



Omada

User Guide

For TP-Link Omada Access Points

1910013169 REV4.7.1

March 2022

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	21
2 Configure the Network.....	22
2.1 Configure the Wireless Parameters.....	23
2.1.1 Configure SSIDs	24
2.1.2 Configure Wireless Advanced Settings	30
Radio Setting.....	30
Load Balance.....	32
Airtime Fairness	32
More Settings	33
2.2 Configure Portal Authentication	35
Configure Portal.....	36
Configure Free Authentication Policy	42
2.3 Configure VLAN.....	45
2.4 Configure MAC Filtering	46
2.5 Configure Scheduler	49
2.6 Configure Band Steering.....	52
2.7 Configure QoS.....	54
2.8 Configure Rogue AP Detection.....	58
Detect Rogue APs and Move the Rogue APs to the Trusted AP List.....	59
Manage the Trusted AP List.....	60

3	Monitor the Network	62
3.1	Monitor the EAP	63
3.2	Monitor the Wireless Parameters.....	65
	Monitor the SSIDs.....	66
	Monitor the Radio Settings.....	67
	Monitor Radio Traffic	67
	Monitor LAN Traffic	68
3.3	Monitor the Clients	70
	View Client Information.....	70
	View Block Client Information	72
4	Manage the EAP	73
4.1	Manage the IP Address of the EAP	74
4.2	Manage System Logs	77
	View System Logs	77
	Configure the Way of Receiving Logs.....	78
4.3	Configure Web Server.....	80
4.4	Configure Management Access	81
	Configure Access MAC Management.....	81
	Configure Management VLAN	82
4.5	Configure LED	83
4.6	Configure Wi-Fi Control (Only for Certain Devices).....	84
4.7	Configure PoE Out (Only for Certain Devices)	85
4.8	Configure SSH.....	86
4.9	Configure SNMP	87
5	Configure the System.....	89
5.1	Configure the User Account	90
5.2	Controller Settings	91
	Enable Cloud-Based Controller Management	91
	Configure Controller Inform URL	93

5.3	Configure the System Time.....	94
	Configure the System Time	95
	Configure Daylight Saving Time	97
5.4	Reboot and Reset the EAP.....	99
5.5	Backup and Restore the Configuration.....	100
5.6	Update the Firmware	101
6	Application Example	102
6.1	Determine the Network Requirements	103
6.2	Build the Network Topology.....	104
6.3	Log in to the EAP	105
6.4	Configure the EAP	106
	Configure SSIDs	106
	Configure Portal Authentication.....	107
	Configure Scheduler.....	109
6.5	Test the Network.....	111

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.

Conventions

Unless otherwise noted, the introduction in this guide takes EAP245 as an example.

Wireless Speed, Range and Connected Devices Disclaimer

Maximum wireless transmission rates are the physical rates derived from IEEE Standard 802.11 specifications. Range and coverage specifications along with the number of connected devices were defined according to test results under normal usage conditions. Actual wireless transmission rate, wireless coverage, and number of connected devices 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.

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.

If you have any suggestions or needs on the product guides, welcome to email techwriter@tp-link.com.cn.

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 (OC200/OC300), 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 Webpage 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.

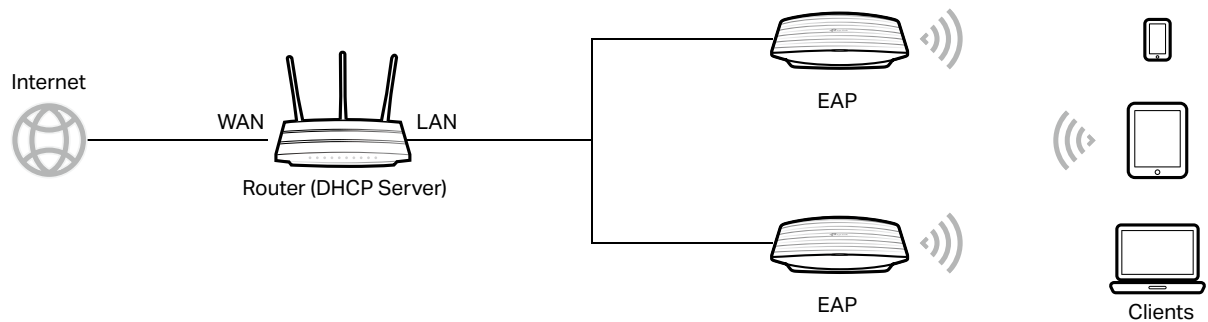
This chapter introduces how to start configuring the EAP in Standalone Mode.

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.



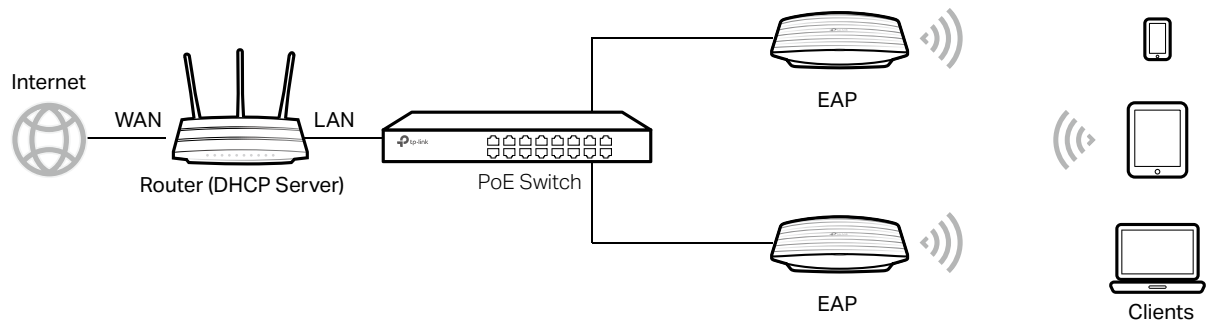
1. Connect the WAN port (or Internet port) of the router to the internet.
2. Connect your EAPs to the LAN port of the router.
3. Connect your wireless clients such as phones, tablets and laptops to the WiFi of the EAP. The default SSID is printed at the bottom of the EAP.



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.
- The dual-band EAP has two default SSIDs named **TP-Link_2.4GHz_XXXXXX** on the 2.4GHz band and **TP-Link_5GHz_XXXXXX** on the 5GHz band, and the single-band EAP has a default SSID named **TP-Link_2.4GHz_XXXXXX** on the 2.4GHz band.

1.3 Log in to the EAP and Change the SSID

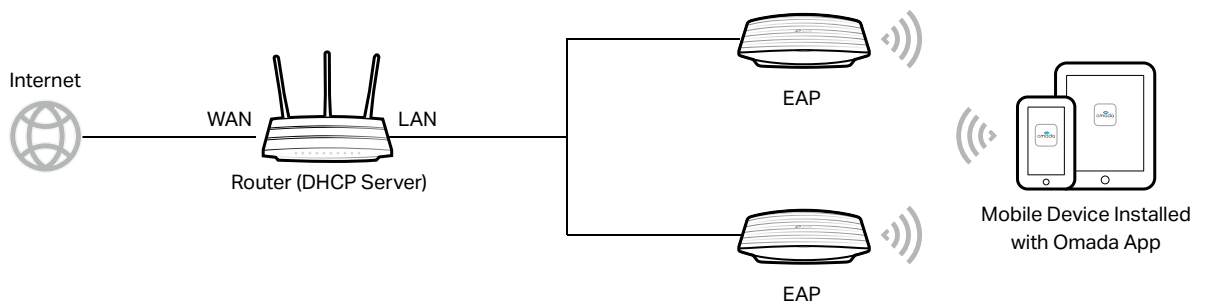
By default, anyone can connect to the WiFi of EAP without authentication, because the default SSID has no password. For security purposes, we recommend changing the default SSID.

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. To install Omada App, launch the Apple App Store (iOS) or Google Play store (Android) and search "TP-Link Omada" or simply scan the QR code to download and install the app.



2. Connect your mobile device to the WiFi of the EAP. The default SSID is printed at the bottom of the EAP.



3. Launch the Omada app, tap **Standalone APs** and wait for the EAP to be discovered.



Tips:

All the EAPs in the same subnet will be discovered by Omada app and shown on the page.

4. Tap on the EAP appearing on the page. Set a new username and password for your login account of the EAP.



The screenshot shows a mobile app interface for EAP setup. At the top, there's a status bar with 'No SIM', signal strength, time '3:20 PM', and battery level. Below the status bar is a navigation bar with a back arrow on the left and a 'Next' button on the right. The main title is 'Setup'. Below the title is a subtitle: 'Set a new username and password for the EAP.' There are two input fields: 'Username' with the text 'user' and 'Password' with masked characters '*****'. A 'Next' button is located to the right of the password field.

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



The screenshot shows a mobile app interface for wireless settings. At the top, there's a status bar with 'No SIM', signal strength, time '3:04 PM', and battery level '41%'. Below the status bar is a navigation bar with a back arrow on the left and a 'Next' button on the right. The main title is 'Wireless Settings'. There are two sections: '2.4GHz Network' and '5GHz Network'. The '2.4GHz Network' section has fields for 'SSID' (TP-Link_test) and 'Password' (tplink123). A note below the password field says 'Password should contain at least 8 characters.' The '5GHz Network' section has a checked checkbox for 'Copy 2.4GHz Network', and fields for 'SSID' (TP-Link_test-5G) and 'Password' (tplink123).

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

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

Next

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

Now join your new wireless network.

2.4GHz Network

SSID
TP-Link_test

Join


Password
tplink123

5GHz Network

SSID
TP-Link_test-5G

Join

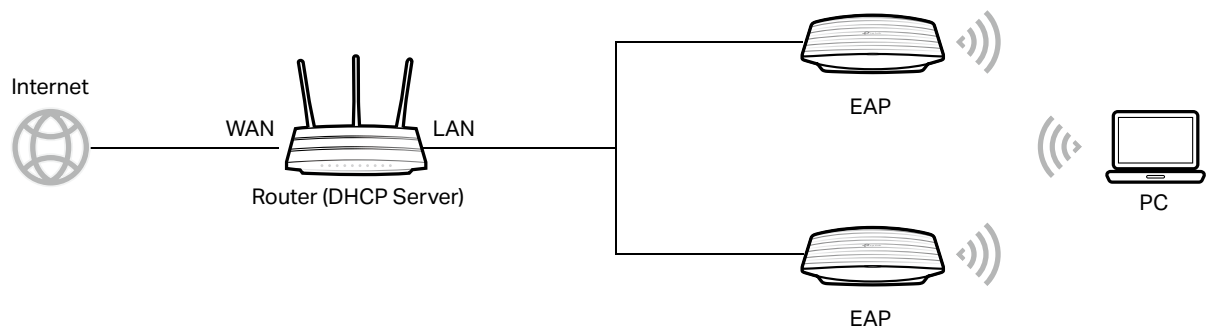
Password
tplink123

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



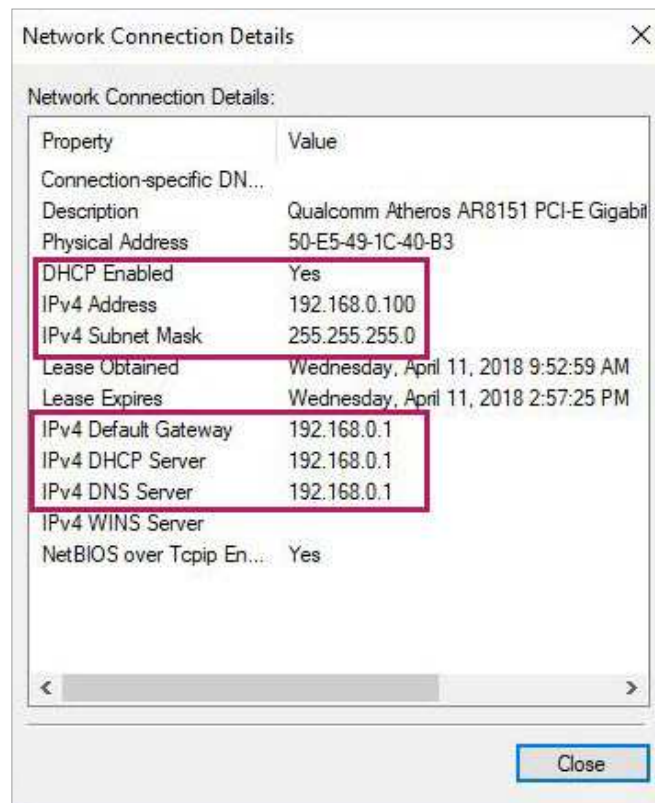
1. Set your PC to obtain an IP address automatically.



2. Connect your PC to the WiFi of the EAP. The default SSID is printed at the bottom of the EAP.



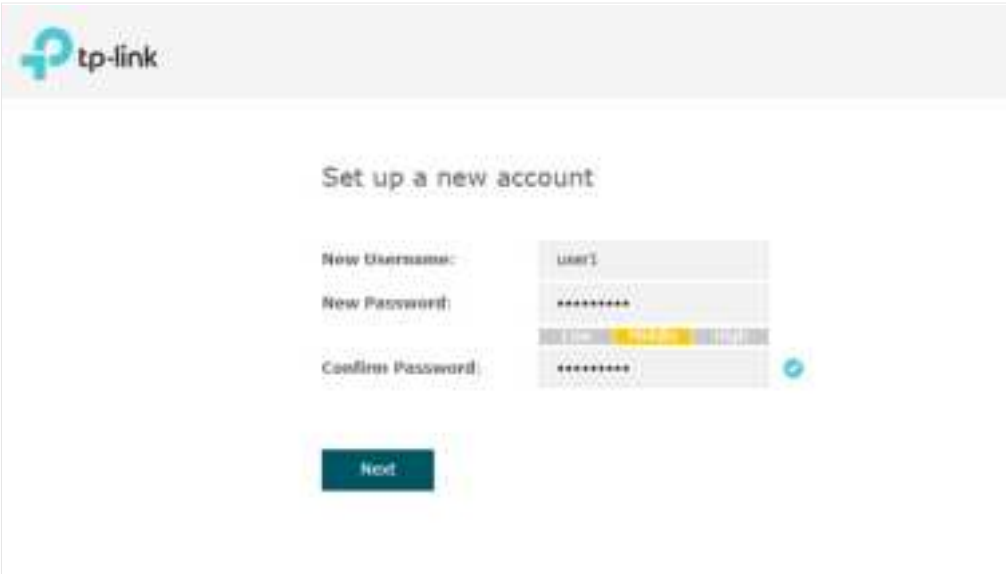
3. Make sure that your PC has got the IP address, default gateway, and DNS server from the DHCP server.



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

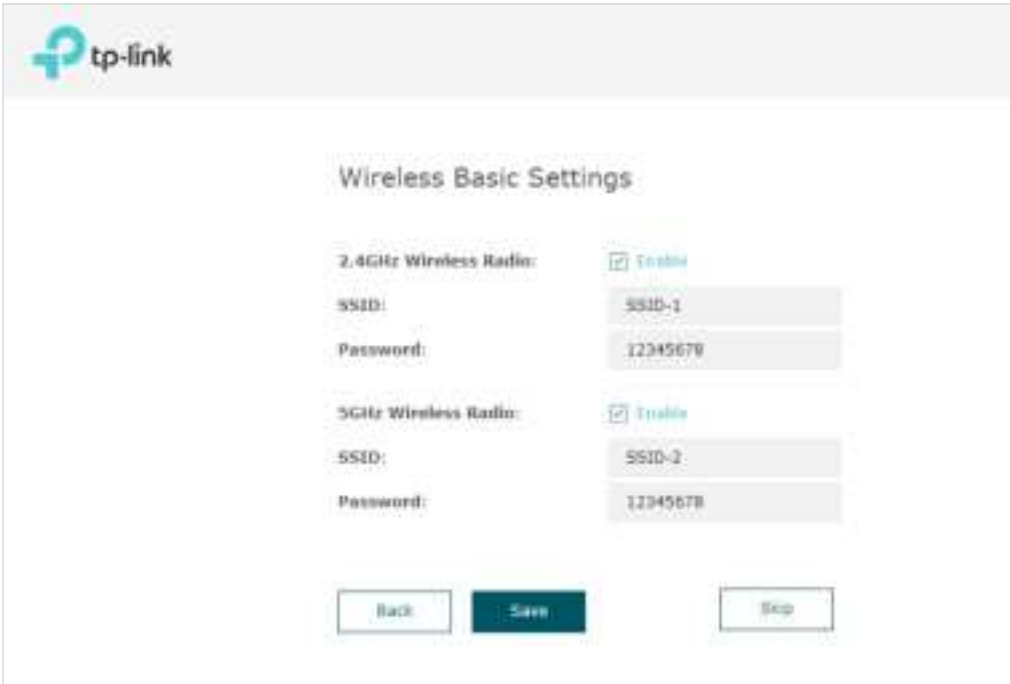


The screenshot shows the 'Set up a new account' page in the TP-Link EAP interface. The page has a light gray header with the TP-Link logo. The main content area is white and contains the following fields:

- New Username:** A text input field with the value 'user1'.
- New Password:** A password input field with a strength indicator bar below it showing a mix of yellow and green segments.
- Confirm Password:** A password input field with a blue checkmark icon to its right, indicating the passwords match.

At the bottom of the form is a dark teal button labeled 'Next'.

6. Configure the SSID and password. For the dual-band EAP, you can configure the SSID and password for both 2.4GHz and 5GHz. Click **Save**.



The screenshot shows the 'Wireless Basic Settings' page in the TP-Link EAP interface. The page has a light gray header with the TP-Link logo. The main content area is white and contains the following settings:

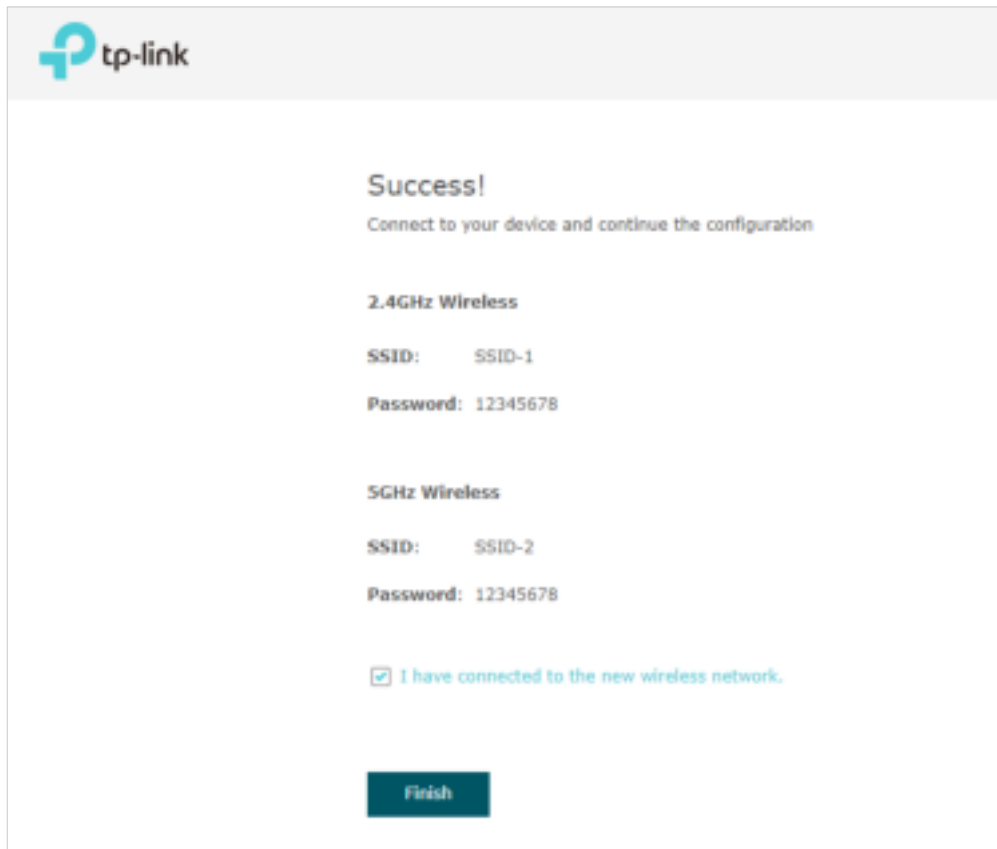
- 2.4GHz Wireless Radio:** A checkbox labeled 'Enable' is checked.
- SSID:** A text input field with the value 'SSID-1'.
- Password:** A password input field with the value '12345678'.
- 5GHz Wireless Radio:** A checkbox labeled 'Enable' is checked.
- SSID:** A text input field with the value 'SSID-2'.
- Password:** A password input field with the value '12345678'.

At the bottom of the page are three buttons: 'Back', 'Save' (dark teal), and 'Skip'.

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](#).

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



The image shows a TP-Link router configuration page. 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 networks. 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 labeled "I have connected to the new wireless network." which is checked. Below the checkbox is a dark blue button labeled "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.

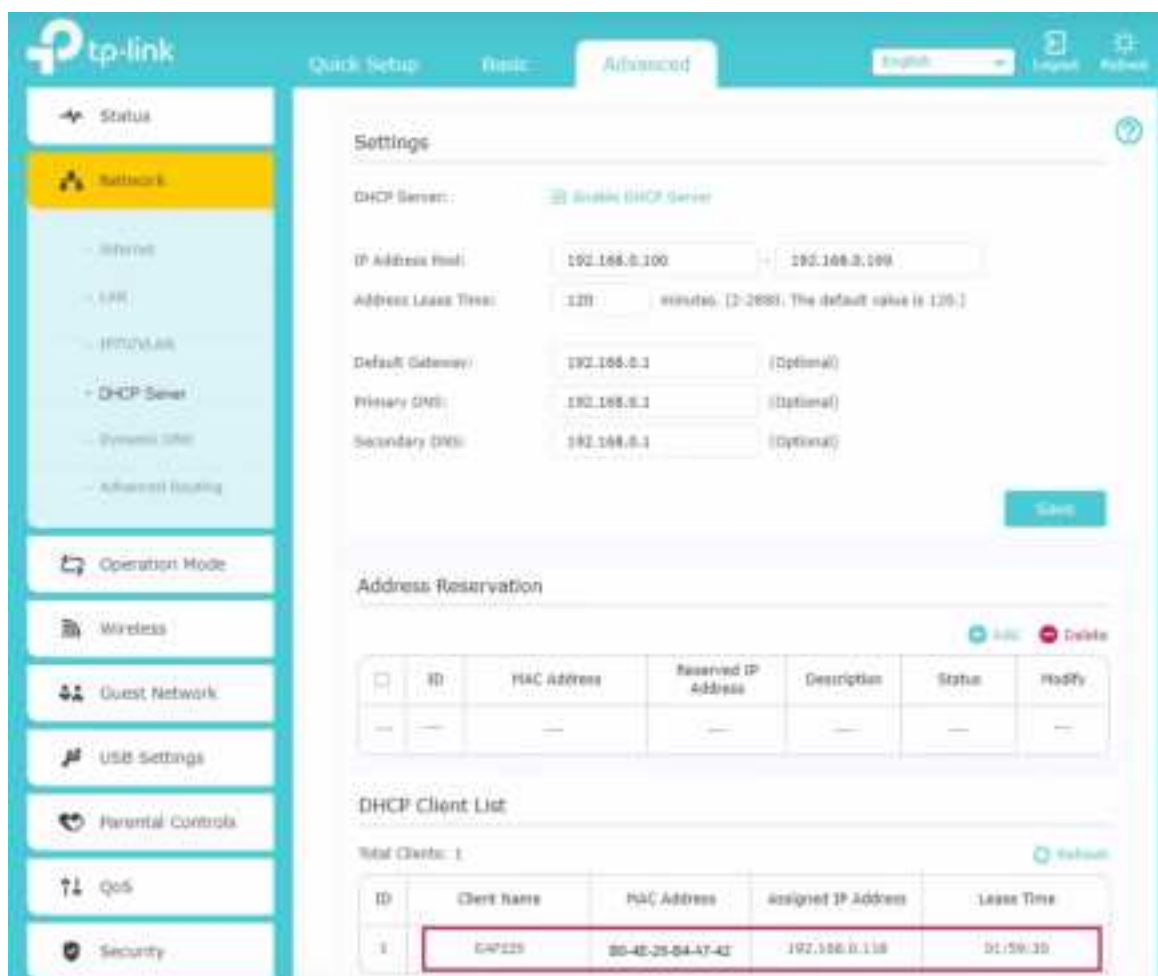
■ Using Web Browser on Your PC and Connecting to the Ethernet

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.



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**.



The screenshot shows a window titled "Discovering EAPs...". At the top, there is a search bar labeled "MAC, IP, Status:". Below it is a table with the following columns: "Select", "MAC Address", "IP Address", "Model", "Version", "Status", and "Action". The table contains one row with the following data: "50:c7:af:17:a6:e2" for MAC Address, "192.168.0.5" for IP Address, "EAP245" for Model, "1.0.1 Build 20170414 R..." for Version, and "Pending" for Status. The "Action" column has a "Manage" button. At the bottom left, it says "Displayed EAP : 1". At the bottom right, there are two buttons: "Select All" and "Batch Setting".

Select	MAC Address	IP Address	Model	Version	Status	Action
<input type="checkbox"/>	50:c7:af:17:a6:e2	192.168.0.5	EAP245	1.0.1 Build 20170414 R...	Pending	Manage

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.

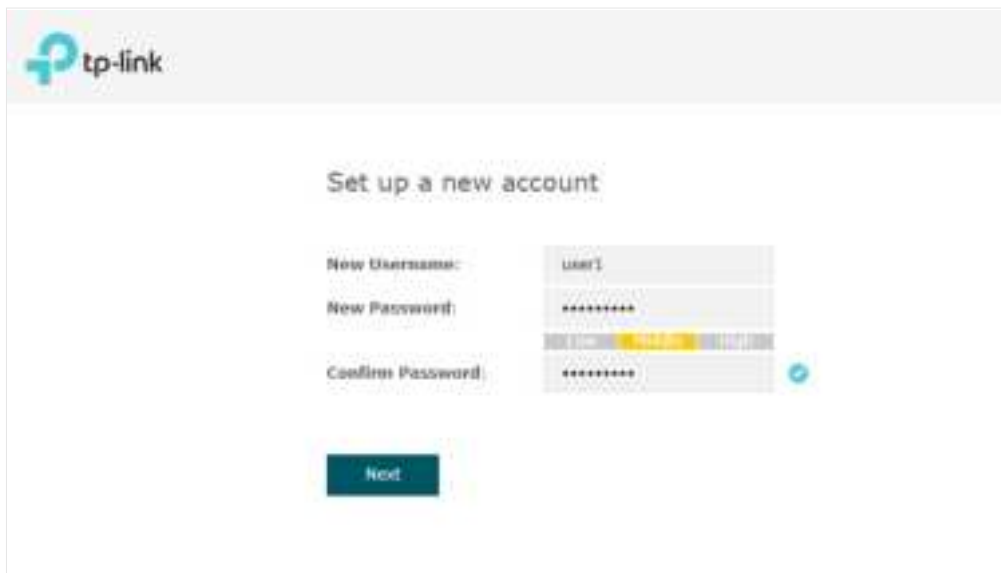
2. To log in to the EAP, launch a web browser and enter the IP address of the EAP in the address bar. The login page will appear. By default, both the username and password are **admin**.



Tips:

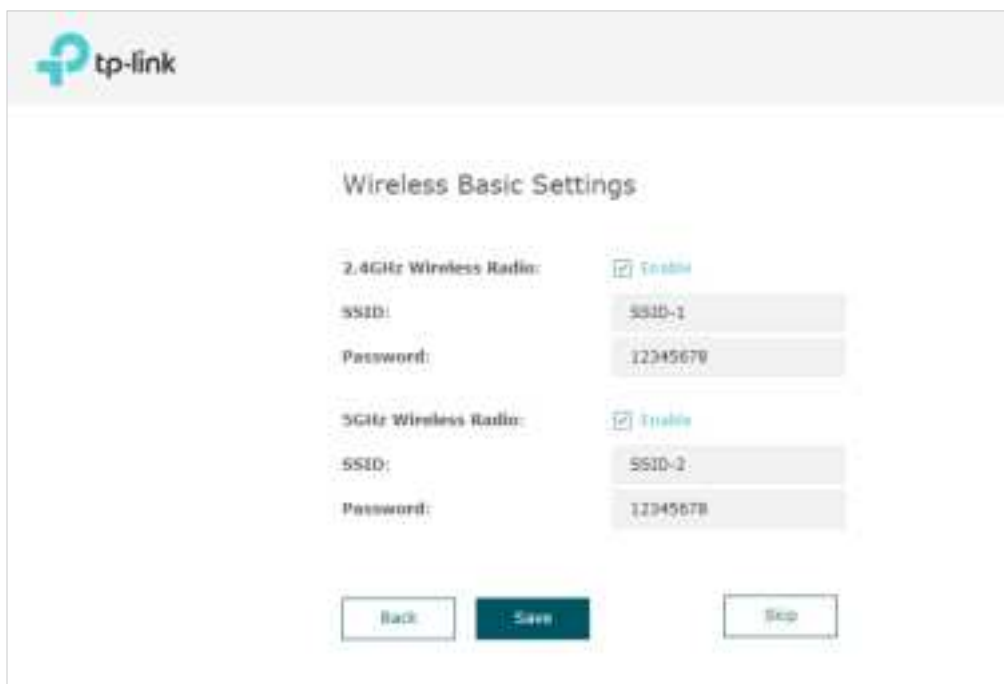
To facilitate access to the EAP, you can set a static IP address for the EAP and remember it well or write it down. But make sure that this IP address is not being used by other devices in the same LAN. For detailed instructions about how to set a static IP address for the EAP, refer to [4.1 Manage the IP Address of the EAP](#).

3. After logging in to the EAP, follow the step-by-step instructions to complete the basic configurations. In the pop-up window, configure a new username and a new password for your user account, then click **Next**.



The image shows a TP-Link web interface for setting up a new account. The header features 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 blue checkmark icon is visible next to the "Confirm Password" field. At the bottom, there is a dark blue button labeled "Next".

4. Configure the SSID and password. For the dual-band EAP, you can configure the SSID and password for both 2.4GHz and 5GHz. Click **Save**.

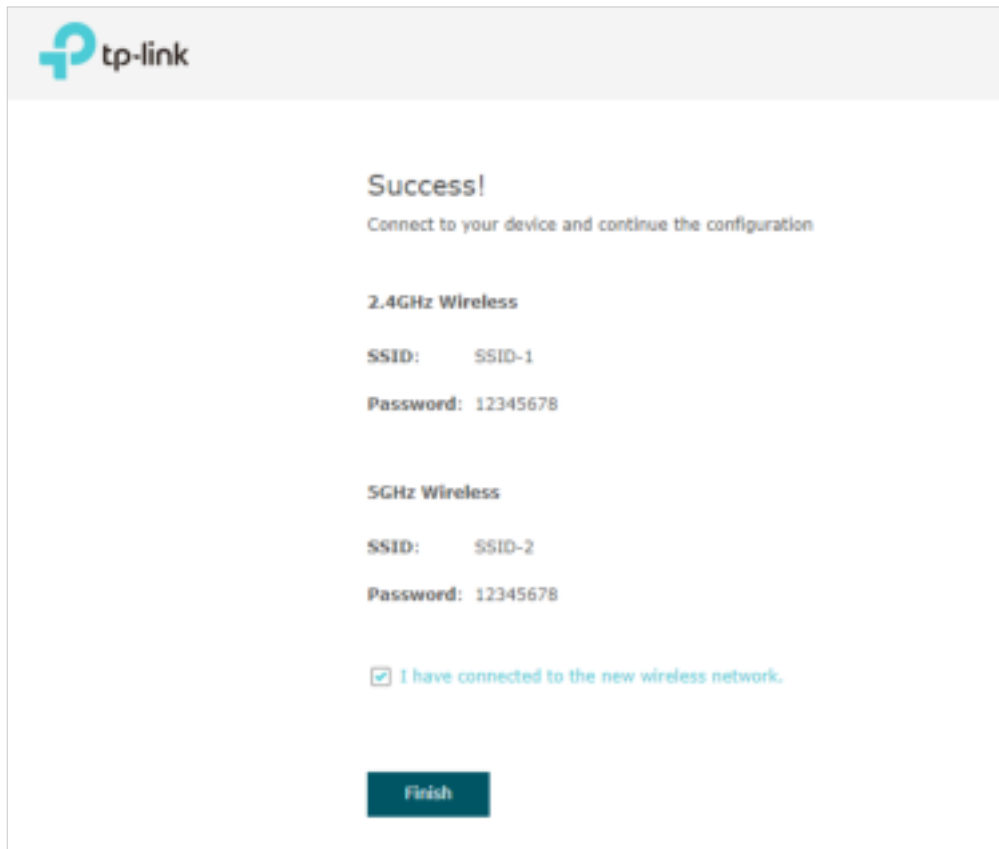


The image shows a TP-Link web interface for configuring wireless settings. The header features the TP-Link logo. The main heading is "Wireless Basic Settings". Below this, there are two sections for configuring wireless radios. The first section is for the "2.4GHz Wireless Radio", which is checked as "Enabled". It has an "SSID:" field with the value "SSID-1" and a "Password:" field with the value "12345678". The second section is for the "5GHz Wireless Radio", which is also checked as "Enabled". It has an "SSID:" field with the value "SSID-2" and a "Password:" field with the value "12345678". At the bottom, there are three buttons: "Back", "Save", and "Skip".

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](#).

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



The image shows a TP-Link web interface for configuring a wireless network. 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 networks. 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 labeled "I have connected to the new wireless network." which is checked. Below the checkbox is a dark blue button labeled "Finish".

tp-link

Success!
Connect to your device and continue the configuration

2.4GHz Wireless
SSID: SSID-1
Password: 12345678

5GHz Wireless
SSID: SSID-2
Password: 12345678

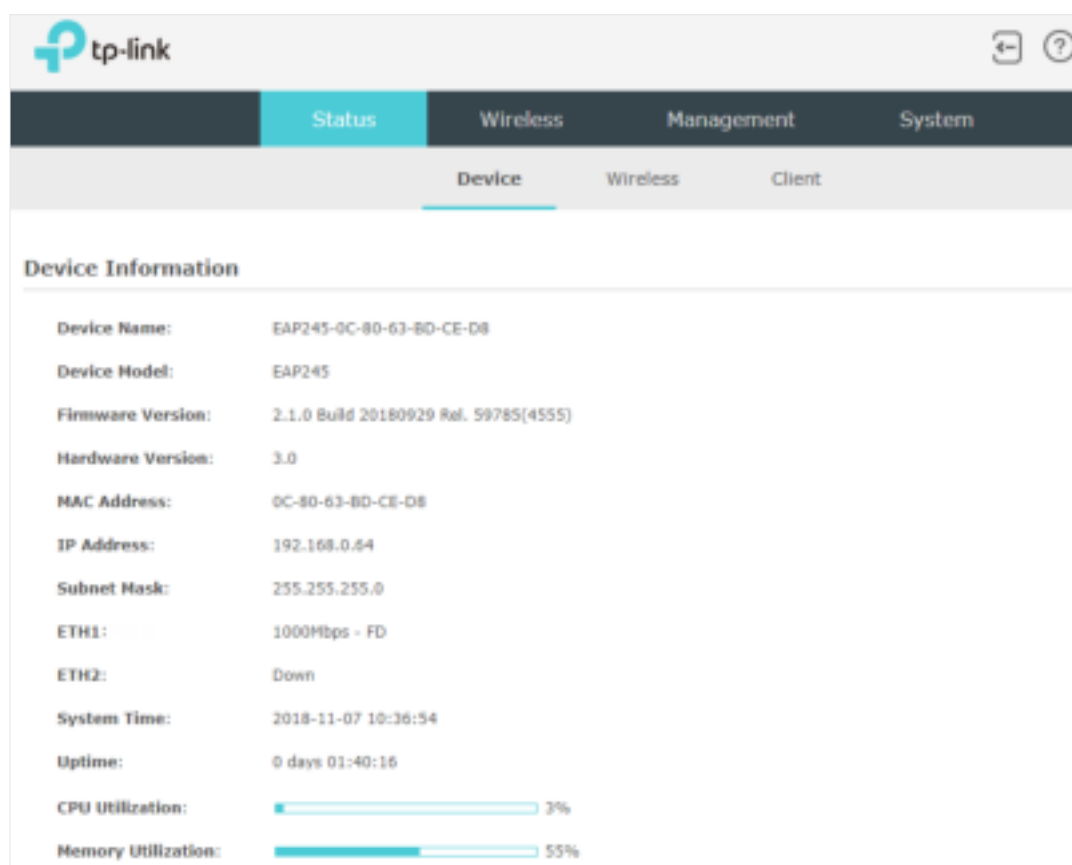
☒ I have connected to the new wireless network.



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*

2.1 Configure the Wireless Parameters

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

The screenshot shows the TP-Link web interface for configuring wireless settings. The top navigation bar includes 'Status', 'Wireless' (highlighted), 'Management', and 'System'. Below this, a sub-menu bar contains 'Wireless Settings' (highlighted with a red box), 'Portal', 'VLAN', 'MAC Filtering', 'Scheduler', 'Band Steering', 'QoS', and 'Rogue AP Detection'. The main content area is for '2.4GHz Wireless Radio' and '2.4GHz SSIDs'.

2.4GHz Wireless Radio

2.4GHz Wireless Radio: ☒ Enable

2.4GHz SSIDs

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

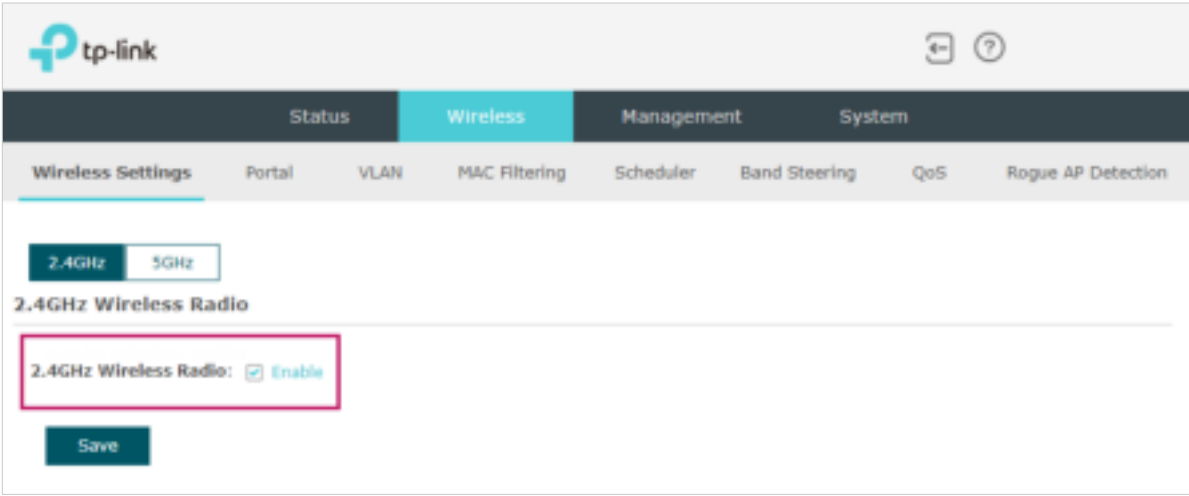
Tx Power(EIRP): -20 dBm(9-20)

Note:
The EIRP transmit power includes the antenna gain.

Save

For a dual-band EAP, there are two bands: 2.4GHz and 5GHz. The wireless parameters are separately set on each band. You can click to select a band and configure the wireless parameters on this band.

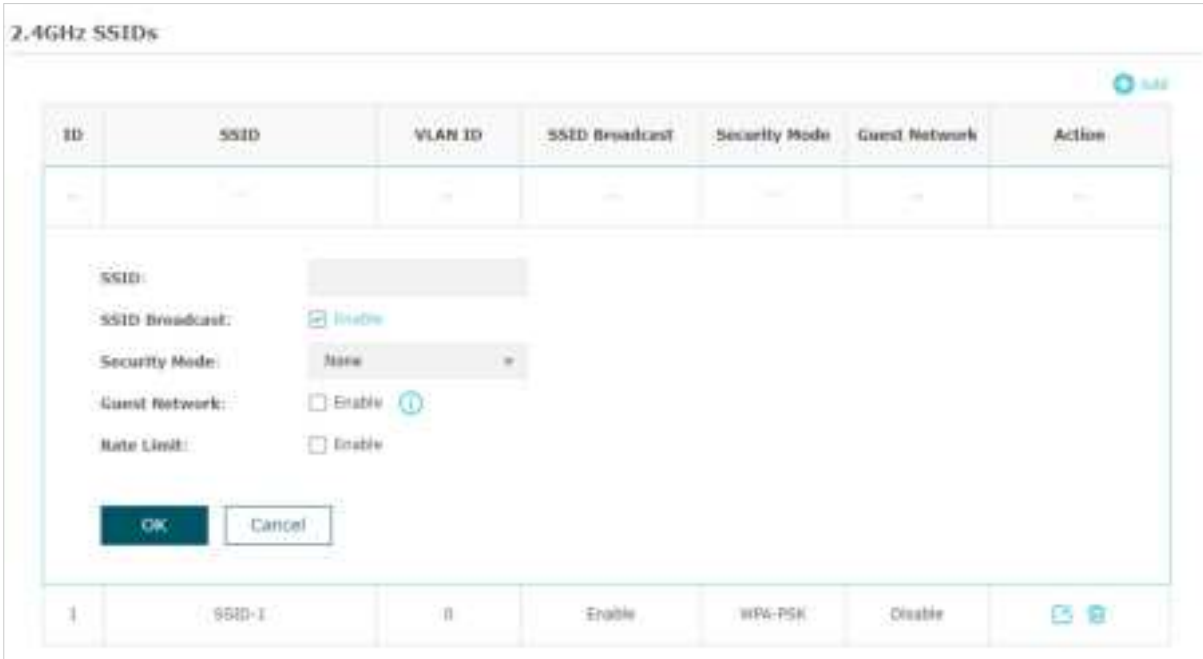
Before configuring the wireless parameters on each band, check the box to enable 2.4GHz or 5GHz Wireless Radio. Only when this option is enabled will the wireless radio on 2.4GHz or 5GHz band works.






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.



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

1. If your EAP is a dual-band device, click   to choose a frequency band on which the new SSID will be created.
2. Click  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/ WPA-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](#) and [WPA-Personal](#).

• WEP

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 window for WEP. The 'Security Mode' is set to 'WEP'. Under 'Type', 'Auto' is selected. 'Key Selected' is set to 'Key1'. Under 'Wep Key Format', 'ASCII' is selected. Under 'Key Type', '64-bit' is selected. The 'Key Value' field contains the text 'weppw'.

The following table detailedly introduces how to configure each item:

Type	<p>Select the authentication type for WEP.</p> <p>Auto: The EAP can select Open System or Shared Key automatically based on the wireless capability and request of the clients.</p> <p>Open System: Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission.</p> <p>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.</p>
Key Selected	Select one key to specify. You can configure four keys at most.
WEP Key Format	<p>Select ASCII or Hexadecimal as the WEP key format.</p> <p>ASCII: With this format selected, the WEP key can be any combination of keyboard characters of the specified length.</p> <p>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.</p>
Key Type	<p>Select the WEP key length for encryption.</p> <p>64Bit: Enter 10 hexadecimal digits or 5 ASCII characters.</p> <p>128Bit: Enter 26 hexadecimal digits or 13 ASCII characters.</p> <p>152Bit: Enter 32 hexadecimal digits or 16 ASCII characters.</p>

Key Value	Enter the WEP keys. The length and valid characters are determined by the key format and key type.
-----------	--

• WPA-Enterprise

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

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	<p>Select the Encryption type. Note that some encryption type is only available under certain circumstances.</p> <p>Auto: The default setting is Auto and the EAP will select TKIP or AES automatically based on the client device's request.</p> <p>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.</p> <p>AES: Advanced Encryption Standard. It is securer than TKIP.</p>
RADIUS Server IP	Enter the IP address of the RADIUS Server.
RADIUS Port	Enter the port number of the RADIUS Server.
RADIUS Password	Enter the shared secret key of the RADIUS server.
RADIUS Accounting	Enable or disable RADIUS accounting feature.
Accounting Server IP	Enter the IP address of the accounting server.
Accounting Server Port	Enter the port number of the accounting server.
Accounting Server Password	Enter the shared secret key of the accounting server.
Interim Update	<p>With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled.</p> <p>Enter the appropriate duration between updates for EAPs in Interim Update Interval.</p>
Interim Update Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the EAP should change the encryption key. 0 means that the encryption key does not change at anytime.

- **WPA-Personal**

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

The screenshot shows a configuration window for WPA-Personal security. The 'Security Mode' is set to 'WPA-Personal'. The 'Version' is set to 'WPA/WPA2-PSK'. Under 'Encryption', the 'Auto' radio button is selected, with 'TKIP' and 'AES' as options. The 'Wireless Password' field contains '12345678'. The 'Group Key Update Period' is set to '0' seconds, with a note that '0 means no update.' The 'Guest Network' and 'Rate Limit' options are both unchecked. 'OK' and 'Cancel' buttons are 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	<p>Select the Encryption type. Note that some encryption type is only available under certain circumstances.</p> <p>Auto: The default setting is Auto and the EAP will select TKIP or AES automatically based on the client device's request.</p> <p>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.</p> <p>AES: Advanced Encryption Standard. It is securer than TKIP.</p>
Wireless Password	<p>Configure the wireless password with ASCII characters.</p> <ul style="list-style-type: none"> • For ASCII, the length should be between 8 and 63 and the valid characters contain numbers, letters (case-sensitive) and common punctuations.
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the EAP should change the encryption key. 0 means that the encryption key does not change at anytime.

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.

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(0-20)

Note:
The EIRP transmit power includes the antenna gain.

Save

Select the frequency band (2.4GHz/5GHz) and configure the following parameters.

Wireless Mode

Select the IEEE 802.11 mode the radio uses.

- For 2.4GHz:

802.11b/g/n/ax mixed: All of 802.11b, 802.11g, 802.11n, and 802.11ax clients operating in the 2.4GHz frequency can connect to the EAP. Note that 802.11ax is only available for certain devices.

802.11b/g/n mixed: All of 802.11b, 802.11g, and 802.11n clients operating in the 2.4GHz frequency can connect to the EAP.

802.11b/g mixed: Both 802.11b and 802.11g clients can connect to the EAP.

802.11n only: Only 802.11n clients can connect to the EAP.

- For 5GHz:

802.11a/n/ac/ax mixed: All of 802.11a, 802.11n, 802.11ac, and 802.11ax clients operating in the 5GHz frequency can connect to the EAP. Note that 802.11ax is only available for certain devices.

802.11a/n/ac mixed: All of 802.11a, 802.11n, and 802.11ac clients operating in the 5GHz frequency can connect to the EAP.

802.11n/ac mixed: Both 802.11n clients and 802.11ac clients operating in the 5GHz frequency can connect to the EAP.

802.11ac only: Only 802.11ac clients can connect to the EAP.

Channel Width

Select the channel width of the EAP. The available options differ among different EAPs.

For some EAPs, available options include **20MHz**, **40MHz** and **Auto**.

For some EAPs, available options include **20MHz**, **40MHz**, **80MHz** and **Auto**.

For other EAPs, available options include **20MHz**, **40MHz**, **80MHz**, **160MHz** and **Auto**.

When the radio mode includes 802.11n, we recommend you set the channel bandwidth to 20/40 MHz or 20/40/80MHz 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	<p>Check the box to enable the Channel Limit function. With this function enabled, the wireless frequency 5150MHz~5350MHz will be disabled. This function can influence the available options in Channel.</p> <p>This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.</p>
Channel	<p>Select the channel used by the EAP. For example, 1/2412MHz means that the channel is 1 and the frequency is 2412MHz.</p> <p>By default, the channel is automatically selected, and we recommend that you keep the default setting.</p>
Tx Power (EIRP)	<p>Specify the transmit power value.</p> <p>If this value is set to be larger than the maximum transmit power that is allowed by the local regulation, the regulated maximum transmit power will be applied in the actual situation.</p> <p>Note: In most cases, it is unnecessary to use the maximum transmit power. Specifying a larger transmit power than needed may cause interference to the neighborhood. Also it consumes more power and reduces longevity of the device.</p>

Load Balance

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

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

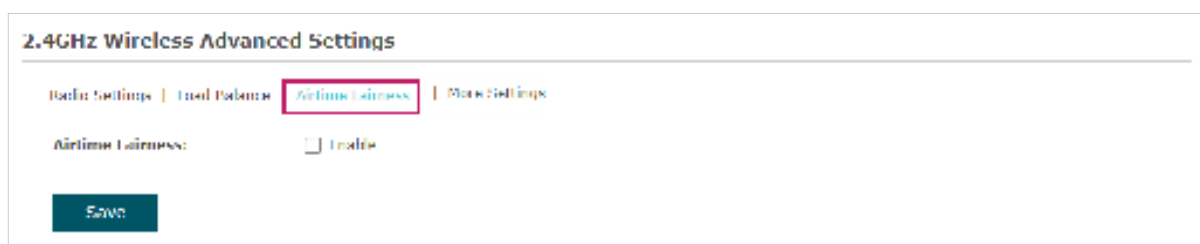
Note:

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.



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. The advanced wireless parameters consist of Beacon Interval, DTIM Period, RTS Threshold, Fragmentation Threshold, and OFDMA.

The screenshot shows the '2.4GHz Wireless Advanced Settings' page. At the top, there are tabs for 'Radio Settings', 'Load Balance', 'Airtime fairness', and 'More Settings' (which is highlighted with a red box). Below the tabs, the settings are as follows:

Setting	Value	Range/Options
Beacon Interval	100	ms (40-100)
DTIM Period	1	(1-255)
RTS Threshold	2347	(1-2347)
Fragmentation Threshold	2346	(256-2346. This works only in 11b/g mode.)
OFDMA	<input type="checkbox"/> Enable	

Below the settings, there is a 'Note:' section stating: 'OFDMA enables multiple users to transmit data simultaneously, and thus greatly improves speed and efficiency. Note: that only when your clients also support OFDMA, can you fully enjoy the benefits.'

At the bottom left, there is a 'Save' button.

The following table introduces how to configure each item:

Beacon Interval	<p>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.</p> <p>You can specify a value between 40 and 100ms. The default is 100ms.</p>
DTIM Period	<p>The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the EAP has buffered data for client devices. The DTIM Period indicates how often the clients served by this EAP should check for buffered data still on the EAP awaiting pickup.</p> <p>You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating that clients check for buffered data at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend you keep the default value.</p>

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

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.

Portal Configuration

SSID: -- Please Select --

Authentication Type: No Authentication

Authentication Timeout: 1 Hour

Redirect: ☐ Enable

Redirect URL:

Portal Customization: Local Web Portal

Term of Use:

☒ I accept the Terms of Use.

Save

Free Authentication Policy

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC Address	Destination Port	Status	Settings
1	1	1	1	1	1	1	1

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.

The screenshot displays the 'Portal Configuration' web interface. It features several configuration fields: 'SSID' with a dropdown menu showing '- Please Select -'; 'Authentication Type' set to 'No Authentication'; 'Authentication Timeout' set to '1 Hour' with a breakdown of 0 days, 1 hour, and 0 minutes; 'Redirect' with an unchecked 'Enable' checkbox; 'Redirect URL' with an empty text box; and 'Portal Customization' set to 'Local Web Portal'. A preview window shows the resulting authentication page, which includes a 'Term of Use' section with a large text area, a checked checkbox for 'I accept the Term of Use', and a 'Login' button. A 'Save' button is located at the bottom left of the configuration panel.

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

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

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

4. Click **Save**.

- **Local Password**

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

The screenshot displays the 'Portal Configuration' interface. It includes fields for SSID (a dropdown menu), Authentication Type (set to 'Local Password'), Password (a text input), Authentication Timeout (set to '1 Hour' with a dropdown and a time picker for days, hours, and minutes), Redirect (a checkbox labeled 'Enable'), Redirect URL (a text input), and Portal Customization (set to 'Local Web Portal'). Below these fields is a preview of the web portal login page, which shows a password input field, a 'Term of Use' section with a checkbox for 'I accept the Term of Use', and a 'Login' button. A 'Save' button is located at the bottom left of the configuration area.

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

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

Password	Specify a password for authentication.
----------	--

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

4. Click **Save**.

- **External RADIUS Server**

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

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:

300

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	<p>With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled.</p> <p>Enter the appropriate duration between updates for EAPs in Interim Update Interval.</p>
Interim Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.
Authentication Timeout	<p>Specify the value of authentication timeout.</p> <p>A client's authentication will expire after the authentication timeout and the client needs to log in to the authentication page again to access the network.</p> <p>Options include 1 Hour, 8 Hours, 24 Hours, 7 Days, and Custom. With Custom selected, you can customize the time in days, hours, and minutes.</p>

Redirect	With this function configured, the newly authenticated client will be redirected to the specific URL.
Redirect URL	With Redirect enabled, you also need to enter the URL in this field. The newly authenticated client will be redirected to this URL.
Portal Customization	<p>Configure the authentication page. There are two options: Local Web Portal and External Web Portal.</p> <ul style="list-style-type: none"> Local Web Portal <p>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.</p> External Web Portal <p>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:</p> <ol style="list-style-type: none"> 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. <div data-bbox="683 1214 1385 1330" data-label="Form"> <p>Portal Customization: External Web Portal</p> <p>External Web Portal URL: <input type="text"/></p> </div> <ol style="list-style-type: none"> 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	<p>Specify an IP range with the subnet and mask length. The clients in this IP range can access the network without authentication.</p> <p>Leaving the field empty means that clients with any IP address can access the specific resources.</p>
Destination IP Range	<p>Specify an IP range with the subnet and mask length. The devices in this IP range can be accessed by the clients without authentication.</p> <p>Leaving the field empty means that all devices in the LAN can be accessed by the specific clients.</p>
Source MAC Address	<p>Specify the MAC address of the client, who can access the specific resources without authentication.</p> <p>Leaving the field empty means that clients with any MAC address can access the specific resources.</p>

Destination Port	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 ▾	<input type="text"/>
2	SSID-2	5GHz	Disable ▾	<input type="text"/>

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: ☐ **Disable**

Save

Station MAC Group

[+ Create New](#)

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

MAC Group Name	Modify

+ Add a Group Member

ID	MAC Address	Modify

- 1) Click **+ Add a Group** and specify a name for the MAC group to be created. Click **OK**. You can create up to eight MAC groups.

Station MAC Group

+ Add a Group

+ Add a Group Member

MAC Group Name: Group 1

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

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.


The screenshot shows the TP-Link web interface for configuring the Scheduler. The top navigation bar includes 'Status', 'Wireless', 'Management', and 'System'. The 'Wireless' tab is active, and the 'Scheduler' sub-tab is highlighted. The 'Settings' section contains a 'Scheduler' checkbox (checked) and an 'Association Mode' dropdown set to 'Associated with SSID'. A 'Save' button is present. The 'Scheduler Configuration' section has a '+ Create Profile' button. The 'Scheduler Association' section contains a table with two rows, each representing an SSID and its associated profile and action.

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


Follow the steps below to configure Scheduler on this page:

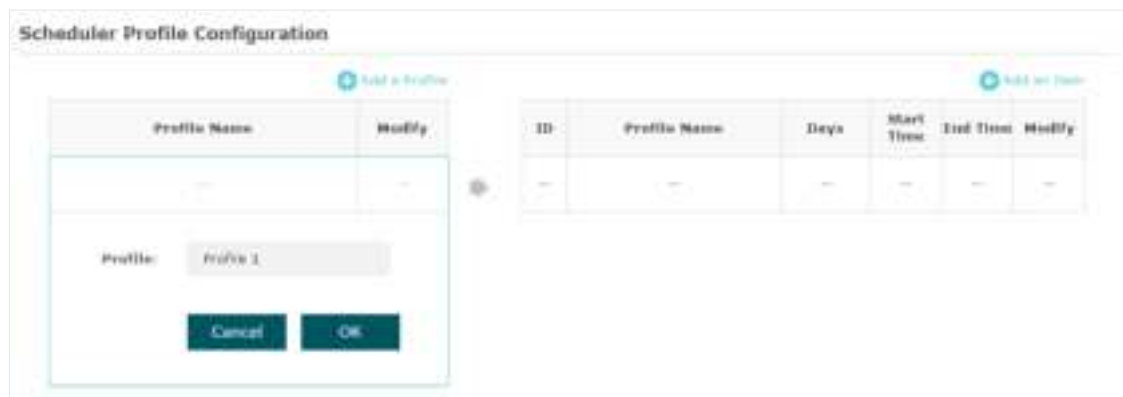
1. In the **Settings** section, check the box to enable **Scheduler** and select the **Association Mode**. There are two modes: **Associated with SSID** (the scheduler profile will be applied to the specific SSID) and **Associated with AP** (the profile will be applied to all SSIDs on the EAP). Then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


This close-up screenshot shows the 'Settings' section of the Scheduler configuration page. It features a 'Scheduler' checkbox that is checked and labeled 'Enable'. Below it, the 'Association Mode' is set to 'Associated with SSID' via a dropdown menu. A 'Save' button is located at the bottom right of this section.

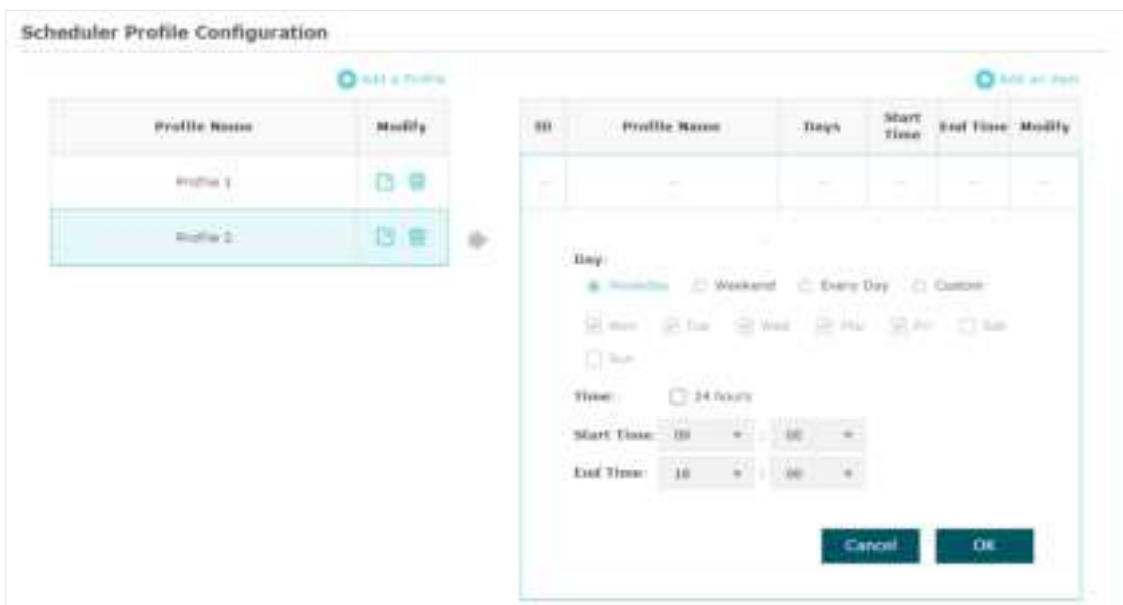
2. In the **Scheduler Profile Configuration** section, click  **Create Profiles** and the following page will appear.



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



- 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**.



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	EAP242-33-C7-9F-17-45-4E	33-C7-9F-17-45-E2	Profile 2	Radio On

Save

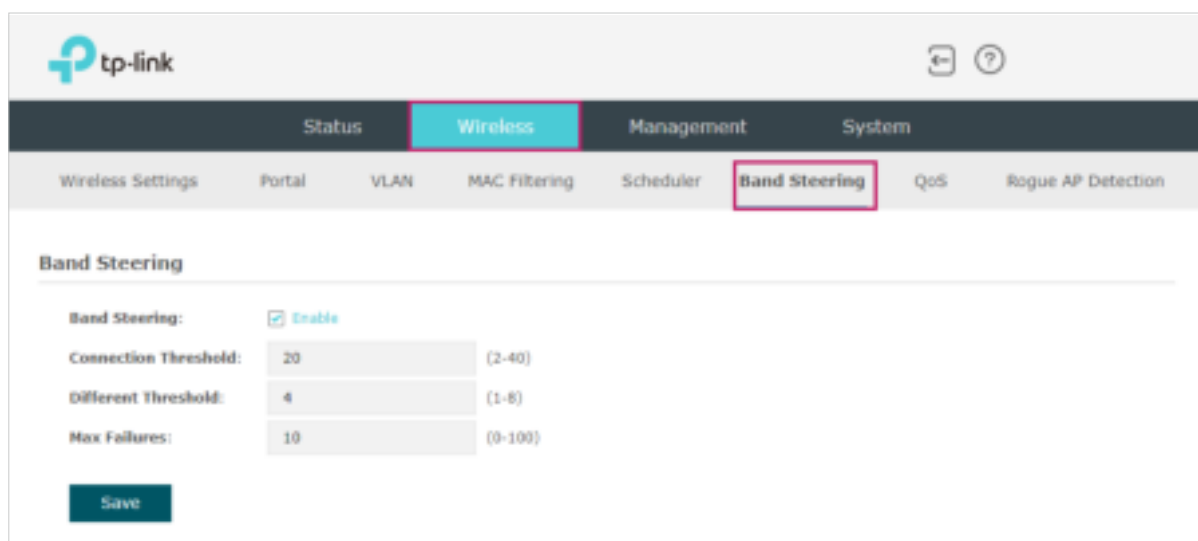
2.6 Configure Band Steering

A client device that is capable of communicating on both the 2.4GHz and 5GHz frequency bands will typically connect to the 2.4GHz band. However, if too many client devices are connected to an EAP on the 2.4GHz band, the efficiency of communication will be diminished. Band Steering can steer dual-band clients to the 5GHz frequency band which supports higher transmission rates and more client devices, and thus to greatly improve the network quality.

Note:

Only the dual-band EAP products support Band Steering.

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



The screenshot shows the TP-Link web interface. At the top, there is a navigation bar with the TP-Link logo and a user icon. Below this is a main menu with tabs: Status, Wireless (highlighted in blue), Management, and System. Under the Wireless tab, there is a sub-menu with links: Wireless Settings, Portal, VLAN, MAC Filtering, Scheduler, Band Steering (highlighted with a red box), QoS, and Rogue AP Detection. The main content area is titled 'Band Steering'. It contains the following settings:

Band Steering:	<input checked="" type="checkbox"/> Enable
Connection Threshold:	20 (2-40)
Different Threshold:	4 (1-8)
Max Failures:	10 (0-100)

At the bottom of the settings area is a 'Save' button.

Follow the steps below to configure Band Steering on this page:

1. Check the box to enable Band Steering function.
2. Configure the following parameters to balance the clients on both frequency bands:

Connection
Threshold/Difference
Threshold

Connection Threshold defines the maximum number of clients connected to the 5GHz band. The value of **Connection Threshold** is from 2 to 40, and the default is 20.

Difference Threshold defines the maximum difference between the number of clients on the 5GHz band and 2.4GHz band. The value of **Difference Threshold** is from 1 to 8, and the default is 4.

When the following two conditions are both met, the EAP prefer to refuse the connection request on 5GHz band and no longer steer other clients to the 5GHz band:

- 1.The number of clients on the 5GHz band reaches the **Connection Threshold** value.
- 2.The difference between the number of clients on the 2.4GHz band and 5GHz band reaches the **Difference Threshold** value.

Max Failures

If a client repeatedly attempts to associate with the EAP on the 5GHz band and the number of rejections reaches the value of **Max Failures**, the EAP will accept the request.

The value is from 0 to 100, and the default is 10.

3. Click **Save**.

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.

tp-link

Status **Wireless** Management System

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

2.4GHz 5GHz

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	3	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)	1	3	7	1504
Data 1 (Video)	1	3	15	3008
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

No Acknowledgment: ☐ Enable

Unscheduled Automatic Power-Save Delivery: ☒ Enable

Save

Follow the steps below to configure QoS on this page:

1. Click **2.4GHz** **5GHz** 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.

Queue	Arbitration Inter-Frame Spacing	Minimum Contention Window	Maximum Contention Window	Maximum Burst
Data 0 (Voice)	1	3 +	7 +	1534
Data 1 (Video)	1	7 +	15 +	3000
Data 2 (Best Effort)	2	15 +	63 +	3
Data 3 (Background)	3	31 +	1023 +	3

The following table detailedly explains these parameters:

Queue	<p>Displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters.</p> <p>Data 0 (Voice): Highest priority queue, minimum delay. Timesensitive data such as VoIP and streaming media are automatically sent to this queue.</p> <p>Data 1 (Video): High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.</p> <p>Data 2 (Best Effort): Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.</p> <p>Data 3 (Background): Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).</p>
Arbitration Inter-Frame Space	<p>A wait time for data frames. The wait time is measured in slots. Valid values are from 0 to 15.</p>

Minimum Contention Window	<p>A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.</p> <p>This value cannot be higher than the value of Maximum Contention Window.</p>
Maximum Contention Window	<p>The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.</p> <p>This value must be higher than the value of Minimum Contention Window.</p>
Maximum Burst	<p>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.</p>

4. 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.

Queue	Arbitration Inter Frame Spacing	Minimum Contention Window	Maximum Contention Window	TXOP Limit
Data 0 (Voice)	2	3	7	1504
Data 1 (Video)	2	3	15	1000
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

The following table detailedly explains these parameters:

Queue	<p>Displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters.</p> <p>Data 0 (Voice): Highest priority queue, minimum delay. Timesensitive data such as VoIP and streaming media are automatically sent to this queue.</p> <p>Data 1 (Video): High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.</p> <p>Data 2 (Best Effort): Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.</p> <p>Data 3 (Background): Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).</p>
--------------	---