrow and a question mark) on the right. Below the navigation bar is a dark grey menu bar with four tabs: "Status", "Wireless", "Management", and "System". The "Management" tab is highlighted with a red border. Below the menu bar is a light grey sub-menu bar with seven items: "Network", "System Log", "Web Server", "Management Access", "LED Control", "SSH", and "SNMP". The "LED Control" item is highlighted with a red border. The main content area is divided into two sections. The first section is titled "LED ON/OFF" and contains a label "LED:" followed by a checked checkbox and the word "Enable". Below this is a dark teal button labeled "Save". The second section is titled "LED Locate" and contains a dark teal button labeled "Locate". Below the "Locate" button is a red "Note:" followed by the text: "Click 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.

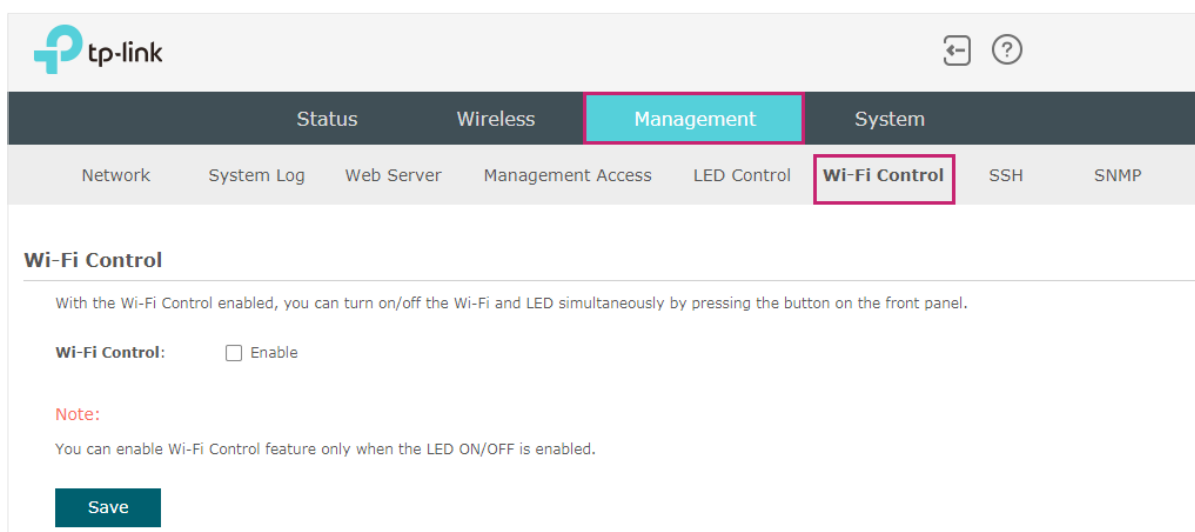
4.8 Configure Wi-Fi Control (Only for Certain Devices)

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.



The screenshot shows the TP-Link web interface. At the top, there is a navigation bar with the TP-Link logo on the left and a help icon on the right. Below the navigation bar is a menu bar with four main categories: Status, Wireless, Management, and System. The Management category is highlighted with a red box. Under the Management category, there are several sub-items: Network, System Log, Web Server, Management Access, LED Control, Wi-Fi Control, SSH, and SNMP. The Wi-Fi Control sub-item is highlighted with a red box. Below the menu bar, the Wi-Fi Control configuration page is displayed. It contains a heading "Wi-Fi Control" and a paragraph explaining the feature: "With the Wi-Fi Control enabled, you can turn on/off the Wi-Fi and LED simultaneously by pressing the button on the front panel." Below this paragraph, there is a label "Wi-Fi Control:" followed by a checkbox and the text "Enable". Below the checkbox, there is a red "Note:" section with the text: "You can enable Wi-Fi Control feature only when the LED ON/OFF is enabled." At the bottom of the page, there is a "Save" button.

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.

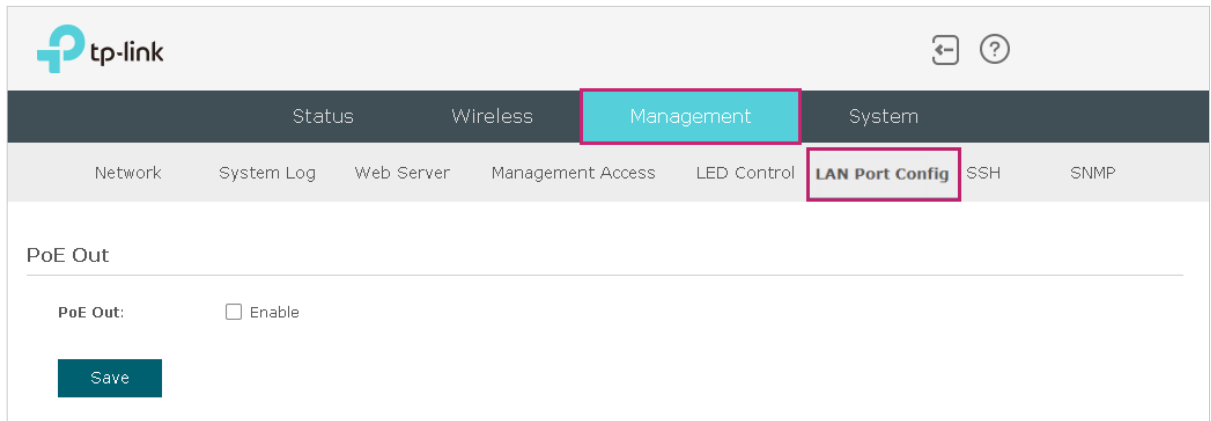
4.9 Configure PoE Out (Only for Certain Devices)

Note:

PoE Out is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If PoE Out is available, there is **Management > LAN Port Config** in the menu structure.

Certain devices have a PoE OUT port that can transmit data and supply power to the client simultaneously. You can also disable PoE Out to make the port transmit data only.

To configure PoE Out, go to the **Management > LAN Port Config** page.



The screenshot shows the TP-Link web interface. At the top left is the TP-Link logo. To the right are icons for a home page and a help page. Below these is a navigation bar with four main tabs: Status, Wireless, Management, and System. The Management tab is highlighted with a red box. Under the Management tab, there is a sub-menu with several options: Network, System Log, Web Server, Management Access, LED Control, LAN Port Config, SSH, and SNMP. The LAN Port Config option is highlighted with a red box. Below the navigation bar, the page title is "PoE Out". Under this title, there is a label "PoE Out:" followed by an unchecked checkbox and the text "Enable". At the bottom of the page, there is a red "Save" button.

Check the box to enable PoE Out and click **Save**.

4.10Configure 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.

The screenshot shows the TP-Link Omada web interface. At the top, there's a navigation bar with 'Status', 'Wireless', 'Management', and 'System'. Below this, a secondary bar shows 'Network', 'System Log', 'Web Server', 'Management Access', 'LED Control', 'SSH', and 'SNMP'. The 'SSH' tab is selected. The main content area is titled 'SSH Server' and contains three settings: 'Server Port' (set to 22), 'Layer-3 Accessibility' (disabled), and 'SSH Login' (disabled). A 'Save' button is located at the bottom left of the settings area.

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**.

4.11 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.

The screenshot shows the TP-Link web interface. The top navigation bar has tabs for Status, Wireless, Management (highlighted), and System. Below this, a secondary navigation bar shows Network, System Log, Web Server, Management Access, LED Control, SSH, and SNMP (highlighted). The main content area is titled 'SNMP Agent' and contains the following configuration options:

- SNMP Agent:** ☐ Enable
- SysContact:** [Text input field]
- SysName:** [Text input field]
- SysLocation:** [Text input field]
- Get Community:** [Text input field with value 'public']
- Get Source:** [Text input field with value '0.0.0.0']
- Set Community:** [Text input field with value 'private']
- Set Source:** [Text input field with value '0.0.0.0']

A 'Save' button is located at the bottom left of the configuration area.

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.

4.12 Configure Power Saving (Only for Certain Devices)

Power saving can reduce the AP's power usage.

To configure power saving, go to the **Power > Power Saving** page.

Power Saving

Trigger by Time:

☒ Enable

Start Time:

00

:

00

End Time:

00

:

00

Note:

Enable Power Saving every day from 00:00 to 00:00.

Trigger by Band:

☒ Enable

Bands:

- Please Select -

Idle Duration:

0

Note:

Enable Power Saving when there are no connections for 0 min on the no band(s).

Save

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

5

Configure the System

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

- *5.1 Configure the User Account*
- *5.2 Controller Settings*
- *5.3 Configure the System Time*
- *5.4 Reboot and Reset the EAP*
- *5.5 Backup and Restore the Configuration*
- *5.6 Update the Firmware*

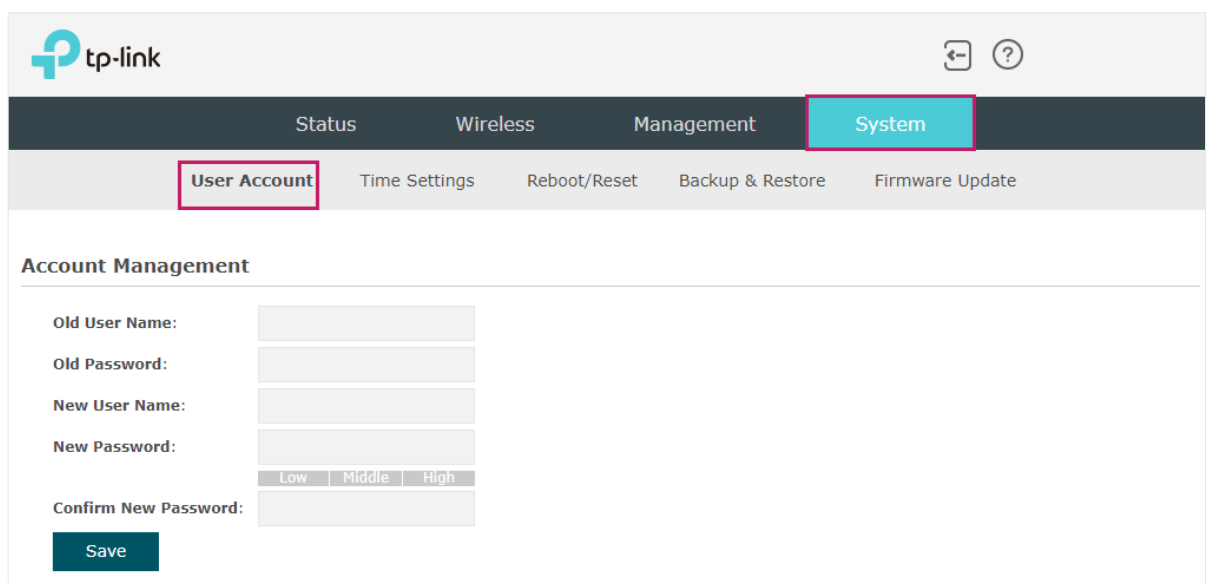
5.1 Configure the User Account

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.



The screenshot shows the TP-Link EAP management interface. At the top, there is a navigation bar with the TP-Link logo and a dark blue menu containing 'Status', 'Wireless', 'Management', and 'System'. The 'System' menu item is highlighted with a red box. Below this, a sub-menu bar contains 'User Account', 'Time Settings', 'Reboot/Reset', 'Backup & Restore', and 'Firmware Update'. The 'User Account' item is also highlighted with a red box. The main content area is titled 'Account Management' and contains the following fields: 'Old User Name:', 'Old Password:', 'New User Name:', 'New Password:', and 'Confirm New Password:'. The 'New Password' field has a strength indicator below it with three tabs: 'Low', 'Middle', and 'High'. A 'Save' button is located at the bottom left of the form.

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**.

5.2 Controller Settings

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.

- If you are using Omada Cloud-Based Controller, [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, and one possible way is to [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 the download center of our official website: <https://www.tp-link.com/support/download/>

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.





StatusWirelessManagementSystem

User AccountController SettingsTime SettingsReboot/ResetBackup & RestoreFirmware Update

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

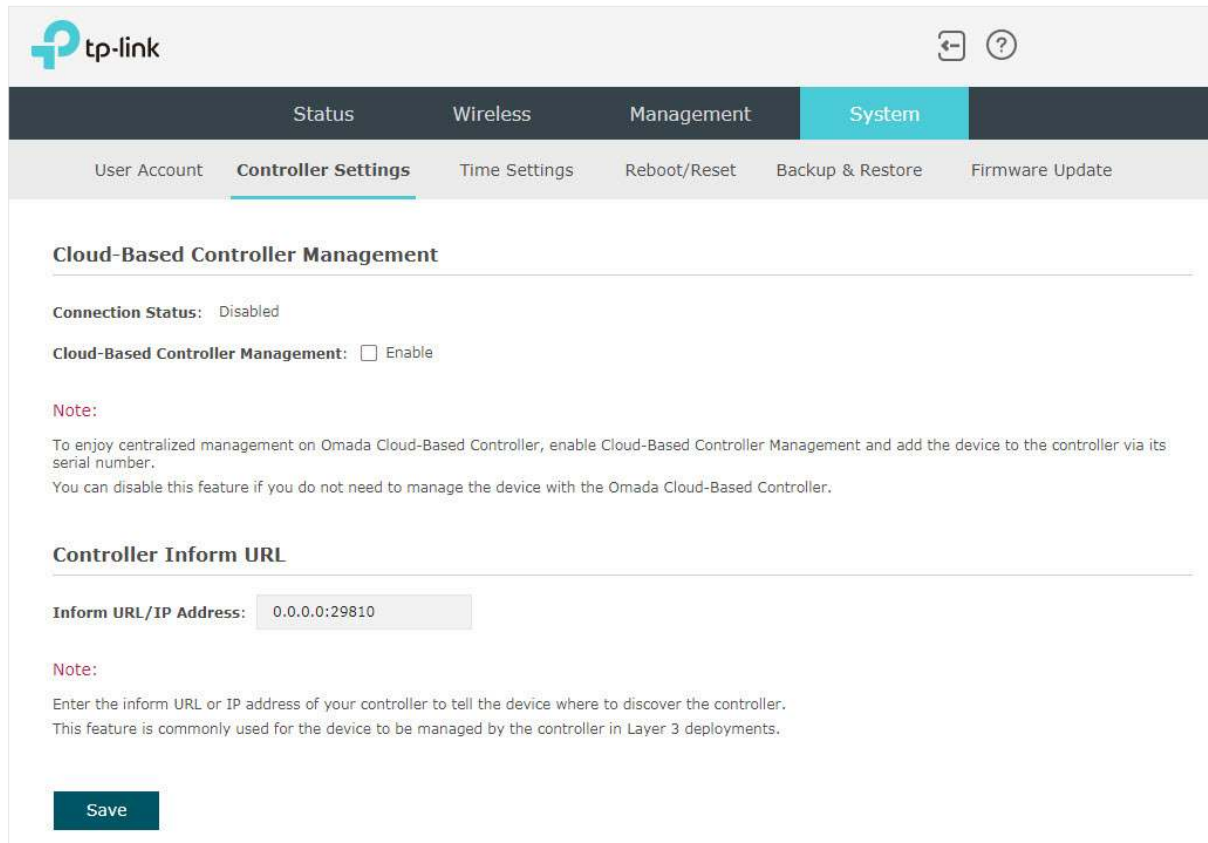
Inform URL/IP Address:

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

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.



The screenshot shows the TP-Link Omada web interface. At the top, the TP-Link logo is on the left, and navigation icons are on the right. Below the logo is a dark navigation bar with tabs: Status, Wireless, Management, and System (which is highlighted in teal). Under the System tab is a sub-navigation bar with links: User Account, Controller Settings (highlighted with a teal underline), Time Settings, Reboot/Reset, Backup & Restore, and Firmware Update.

The main content area is titled "Cloud-Based Controller Management" and contains the following information:

- 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.

Below this section is the "Controller Inform URL" section, which includes:

- Inform URL/IP Address:** A text input field containing the value "0.0.0.0:29810".
- 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.

At the bottom of the page is a dark teal button labeled "Save".

5.3 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.

The screenshot shows the TP-Link EAP web interface. At the top, the 'tp-link' logo is on the left, and 'Access Point' with a dropdown arrow, a refresh icon, and a help icon are on the right. Below this is a navigation bar with tabs: 'Network', 'Wireless', 'Monitoring', 'Management', and 'System' (which is highlighted in teal). Under the 'System' tab, there are sub-tabs: 'User Account', 'Time Settings' (which is underlined), 'Reboot/Reset', 'Backup & Restore', and 'Firmware Update'. The main content area is titled 'Time Settings'. It contains the following fields: 'Time zone:' with a dropdown menu showing '(GMT+08:00) Beijing, Hong Kong, Perth, Singapore'; 'Date:' with a text input '06/01/2024' and the format 'MM/DD/YYYY'; 'Time:' with three dropdown menus for hours (14), minutes (36), and seconds (21), followed by the format '(HH/MM/SS)'; 'Primary NTP Server:' with a text input and '(optional)' label; and 'Secondary NTP Server:' with a text input and '(optional)' label. Below these fields are two buttons: 'Get GMT' and 'Synchronize with PC'. A 'Save' button is located at the bottom right of this section. The second section is titled 'Daylight Saving'. It contains: 'Daylight Saving:' with an 'Enable' checkbox; 'Mode:' with three radio buttons: 'Predefined Mode' (selected), 'Recurring Mode', and 'Date Mode'; and 'Predefine Country:' with a dropdown menu showing 'European'. A 'Save' button is located at the bottom right of this section.

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

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*.

Time Settings

Time zone:

(GMT+08:00) Beijing, Hong Kong, Perth, Singapore

Date:

06/01/2024

MM/DD/YYYY

Time:

14

:

36

:

21

(HH/MM/SS)

Primary NTP Server:

(optional)

Secondary NTP Server:

(optional)

Get GMT

Synchronize with PC

Save

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.

Note:

If you use an NTP server on the internet, make sure that the gateway address is set correctly on the EAP. Otherwise, the EAP cannot get the system time from the NTP server successfully. To set the gateway address, refer to [2.1 Configure the Wireless Parameters](#).

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.

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.

Daylight Saving

Daylight Saving:

☐ Enable

Mode:

☒ Predefined Mode ☐ Recurring Mode ☐ Date Mode

Predefine Country:

European ▼

Save

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.

Mode:

☒ Predefined Mode ☐ Recurring Mode ☐ Date Mode

Predefine Country:

European ▼

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 screenshot shows the 'Recurring Mode' configuration interface. At the top, 'Mode:' is set to 'Recurring Mode' (selected with a radio button). Below it, 'Time Offset:' is set to '60 minutes (1-180)'. The 'Start:' field is configured as 'Last' day of the 'Sun' month of 'Mar' at '01:00'. The 'End:' field is configured as 'Last' day of the 'Sun' month of 'Oct' at '01:00'.

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

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 screenshot shows the 'Date Mode' configuration interface. At the top, 'Mode:' is set to 'Date Mode' (selected with a radio button). Below it, 'Time Offset:' is set to '60 minutes (1-180)'. The 'Start:' field is configured as '2024' year, 'Mar' month, '01' day at '01:00'. The 'End:' field is configured as '2024' year, 'Oct' month, '01' day at '01:00'.

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

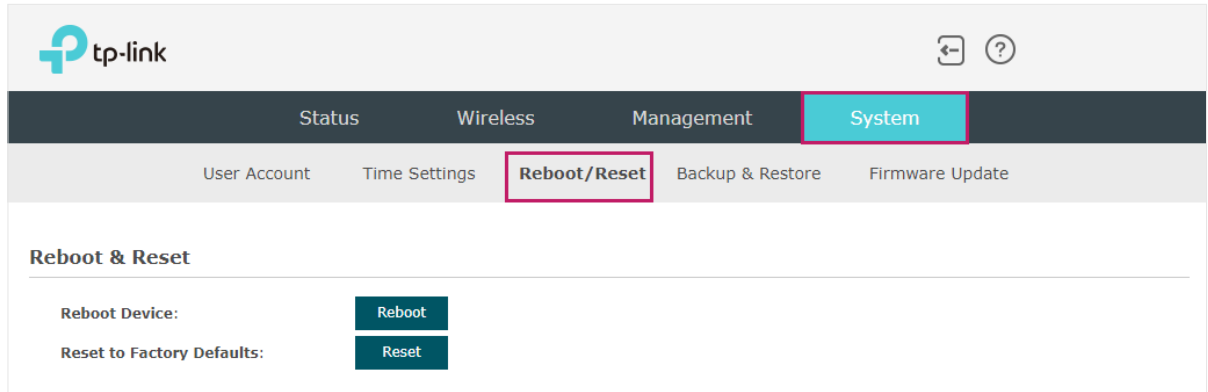
Time Offset	Specify the time to set the clock forward by.
Start	Specify the start time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).
End	Specify the end time of daylight saving time. The interval between the start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

4. Click **Save**.

5.4 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.



- 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.

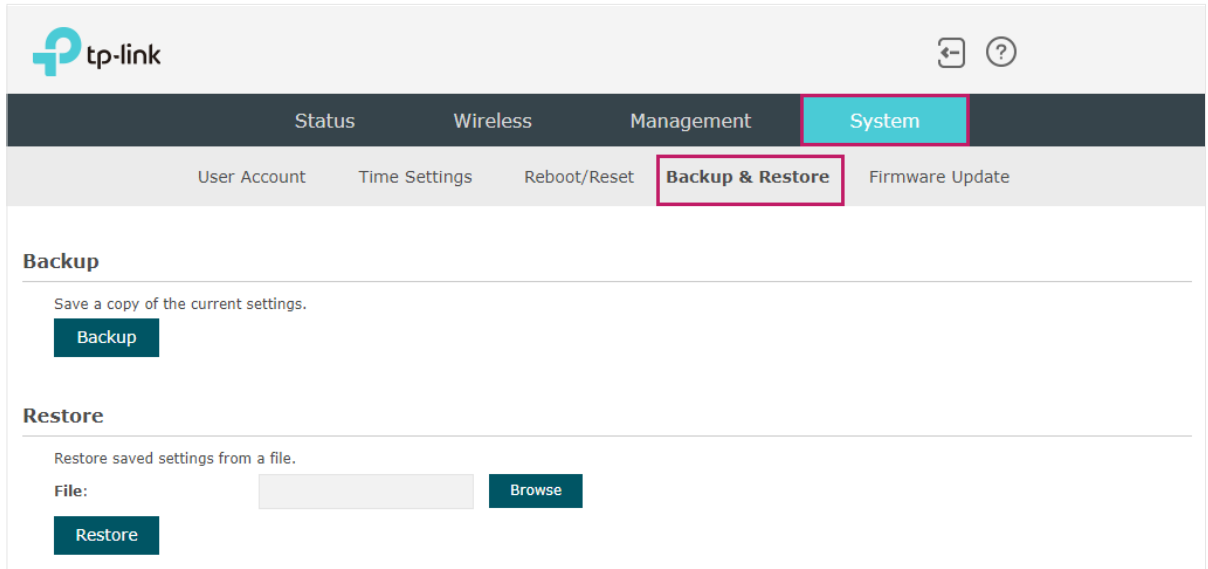
Note:

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.

5.5 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.



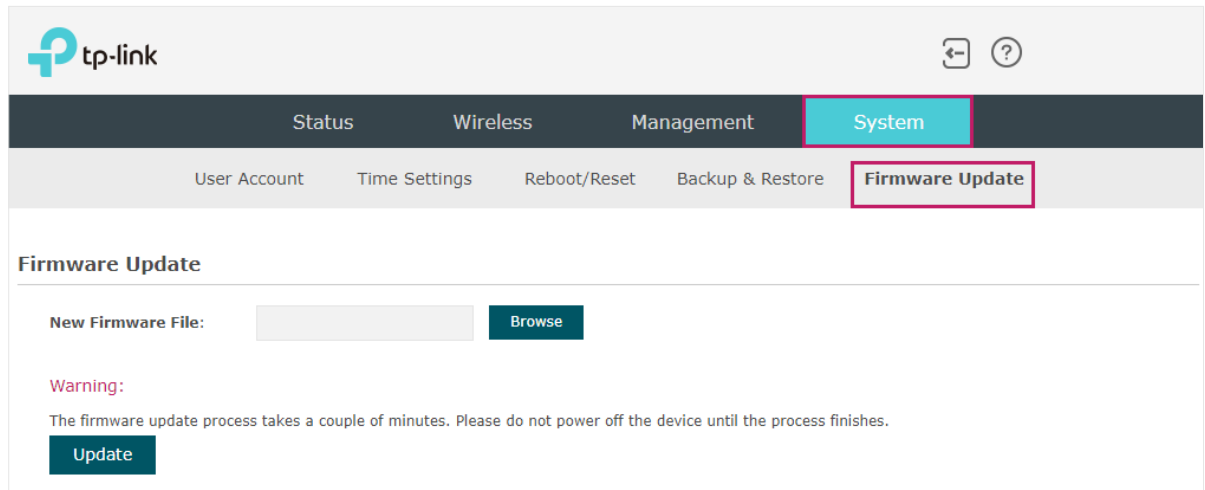
The screenshot shows the TP-Link web interface. At the top, the 'tp-link' logo is on the left, and navigation icons are on the right. Below the logo is a dark navigation bar with tabs: 'Status', 'Wireless', 'Management', 'System' (highlighted in teal), and an unlabeled tab. Under the 'System' tab is a sub-menu bar with 'User Account', 'Time Settings', 'Reboot/Reset', 'Backup & Restore' (highlighted with a red border), and 'Firmware Update'. The main content area is divided into two sections: 'Backup' and 'Restore'. The 'Backup' section has the text 'Save a copy of the current settings.' and a teal 'Backup' button. The 'Restore' section has the text 'Restore saved settings from a file.', a 'File:' label, a text input field, a teal 'Browse' button, and a teal 'Restore' button.

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

5.6 Update the Firmware

We occasionally 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.



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

1. Go to our website <https://www.tp-link.com> and search your EAP model. Download the proper firmware file on the support page of the EAP.
2. Click the button **Browse**, locate and choose the correct firmware file from your host.
3. Click the button **Update** 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.

6

Application Example

This chapter provides an application example about how to establish and manage a EAP wireless network:

A restaurant wants to provide the wireless internet access for the employees and guests. The restaurant now has a router, a switch, a dual-band EAP and a computer. Follow the steps below to establish the wireless network:

6.1 Determine the Network Requirements

6.2 Build the Network Topology

6.3 Log in to the EAP

6.4 Configure the EAP

6.5 Test the Network

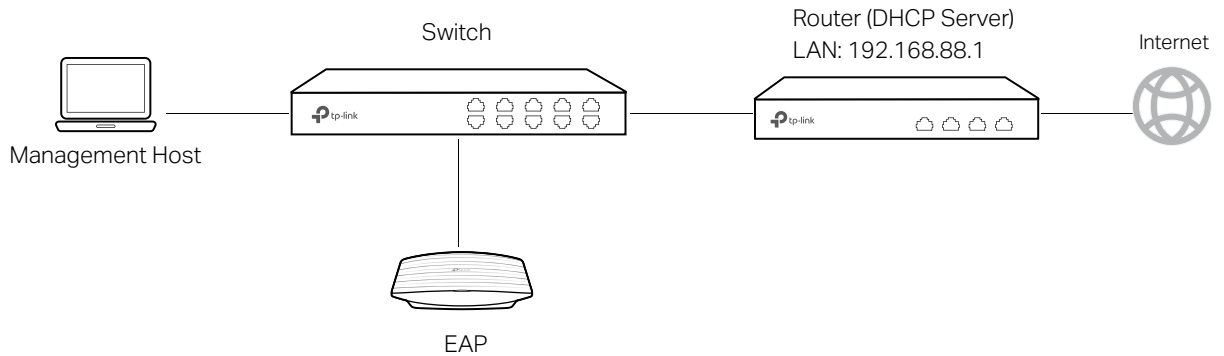
6.1 Determine the Network Requirements

Before starting to build the network, we need to first analyze and determine the network requirements. In this restaurant example, the network requirements are as follows:

- On both 2.4GHz and 5GHz bands, there are two SSIDs needed: one for the restaurant employees and one for the guests.
- In order to advertise the restaurant, the Portal feature needs to be configured on the SSIDs for the guests. In this way, the guests who have passed the portal authentication will be redirected to the restaurant's official website <http://www.restaurant1.com>.
- The employees of the restaurant can use the correct password to access the internet and do not need to pass the portal authentication. For security, the SSIDs for the employees should be encrypted with WPA2-PSK.
- To reduce power consumption, the Scheduler feature needs to be configured. The radio should operate only during the working time (9:00 am to 22:00 pm).

6.2 Build the Network Topology

Build the network topology as the following figure shows.



- The router is the gateway of the network and acts as a DHCP server to assign dynamic IP addresses to the management host, EAP and clients. The LAN IP of the router is 192.168.88.1/24.
- Connect the switch to the LAN port of the router.
- Connect the management host and the EAP to the switch. The IP address mode of the management host and EAP is dynamic, which means that they will get dynamic IP addresses from the router.

Tips:

If the router has more than one LAN port, we can also respectively connect the management host and the EAP to the LAN ports of the router.

6.3 Log in to the EAP

After building the network topology, follow the steps below to log in to the web page of the EAP:

1. On the management host, launch the web browser and enter "192.168.88.1" in the address bar. Then log in to the router and find the IP address of the EAP. As the following figure shows, the IP address of the EAP is 192.168.88.101.

LANDHCPDHCP ClientDHCP Reservation

List of DHCP Client

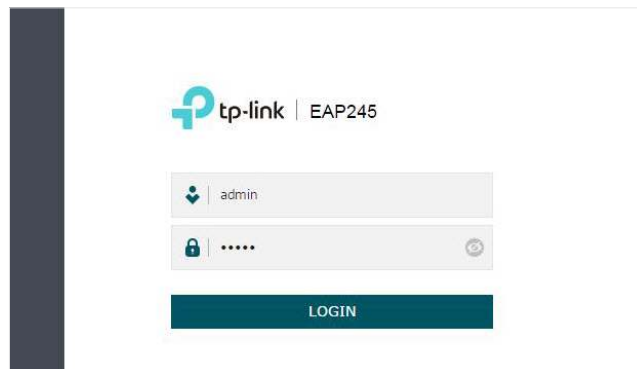
No.	Host Name	MAC Address	IP Address	Lease Time
1	EAP245-50-C7-BF	50-C7-BF-17-A6-E2	192.168.88.101	00:00:43
2	tplink2	F8-BC-12-9B-93-A4	192.168.88.100	00:00:58

Refresh

Search

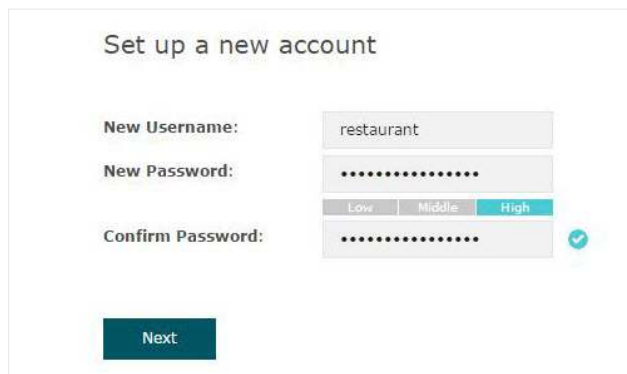
Help

2. Enter "192.168.88.101" in the address bar to load the login page of the EAP. Type the default username and password (both admin) in the two fields and click **LOGIN**.



The login page for the TP-Link EAP245 device. It features the TP-Link logo and the model name "EAP245". Below the logo, there are two input fields: one for the username, which already contains "admin", and one for the password, which contains six dots. A "LOGIN" button is positioned below the password field.

3. In the pop-up window, specify a new username and a new password for the user account. Click **Next**.



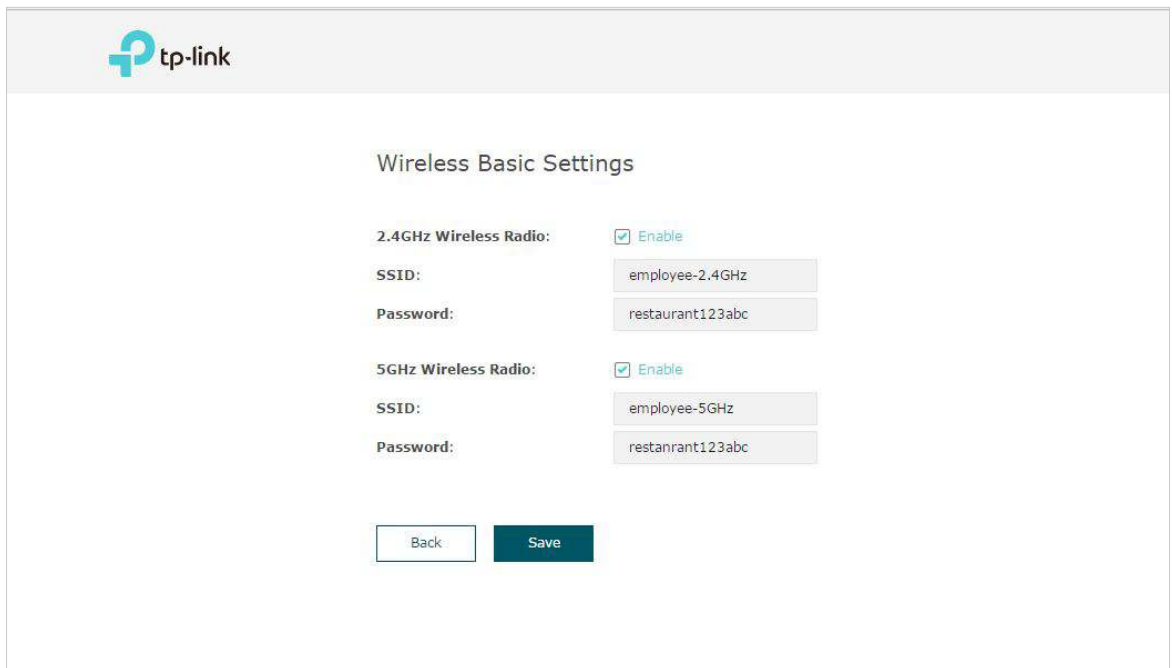
The "Set up a new account" page. It contains three input fields: "New Username:" with the value "restaurant", "New Password:" with ten dots, and "Confirm Password:" with ten dots. To the right of the password fields, there are three tabs: "Low", "Middle", and "High", with "High" selected. A green checkmark icon is visible to the right of the "Confirm Password" field. A "Next" button is located at the bottom left of the form.

6.4 Configure the EAP

To achieve the network requirements in this application example, we need to [Configure SSIDs](#), [Configure Portal Authentication](#) and [Configure Scheduler](#).

Configure SSIDs

1. After Logging in to EAP, follow the step-by-step instructions to complete the basic configurations of creating SSIDs. Configure the **SSID** as "employee_2.4GHz" and "employee_5GHz", specify the **Password** as "restaurant123abc". Click **Save**.



tp-link

Wireless Basic Settings

2.4GHz Wireless Radio: ☒ Enable

SSID: employee-2.4GHz

Password: restaurant123abc

5GHz Wireless Radio: ☒ Enable

SSID: employee-5GHz

Password: restaurant123abc

2. Go to the **Wireless > Wireless Settings** page. Create SSIDs for guests on 2.4GHz. Click  **Add** to add a new SSID.

2.4GHz SSIDs							 Add
ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action	
1	employee-2.4GHz	0	Enable	WPA-PSK	Disable	 	

3. The following page will appear. Configure this SSID as "guest_2.4GHz", keep the **Security Mode** as "None" and check the box to enable the **Portal** feature for this SSID. Click **OK**.

2.4GHz SSIDs

SSID:

guest-2.4GHz

SSID Broadcast:

☒ Enable

Security Mode:

None

Guest Network:

☐ Enable

Rate Limit:

☐ Enable

OK

Cancel

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
--	--	--	--	--	--	--
1	employee-2.4GHz	0	Enable	WPA-PSK	Disable	 

4. Click 2.4GHz 5GHz to enter the configuration page for the 5GHz band. Similarly to the configurations for the 2.4GHz band, configure another SSID for the guests on the 5GHz band.

Configure Portal Authentication

Follow the steps below to configure portal authentication:

1. Go to the **Wireless > Portal** page.

2. Configure the portal feature as the following figure shows.

The screenshot displays the TP-Link web interface for configuring the Portal feature. The top navigation bar includes 'Status', 'Wireless', 'Management', and 'System'. The 'Wireless' tab is active, and the 'Portal' sub-tab is selected. The 'Portal Configuration' section contains the following settings:

- SSID:** guest-2.4GHz, guest-5GHz
- Authentication Type:** Local Password
- Password:** restaurant123
- Authentication Timeout:** Custom (0 D, 2 H, 0 M)
- Redirect:** ☒ Enable
- Redirect URL:** http://restaurant1.com
- Portal Customization:** Local Web Portal

The 'Local Web Portal' preview shows a login page with the following elements:

- Welcome to XXX restaurant
- Password input field
- Term of Use section with a list of terms (1.xxxxxxx, 2.xxxxxxxxxx)
- ☒ I accept the Term of Use
- Login button

A 'Save' button is located at the bottom left of the configuration area.

- 1) Select the SSIDs for the guests on which the portal will take effect.
- 2) Select the **Authentication Type** as "Local Password" and specify the **Password** as "restaurant123".
- 3) Configure **Authentication Timeout**. Here we customize the timeout as 2 hours. It means that guests will be logged out after they have been authenticated for 2 hours. To continue to use the internet service, these guests need to enter the password to pass the portal authentication once again.
- 4) Check the box to enable **Redirect**, and enter the website of the restaurant: **http://www.restaurant1.com**.

- 5) Configure the authentication page. Specify the title and the term of use. To access the internet, guests need to enter the correct password in the **Password** field, accept the **Term of Use**, and click the **Login** button.

3. Click **Save**.

Configure Scheduler

Follow the steps below to schedule the radio to operate only during the working time (9:00 am to 22:00 pm).

1. Go to the **Wireless > Scheduler** page.
2. In the **Settings** section, check the box to enable **Scheduler**, and select the **Association Mode** as "Associated with AP". Click **Save**.

Settings

Scheduler: ☒ Enable

Association Mode: Associated with AP ▼

Save

3. In the **Scheduler Profile Configuration** section, click  **Create Profiles**.

Scheduler Profile Configuration

 Create Profiles

- 1) The following page will appear. Click  **Add a Profile** and specify the profile name as "worktime". Click **OK**.

Scheduler Profile Configuration

 Add a Profile

Profile Name	Modify
--	--

Profile:

Cancel OK

 Add an item

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

- 2) Choose the newly added profile "worktime", and click [+ Add an item](#). Then the item configuration page will appear. Specify the time range as everyday 9:00 to 22:00. Click **OK**.

Scheduler Profile Configuration

[+ Add a Profile](#)

Profile Name	Modify
worktime	

[+ Add an item](#)

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

Day:

☐ Weekday
 ☐ Weekend
 ☒ Every Day
 ☐ Custom

☒ Mon
 ☒ Tue
 ☒ Wed
 ☒ Thu
 ☒ Fri
 ☒ Sat
 ☒ Sun

Time: ☐ 24 hours

Start Time: 09 : 00

End Time: 22 : 00

4. In the **Scheduler Association** section, select "worktime" in the **Profile Name** column and select "Radio On" in the **Action** column. Click **Save**.

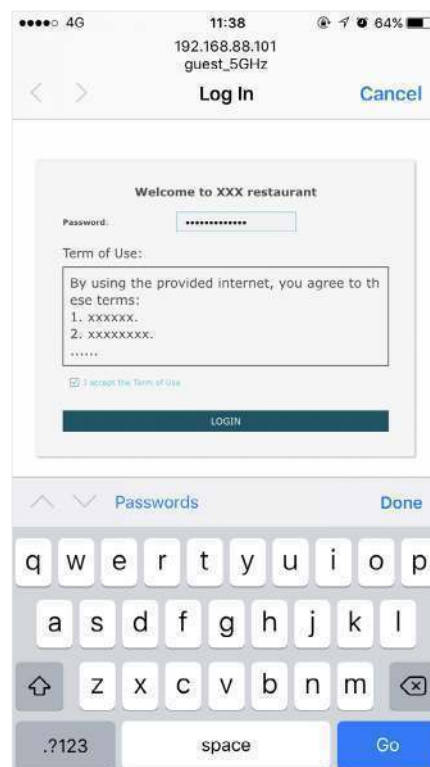
Scheduler Association

ID	AP	AP MAC	Profile Name	Action
1	EAP245-50-c7-bf-17-a6-e2	50-C7-BF-17-A6-E2	worktime	Radio On

6.5 Test the Network

To ensure that the employees and guests can surf the internet via the wireless network, we can use a client device, such as a telephone, to test whether the SSIDs are working normally.

- To test the SSIDs for the employees, follow the steps below:
 - 1) Enable the Wi-Fi feature of the client device.
 - 2) Choose the SSID "employee_2.4GHz" or "employee_5GHz" among the detected SSIDs.
 - 3) Enter the password "restaurant123abc" to join the wireless network.
 - 4) Check whether internet websites can be visited successfully.
- To test the SSIDs for the guests, follow the steps below:
 - 1) Enable the Wi-Fi feature of the client device.
 - 2) Choose the SSID "guest_2.4GHz" or "guest_5GHz" among the detected SSIDs.
 - 3) The default web browser on the device will pop up and the authentication page will appear. Enter the password "restaurant123", check the box to accept the term of use, and click the **LOGIN** button.



Tips:

Generally, the web browser pops up automatically. But if the web browser does not pop up, we can manually launch the web browser and visit any http website. Then the authentication page will appear.

- 4) If the network is working normally, we will be redirected to the website of the restaurant: <http://www.restaurant1.com>.

