User Guide

AX1800 Gigabit Wi-Fi 6 Access Point
TL-WA1801

© 2023 TP-Link 1910013390 REV1.0.0

Contents

About This Guide 1

Chapter 1. Get to Know About Your Access Point 3

1. 1. Product Overview. 4
1. 2. Panel Layout. 4
1. 2. 1.Top View 4
1. 2. 2.Back Panel 5

Chapter 2. Set Up Internet Connection 7

2. 1. Position Your Access Point. 8
2. 2. Set Up Your Access Point 9
2. 2. 1.Access Point Mode (Default). 9
2. 2. 2.Range Extender Mode. 10
2. 2. 3.Client Mode 11
2. 2. 4.Multi-SSID Mode 12

Chapter 3. TP-Link Cloud Service (for Access Point Mode). 14

3. 1. Register a TP-Link ID. 15
3. 2. Change Your TP-Link ID Information. 15
3. 3. Manage the User TP-Link IDs 16
3. 3. 1.Add TP-Link ID to Manage the Access Point 17
3. 3. 2.Remove TP-Link ID(s) from Managing the Access Point 17
3. 4. Manage the Access Point via the TP-Link Tether App 18

Chapter 4. Wireless Settings 19

4. 1. Specify Wireless Settings. 20
4. 1. 1.Access Point Mode. 20
4. 1. 2.Range Extender Mode. 22
4. 1. 3.Client Mode 24
4. 1. 4.Multi-SSID Mode 25
4. 2. Use WPS for Wireless Connection (for Access Point/Multi-SSID Mode) 27
4. 3. Check Advanced Wireless Settings (for Access Point/Multi-SSID Mode). 29
4. 4. Monitor Wireless Statistics (for Access Point/Multi-SSID Mode) 30
4. 5. Monitor the Traffic Throughput (for Access Point/Multi-SSID Mode) 31

Chapter 5. Portal (for Access Point/Multi-SSID Mode) 32

Chapter 6. Access Control 35

Chapter 7. Customize Network Settings 39

7. 1. Change the LAN Settings 40
7. 2. Specify DHCP Server Settings 40

Chapter 8. Manage Your Access Point 42

8. 1. Set the System Time and Language 43
8. 2. Control LEDs 45
8. 3. Configure the SNMP Agent 46
8. 4. Configure the Ping Watchdog 47
8. 5. Update the Firmware 48
8. 5. 1.Auto Update 48
8. 5. 2.Online Update 49
8. 5. 3.Local Update 50
8. 6. Backup and Restore Configuration Settings 50
8. 7. Reboot the Access Point 51
8. 8. Change the Login Password 52
8. 9. Password Recovery 53
8. 10. Local Management 53
8. 11. Test the Network Connectivity 55
8. 12. System Log 56

FAQ 59

About This Guide

This guide is a complement of Quick Installation Guide. The Quick Installation Guide instructs you on quick internet setup, and this guide provides details of each function and shows you the way to configure these functions appropriate to your needs.

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

Conventions

In this guide the following conventions are used:

Convention	Description
Underlined	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, System > Firmware Update means the Firmware Update page is located in the System tab.
Note:	Ignoring this type of note might result in a malfunction or damage to the device.
Tips:	Indicates important information that helps you make better use of your device.
symbols on the web page	• : Click to edit the corresponding entry. • : Click to delete the corresponding entry. • : Click to enable or disable the corresponding entry. • : Click to view more information about items on the page.

More Info

The latest software, management app and utility can be found at Download Center at https://www.tp-link.com/support/download.

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

Specifications can be found on the product page at https://www.tp-link.com.

TP-Link Community is provided for you to discuss our products and share knowledge at https://community.tp-link.com.

Our Technical Support contact information can be found at the Contact Technical Support page at https://www.tp-link.com/support.

*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput 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.

*Use of Wi-Fi 6 (802.11ax), and features including OFDMA, 1024-QAM, and HT160 require clients to also support the corresponding features.

*Saving clients' battery power requires clients to also support the 802.11ax Wi-Fi standard. Actual power reduction may vary as a result of network conditions, client limitations, and environmental factors.

*Use of WPA3 requires clients to also support the corresponding feature.

*This device may not support all the mandatory features as ratified in Draft 3.0 of IEEE 802.11ax specification.

*Further software upgrades for feature availability may be required.

Chapter 1

Get to Know About Your Access Point

This chapter introduces what the access point can do and shows its appearance.

It contains the following sections:

- Product Overview
- Panel Layout

1. 1. Product Overview

The TP-Link access point, with multiple operation modes, is designed to establish or expand a scalable high-speed wireless network or to connect your Ethernet enabled device to a wireless network, such as the game console, digital media adapter, printer, or network attached storage device. The access point supports a host of different functions that make your wireless networking experience more flexible than ever before. Now, you can enjoy a better internet experience when downloading, gaming, video streaming or with any other application that you may wish to use.

1. 2. Panel Layout

1. 2. 1. Top View

The access point's LEDs (view from left to right) are located on the top panel. You can check the access point's working status by following the LED Explanation table.

LED Explanation

Name	Status	Indication
(Power)	On	Power is on.
	Blinking once every second	The system is starting up or the firmware upgrade is in progress. Do not disconnect or power off your access point.
	Blinking twice every second	WPS connection is in progress. This may take up to 2 minutes.
	Off	Power is off.
(Ethernet)	On	The Ethernet port is connected to a powered-on device.
	Off	The Ethernet port is not connected to a powered-on device.
(2.4GHz)	On/Off	**For Access Point/Multi-SSID mode:** The 2.4GHz wireless band is enabled or disabled. **For Range Extender/Client mode:** The device is connected or not connected to a 2.4GHz main network.
(5GHz)	On/Off	**For Access Point/Multi-SSID mode:** The 5GHz wireless band is enabled or disabled. **For Range Extender/Client mode:** The device is connected or not connected to a 5GHz main network.

1. 2. 2. Back Panel

The following parts (view from left to right) are located on the back panel.

Ports or Buttons	Description
Power Port	For connecting the access point to a power socket via the provided power adapter.
On/Off Button	Press this button to power on or off the access point.
Reset	Press and hold this button until the Power LED blinks to reset the access point to its factory default settings.
WPS	Press this button and immediately press the WPS button on another device to quickly establish a wireless connection.
Ethernet Port	For connecting an Ethernet enabled device, such as a router or desktop.
Antennas	Used for wireless operation and data transmitting. Upright them for the best Wi-Fi performance.

Chapter 2

Set Up Internet Connection

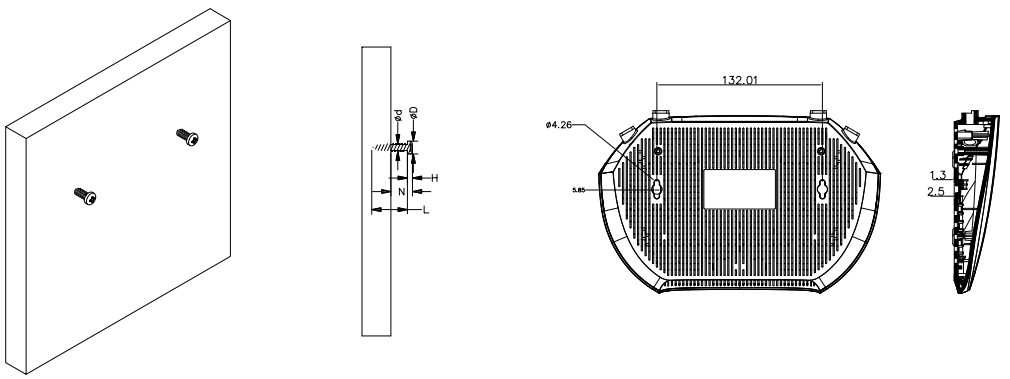
This chapter introduces how to quickly set up the access point.

It contains the following sections:

- Position Your Access Point
- Set Up Your Access Point

2. 1. Position Your Access Point

- The product should not be located in a place where it will be exposed to moisture or excessive heat.
- Place the access point in a location where it can be connected to various devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.
- The access point can be placed on a shelf or desktop.
- Keep the access point away from devices with strong electromagnetic interference, such as Bluetooth devices, cordless phones and microwaves.
- Generally, the access point is placed on a horizontal surface, such as on a shelf or desktop. The device also can be mounted on the wall as shown in the following figure.



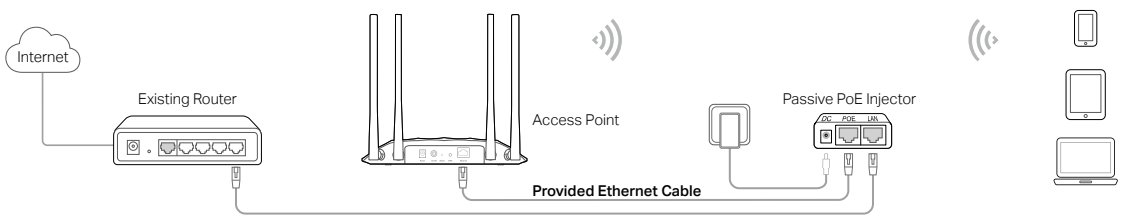
NOTE:
4.76mm<D<5.35mm;
H<2.5mm;
N>3.8mm;
L>11mm

Note:
The diameter of the screw head, 4.76 mm < D < 5.35 mm, and the distance of two screws is 132 mm. The screw that project from the wall need around 3.8 mm based, and the length of the screw need to be at least 11 mm to withstand the weight of the product.

- If the access point is located far from a power outlet, you can power the device with the provided passive PoE injector. Use the **Ethernet cable (included in the box)** to connect your Access Point and the passive PoE injector.

Note:
The passive PoE injector supports a cable length up to 30 meters, but the value may vary due to the environment.

Power on via Passive PoE Injector

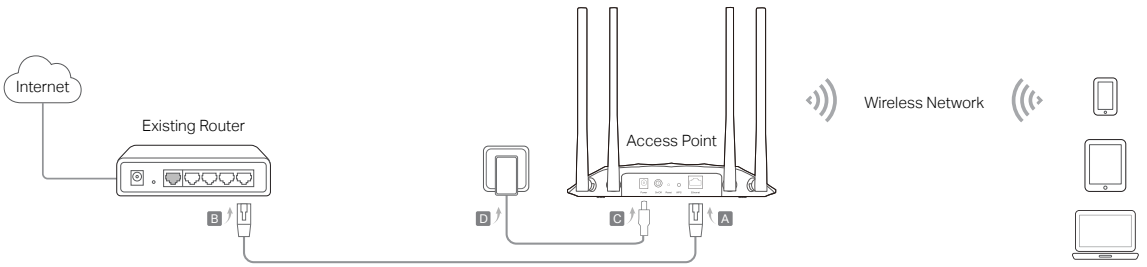


2. 2. Set Up Your Access Point

There are four operation modes supported by this access point: Access Point, Range Extender, Client, and Multi-SSID. Please determine which operation mode you need and complete the corresponding setup.

2. 2. 1. Access Point Mode (Default)

In this mode, the access point transforms your existing wired network to a wireless one. This mode is suitable for dorm rooms or homes where there's already a wired router but you need a wireless network.

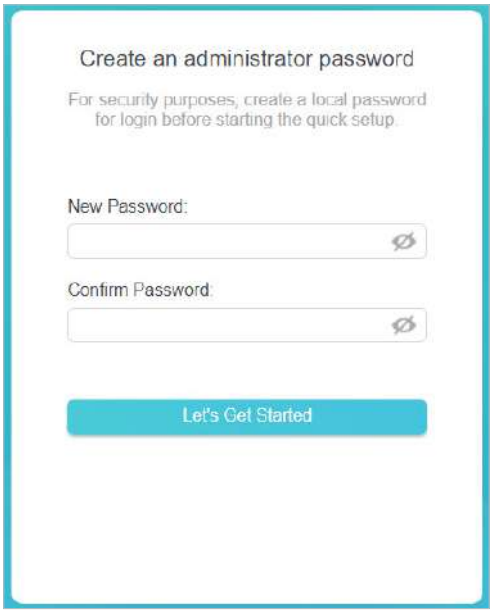


1. Connect the access point according to Step A to D in the diagram.
2. Turn on the power, and wait for about 2 minutes until the Power and Wi-Fi LEDs are lit and stable.
3. Use the default SSID and Password printed on the label of the access point to join its Wi-Fi network.

Note:
You can surf the internet now. For your wireless network security, it is recommended to change the default SSID (network name) and the password of your Wi-Fi network. To do so, perform the following steps.

4. Launch a web browser and enter http://tplinkap.net. Create a password to log in.

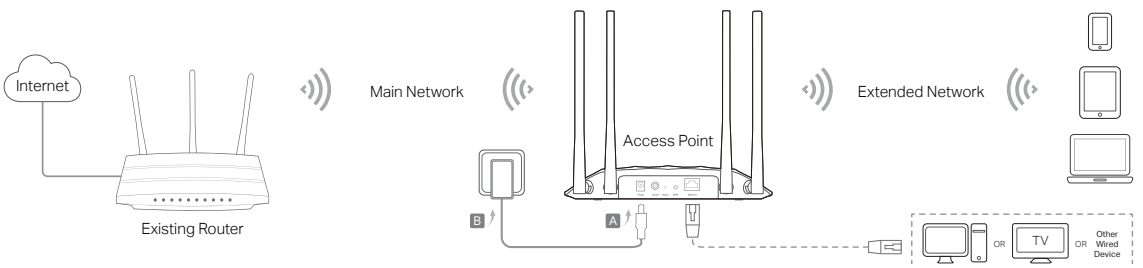
Note:
If the login window does not appear, please refer to the FAQ section.



5. Follow the step-by-step instructions to complete the configuration.
6. Now, reconnect your wireless devices to the new Wi-Fi network and enjoy the internet!

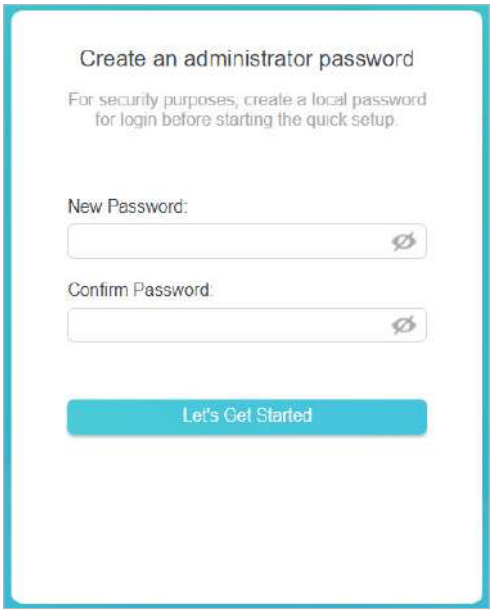
2. 2. 2. Range Extender Mode

In this mode, the access point extends the range of an existing Wi-Fi network. This mode is suitable when you are in a Wi-Fi dead-zone or a place with weak wireless signal, and you want to have a larger effective range of the wireless signal throughout your home or office.



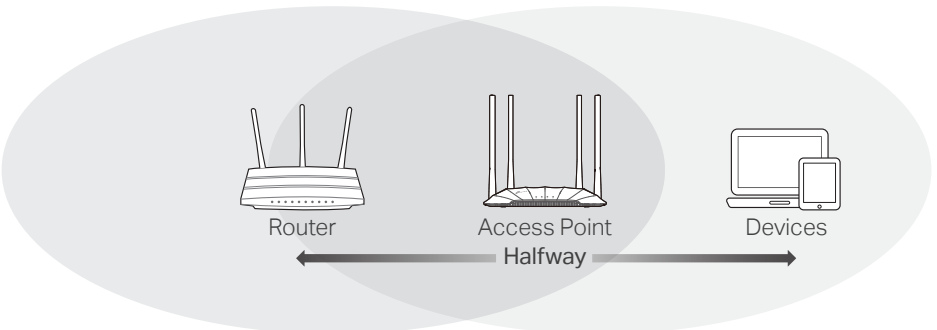
1. Connect the access point according to Step A and B in the diagram.
2. Turn on the power, and wait for about 2 minutes until the Power and Wi-Fi LEDs are lit and stable.
3. Connect your computer to the access point via an Ethernet cable.
4. Launch a web browser and enter http://tplinkap.net. Create a password to log in.

Note:
If the login window does not appear, please refer to the FAQ section.



5. Click Change Mode in the upper right corner and switch to the Range Extender mode.
6. Wait until the access point reboots, then log in again.
7. Follow the step-by-step instructions to complete the configuration.
8. Relocate the access point about halfway between your host router and the Wi-Fi dead zone.

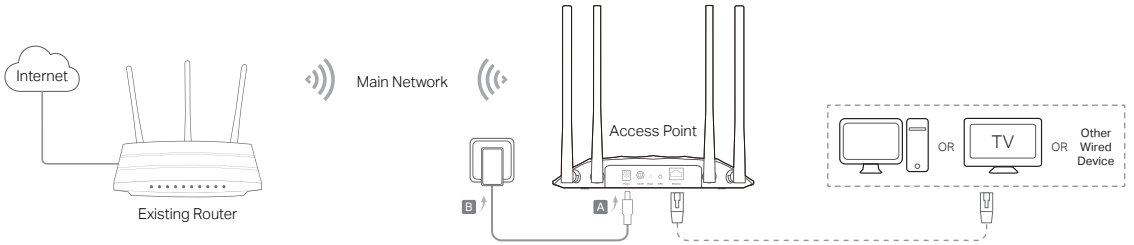
Tip: To maximize the signal strength, refer to the FAQ section.



9. Now, connect your devices to the access point wirelessly or via an Ethernet cable, and enjoy the internet!

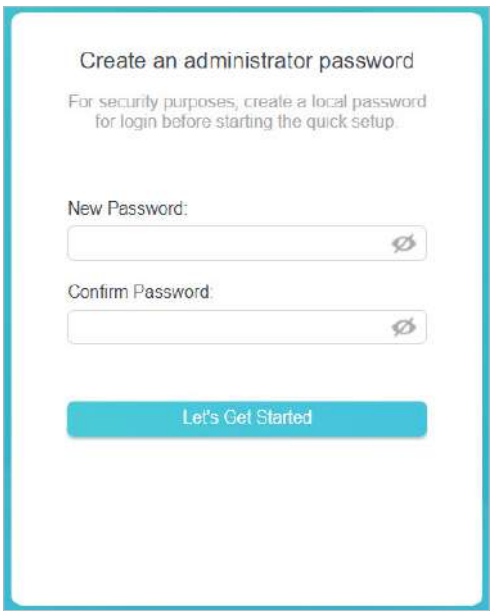
2. 2. 3. Client Mode

In this mode, the access point connects your wired device to a wireless network. This mode is suitable when you have a wired device with an Ethernet port and no wireless capability, for example, a smart TV or game console and you want to connect it to the internet wirelessly.



1. Connect the access point according to Step A to B in the diagram.
2. Turn on the power, and wait for about 2 minutes until the Power and Wi-Fi LEDs are lit and stable.
3. Connect your computer to the access point via an Ethernet cable.
4. Launch a web browser and enter http://tplinkap.net. Create a password to log in.

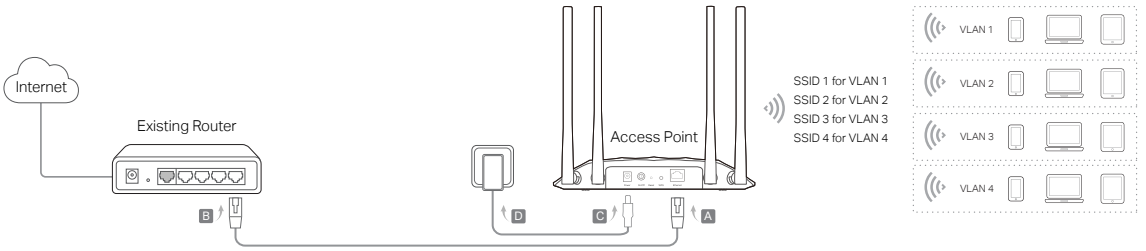
Note:
If the login window does not appear, please refer to the FAQ section.



5. Click Change Mode in the upper right corner and switch to the Client mode.
6. Wait until the access point reboots, then log in again.
7. Follow the step-by-step instructions to complete the configuration.
8. Now, connect your wired device to the access point via an Ethernet cable, and enjoy the internet!

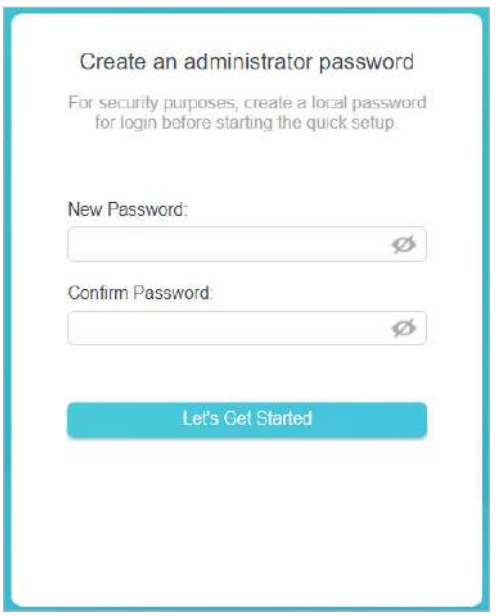
2. 2. 4. Multi-SSID Mode

In this mode, the access point creates multiple wireless networks to provide different security and VLAN (Virtual Local Area Network) groups. This mode is suitable when you want your devices connected to different wireless networks and become isolated by VLANs.



1. Connect the access point according to Step A to D in the diagram.
2. Turn on the power, and wait for about 2 minutes until the Power and Wi-Fi LEDs are lit and stable.
3. Use the default SSID and Password printed on the label of the access point to join its Wi-Fi network.
4. Launch a web browser and enter http://tplinkap.net. Create a password to log in.

Note:
If the login window does not appear, please refer to the FAQ section.



5. Click Change Mode in the upper right corner and switch to the Multi-SSID mode.
6. Wait until the access point reboots, then reconnect to the access point and log in again.
7. Follow the step-by-step instructions to complete the configuration.
8. Now, connect your wireless devices to the Wi-Fi networks and enjoy the internet!

Tip:
If you want to isolate different networks, go to Wireless > Wireless Settings, click the edit icon of each SSID entry and set different VLAN IDs.

Chapter 3

TP-Link Cloud Service

(for Access Point Mode)

TP-Link Cloud service provides a better way to manage your cloud devices. Log in to your access point with a TP-Link ID, and you can easily monitor and manage your home network when you are out and about via the Tether app. To ensure that your access point stays new and gets better over time, the TP-Link Cloud will notify you when an important firmware upgrade is available. Surely you can also manage multiple TP-Link Cloud devices with a single TP-Link ID.

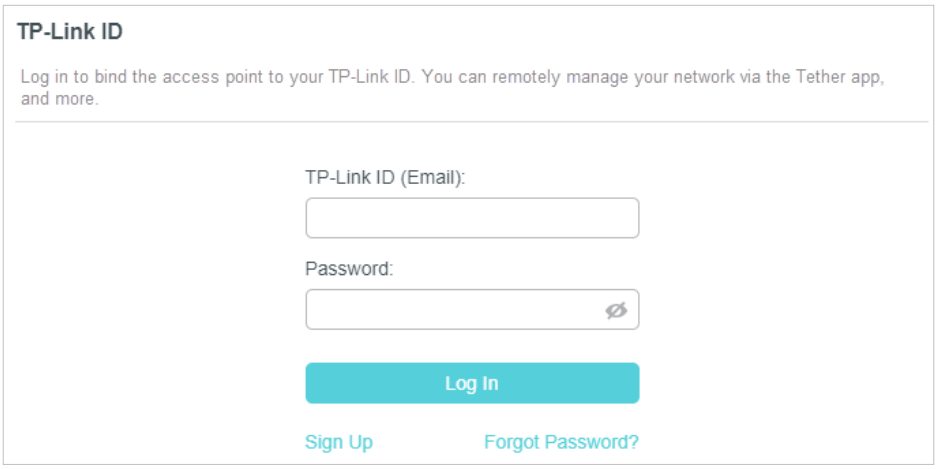
This chapter introduces how to register a new TP-Link ID, bind or unbind TP-Link IDs to manage your access point, and the Tether app with which you can manage your home network no matter where you may find yourself.

It contains the following sections:

- Register a TP-Link ID
- Change Your TP-Link ID Information
- Manage the User TP-Link IDs
- Manage the Access Point via the TP-Link Tether App

3. 1. Register a TP-Link ID

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > TP-Link ID or click TP-Link ID in the upper right corner of the page.
3. Click Sign Up and follow the instructions to register a TP-Link ID.



4. After activating your TP-Link ID, come back to the TP-Link ID page to log in. The TP-Link ID used to log in to the access point for the first time will be automatically bound as an Admin.

Note:

- To learn more about the Admin and User TP-Link ID, refer to Manage the User TP-Link IDs.
- Once you have registered a TP-Link ID on the web management page, you can only register another TP-Link ID via the Tether APP. Please refer to Manage the Access Point via the TP-Link Tether App to install the app.
- If you want to unbind the admin TP-Link ID from your access point, please go to Advanced > TP-Link ID, an click Unbind in the Device Information section.

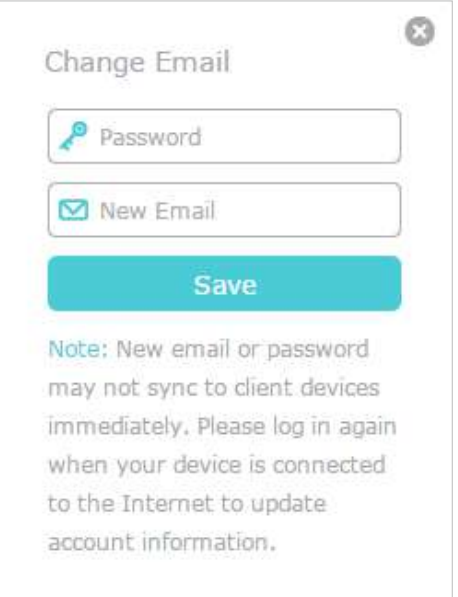
3. 2. Change Your TP-Link ID Information

Follow the steps below to change your email address and password of your TP-Link ID as needed.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > TP-Link ID, and focus on the Account Information section.

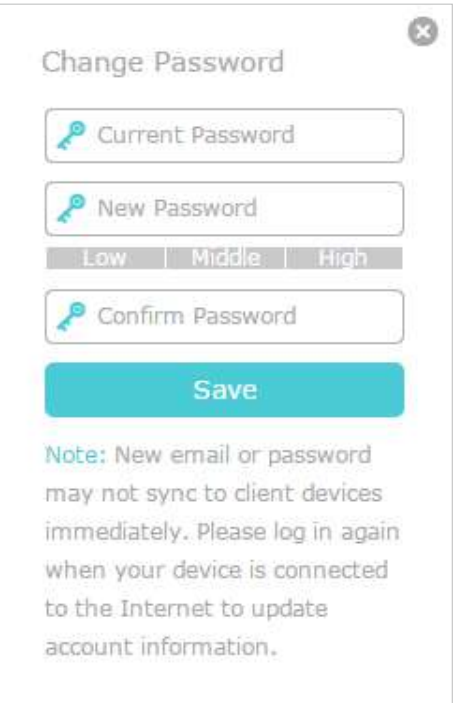
- **To change your email address**:

1. Click behind the Email.
2. Enter the password of your TP-Link ID, then a new email address. And click SAVE.



- **To change your password:**

1. Click behind the Password.
2. Enter the current password, then a new password twice. And click SAVE.



3. 3. Manage the User TP-Link IDs

The TP-Link ID used to log in to the access point for the first time will be automatically bound as the Admin account. An admin account can add or remove other TP-Link IDs

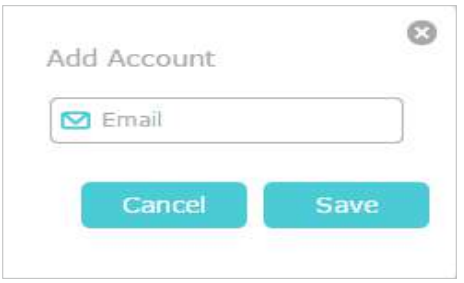
to or from the same access point as Users. All accounts can monitor and manage the access point locally or remotely, but user accounts cannot:

- Reset the access point to its factory default settings either on the web management page or in the Tether app.
- Add/remove other TP-Link IDs to/from the access point.

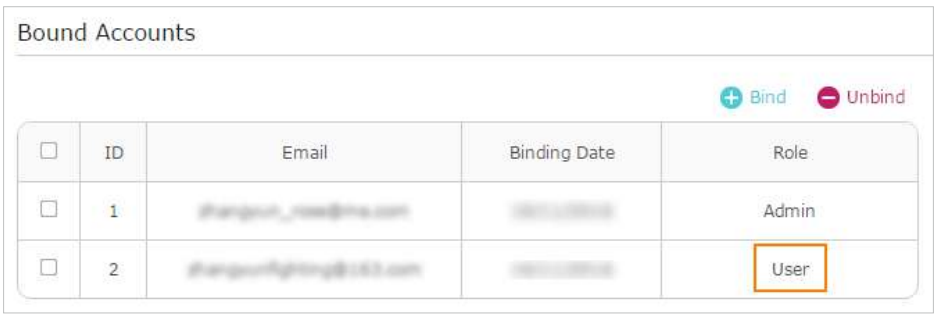
3. 3. 1. Add TP-Link ID to Manage the Access Point

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > TP-Link ID, and focus on the Bound Accounts section.
3. Click Bind , enter another TP-Link ID as needed and click SAVE.

Note: If you need another TP-Link ID, please register a new one via the Tether app. Refer to Manage the Access Point via the TP-Link Tether App to install the app and register a new TP-Link ID.

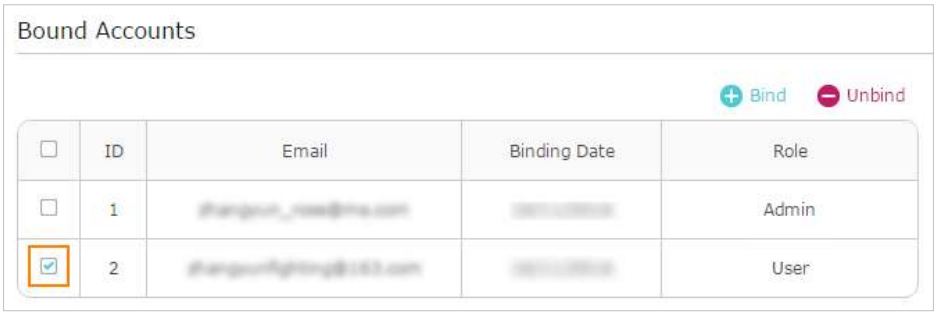


4. The new TP-Link ID will be displayed in the Bound Accounts table as a User.



3. 3. 2. Remove TP-Link ID(s) from Managing the Access Point

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > TP-Link ID, and focus on the Bound Accounts section.
3. Tick the checkbox(es) of the TP-Link ID(s) you want to remove and click Unbind.



3. 4. Manage the Access Point via the TP-Link Tether App

The Tether app runs on iOS and Android devices, such as smartphones and tablets.

1. Launch the Apple App Store or Google Play store and search "TP-Link Tether" or simply scan the QR code to download and install the app.

2. Launch the Tether app and log in with your TP-Link ID.

Note: If you don't have a TP-Link ID, create one first.

3. Connect your device to the access point's wireless network.
4. Go back to the Tether app, select your access point and log in with the password you set for the access point.
5. Manage your access point as needed.

Note:

If you need to remotely access your access point from your smart devices, you need to:

- Log in with your TP-Link ID. If you don't have one, refer to Register a TP-Link ID.
- Make sure your smartphone or tablet can access the internet with cellular data or a Wi-Fi network.

Chapter 4

Wireless Settings

This chapter guides you on how to configure the wireless settings.

It contains the following sections:

- Specify Wireless Settings
- Use WPS for Wireless Connection (for Access Point/Multi-SSID Mode)
- Check Advanced Wireless Settings (for Access Point/Multi-SSID Mode)
- Monitor Wireless Statistics (for Access Point/Multi-SSID Mode)
- Monitor the Traffic Throughput (for Access Point/Multi-SSID Mode)

4. 1. Specify Wireless Settings

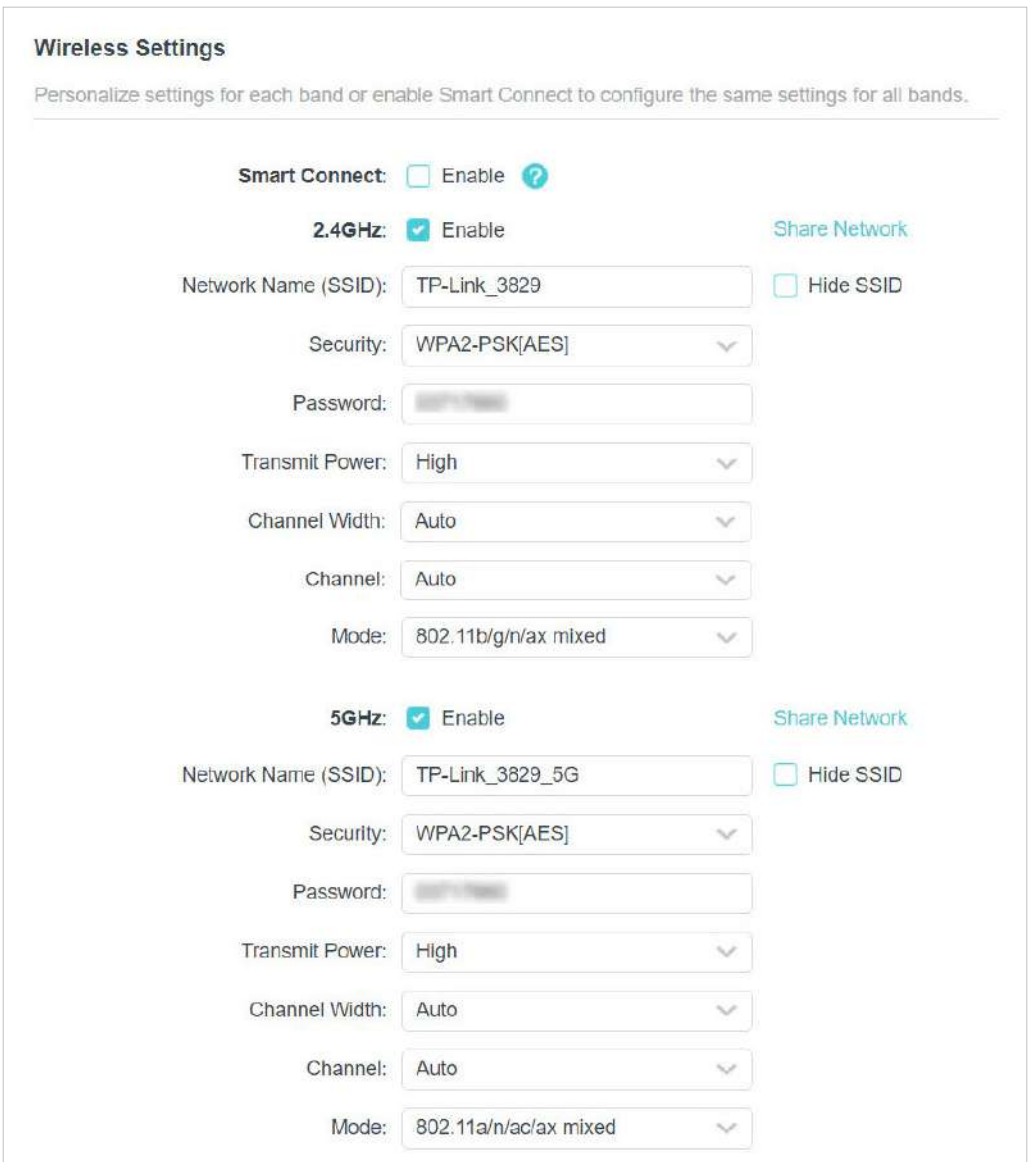
The access point's wireless network names (SSIDs), password, and security option are preset in the factory. The preset SSIDs and password can be found on the label of the access point.

Wireless settings differ with operation mode.

4. 1. 1. Access Point Mode

When the device works in Access Point mode, you can customize its wireless network.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Wireless Settings.



3.

- **To use the Smart Connect function:**

Smart Connect combines the 2.4 GHz and 5 GHz bands and assigns your devices between them to balance network demands.

1. Go to Wireless > Wireless Settings.
2. Enable Smart Connect.

3. Keep the default values or set a new SSID and password, and click SAVE. This SSID and password will be applied for the 2.4 GHz and 5 GHz wireless networks. If you want to configure the wireless settings separately for each band, deselect the checkbox to disable this feature.

- **To enable or disable a wireless band:**

1. Go to Wireless > Wireless Settings.
2. The wireless bands are enabled by default. If you want to disable a wireless band, just deselect its Enable checkbox.

- **To change the wireless network name (SSID) and wireless password:**

1. Go to Wireless > Wireless Settings.
2. Create a new SSID in Network Name (SSID) and customize the password for the network in Password. The value is case-sensitive.

Note: If you change the wireless settings with a wireless device, you will be disconnected when the settings are effective. Please write down the new SSID and password for future use.

- **To hide SSID:**

1. Go to Wireless > Wireless Settings.
2. Select Hide SSID, then your SSID won't display when wireless devices scan for wireless networks and you will need to manually enter the SSID to join the network.

- **To change the security option:**

1. Go to Wireless > Wireless Settings.
2. Select an option from the Security drop-down list. We recommend you don't change the default settings unless necessary.

- **To change the transmit power:**

1. Go to Wireless > Wireless Settings.
2. Select an option from the Transmit Power drop-down list.

- **To change channel and mode settings:**

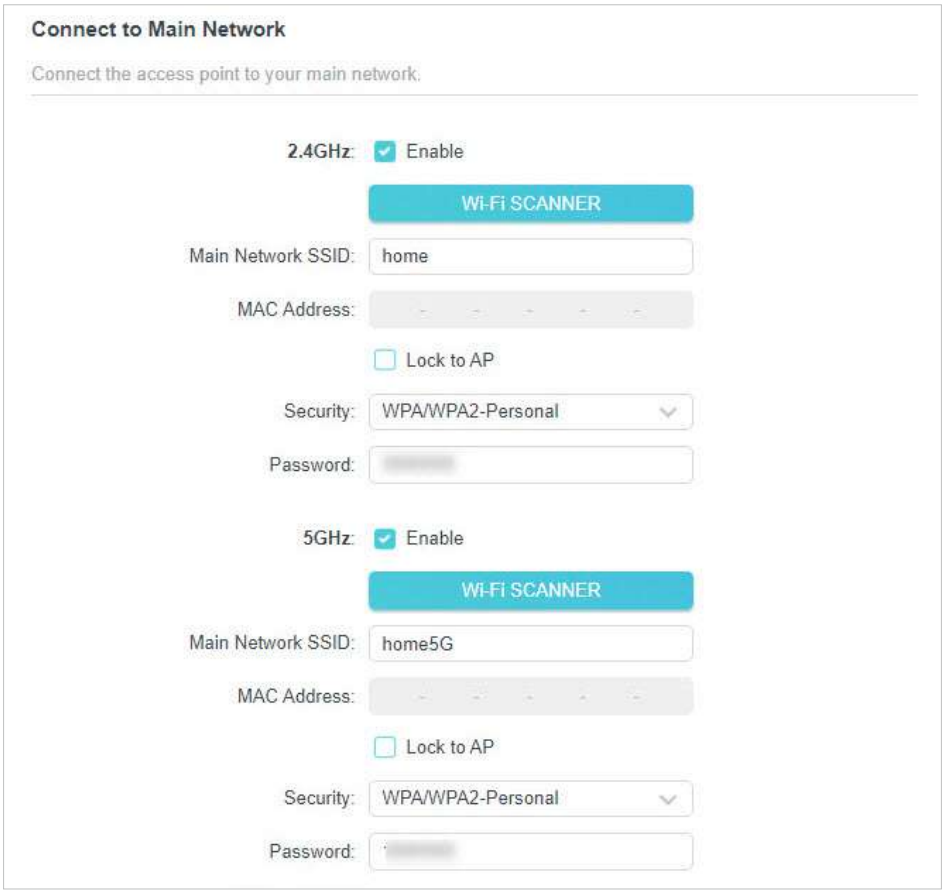
1. Go to Wireless > Wireless Settings.

2. Make sure Smart Connect is disabled. Channel and mode settings are not available when Smart Connect is enabled.
3. Select a Channel Width (bandwidth) for the wireless network. It is recommended to just leave it as default.
4. Select an operating Channel for the wireless network. It is recommended to leave the channel to Auto if you are not experiencing the intermittent wireless connection issue.
5. Select a transmission Mode according to your wireless client devices. It is recommended to just leave it as default.
6. Click SAVE.

4. 1. 2. Range Extender Mode

When the device works in Range Extender mode, you can reselect the networks to extend and customize the extended networks.

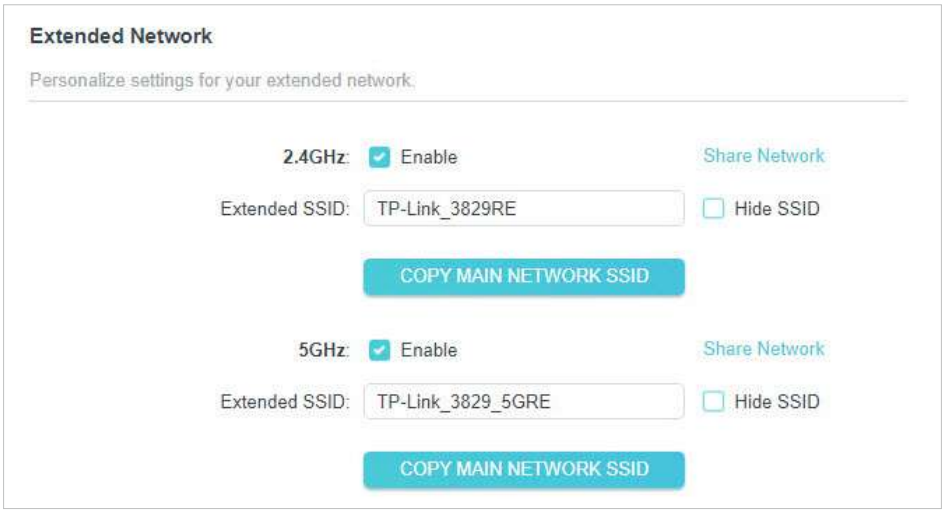
1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Wireless Settings.
3. In the Connect to Main Network section, select the 2.4GHz and/or 5GHz network(s), click Wi-Fi SCANNER to find and select the network to extend. If the selected network is encrypted, enter the network password.



4. In the Extended Network section, customize the extended networks as you need. You can:
   - Enable or disable a wireless network.
   - Change the extended SSIDs or copy main network SSIDs.

   Note: Extended passwords are the same as the main network passwords and cannot be changed.

   - Select Hide SSID for a network, then your SSID won't display when wireless devices scan for wireless networks and you will need to manually enter the SSID to join the network.

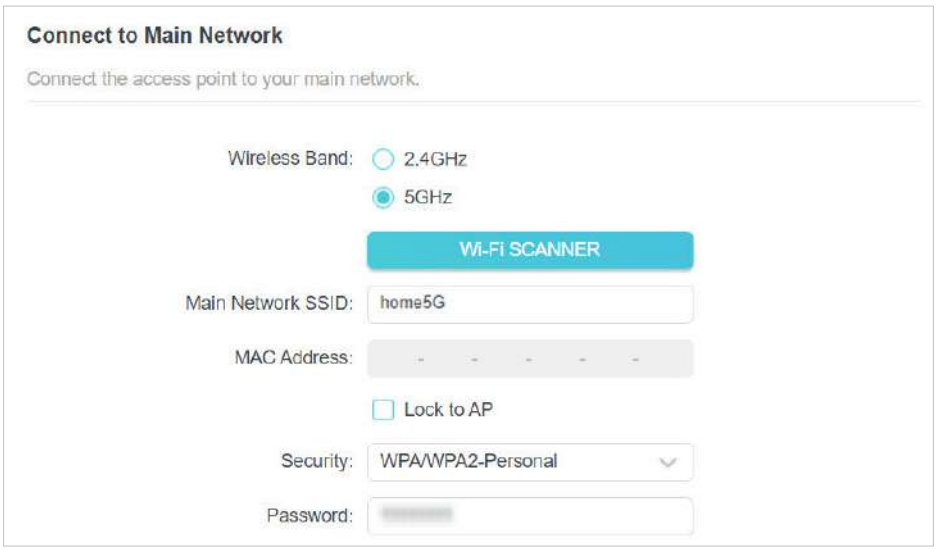


5. Click SAVE.

4. 1. 3. Client Mode

When the device works in Client mode, you can connect to another network.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Wireless Settings.



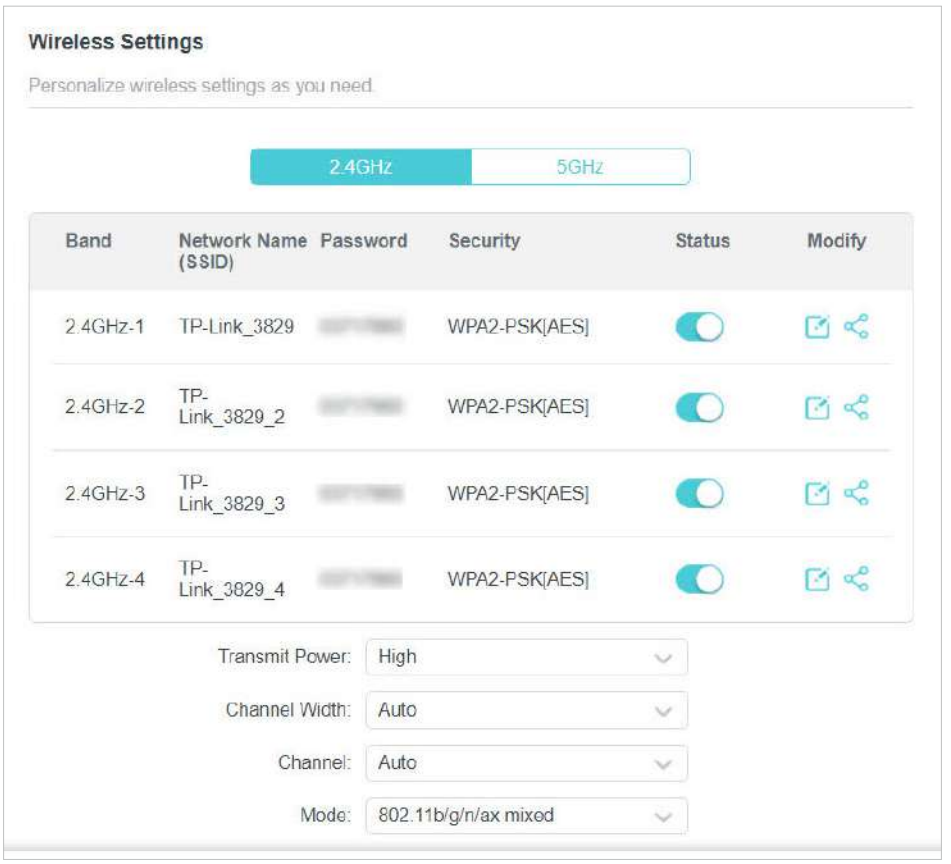
3. Select the 2.4GHz or 5GHz band.
4. Click Wi-Fi SCANNER to find and select the network to connect. Main network SSID and MAC address will be automatically filled in.
5. (Optional) If you want to lock the connection to the specified AP, enable Lock to AP. The access point will not switch connection to other APs even if they use the same network name and password as the specified one.
6. Enter the network password.

7. Click SAVE.

4. 1. 4. Multi-SSID Mode

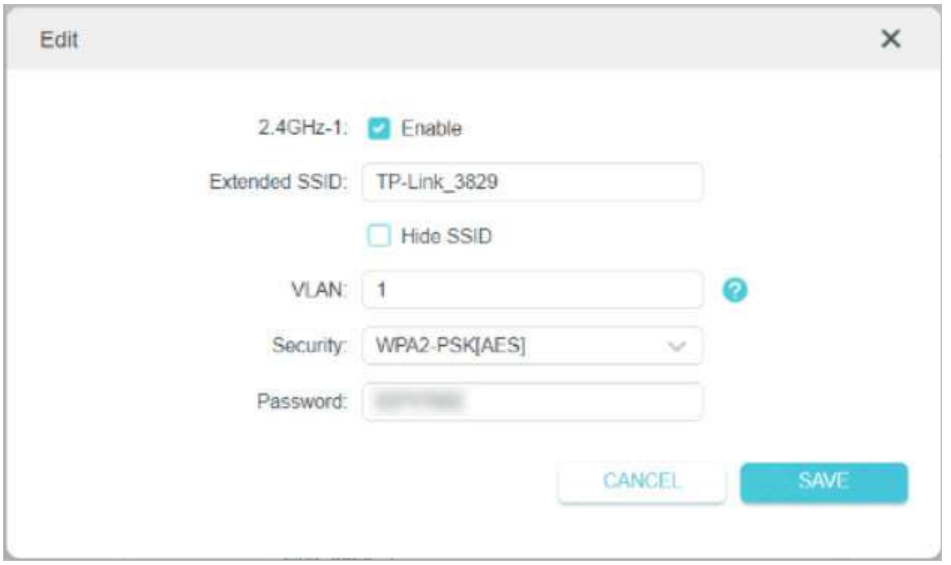
When the device works in Multi-SSID mode, you can customize and isolate multiple wireless networks.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Wireless Settings.



- **To customize a wireless network:**

1. Go to Wireless > Wireless Settings.
2. Click 2.4GHz or 5 GHz, select a network and click .



3. Customize the network according to your needs. You can:
   - Enable or disable the network.
   - Change the extended SSID, password, and security option.
   - Select Hide SSID for the network, then your SSID won't display when wireless devices scan for wireless networks and you will need to manually enter the SSID to join the network.
4. Click SAVE.

- **To isolate wireless networks:**

1. Go to Wireless > Wireless Settings.
2. Click of each SSID entry and set different VLAN IDs. Only the networks with the same VLAN ID can access each other. Wireless networks will be isolated by VLANs.

3. Click SAVE.

- **To change the transmit power:**

1. Go to Wireless > Wireless Settings.
2. Click 2.4GHz or 5 GHz.
3. Select an option from the Transmit Power drop-down list.

- **To change channel settings:**

1. Go to Wireless > Wireless Settings.
2. Click 2.4GHz or 5 GHz.
3. Select a Channel Width (bandwidth) for the wireless network. It is recommended to just leave it as default.
4. Select an operating Channel for the wireless network. It is recommended to leave the channel to Auto if you are not experiencing the intermittent wireless connection issue.
5. Click SAVE.

- **To change the transmission mode:**

1. Go to Wireless > Wireless Settings.
2. Click 2.4GHz or 5 GHz.
3. Select a transmission Mode according to your wireless client devices. It is recommended to just leave it as default.
4. Click SAVE.

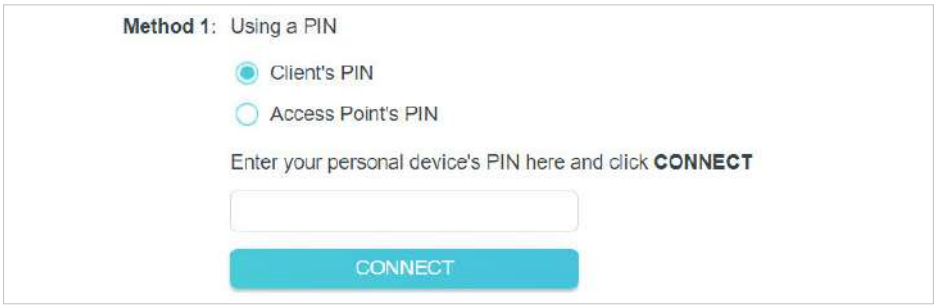
4. 2. Use WPS for Wireless Connection (for Access Point/Multi-SSID Mode)

Wi-Fi Protected Setup (WPS) provides an easier approach to set up a security-protected Wi-Fi connection.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > WPS.
3. Follow one of the following methods to connect your WPS-enabled client to the access point's Wi-Fi network.

- **Connect via the client's PIN**

  1) Click Client's PIN.

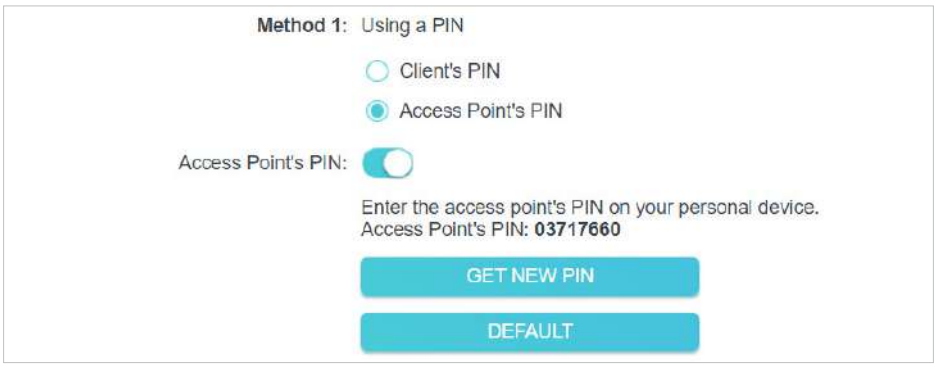


2) Enter your client's PIN, and then click CONNECT.

3) A success message will appear on the WPS page when the device successfully join the access point's network.

- **Connect via the access point's PIN**

1) Click Access Point's PIN.

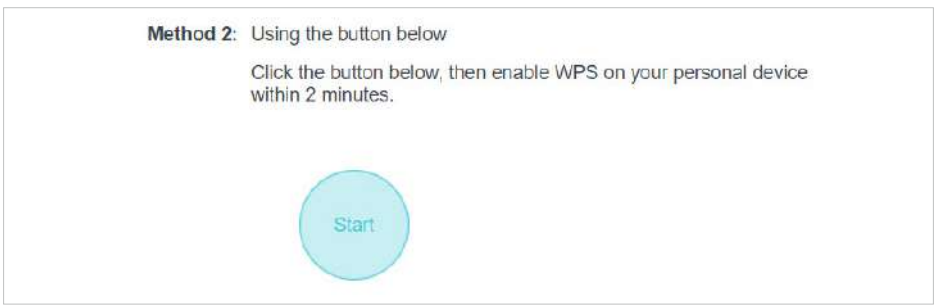


2) Check your access point's PIN. You can use the default PIN or generate a new one.

3) Enter this PIN on your client for it to join the access point's network.

- **Connect via the Start button on the WPS page**

1) Click the Start button on the WPS page.



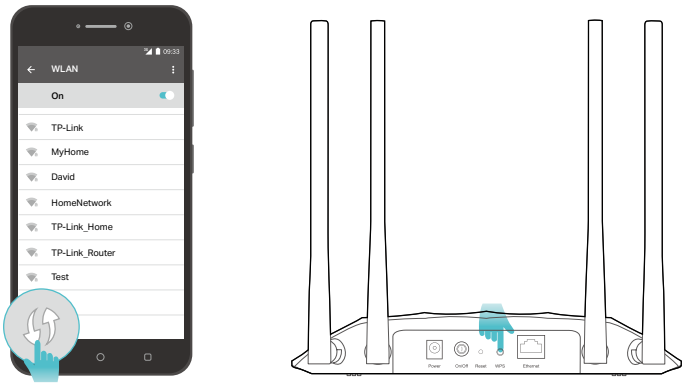
2) Within 2 minutes, enable WPS on your client.

3) A success message will appear on the WPS page when the device successfully join the access point's network.

- **Connect via the WPS button on the access point**

1) Press the WPS button on the back panel of the access point.

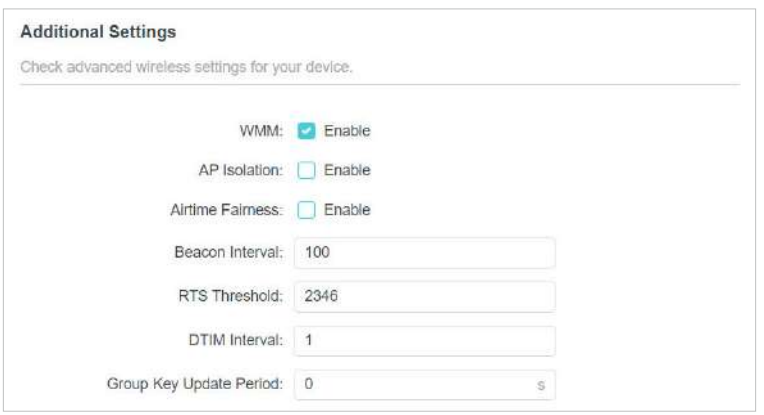
2) Within 2 minutes, enable WPS on your client. The client will connect to the access point.



4. 3. Check Advanced Wireless Settings (for Access Point/Multi-SSID Mode)

You can check advanced wireless settings for the device. It is recommended that you keep the default settings. Improper settings may affect network performance.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Wireless Advanced.
3. Check the advanced settings of your wireless network.



- WMM – This function can guarantee the packets with high-priority messages being transmitted preferentially.
- AP Isolation – This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.
- Airtime Fairness – This function can improve the overall network performance by sacrificing a little bit of network time on your slow devices.

- Beacon Interval – Enter a value between 40 and 1000 in milliseconds to determine the duration between beacons packets that are broadcasted by the access point to synchronize the wireless network. The default value is 100 milliseconds.
- RTS Threshold – Enter a value between 1 and 2346 to determine the packet size of data transmission trough the access point. If the packet is larger than the specified threshold, the access point will send RTS (Request to Send) frames to a particular receiving station and negotiate the sending of a data frame. Or else the packet will be sent immediately. The default value is 2346.
- DTIM Interval – This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Enter a value between 1 and 15 Beacon Intervals. The default value is 1, indicating that the DTIM Interval is the same as Beacon Interval.
- Group Key Update Period – Enter the number of seconds (minimum 30) to control the time interval for the encryption key automatic renewal. The default value is 0, indicating no key renewal.

4. 4. Monitor Wireless Statistics (for Access Point/ Multi-SSID Mode)

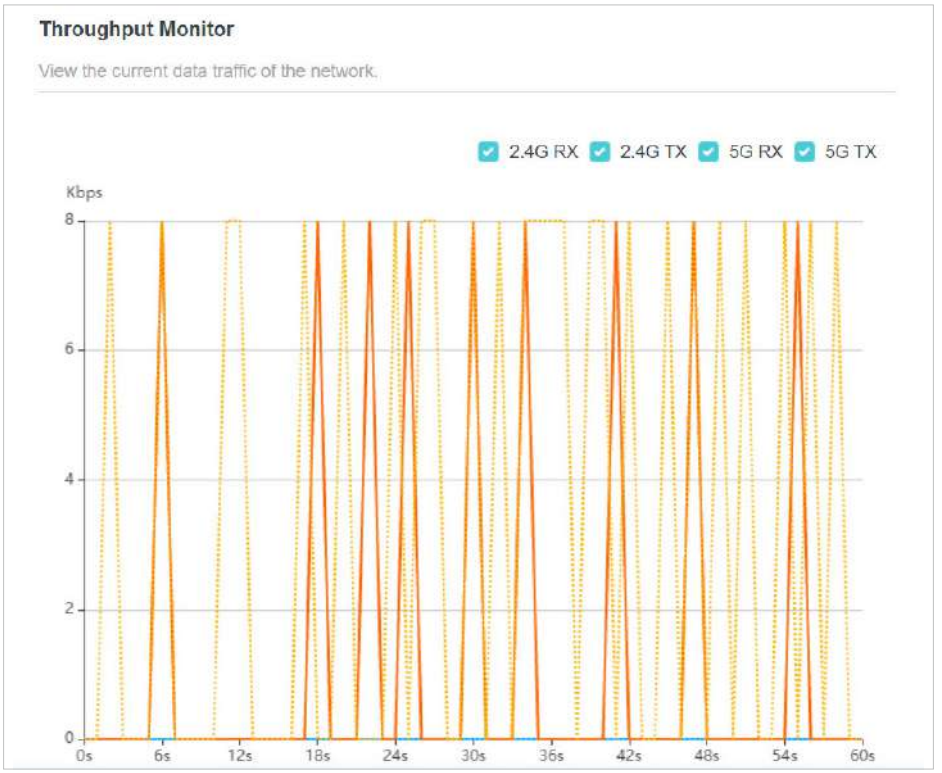
The Wireless Statistics page displays the data statistics of wireless clients.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Wireless Statistics.
3. View the data statistics of wireless clients.

4. 5. Monitor the Traffic Throughput (for Access Point/Multi-SSID Mode)

The throughput chart displays the current data traffic of the network.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Throughput Monitor.
3. Select 2.4G RX, 2.4G TX, 5G RX and/or 5G TX to view the data rates.



Chapter 5

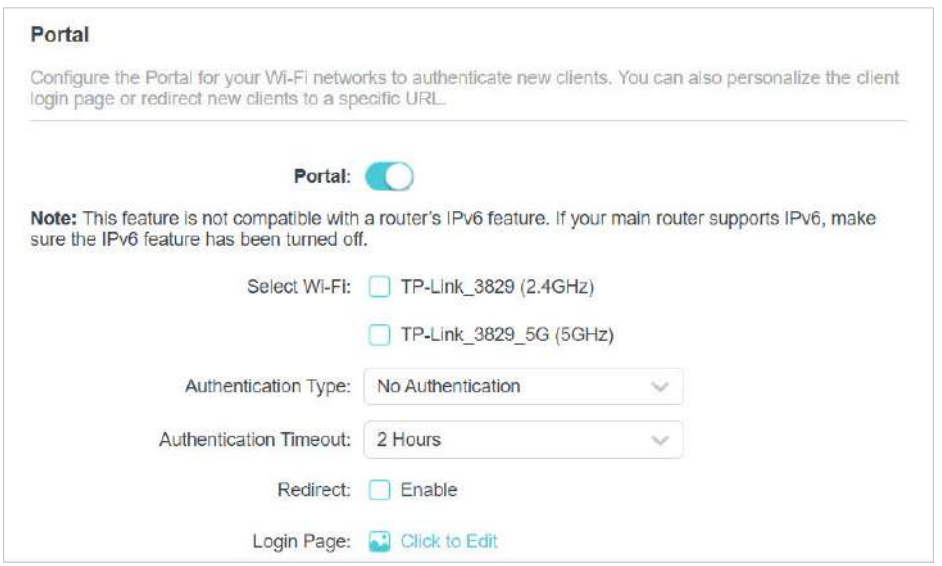
Portal

(for Access Point/Multi-SSID Mode)

Imagine that you run a small shop and provide Wi-Fi access for your customers. You want to seize every opportunity to promote your shop, which makes portal authentication an excellent choice. Customers will be directed to a web page for access verification, on which your personalized promotion is displayed. Moreover, you can specify a web link so that the newly connected guest will be redirected to, for example, the official website of your shop.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Portal.
3. Enable Portal.

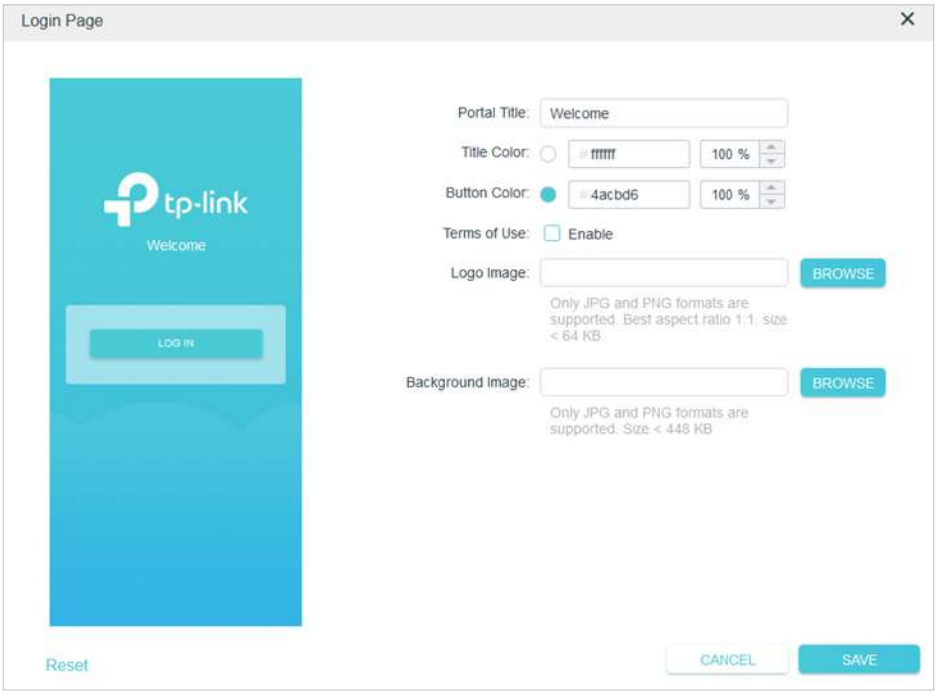
Note: The figure below uses the Portal page of the Access Point mode as an example. In the Multi-SSID mode, more Wi-Fi networks will be available to select.



4. Select the Wi-Fi networks for portal authentication.
5. Select the Authentication Type.

- If you select No Authentication, clients can access the specified Wi-Fi networks without any authentication.
- If you select Simple Password, you can set a password for clients.

6. Select a time for Authentication Timeout. A client has to reconnect to the network when its authentication expires.
7. (Optional) Enable Redirect and enter your desired website. Newly connected clients will be redirected to the specified website.
8. (Optional) Click to edit the Login Page. You can personalize the appearance and content of the login page for newly connected clients.


Login Page
tp-link
Welcome
LOG IN
Portal Title:
Welcome
Title Color:
ffffff
100 %
Button Color:
4acbd6
100 %
Terms of Use:
Enable
Logo Image:
BROWSE
Only JPG and PNG formats are supported. Best aspect ratio 1:1, size < 64 KB
Background Image:
BROWSE
Only JPG and PNG formats are supported. Size < 448 KB
Reset
CANCEL
SAVE

9. Click SAVE.

Chapter 6

Access Control

Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or allowed devices (Whitelist).

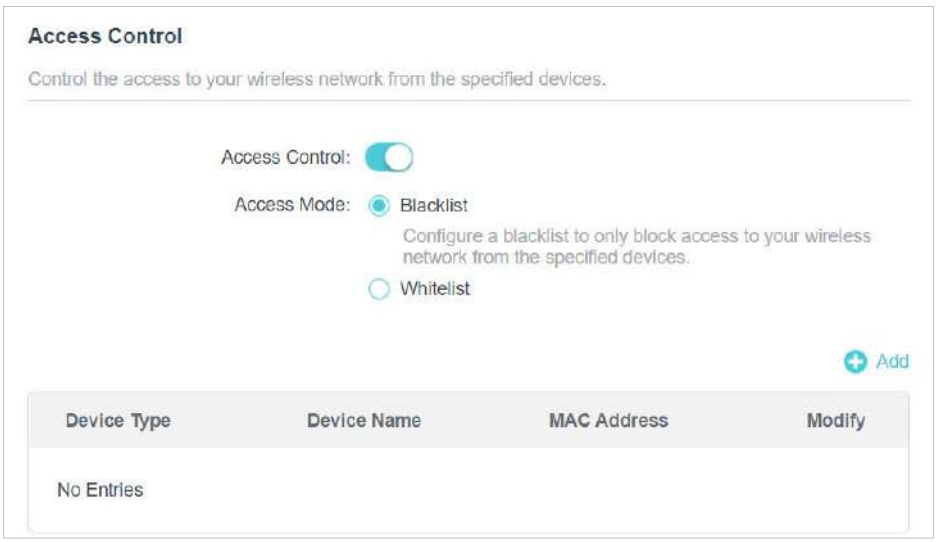
1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Internet > Access Control.

Note: Access Control is not available in Client mode.

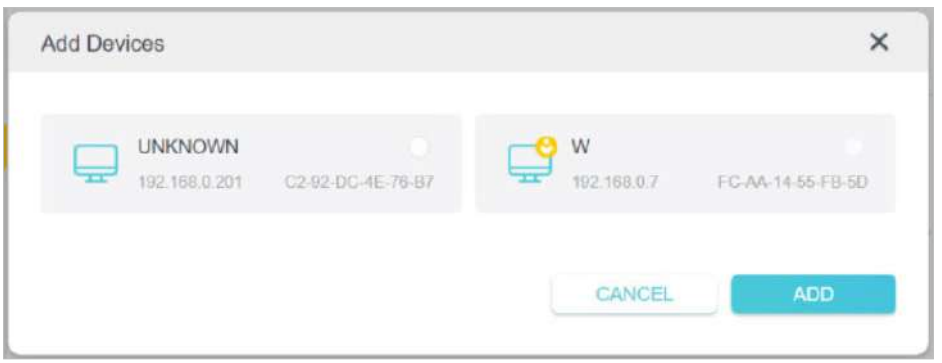
3. Turn on Access Control.
4. Select the access mode to either block (recommended) or allow specific device(s).

To block specific devices:

1) Click Blacklist.



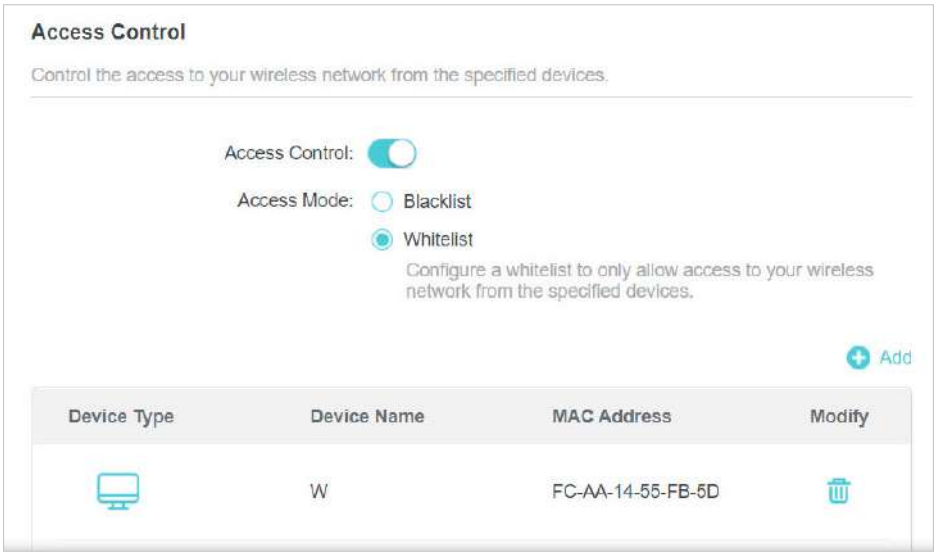
2) Click Add.



3) Select the devices you want to block and click ADD.

To allow specific devices:

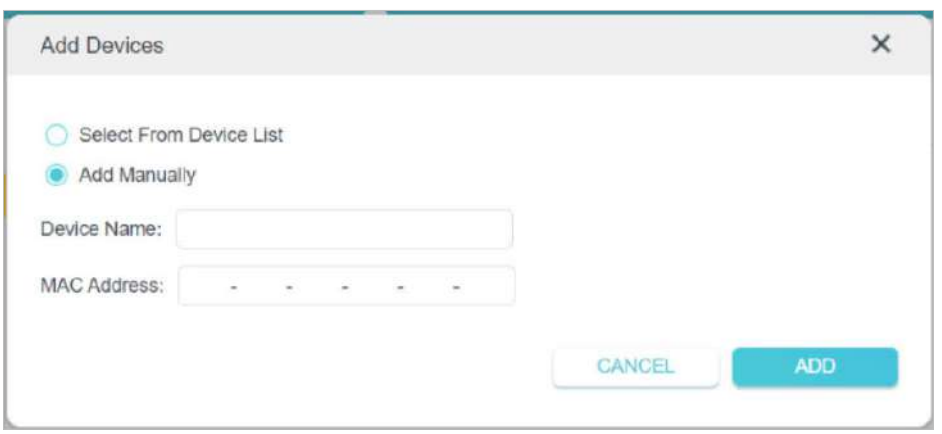
1) Click Whitelist and click SAVE. Your current device will be automatically added to the whitelist.



2) Click Add to add other devices you want to allow.

3) Click Select From Device List, choose devices, then click ADD.

Alternatively, click Add Manually, enter the device name and MAC address, then click ADD.



Done!

Now you can block or allow specific client devices to access your network using the Blacklist or Whitelist.

Chapter 7

Customize Network Settings

This chapter introduces how to customize your network settings.

It contains the following sections:

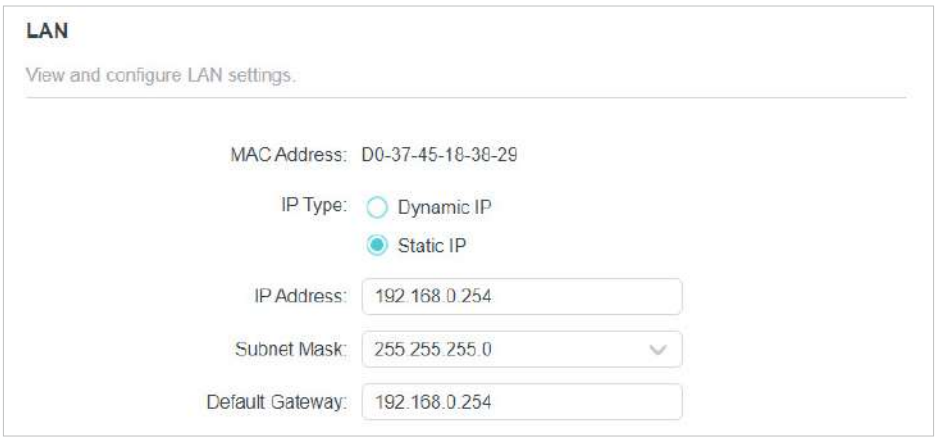
- Change the LAN Settings
- Specify DHCP Server Settings

7. 1. Change the LAN Settings

The access point is preset with Dynamic IP, which allows it to dynamically obtain an IP address and gateway from the main router/AP. It is recommended that you keep the default LAN settings to avoid IP conflict with the main router/AP or other devices on your local network.

If you want to set a static IP address for the access point, follow the steps below:

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Internet > LAN.
3. Choose Static IP.
4. Set an IP address, which should be in the same subnet as the main router/AP.



5. Leave other parameters as the default settings.
6. Click SAVE.

Tip:
After setting a static IP address, you can use the new IP address to log into the web management page besides http://tplinkap.net.

7. 2. Specify DHCP Server Settings

By default, the DHCP (Dynamic Host Configuration Protocol) server works in Auto mode to avoid IP conflict. It will automatically assign IP addresses to clients from its IP address pool only when the DHCP server of the main router/AP is disabled.

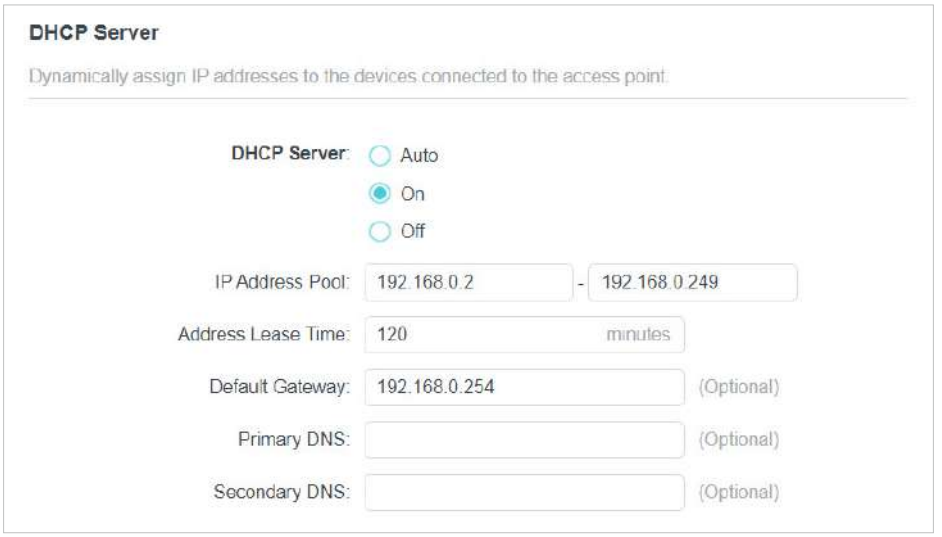
You can change the DHCP server settings if necessary, and you can reserve LAN IP addresses for specified client devices.

Note:
If you disable the DHCP server and there is no other DHCP server within your LAN, you have to configure the IP address for each client manually.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Internet > DHCP Server.

- **To specify the IP address range that the access point assigns:**

1. Turn on DHCP Server.

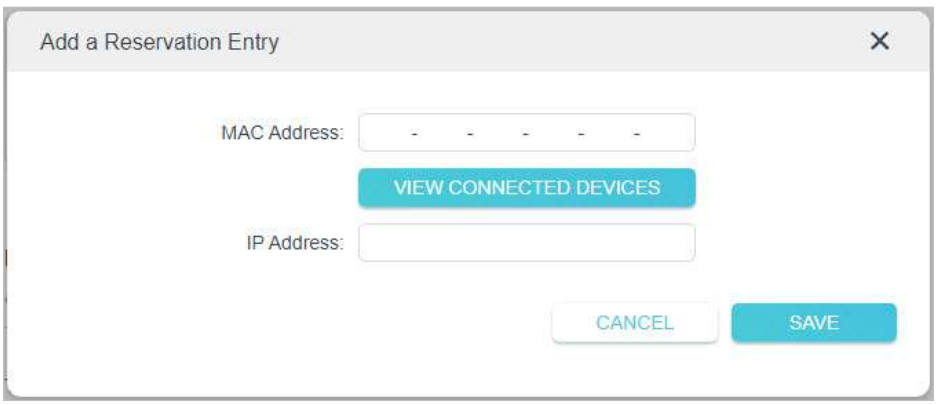


2. Enter the starting and ending IP addresses of the IP Address Pool.
3. Leave other parameters as the default settings.
4. Click SAVE.

- **To reserve an IP address for a specified client device:**

The DHCP server of the access point works when it is turned on, or when it is in Auto mode with the DHCP server of the main router/AP disabled. When it is working, you can view the DHCP clients and reserve IP addresses for them.

1. In the Address Reservation section, click Add.



2. Click VIEW CONNECTED DEVICES and select the device you want to reserve an IP for. The MAC Address will be automatically filled in. You can also enter the MAC address of the client device manually.
3. Enter the IP address to reserve for the client device.
4. Click SAVE.

Chapter 8

Manage Your Access Point

This chapter will show you how to configure and manage your access point.

It contains the following sections:

- Set the System Time and Language
- Control LEDs
- Configure the SNMP Agent
- Configure the Ping Watchdog
- Update the Firmware
- Backup and Restore Configuration Settings
- Reboot the Access Point
- Change the Login Password
- Password Recovery
- Local Management
- Test the Network Connectivity
- System Log

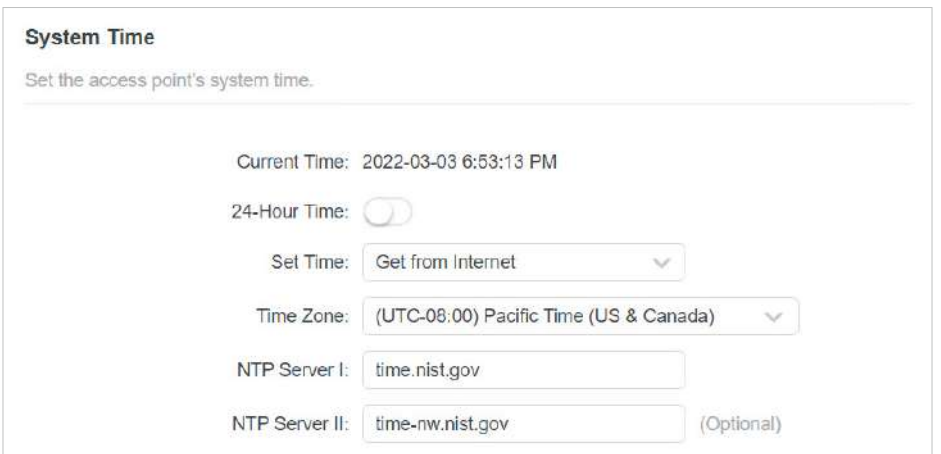
8. 1. Set the System Time and Language

System time is the time displayed while the access point is running. The system time you configure here will be used for other time-based functions like Reboot Schedule. You can choose the way to obtain the system time as needed.

System language is the language displayed when you log into the access point. You can change the system language as needed.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Time & Language.
3. (Optional) Enable 24-Hour Time if you want to display the time in 24-hour format.
4. Set the system time and languange according to your needs.
   - **To set system language:**
     1) Select the language from the dropdown list.

     2) Click SAVE.
   - **To get the system time from the internet:**
     1) In the Set Time field, select Get from Internet.



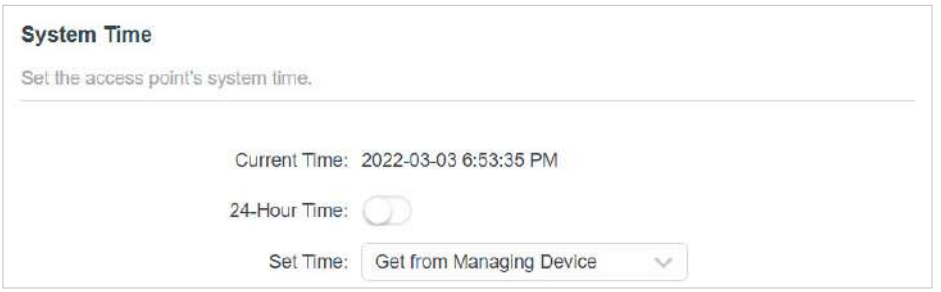
     2) Select your local Time Zone from the drop-down list.
     3) In the NTP Server I field, enter the IP address or domain name of your desired NTP Server.

4) (Optional) In the NTP Server II field, enter the IP address or domain name of the second NTP Server.

5) Click SAVE.

- **To get the system time from the managing device:**

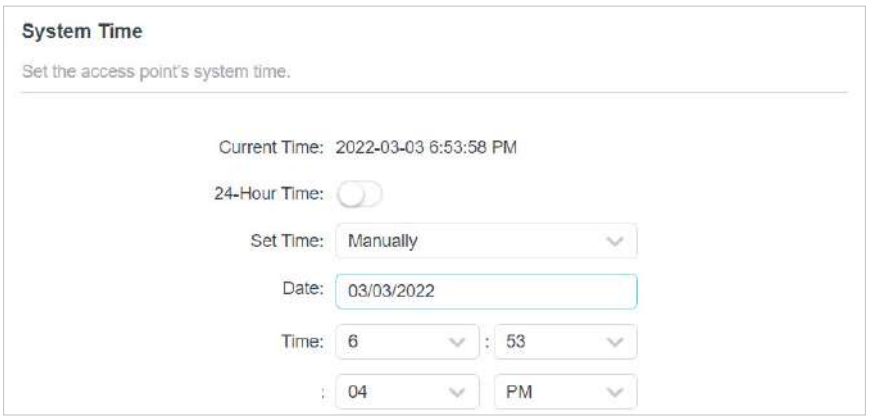
1) In the Set Time field, select Get from Managing Device.



2) Click SAVE.

- **To manually set the system time:**

1) In the Set Time field, select Manually.



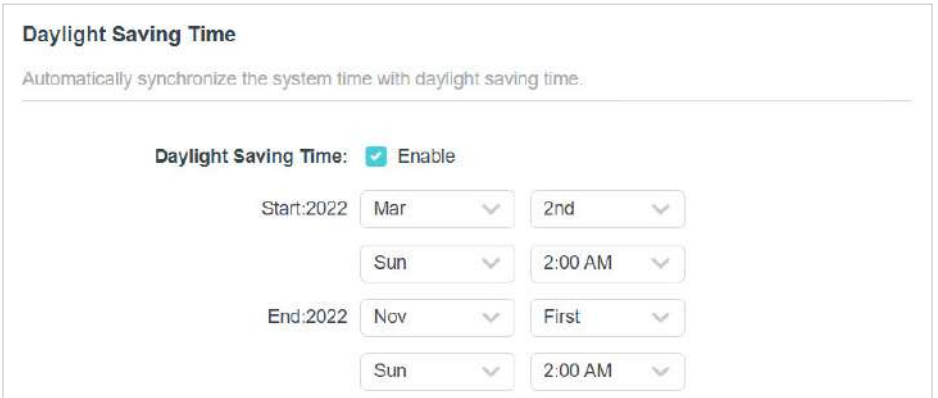
2) Set the current Date (In MM/DD/YYYY format).

3) Set the current Time (In HH/MM/SS format).

4) Click SAVE.

- **To set up Daylight Saving Time:**

1) Enable Daylight Saving Time.



2) Select the correct Start date and time when daylight saving time starts at your local time zone.

3) Select the correct End date and time when daylight saving time ends at your local time zone.

4) Click SAVE.

8. 2. Control LEDs

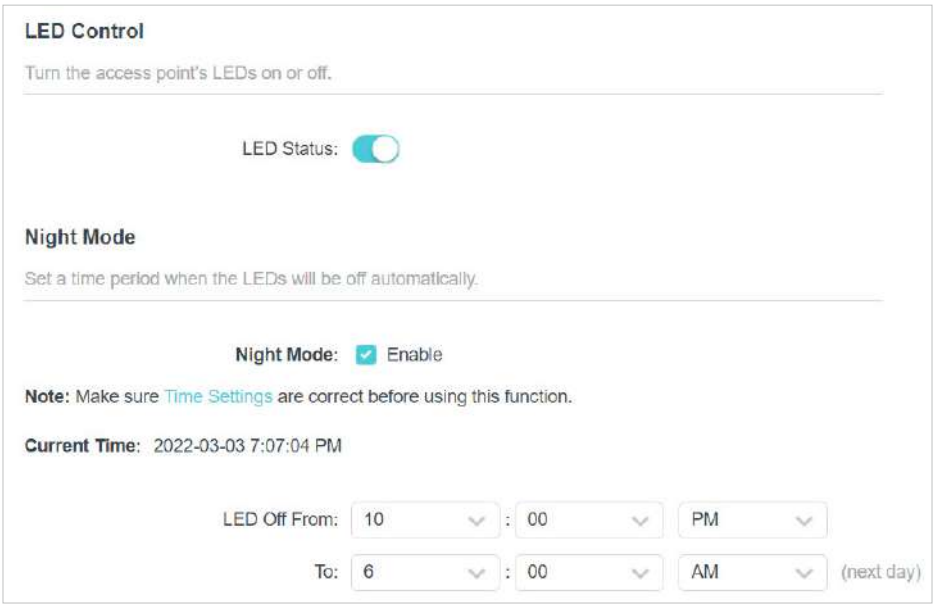
The LEDs of access point indicate its activities and status. You can turn off the LEDs when you don't need them.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > LED Control.
3. Turn off the LEDs when you don't need them.

- If you want to turn off LEDs immediately, turn off LED Status.

- If you want to turn off LEDs during a specific time period, follow the steps below:

  1) Enable LED Status and Night Mode.



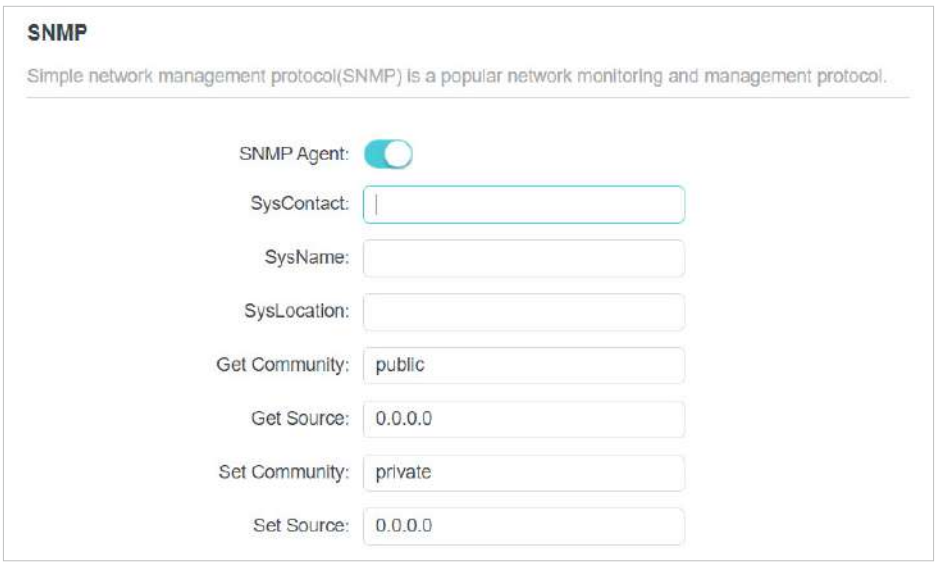
2) Specify the LED Off Time as needed, and the LEDs will be off during the period.

4. Click SAVE.

8. 3. Configure the SNMP Agent

SNMP (Simple Network Management Protocol) is a popular network monitoring and management protocol. You can configure the SNMP agent to communicate with your network monitoring tool or network management system.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > SNMP.
3. Enable SNMP Agent.



4. Configure the SNMP agent according to your actual network requirement.

- SysContact – Enter the contact email address of the node to be managed.
- SysName – Set a user-defined name for the node to be managed.
- SysLocation – Enter the physical location of the node to be managed.
- Get Community – Enter the community name that allows read-only access to the device's SNMP information. The community name is considered as a group password. The default setting is public.
- Get Source – Enter the IP address or subnet that management systems can read information from this 'get' community.

  Note: A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If 0.0.0.0 is specified as the IP address, the agent will accept all requests under the corresponding community name.

- Set Community – Enter the community name that allows read/write access to the device's SNMP information. The community name can be considered as a group password. The default setting is private.
- Set Source – Enter the IP address or subnet that management systems can read and write to this 'set' community.

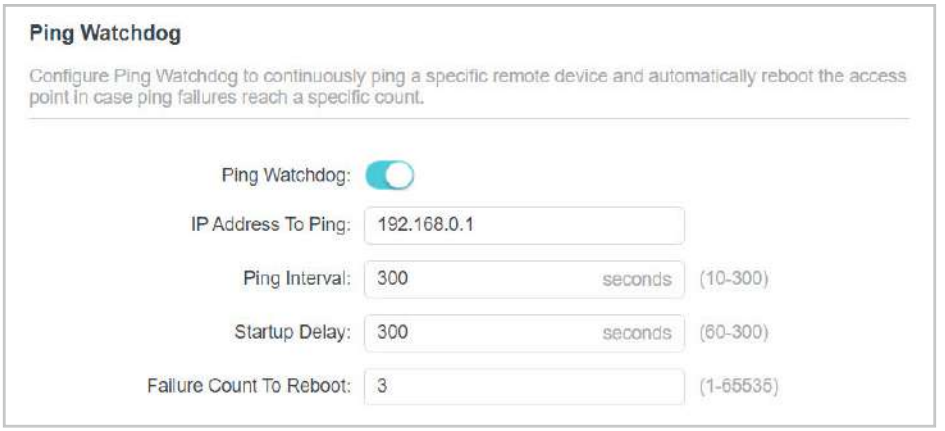
  Note: A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If 0.0.0.0 is specified as the IP address, the agent will accept all requests under the corresponding community name.

5. Click SAVE.

8. 4. Configure the Ping Watchdog

Ping Watchdog allows the access point to continuously ping a specific remote host for connection status using a user-defined IP address (or an internet gateway). If it is unable to ping the target IP address under the user-defined constraints, the device will automatically reboot.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Ping Watchdog.
3. Enable Ping Watchdog.



4. In IP Address To Ping field, enter the IP address of the target host that you want to send ping packets to.
5. In Ping Interval field, enter the time interval between two continuous ping packets.
6. In Startup Delay field, enter the time delay before the first ping packet is sent out when the device is restarted.
7. In Fail Count To Reboot field, enter a number of ping count(s) that the device can send continuously. If ping failures reaches the value, the device will restart automatically.
8. Click SAVE.

8. 5. Update the Firmware

TP-Link is committed to improving product features, giving you a better network experience.

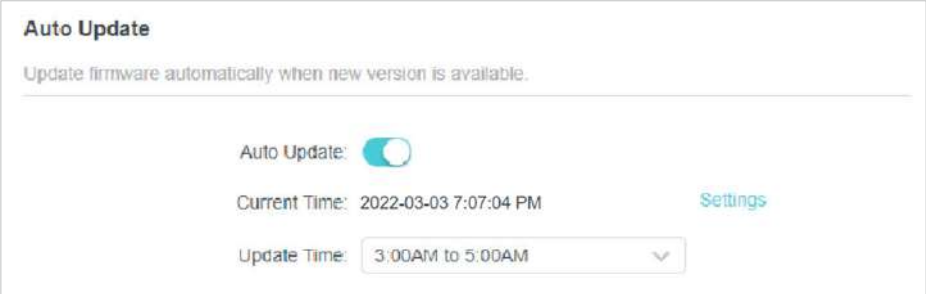
We will inform you through the web management page if there's any new firmware available for your access point. Also, the latest firmware will be released at the TP-Link official website www.tp-link.com, and you can download it from the Support page for free.

Note:

- Make sure the latest firmware file matches the hardware version (as shown in the download section of the Support page).
- Make sure that you have a stable connection between the access point and your computer. Wired connection is recommended.
- Back up your access point's configurations before firmware update.
- Do NOT turn off the access point during the firmware update.

8. 5. 1. Auto Update

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Firmware Update.
3. Enable Auto Update.



4. Specify the Update Time and save the settings.

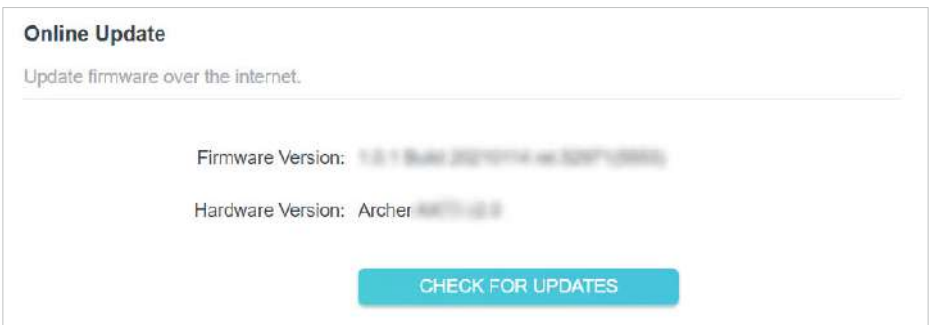
When a new version is available, the access point will update the firmware automatically at the specified time.

8. 5. 2. Online Update

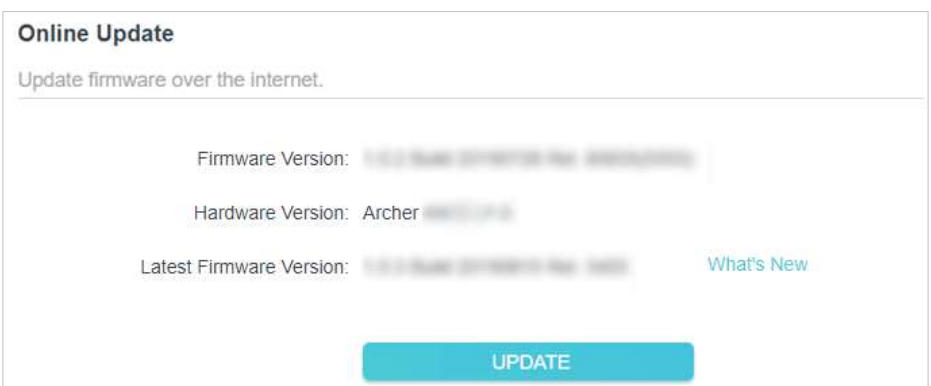
1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Firmware Update.

Tip: When new firmware is available for your access point, the update icon will display in the top-right corner of the web page. You can click the icon to go to the Firmware Update page.

3. Focus on the Online Update section, click CHECK FOR UPDATES to see whether new firmware is available.



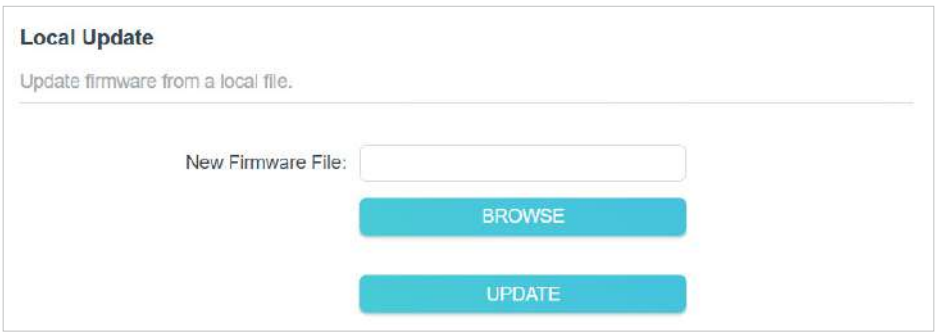
4. Click UPDATE if there is new firmware.



5. Wait a few minutes for the update and reboot to complete.

8. 5. 3. Local Update

1. Download the latest firmware file for the access point from www.tp-link.com.
2. Visit http://tplinkap.net, and log in with the password you set for the access point.
3. Go to System > Firmware Update.
4. Focus on the Local Update section, click BROWSE to locate the downloaded new firmware file, and click UPDATE.



5. Wait a few minutes for the update and reboot to complete.

Note: If you fail to update the firmware for the access point, please contact our Technical Support.

8. 6. Backup and Restore Configuration Settings

The configuration settings are stored as a configuration file in the access point. You can back up the configuration file to your computer for future use and restore the access point to previous settings from the backup file when needed. Moreover, if necessary, you can erase the current settings and reset the access point to its factory settings.

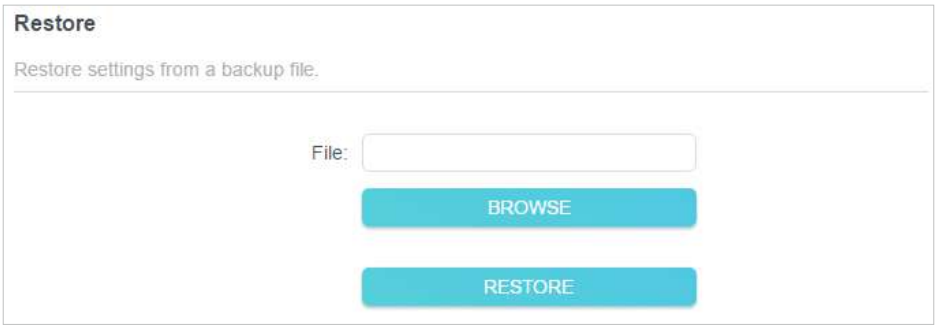
1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Backup & Restore.

- **To back up configuration settings**

  Click BACK UP to save a copy of the current settings to your local computer. A '.bin' file of the current settings will be stored on your computer.

- **To restore configuration settings**

  1) Click BROWSE to locate the backup configuration file stored on your computer, and click RESTORE.

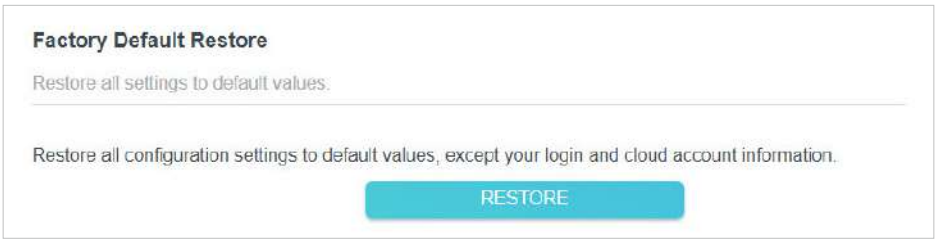


2) Wait a few minutes for the restore and reboot.

Note: During the restore process, do not power off or reset the access point.

- **To reset the access point except your login password and cloud account information:**

1) In the Factory Default Restore section, click RESTORE.



2) Wait a few minutes for the resetting and rebooting.

Note:
- During the resetting process, do not turn off the access point.
- After reset, you can still use the current login password or the TP-Link ID to log in to the web management page.

- **To reset the access point to its factory settings:**

1) In the Factory Default Restore section, click FACTORY RESTORE.

2) Wait a few minutes for the resetting and rebooting.

Note:
- During the resetting process, do not turn off or reset the access point.
- We strongly recommend you back up the current configuration settings before resetting the access point.

8. 7. Reboot the Access Point

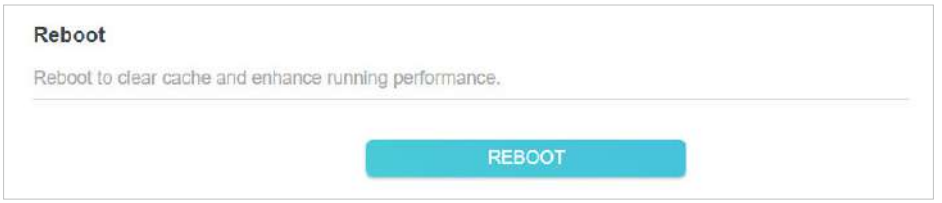
Rebooting help clean cache and enhance running performance of the access point. You can reboot the access point immediately or schedule it to reboot periodically.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.

2. Go to System > Reboot.

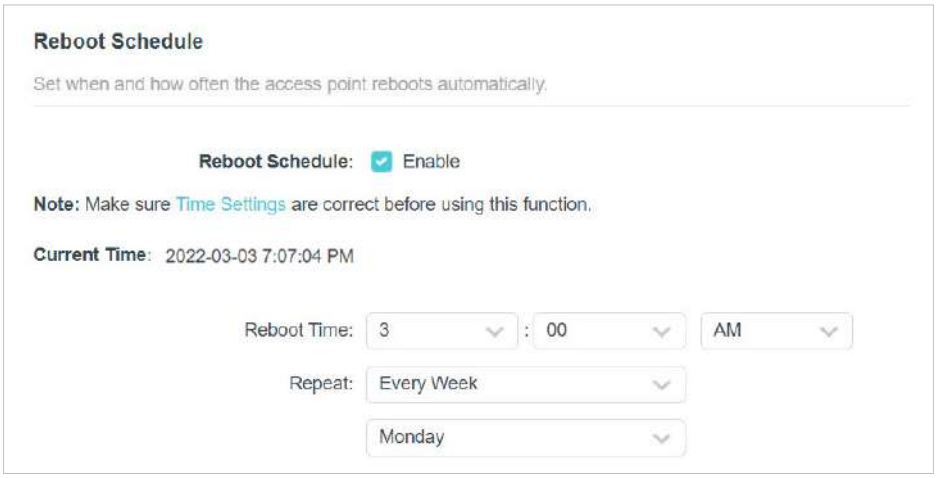
- **To reboot the access point immediately:**

  Click REBOOT.



- **To schedule the access point to reboot periodically:**

  1) Enable Reboot Schedule.



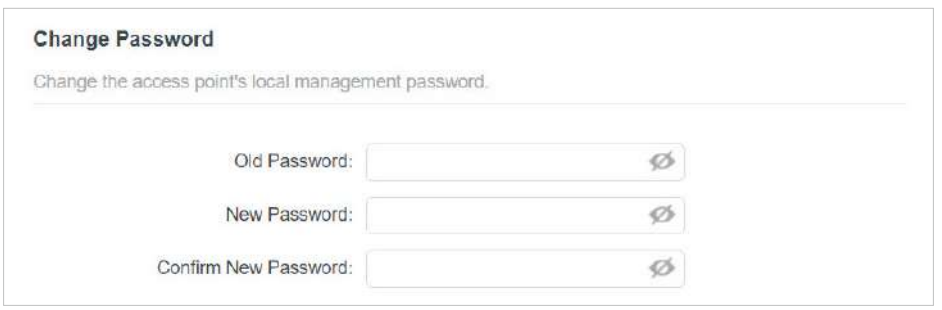
  2) Set the Reboot Time and Repeat time.

  3) Click SAVE. The access point will reboot periodically as scheduled.

8. 8. Change the Login Password

The account management feature allows you to change your login password of the web management page.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Administration.

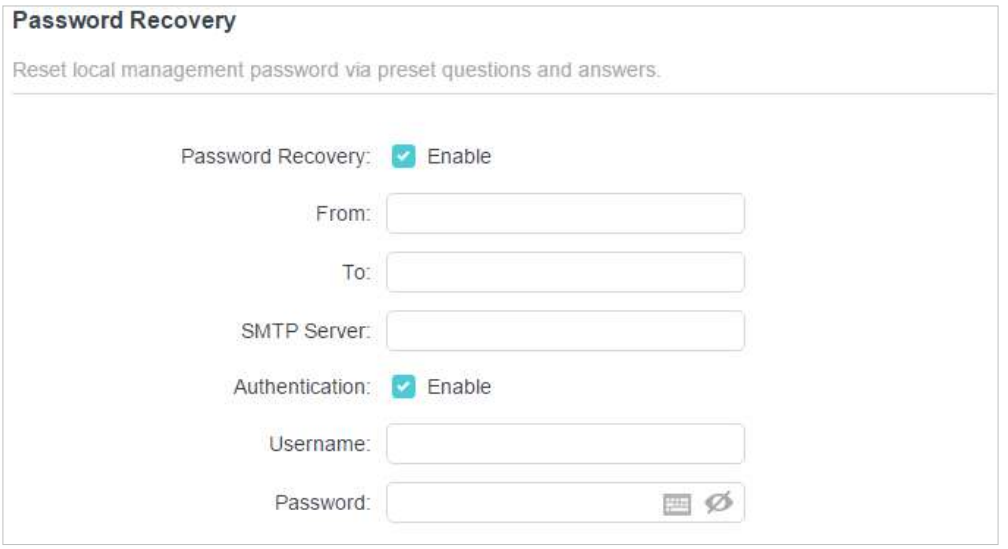


3. Enter the old password, and then enter a new password twice (both case-sensitive).
4. Click SAVE and use the new password for future logins.

8. 9. Password Recovery

This feature allows you to recover the login password you set for you access point in case you forget it.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Administration and focus on the Password Recovery section.
3. Enable Password Recovery.



4. Specify a mailbox (From) for sending the recovery letter and enter its SMTP Server address.
5. Specify a mailbox (To) for receiving the recovery letter.
6. If the mailbox (From) to send the recovery letter requires encryption, tick the Enable box of Authentication and enter its username and password.

   Tips:

   - SMTP server is available for users in most webmail systems. For example, the SMTP server address of Gmail is smtp.gmail.com.
   - Generally, Authentication should be enabled if the login of the mailbox requires username and password.

7. Click SAVE.

To recover the login password, visit http://tplinkap.net, click Forgot Password? on the login page and follow the instructions to set a new password.

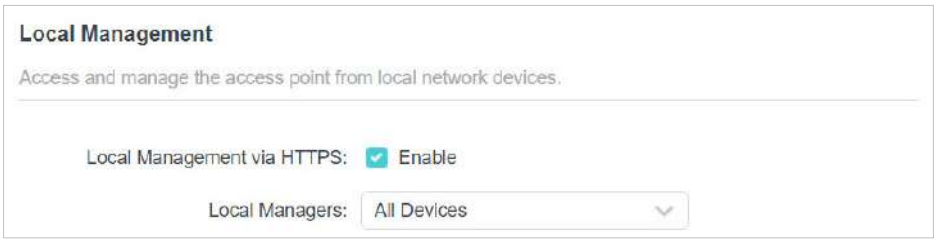
8. 10. Local Management

This feature allows you to limit the number of client devices on your LAN from accessing the access point by using the MAC address-based authentication.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Administration and focus on the Local Management section.

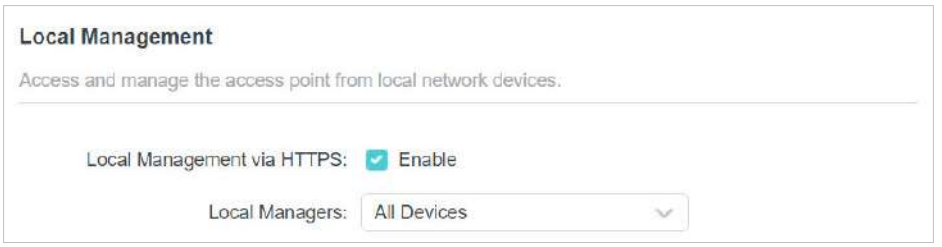
- **Access the access point via HTTPS and HTTP:**

Tick the Enable box of Local Management via HTTPS to access the access point via HTTPS and HTTP, or keep it disabled to access the access point only via HTTP.



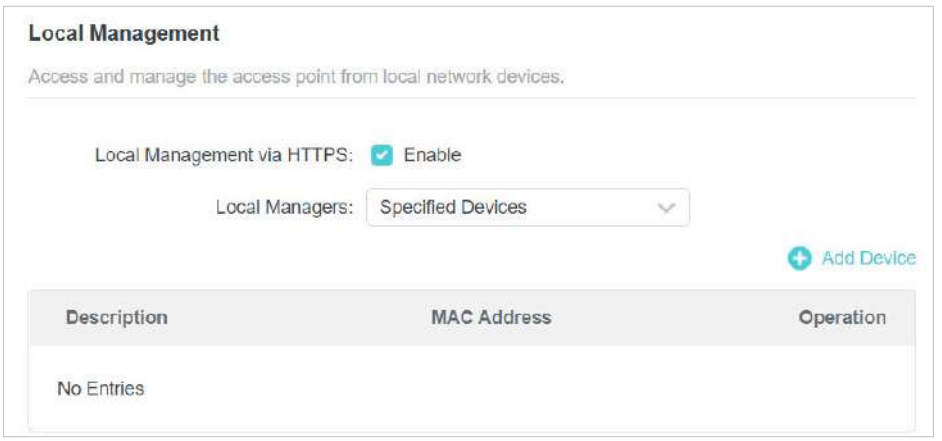
- **Allow all LAN connected devices to manage the access point:**

Select All Devices for Local Managers.

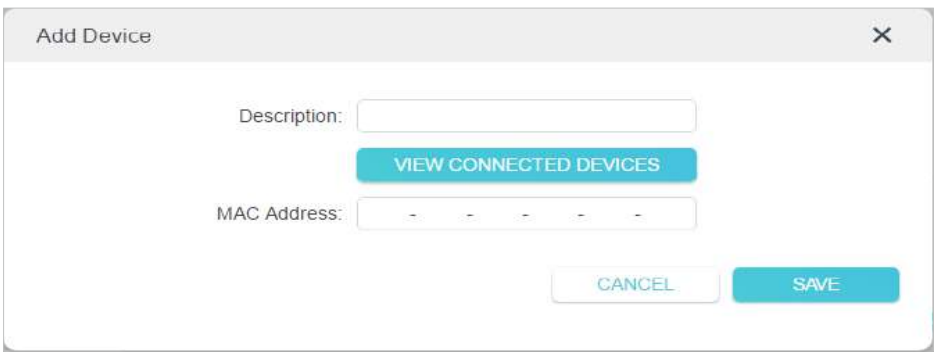


- **Allow specific devices to manage the access point:**

1. Select Specified Devices for Local Managers and click SAVE.



2. Click Add Device.



3. Click VIEW CONNECTED DEVICES and select the device to manage the access point from the devices list, or enter the MAC address of the device manually.
4. Specify a Description for this entry.
5. Click SAVE.

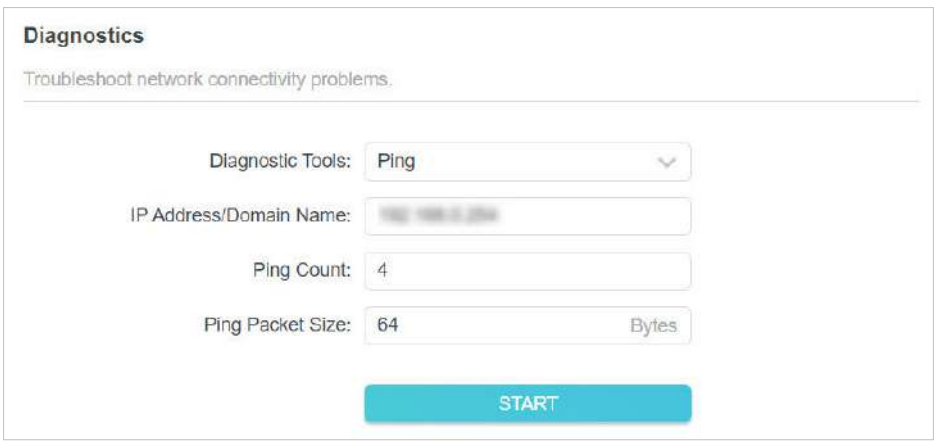
8. 11. Test the Network Connectivity

Diagnostics is used to test the connectivity between the access point and the host or other network devices.

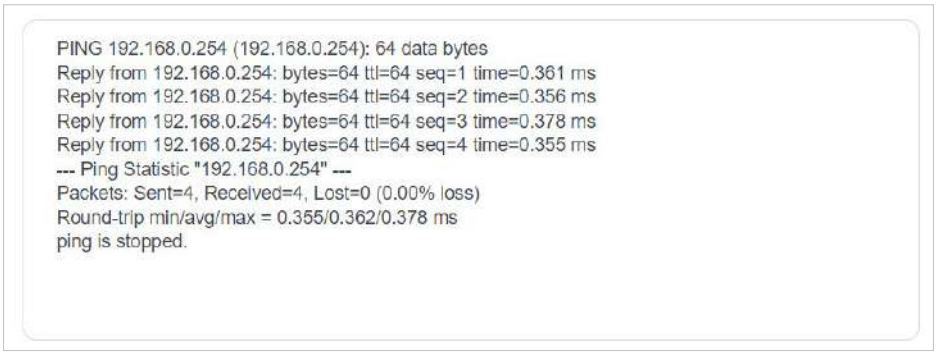
Ping is used to test the connectivity between the access point and the tested host, and measure the round-trip time.

Traceroute is used to display the route (path) your access point has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > Diagnostics.
   - **To test the connectivity via Ping:**
     1) Choose Ping as the diagnostic tool.

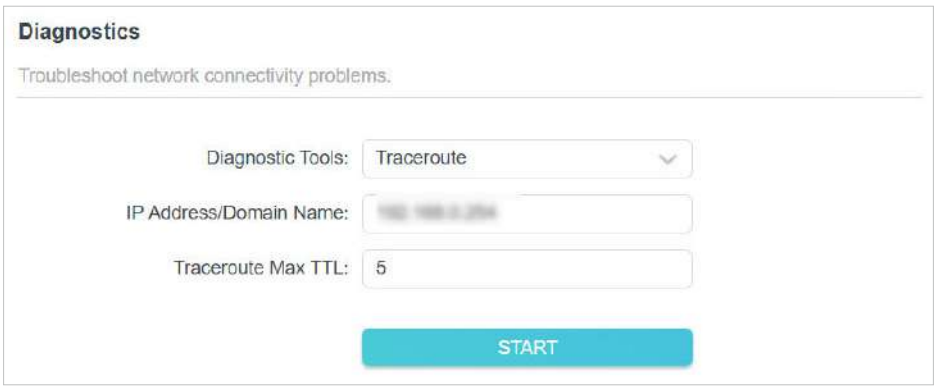


     2) Enter the IP Address or Domain Name of the tested host.
     3) Keep the default Ping Count and Ping Packet Size.
     4) Click START to begin the diagnostics. The diagnostics result will be displayed.



- **To test the connectivity via Traceroute:**

1) Choose Traceroute as the diagnostic tool.



2) Enter the IP Address or Domain Name of the tested host.

3) Keep the default Traceroute Max TTL.

4) Click START to begin the diagnostics. The diagnostics result will be displayed.

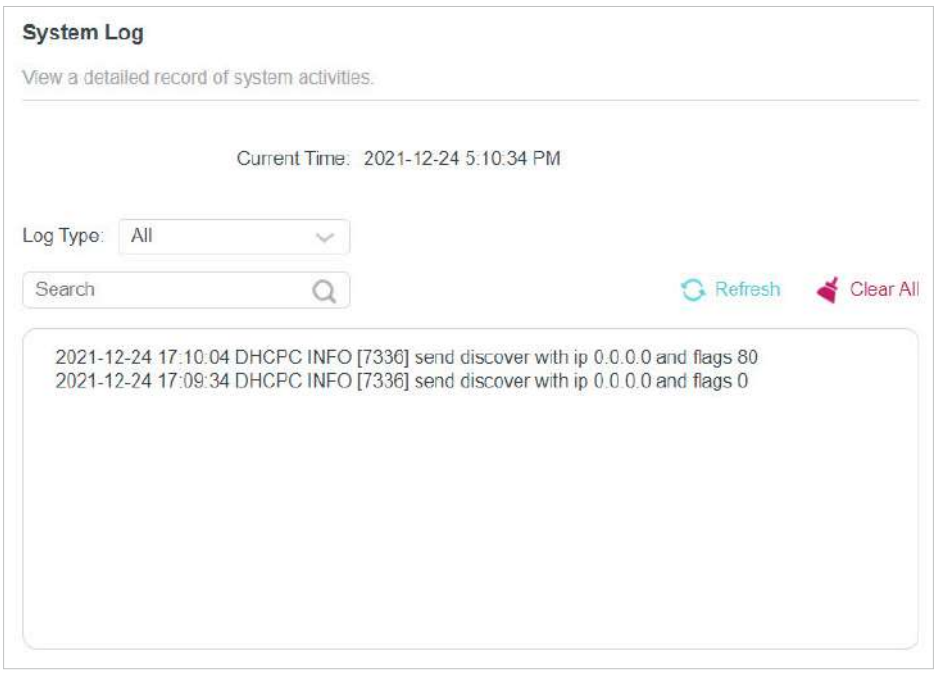
8. 12. System Log

When the access point does not work normally, you can save the system log and send it to the technical support for troubleshooting.

- **To save the system log locally:**

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > System Log.

3. Choose the type and level of the system logs as needed.

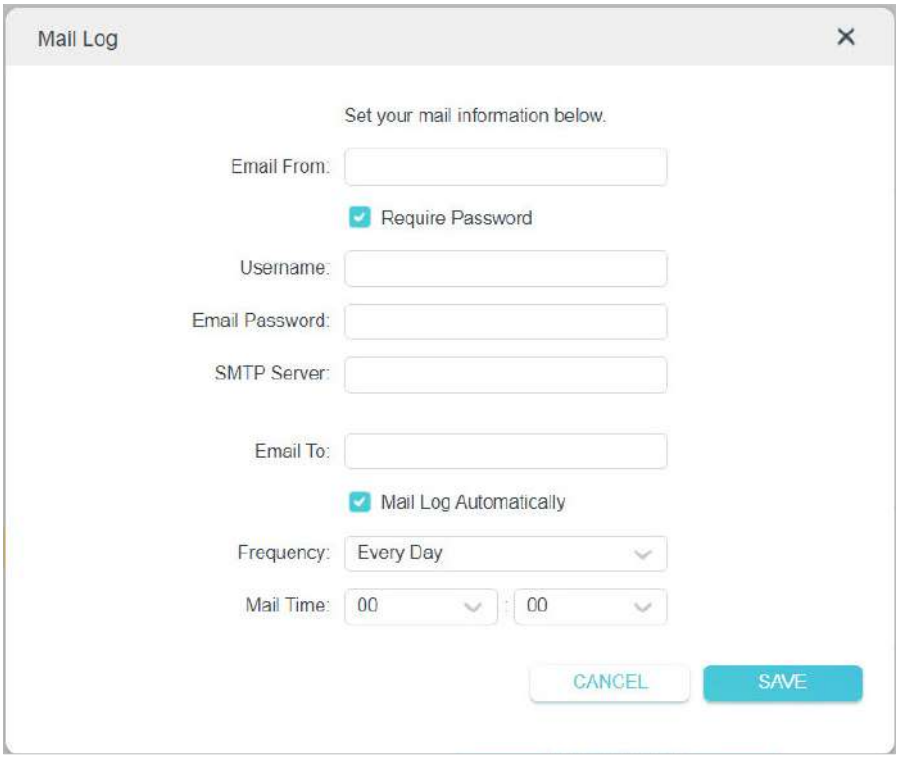


4. In the Save Log section, click SAVE TO LOCAL to save the system logs to a local disk.

- **To send the system log to a mailbox at a fixed time:**

For example, I want to check my access point's working status at a fixed time every day, however, it's too troublesome to log in to the web management page every time I want to go checking. It would be great if the system logs could be sent to my mailbox at 8 a.m. every day.

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to System > System Log.
3. In the Save Log section, click MAIL LOG.
4. Enter the information required:



1) Email From: Enter the email address used for sending the system log.

2) Select Require Password.

Tips: Generally, Require Password should be selected if the login of the mailbox requires username and password.

3) Username: Enter the user name to log in to the sender's email address.

4) Email Password: Enter the password to log in to the sender's email address.

5) SMTP Server: Enter the SMTP server address.

Tips: SMTP server is available for users in most webmail systems. For example, the SMTP server address of Hotmail is smtp-mail.outlook.com.

6) Email To: Enter the recipient's email address, which can be the same as or different from the sender's email address.

7) Select Mail Log Automatically.

Tips: The access point will send the system log to the designated email address if this option is enabled.

8) Frequency: This determines how often the recipient will receive the system log.

9) Mail Time: Set the time when the recipient will receive the system log.

5. Click SAVE.

FAQ

Q1. How do I restore the access point to its factory default settings?

With the access point powered on, use a pin to press and hold the Reset button until the Power LED blinks, then release the button.

Note: Resetting the access point will clear all previous configurations, and the access point will reset to the default Access Point mode.

Q2. What should I do if I cannot access the web management page?

- If the computer has a static IP address, change its settings to obtain an IP address automatically.
- Verify that http://tplinkap.net or http://192.168.0.254 is correctly entered in the web browser.
- Use another web browser and try again.
- Reboot your access point and try again.
- Power off your host AP and enter http://tplinkap.net in the web browser to try again.

Q3. What should I do if I forget my wireless password?

The default wireless password is printed on the label of the access point. If the password has been altered, please connect your computer to the access point using an Ethernet cable and follow the steps below:

1. Visit http://tplinkap.net, and log in with the password you set for the access point.
2. Go to Wireless > Wireless Settings to retrieve or reset your wireless password.

Q4. What should I do if I forget my login password of the web management page?

1. Refer to Q1 to reset the access point to its factory default settings.
2. Visit http://tplinkap.net, and create a new login password.

Note: You'll need to reconfigure the access point to surf the internet once the access point is reset, and please mark down your new password for future use.

Q5. What should I do if my wireless is not stable?

This could be caused by interference. You can try the following methods:

- Log in to the web management page. Go to Wireless > Wireless Settings and change your wireless channel to a different one.
- Move the access point to a new location away from Bluetooth devices and other household electronics, such as cordless phones, microwaves, and baby monitors, to minimize signal interference.

Q6. What should I do to maximize my signal strength in Range Extender mode?

When choosing an ideal location to optimize wireless signal in Range Extender mode, please refer to the following recommendations.

- Halfway is the best way.

  Generally, the ideal location for an access point is about halfway between your wireless router and your wireless clients and make sure that the location you choose is within the range of the host router. If that is not possible, place it closer to your wireless router to ensure stable performance.

- Fewer obstacles ensure better performance.

  Choose a location with less obstacles around that may block the signal between the access point and the host network. An open corridor or a spacious location is ideal.

- Less interference provides more stability.

  Choose a location away from Bluetooth devices and other household electronics, such as cordless phones, microwaves, and baby monitors to minimize signal interference.

FCC compliance information statement

Product Name: AX1800 Gigabit Wi-Fi 6 Access Point

Model Number: TL-WA1801

Component Name	Model
I.T.E. Power Supply	T480038-2B1

Responsible party:

TP-Link USA Corporation

Address: 10 Mauchly, Irvine, CA 92618

Website: http://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6804

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC compliance information statement

Product Name: I.T.E. Power Supply
Model Number: T480038-2B1
Responsible party:
TP-Link USA Corporation
Address: 10 Mauchly, Irvine, CA 92618
Website: http://www.tp-link.com/us/
Tel: +1 626 333 0234
Fax: +1 909 527 6804
E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2023-09-12

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

OPERATING FREQUENCY(the maximum transmitted power)

2400 MHz – 2483.5 MHz (18dB)

5150 MHz – 5250 MHz (20dB)

EU Declaration of Conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/53/EU, 2009/125/EC, 2011/65/EU and (EU)2015/863.

The original EU Declaration of Conformity may be found at
https://www.tp-link.com/en/support/ce/

RF Exposure Information

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm from your body.

National Restrictions

Frequency band: 5150 - 5250 MHz:

Indoor use: Inside buildings only. Installations and use inside road vehicles and train carriages are not permitted. Limited outdoor use: If used outdoors, equipment shall not be attached to a fixed installation or to the external body of road vehicles, a fixed infrastructure or a fixed outdoor antenna. Use by unmanned aircraft systems (UAS) is limited to within the 5170 - 5250 MHz band.

	AT	BE	BG	CH	CY	CZ	DE	DK
	EE	EL	ES	FI	FR	HR	HU	IE
	IS	IT	LI	LT	LU	LV	MT	NL
	NO	PL	PT	RO	SE	SI	SK	UK(NI)

UKCA Mark

UK Declaration of Conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK Declaration of Conformity may be found at
https://www.tp-link.com/support/ukca

National Restrictions

Attention: This device may only be used indoors in Great Britain.

!	UK

Canadian Compliance Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution:

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice:

注意！

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前述合法通信，指依電信管理法規定作業之無線電通信。

低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

應避免影響附近雷達系統之操作。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

限用物質含有情況標示聲明書

設備名稱：AX1800 Gigabit Wi-Fi 6 Access Point Equipment name	型號（型式）：TL-WA1801 Type designation (Type)

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	—	○	○	○	○	○
其他及其配件	—	○	○	○	○	○

備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值

Note 1: "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2: "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3.〝—〞係指該項限用物質為排除項目。

Note 3: The "—" indicates that the restricted substance corresponds to the exemption.

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

EAC

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.
- Operating Temperature: 0°C ~ 40°C (32°F ~ 104°F)
- This product uses radios and other components that emit electromagnetic fields. Electromagnetic fields and magnets may interfere with pacemakers and other

implanted medical devices. Always keep the product and its power adapter more than 15 cm (6 inches) away from any pacemakers or other implanted medical devices. If you suspect your product is interfering with your pacemaker or any other implanted medical device, turn off your product and consult your physician for information specific to your medical device.

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

Explanation of the symbols on the product label

Symbols may vary from products.

Note: The product label can be found at the bottom of the product and its I.T.E. power supply.

Symbol	Explanation
	Class II equipment
	Class II equipment with functional earthing
	Alternating current
	DC voltage
	Polarity of output terminals
	Indoor use only
	Dangerous voltage
	Caution, risk of electric shock
VI	Energy efficiency Marking
	Protective earth
	Earth
	Frame or chassis

Symbol	Explanation
	Functional earthing
	Caution, hot surface
	Caution
	Operator's manual
	Stand-by
	"ON"/"OFF" (push-push)
	Fuse
N	Fuse is used in neutral N
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.
	Caution, avoid listening at high volume levels for long periods
	Disconnection, all power plugs
m	Switch of mini-gap construction
μ	Switch of micro-gap construction (for US version) Switch of micro-gap / micro-disconnection construction (for other versions except US)
ε	Switch without contact gap (Semiconductor switching device)