



User Guide

300Mbps Wireless N Access Point
TL-WA801ND

Contents

About This Guide	1
 Chapter 1. Get to Know About Your Access Point	 2
1. 1. Product Overview	3
1. 2. Panel Layout	3
1. 2. 1.Top View	3
1. 2. 2.The Back Panel	4
 Chapter 2. Connect the Hardware	 6
2. 1. Position Your Access Point	7
2. 2. Connect Your Access Point	7
2. 2. 1.Access Point Mode	7
2. 2. 2.Repeater/Bridge Mode	8
2. 2. 3.Client Mode	8
2. 2. 4.Multi-SSID Mode	9
 Chapter 3. Set Up Internet Connection Via Quick Setup Wizard	 10
3. 1. Log In to the Access Point	11
3. 2. Configure the Access Point	11
3. 2. 1.Access Point Mode	12
3. 2. 2.Repeater/Bridge Mode	13
3. 2. 3.Client Mode	14
3. 2. 4.Multi-SSID Mode	15
3. 3. Set up Internet Connection by WPS (Repeater/Bridge, Client)	17
 Chapter 4. Configure the Access Point	 18
4. 1. Status	19
4. 2. Network	20
4. 2. 1. LAN	20
4. 3. Wireless	21
4. 3. 1.Basic Settings (Access Point, Client, Multi-SSID)	21
4. 3. 2.Connect to Network (Repeater/Bridge)	24
4. 3. 3. WPS	25
4. 3. 4.Wireless Security (Access Point, Multi-SSID)	27
4. 3. 5.Extended Network (Repeater/Bridge)	30

4. 3. 6.	Wireless MAC Filtering	31
4. 3. 7.	Wireless Advanced	32
4. 3. 8.	Wireless Statistics	33
4. 3. 9.	Throughput Monitor	34
4. 4.	DHCP	34
4. 4. 1.	DHCP Settings	34
4. 4. 2.	DHCP Client List	36
4. 4. 3.	Address Reservation	36
4. 5.	System Tools	37
4. 5. 1.	Diagnostic	37
4. 5. 2.	SNMP Settings	39
4. 5. 3.	Ping Watch Dog	40
4. 5. 4.	Firmware Upgrade	41
4. 5. 5.	Factory Defaults	41
4. 5. 6.	Backup & Restore	42
4. 5. 7.	Reboot	42
4. 5. 8.	Password	43
4. 5. 9.	System Log	43
4. 6.	Log Out	44
FAQ		45

About This Guide

This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick Internet setup, while this guide contains details of each function and demonstrates how to configure them.

When using this guide, please notice that features of the access point may vary slightly depending on the model and software version you have, and on your location, language, and internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide the following conventions are used:

Convention	Description
<u>Underlined</u>	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 and so on.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > MAC Filtering means the MAC Filtering function page is under the Wireless menu that is located in the Advanced 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.

More Info

The latest software, management app and utility are available from the [Download Center](#) at www.tp-link.com/support.

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

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

A Technical Support Forum is provided for you to discuss our products at <http://forum.tp-link.com>.

Our Technical Support contact information can be found at the [Contact Technical Support](#) page at www.tp-link.com/support.

Speed/Coverage Disclaimer

*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.

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 Wireless N Access Point, with multiple operation modes, is designed to establish or expand a scalable high-speed wireless N network or to connect multiple Ethernet enabled devices to a wireless network, such as game consoles, digital media adapters, printers, or network attached storage devices. The AP 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 front 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.
	Flashing	The system is starting up or the firmware is being upgraded. Do not disconnect or power off your access point.
	Off	Power is off.
📶 (Wireless)	On	The wireless function is enabled.
	Off	The wireless function is disabled.
🌐 (Ethernet)	On	The ETHERNET port is connected to a powered-on device.
	Off	The ETHERNET port is not connected to a powered-on device.
🔒 (WPS)	On/Off	This light remains on for 2 minutes when a WPS connection is established, then turns off.
	Flashing	WPS connection is in progress. This may take up to 2 minutes.

1.2.2. The Back Panel



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

Ports or Buttons	Description
ON/OFF	To power on or off the access point.
Power	For connecting the access point to a power socket via the provided power adapter.
ETHERNET	The 10/100Mbps LAN port connects to a network device, such as a switch or a router.
WPS	If your client devices, such as wireless adapters, support Wi-Fi Protected Setup, then you can press this button to quickly establish a connection between the access point and the client devices, which automatically configures wireless security for your wireless network.
RESET	Press and hold this button until all the LEDs turn on momentarily.
Antennas	Used for wireless operation and data transmitting. Upright them for the best Wi-Fi performance.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- [Position Your Access Point](#)
- [Connect Your Access Point](#)

2.1. Position Your Access Point

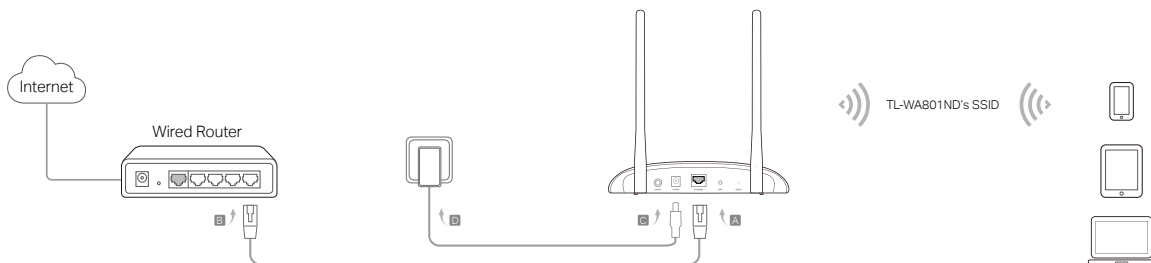
- The product should not be located in a place where it will be exposed to moisture or excessive heat.
- Place the access point in a location where it can be connected to various devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not 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.

2.2. Connect Your Access Point

There are four operation modes supported by this access point: Access Point, Repeater/Bridge, Client and Multi-SSID. Please determine which operation mode you need and carry out the corresponding steps.

2.2.1. Access Point Mode

In Access Point 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. Power on the access point, wait until the Power (🔌) and Wireless (📶) LEDs are lit and stable, and 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.

2.2.2. Repeater/Bridge Mode

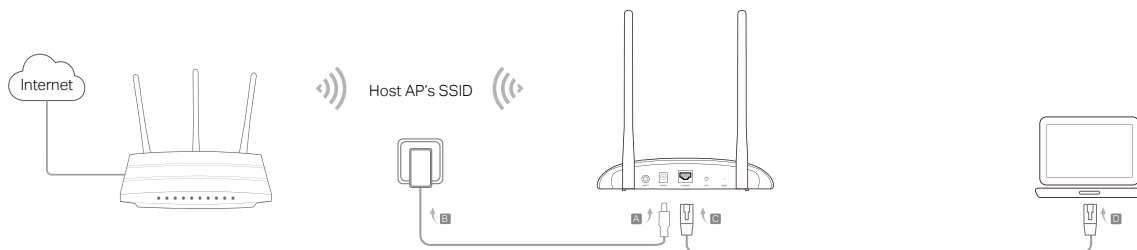
In Repeater/Bridge mode, the access point extends the range of an existing Wi-Fi network. This mode is suitable when you are in a Wi-Fi dead-zone or a place with weak wireless signal, and you want to have a larger effective range of the wireless signal throughout your home or office.



1. Connect the access point according to Step A and B in the diagram.
2. Power on the access point, wait until the Power (🔌) and Wireless (📶) LEDs are lit and stable, and use the default SSID and Password printed on the label of the access point to join its Wi-Fi network.

2.2.3. Client Mode

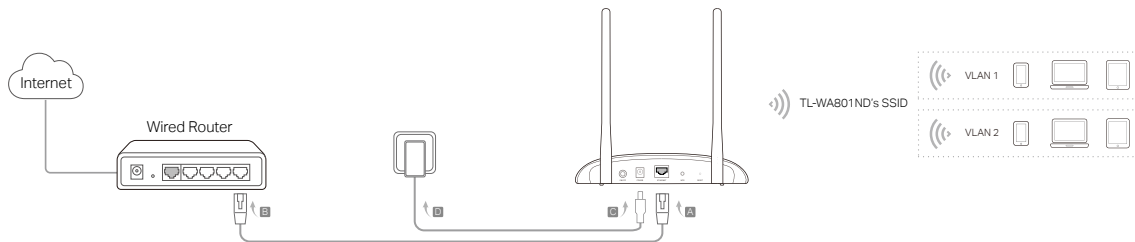
In Client mode, the access point connects your wired devices to a wireless network. This mode is suitable when you have a wired device with an Ethernet port and no wireless capability, for example, a smart TV, media player, or game console and you want to connect it to the internet wirelessly.



1. Connect the access point according to Step A to D in the diagram.
2. Power on the access point, wait until the Power (🔌) and Wireless (📶) LEDs are lit and stable, and use the default SSID and Password printed on the label of the access point to join its Wi-Fi network.

2.2.4. Multi-SSID Mode

In Multi-SSID mode, the access point creates multiple wireless networks to provide different security and VLAN 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. Power on the access point, wait until the Power (🔌) and Wireless (📶) LEDs are lit and stable, and use the default SSID and Password printed on the label of the access point to join its Wi-Fi network.

Chapter 3

Set Up Internet Connection Via Quick Setup Wizard

This chapter introduces how to connect your access point to the internet via the web-based Quick Setup Wizard.

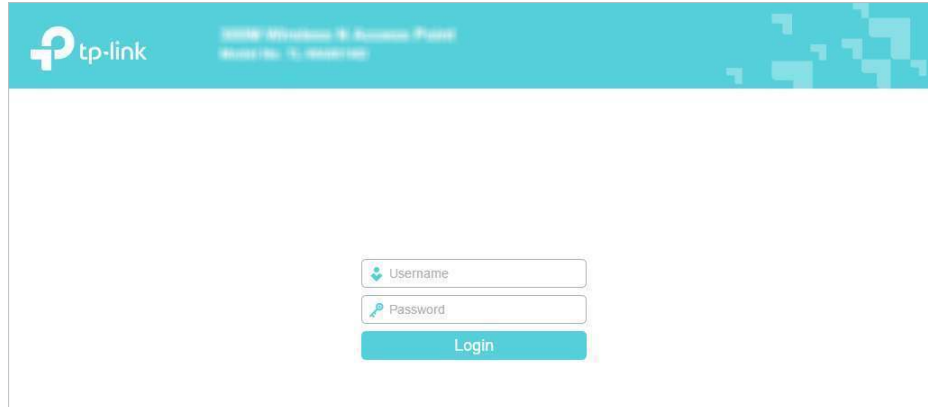
It contains the following sections:

- [Log In to the Access Point](#)
- [Configure the Access Point](#)

3.1. Log In to the Access Point

With a web-based utility, it is easy to configure and manage the access point. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

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

The image shows the login page of the TP-Link web-based utility. At the top, there is a teal header with the TP-Link logo on the left and the text "TP-Link Wireless & Access Point" and "Access Point: 192.168.1.1" on the right. Below the header, the main content area is white and contains a login form. The form has two input fields: "Username" and "Password", each with a small icon to its left. Below these fields is a teal "Login" button.

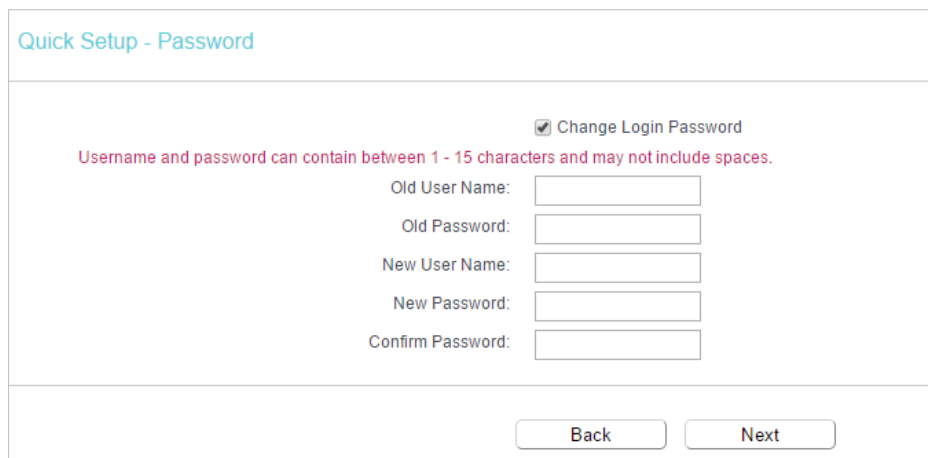
Note:

If the login window does not appear, please refer to the [FAQ](#) Section.

3.2. Configure the Access Point

The Quick Setup Wizard will guide you through the process to set up your access point.

1. Go to [Quick Setup](#) and click [Next](#) to start.
2. If you want to change your login account, tick [Change Login Password](#). Then enter your old username and password, then a new username and password. If not, click [Next](#) to move on.

The image shows the "Quick Setup - Password" page. At the top, there is a teal header with the text "Quick Setup - Password". Below the header, the main content area is white. It features a checkbox labeled "Change Login Password" which is checked. Below the checkbox, there is a red warning message: "Username and password can contain between 1 - 15 characters and may not include spaces." Below this message, there are five input fields: "Old User Name:", "Old Password:", "New User Name:", "New Password:", and "Confirm Password:". At the bottom of the page, there are two buttons: "Back" and "Next".

3. Choose the operation mode you need and click [Next](#). Then follow the corresponding steps to configure your access point.

Quick Setup - Operation Mode

Choose Operation Mode:

☒ Access Point
Set up Wi-Fi on an existing wired network

☐ Repeater/Bridge

☐ Client

☐ Multi-SSID

Back Next

3.2.1. Access Point Mode

1. Either customize your **Wireless Network Name** and **Wireless Password** or keep the default ones, and then click **Next**.

Quick Setup - Wireless

Wireless Network Name: (Also called SSID)

Security:

☒ WPA2-PSK (Recommended)
Wireless Password
(Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

☐ Disable Wireless Security

☐ More Advanced Wireless Settings

Back Next

2. Select the LAN IP type of the access point or leave the default setting **Smart DHCP** for most cases, and then click **Next**.

Quick Setup - Network Setting

Type:

Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)
(In this situation the device will help you configure the IP parameters automatically as you need).

IP Address:

Subnet Mask:

We recommend you configure this AP with the same IP subnet and subnet mask, but different IP address from your root AP/Router.

DHCP Server: ☒ Enable ☐ Disable

Back Next

3. Click **Finish** to complete the configuration. Reconnect your wireless devices to the new Wi-Fi network.

Quick Setup - Review Setting

Congratulations! The settings is finish, please click finish button to make it work. For detailed settings, please click other menus if necessary.

Confirm the configuration you have set. If anything wrong please go Back to reset.
It's recommended to take a note of these settings that you'll need later for reference.

Wireless Settings

Operation Mode: Access Point
Wireless Channel: auto
Wireless Network Name(SSID): TP-Link_AP_237F
Wireless Security Mode: WPA-PSK/WPA2-PSK
Wireless Password: 27025406

LAN Settings

LAN Type: Smart DHCP

Back Finish

3.2.2. Repeater/Bridge Mode

1. Choose a network you want to extend from the [AP List](#) and click [Connect](#). Enter the host network's password in the [Password](#) field, choose to copy the wireless name from the host network or customize your own, and then click [Next](#).

Quick Setup - Wireless

SSID(to be bridged): TP-Link_22EF
MAC Address(to be bridged): 00:0A:EB:11:22:EE e.g. 00:1D:0F:11:22:33
Scan
Key Type: WPA2-PSK
Encryption: AES
Password: 123456789
Wireless Name of Range Extender: ☒ Copy from Root AP
TP-Link_22EF
☐ Customize
TP-Link_22EF_Ext

Back Next

2. Select the LAN IP type of the access point or leave the default setting [Smart IP](#) for most cases, and then click [Next](#).

Quick Setup - Network Setting

Type: **Smart IP(DHCP)**

Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)
(In this situation the device will help you configure the IP parameters automatically as you need).

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

We recommend you configure this AP with the same IP subnet and subnet mask, but different IP address from your root AP/Router.

DHCP Server: ☒ Enable ☐ Disable

[Back](#) [Next](#)

3. Click **Finish** to complete the configuration.

Quick Setup - Review Setting

Congratulations! The settings is finish, please click finish button to make it work. For detailed settings, please click other menus if necessary.

Confirm the configuration you have set. If anything wrong, please go Back to reset.
It's recommended to take a note of these settings that you'll need later for reference.

Wireless Settings

Operation Mode: Repeater

Wireless Channel: 2

Wireless Network Name(SSID): TP-Link_22EF

Wireless Security Mode: WPA2-PSK

Wireless Password: 123456789

LAN Settings

Default Access: http://tplinkap.net

LAN Type: Smart DHCP

[Back](#) [Finish](#)

4. Relocate the access point about **halfway** between your host AP and the Wi-Fi dead zone.

3. 2. 3. Client Mode

1. Choose a network you want to connect to from the **AP List** and click **Connect**. Enter the host network's password in the **Wireless Password** field, and then click **Next**.

Quick Setup - Wireless

SSID(to be bridged): TP-Link_22EF

MAC Address(to be bridged): 00:0A:EB:11:22:EE e.g. 00:1D:0F:11:22:33

[Scan](#)

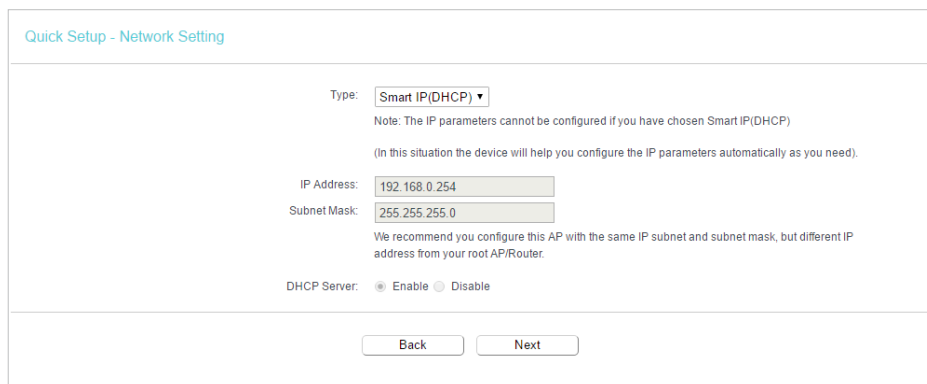
Key Type: WPA2-PSK

Encryption: AES

Password:

[Back](#) [Next](#)

2. Select the LAN IP type of the access point or leave the default setting **Smart IP** for most cases, and then click **Next**.



Quick Setup - Network Setting

Type: **Smart IP(DHCP)** ▼

Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)
(In this situation the device will help you configure the IP parameters automatically as you need).

IP Address: 192.168.0.254

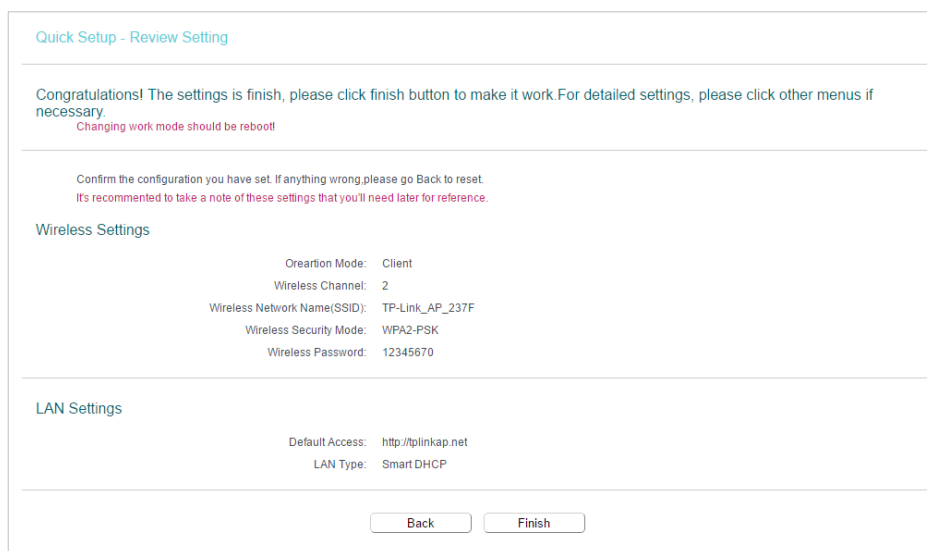
Subnet Mask: 255.255.255.0

We recommend you configure this AP with the same IP subnet and subnet mask, but different IP address from your root AP/Router.

DHCP Server: ☒ Enable ☐ Disable

Back **Next**

3. Click **Finish** to complete the configuration. Now your wired device can surf the internet.



Quick Setup - Review Setting

Congratulations! The settings is finish, please click finish button to make it work. For detailed settings, please click other menus if necessary.
Changing work mode should be reboot!

Confirm the configuration you have set. If anything wrong, please go Back to reset.
It's recommended to take a note of these settings that you'll need later for reference.

Wireless Settings

Creation Mode: Client

Wireless Channel: 2

Wireless Network Name(SSID): TP-Link_AP_237F

Wireless Security Mode: WPA2-PSK

Wireless Password: 12345670

LAN Settings

Default Access: http://tplinkap.net

LAN Type: Smart DHCP

Back **Finish**

3.2.4. Multi-SSID Mode

1. Enable the VLAN function and check SSIDs you want to enable. Customize the SSIDs and the passwords as needed and click **Next**.

Multi-SSID Wireless Setting

Enable VLAN: ☐ OFF ☒ ON

☒ SSID 1: TP-Link_AP_237F_01 VLAN ID: 1
Security: WPA2-PSK
Password: 27025406

☐ SSID 2: TP-Link_AP_237F_02 VLAN ID: 1

☐ SSID 3: TP-Link_AP_237F_03 VLAN ID: 1

☐ SSID 4: TP-Link_AP_237F_04 VLAN ID: 1

☐ More Advanced Wireless Settings

Back Next

2. Select the LAN IP type of the access point or leave the default setting **Smart IP** for most cases, and then click **Next**.

Quick Setup - Network Setting

Type: Smart IP(DHCP)

Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)
(In this situation the device will help you configure the IP parameters automatically as you need).

IP Address: 192.168.0.254
Subnet Mask: 255.255.255.0

We recommend you configure this AP with the same IP subnet and subnet mask, but different IP address from your root AP/Router.

DHCP Server: ☒ Enable ☐ Disable

Back Next

3. Click **Finish** to complete the configuration.

Quick Setup - Review Setting

Congratulations! The settings is finish, please click finish button to make it work. For detailed settings, please click other menus if necessary.
 Changing work mode should be reboot!

Confirm the configuration you have set. If anything wrong, please go Back to reset.
 It's recommended to take a note of these settings that you'll need later for reference.

Wireless Settings

Creation Mode:	Multi-SSID
Wireless Channel:	Auto
SSID1:	TP-Link_AP_237F_01
VLAN ID:	1
Security:	WPA2-PSK
Password:	27025406
SSID2:	TP-Link_AP_237F_02
VLAN ID:	1
Security:	WPA2-PSK
Password:	27025406

LAN Settings

Default Access:	http://tplinkap.net
LAN Type:	Smart DHCP

Back Finish

4. Connect your wireless devices to the different Wi-Fi networks to be isolated by VLANs.

3.3. Set up Internet Connection by WPS (Repeater/Bridge, Client)

In Repeater/Bridge and Client modes, after hardware connection, you can use the WPS (Wi-Fi Protected Setup) function to set up internet connection simply by pressing the WPS button of your access point and the host router.

1. Connect the hardware of your access point according to the mode needed.
2. Press the WPS button of your access point.
3. Within 2 minutes, press the WPS button of the host router.
4. The WPS LED of your access point starts flashing, and when it turns on, the internet connection has been set up successfully.

Note:

1. The WPS LED remains on for 2 minutes and then turns off.
2. In Repeater/Bridge mode, the access point shares the same SSID (network name) and password with the host router.

Chapter 4

Configure the Access Point

This chapter presents how to configure the various features of your access point.

It contains the following sections:

- [Status](#)
- [Network](#)
- [Wireless](#)
- [DHCP](#)
- [System Tools](#)
- [Log Out](#)

4.1. Status

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to [Status](#). You can view the current status information of the access point.

Status	
	Firmware Version: 1.0.0.0 Hardware Version: 1.0.0.0
LAN	MAC Address: 00:0A:EB:11:23:7F IP Address: 192.168.0.254 Subnet Mask: 255.255.255.0
Wireless	Operation Mode: Access Point Wireless Radio: Enabled Name(SSID): TP-Link_AP_237F Mode: 11bgn mixed Channel: Auto(Channel 2) Channel Width: Auto MAC Address: 00:0A:EB:11:23:7F
	System Up Time: 0 day(s) 00:02:58 Refresh

- **Firmware Version** - The version information of the access point's firmware.
- **Hardware Version** - The version information of the access point's hardware.
- **LAN** - This field displays the current settings of the LAN, and you can configure them on the **Network > LAN** page.
 - **MAC address** - The physical address of the access point.
 - **IP address** - The LAN IP address of the access point.
 - **Subnet Mask** - The subnet mask associated with the LAN IP address.
- **Wireless** - This field displays the basic information or status of the wireless function, and you can configure them on the **Wireless > Wireless Settings** page.
 - **Operation Mode** - The current wireless working mode in use.
 - **Wireless Radio** - The status of wireless radio.
 - **Name (SSID)** - The SSID of the access point.

- **Mode** - The current wireless mode which the access point works on.
- **Channel** - The current wireless channel in use.
- **Channel Width** - The current wireless channel width in use.
- **MAC Address** - The physical address of the access point.
- **WDS Status** - The status of WDS connection is displayed.
- **System Up Time** - The length of the time since the access point was last powered on or reset.

Click **Refresh** to get the latest status and settings of the access point.

4.2. Network

4.2.1. LAN

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **Network > LAN**.
3. Configure the IP parameters of the LAN and click **Save**.

LAN

Type: **Smart DHCP** ▼

Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)
(In this situation the device will help you configure the IP parameters automatically as you need).

MAC Address: 00:0A:EB:11:23:7F

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

Save

- **Type** - Either select **Smart IP(DHCP)** to get IP address from DHCP server, or **Static IP** to configure IP address manually.
- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation if your select **Static IP** (factory default - 192.168.0.254).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

■ Note:

- If you have changed the IP address, you must use the new IP address to log in.
- If you select **Smart IP(DHCP)**, the DHCP server of the access point will not start up.

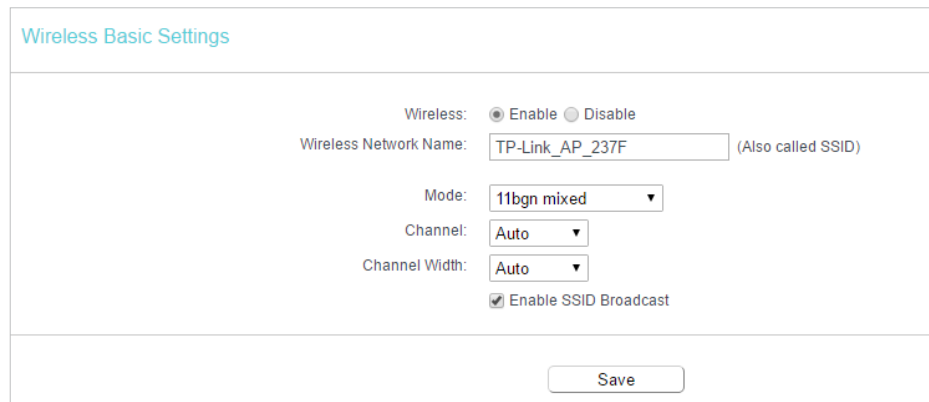
- If the new IP address you set is not in the same subnet as the old one, the IP Address pool in the DHCP Server will be configured automatically.

4.3. Wireless

4.3.1. Basic Settings (Access Point, Client, Multi-SSID)

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to [Wireless](#) > [Basic Settings](#).
3. 3 operation modes are supported here, including [Access Point](#), [Client](#), and [Multi - SSID](#).

Access Point Mode



Wireless Basic Settings

Wireless: ☒ Enable ☐ Disable

Wireless Network Name: (Also called SSID)

Mode:

Channel:

Channel Width:

☒ Enable SSID Broadcast

- [Wireless](#) - Enable or disable wireless radio.
- [Wireless Network Name](#) - Identifies your wireless network name. Create a name up to 32 characters and make sure all wireless points in the wireless network with the same SSID. The default SSID is TP-Link_AP_XXXX (XXXX indicates the last unique four characters of each device's MAC address). This value is case-sensitive. For example, TEST is NOT the same as test.
- [Mode](#) - Select the desired wireless mode. The options are:
 - [11bg mixed](#) - Both 802.11b and 802.11g wireless stations can connect to the device.
 - [11bgn mixed](#) - All 802.11b, 802.11g and 802.11n wireless stations can connect to the device.
- [Channel](#) - Determines the operating frequency to be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Channel Width** - Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Enable SSID Broadcast** - Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.

Note:

To apply any settings you have altered on the page, please click the [Save](#) button, and then you will be reminded to reboot the device.

Client Mode

- **SSID (to be bridged)** - Enter the case-sensitive SSID of the host network which the extender will be connecting to or click [Wireless Scanner](#) and select a Wi-Fi network.
- **MAC Address (to be bridged)** - Enter the MAC Address of the host network which the extender will be connecting to or click [Wireless Scanner](#) and select a Wi-Fi network.
- **Security** - Select one of the security options to match with the host network.
 - **No Security** - This option disables the wireless security.
 - **WPA-PSK** - This option supports implementation of the WPA (Wi-Fi Protected Access) standard. It is recommended.
 - **Password** - You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
 - **WPA2-PSK** - This option supports implementation of the WPA2 (Wi-Fi Protected Access) standard. It is also recommended.
 - **Password** - You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
 - **WEP** - This option is the most basic form of wireless security that can be used if your client devices can only access wireless using WEP (Wireless Equivalent Privacy).
 - **Index** - Select which of the four keys will be used.
 - **Authentication Type** - Select Shared Key or Open System authentication type.
 - **WEP KeyFormat** - Select ASCII or Hexadecimal format.
 - **Password** - Enter the matching WEP key information for your network.

Note:

To apply any settings you have altered on the page, please click the [Save](#) button, and then you will be reminded to reboot the device.

Multi-SSID Mode

The image shows a web interface titled "Wireless Basic Settings". It contains the following fields and controls:

- Wireless:** Radio buttons for ☒ Enable and ☐ Disable.
- SSID1:** ☒ checkbox, text field "TP-Link_AP_237F_01", and "VLAN ID: 1" field.
- SSID2:** ☐ checkbox, text field "TP-Link_AP_237F_02", and "VLAN ID: 1" field.
- SSID3:** ☐ checkbox, text field "TP-Link_AP_237F_03", and "VLAN ID: 1" field.
- SSID4:** ☐ checkbox, text field "TP-Link_AP_237F_04", and "VLAN ID: 1" field.
- Mode:** Dropdown menu set to "11bgn mixed".
- Channel:** Dropdown menu set to "Auto".
- Channel Width:** Dropdown menu set to "Auto".
- Enable SSID Broadcast:** ☒ checkbox.
- Enable VLAN:** ☐ checkbox.
- Save:** A button at the bottom right.

- **Wireless** - Enable or disable wireless radio.
- **SSID (1-4)** - Up to four SSIDs for each BSS (Basic Service Set) can be entered in the field SSID1 ~ SSID4. The name can be up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. If Enable VLAN is checked, the wireless stations connecting to SSID of different VLANID can not communicate with each other.
- **VLAN ID (1-4)** - Provide a number between 1 and 4095 for VLAN. This will cause the device to send packets with VLAN tags. The switch connecting with the device must support VLAN IEEE802.1Q frames. The wireless stations connecting to the SSID of a specified VLAN ID can communicate with the PC connecting to the port with the same VLAN ID on the Switch.
- **Mode** - This field determines the wireless mode which the device works on.
 - **11bg mixed** - Both 802.11b and 802.11g wireless stations can connect to the device.
 - **11bgn mixed** - All 802.11b, 802.11g and 802.11n wireless stations can connect to the device.
- **Channel Width** - Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Enable SSID Broadcast** - If you select the Enable SSID Broadcast checkbox, the AP will broadcast its name (SSID) on the air.

- **Enable VLAN** - Check this box and then you can change the VLAN ID of each SSID. If you want to configure the Guest and Internal networks on VLAN, the switch you are using must support VLAN. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE802.1Q standard, and enable this field.

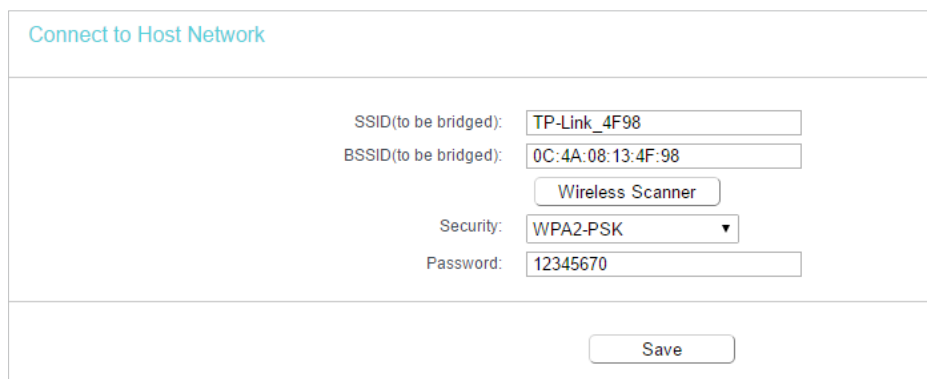
Note:

To apply any settings you have altered on the page, please click the Save button, and then you will be reminded to reboot the device.

4.3.2. Connect to Network (Repeater/Bridge)

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **Wireless > Connect to Network**.
3. **Repeater/Bridge** mode is supported here.

Repeater/Bridge Mode



- **SSID (to be bridged)** - Enter the case-sensitive SSID of the host network which the extender will be connecting to or click **Wireless Scanner** and select a Wi-Fi network.
- **BSSID (to be bridged)** - Enter the MAC Address of the host network which the extender will be connecting to or click **Wireless Scanner** and select a Wi-Fi network.
- **Security** - Select one of the security options to match with the host network.
 - **No Security** - This option disables the wireless security.
 - **WPA-PSK** - This option supports implementation of the WPA (Wi-Fi Protected Access) standard. It is recommended.
 - **Password** - You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
 - **WPA2-PSK** - This option supports implementation of the WPA2 (Wi-Fi Protected Access) standard. It is also recommended.
 - **Password** - You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.

- **WEP** - This option is the most basic form of wireless security that can be used if your client devices can only access wireless using WEP (Wireless Equivalent Privacy).
 - **Index** - Select which of the four keys will be used.
 - **Authentication Type** - Select Shared Key or Open System authentication type.
 - **WEP KeyFormat** - Select ASCII or Hexadecimal format.
 - **Password** - Enter the matching WEP key information for your network.

Note:

To apply any settings you have altered on the page, please click the **Save** button, and then you will be reminded to reboot the device.

4.3.3. WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to your access point's network quickly via WPS.

Note:

- The WPS function cannot be configured if the wireless function of the access point is disabled. Please make sure the wireless function is enabled before configuration.
- When working in Repeater/Bridge or Client mode, the WPS function of the access point is disabled.

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

Method ONE: Press the WPS Button on Your Client Device

1. Keep the WPS Status as **Enabled** and click **Add Device**.



WPS (Wi-Fi Protected Setup)

WPS: Enabled

Current PIN: 27025406

☐ Disable device PIN

Add a new device:

2. Select **Press the button of the new device in two minutes** and click **Connect**.

WPS Settings

☐ Enter new device PIN.
PIN:

☒ Press the WPS button of the new device within the next two minutes.

3. Within two minutes, press the WPS button on your client device.
4. A success message will appear on the WPS page if the client device has been successfully added to the access point's network.

Method TWO: Enter the Client's PIN

1. Keep the WPS Status as **Enabled** and click **Add Device**.

WPS (Wi-Fi Protected Setup)

WPS: **Enabled**

Current PIN: **27025406**

☐ Disable device PIN

Add a new device:

2. Select **Enter the new device's PIN**, enter your client device's current PIN in the **PIN** field and click **Connect**.

WPS Settings

☒ Enter new device PIN.
PIN:

☐ Press the WPS button of the new device within the next two minutes.

3. A success message will appear on the WPS page if the client device has been successfully added to the access point's network.

Method Three: Enter the Access Point's PIN

1. Keep the WPS Status as **Enabled** and get the **Current PIN** of the access point.

WPS (Wi-Fi Protected Setup)

WPS: **Enabled**

Current PIN: **27025406**

☐ Disable device PIN

Add a new device:

2. Enter the access point's current PIN on your client device to join the access point's Wi-Fi network.

4. 3. 4. Wireless Security (Access Point, Multi-SSID)

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **Wireless > Basic Settings**.
3. 2 operation modes are supported here, including **Access Point**, and **Multi - SSID**.
4. Configure the security settings of your wireless network and click **Save**. The security options are different for different operation mode.

Access Point

Wireless Security Settings

Note: WEP security, WPA/WPA2 - Enterprise authentication and TKIP encryption are not supported with WPS enabled.
For network security, it is strongly recommended to enable wireless security and select WPA2-PSK AES encryption.

☐ Disable Wireless Security

☒ WPA/WPA2 - Personal(Recommended)

Authentication Type: WPA2-PSK

Encryption: AES

Wireless Password: 27025406

Group Key Update Period: 0

☐ WPA/WPA2 - Enterprise

Authentication Type: Auto

Encryption: Auto

RADIUS Server IP:

RADIUS Server Port: 1812 (1-65535, 0 stands for default port 1812)

RADIUS Server Password:

Group Key Update Period: 0

☐ WEP

Authentication Type: Open System

WEP Key Format: Hexadecimal

Selected Key:	WEP Key	Key Type
Key 1: ☒		Disabled
Key 2: ☐		Disabled
Key 3: ☐		Disabled
Key 4: ☐		Disabled

Save

- **Disable Wireless Security** - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the access point without a password. It's strongly recommended to choose one of the following modes to enable security.
- **WPA-PSK/WPA2-Personal** - It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - **Authentication Type** - Select **Auto**, **WPA-PSK** or **WPA2-PSK**.

- **Encryption** - Select [Auto](#), [TKIP](#) or [AES](#).
 - **Wireless Password** - Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
 - **Group Key Update Period** - Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.
- **WPA /WPA2-Enterprise** - It's based on Radius Server.
 - **Authentication Type** - Select [Auto](#), [WPA](#) or [WPA2](#).
 - **Encryption** - Select [Auto](#), [TKIP](#) or [AES](#).
 - **RADIUS Server IP** - Enter the IP address of the Radius server.
 - **RADIUS Server Port** - Enter the port that Radius server used.
 - **RADIUS Server Password** - Enter the password for the Radius server.
 - **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- **WEP** - It is based on the IEEE 802.11 standard.
 - **Authentication Type** - The default setting is [Auto](#), which can select Shared Key or Open System authentication type automatically based on the wireless client's capability and request.
 - **WEP Key Format** - Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
 - **WEP Key (Password)** - Select which of the four keys will be used and enter the matching WEP key. Make sure these values are identical on all wireless clients in your network.
 - **Key Type** - Select the WEP key length (64-bit, 128-bit or 152-bit) for encryption. [Disabled](#) means this WEP key entry is invalid.
 - **64-bit** - Enter 10 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 5 ASCII characters.
 - **128-bit** - Enter 26 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 13 ASCII characters.

■ **Note:**

- If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.
- You will be reminded to reboot the device after clicking the [Save](#) button.

Multi-SSID

Wireless Security Settings

For network security, it is strongly recommended to enable wireless security and use WPA-PSK AES encryption.

SSID: TP-Link_AP_237F_01 ▼

☐ Disable Wireless Security

☒ WPA/WPA2 - Personal(Recommended)

Authentication Type: WPA2-PSK ▼

Encryption: AES ▼

Wireless Password: 27025406

Group Key Update Period: 0

☐ WPA/WPA2 - Enterprise

Authentication Type: Auto ▼

Encryption: Auto ▼

RADIUS Server IP:

RADIUS Server Port: 1812 (1-65535, 0 stands for default port 1812)

RADIUS Server Password:

Group Key Update Period: 0

Save

- **Disable Wireless Security** - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the access point without a password. It's strongly recommended to choose one of the following modes to enable security.
- **WPA-PSK/WPA2-Personal** - It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - **Authentication Type** - Select **Auto**, **WPA-PSK** or **WPA2-PSK**.
 - **Encryption** - Select **Auto**, **TKIP** or **AES**.
 - **Wireless Password** - Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
 - **Group Key Update Period** - Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.
- **WPA /WPA2-Enterprise** - It's based on Radius Server.
 - **Authentication Type** - Select **Auto**, **WPA** or **WPA2**.
 - **Encryption** - Select **Auto**, **TKIP** or **AES**.
 - **RADIUS Server IP** - Enter the IP address of the Radius server.
 - **RADIUS Server Port** - Enter the port that Radius server used.
 - **RADIUS Server Password** - Enter the password for the Radius server.
 - **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

Note:

- If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.
- You will be reminded to reboot the device after clicking the [Save](#) button.

4.3.5. Extended Network (Repeater/Bridge)

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to [Wireless](#) > [Basic Settings](#).
3. [Repeater/Bridge](#) operation mode is supported here.
4. Configure the security settings of your wireless network and click [Save](#). The security options are different for different operation mode.

Extended Network Settings

Extended 2.4GHz SSID: [Copy Host SSID](#)

Extended 2.4GHz Security:

Extended 2.4GHz Password:

[Save](#)

- [Extended 2.4GHz](#) - Enable or disable the 2.4GHz wireless function of the range extender.
- [Extended 2.4GHz SSID](#) - Either use the Copy Host SSID button to automatically copy the main router/AP's SSID or enter a new name (up to 32 characters long). This field is case-sensitive.
- [Copy Host SSID](#) - Click to copy the Host SSID. When selected, the extended network will share the SSID of your host network.
- [Extended 2.4GHz Security](#) - Select one of the security options to set local extended wireless network.
 - [No Security](#) - This option disables the wireless security.
 - [WPA-PSK/WPA2-PSK](#) - This option supports multiple implementation of the WPA (Wi-Fi Protected Access) standard, such as WPA and WPA2. It is recommended.
 - [WEP](#) - This option is the most basic form of wireless security that can be used if your client devices can only access wireless using WEP (Wired Equivalent Privacy).

4.3.6. Wireless MAC Filtering

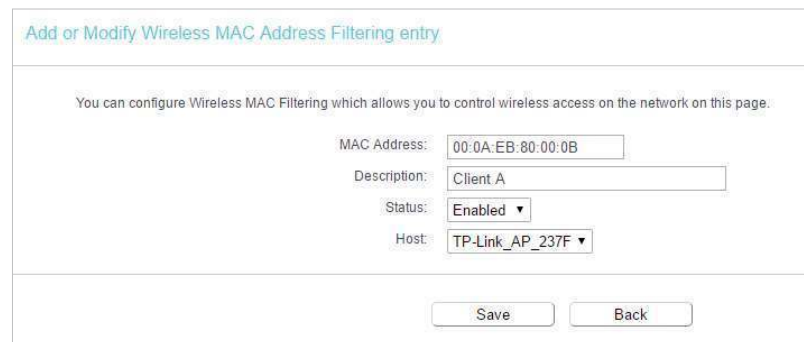
Wireless MAC Filtering is used to deny or allow specific wireless client devices to access your network by their MAC addresses. This function is not available when the operation is set to Client. As the configuration is the same in each operation mode, here we just take the Access Point for example.

I want to:

Deny or allow specific wireless client devices to access my network by their MAC addresses.

For example, you want the wireless client A with the MAC address 00-0A-EB-B0-00-0B and the wireless client B with the MAC address 00-0A-EB-00-07-5F to access the access point, but other wireless clients cannot access the access point.

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to [Wireless > Wireless MAC Filtering](#).
3. Click [Enable](#) to enable the Wireless MAC Filtering function.
4. Select [Allow the stations specified by any enabled entries in the list to access](#) as the filtering rule.
5. Delete all or disable all entries if there are any entries already.
6. Click [Add New](#) and fill in the blank.



[Add or Modify Wireless MAC Address Filtering entry](#)

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

MAC Address:

Description:

Status:

Host:

- 1) Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the MAC Address field.
- 2) Enter wireless client A/B in the Description field.
- 3) Select [Enabled](#) in the Status drop-down list.
- 4) Click [Save](#) and click [Back](#).
7. The configured filtering rules should be listed as the picture shows below.

Wireless MAC Filtering

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

Wireless MAC Filtering: ☒ Enabled ☐ Disable

Filtering Rules

☐ Deny the stations specified by any enabled entries in the list to access.

☒ Allow the stations specified by any enabled entries in the list to access.

☐	MAC Address	Status	Host	Description	Edit
☒	00:0A:EB:80:00:0B	Enabled	TP-Link_AP_237F	Client A	Edit
☒	00:0A:EB:00:07:5F	Enabled	TP-Link_AP_237F	Client B	Edit

Done!

Now only client A and client B can access your network.

4.3.7. Wireless Advanced

The configuration of each operation mode is almost the same. We take Access Point mode for example here.

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

Note:

If you are not familiar with the setting items on this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

Wireless Advanced

Notice: For better performance, Fragmentation Threshold is disabled when wireless mode include 11n or 11ac.

Transmit Power:

Beacon Interval: (25-1000)

RTS Threshold: (1-2346)

Fragmentation Threshold: (256-2346)

DTIM Interval: (1-255)

☒ Enable Short GI
☐ Enable Client Isolation
☒ Enable WMM

- **Transmit Power** - Select **High**, **Middle** or **Low** which you would like to specify for the access point. **High** is the default setting and recommended.
- **Beacon Interval** - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons are the packets sent by the access point to synchronize a wireless network. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the access point will send RTS

frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.

- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting a low value for the Fragmentation Threshold may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **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. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **Enable Client Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.
- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

4.3.8. Wireless Statistics

The configuration of each operation mode is almost the same. We take Access Point mode for example here.

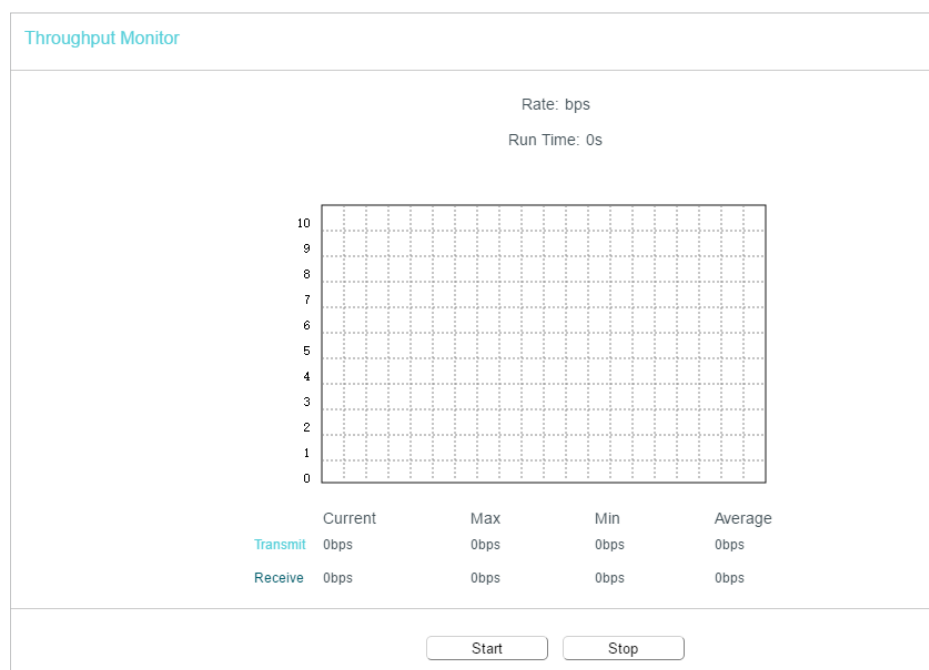
1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **Wireless > Wireless Statistics** to check the data packets sent and received by each client device connected to the access point.

Wireless Stations Status					
Wireless Stations Currently Connected: 0 Refresh					
ID	MAC Address	Current Status	Received Packets	Sent Packets	SSID

- **MAC Address** - The MAC address of the connected wireless client.
- **Current Status** - The running status of the connected wireless client.
- **Received Packets** - Packets received by the wireless client.
- **Sent Packets** - Packets sent by the wireless client.
- **SSID** - SSID that the station associates with.

4.3.9. Throughput Monitor

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **Wireless > Throughput Monitor** to view the wireless throughput information.



- **Rate** - The Throughput unit.
- **Run Time** - How long this function is running.
- **Transmit** - Wireless transmit rate information.
- **Receive** - Wireless receive rate information.

Click **Start/Stop** to start or stop wireless throughput monitor.

4.4. DHCP

By default, the DHCP (Dynamic Host Configuration Protocol) Server is enabled and the access point acts as a DHCP server; it dynamically assigns TCP/IP parameters to client devices from the IP Address Pool. You can change the settings of DHCP Server if necessary, and you can reserve LAN IP addresses for specified client devices.

4.4.1. DHCP Settings

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **Network > DHCP Settings**.
3. Specify DHCP server settings and click **Save**.

DHCP Settings

DHCP Server: ☐ Disable ☒ Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1~2880 minutes, the default value is 120)

Default Gateway: (optional)

Default Domain: (optional)

DNS Server: (optional)

Secondary DNS Server: (optional)

Save

- **DHCP Server** - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.
- **Address Lease Time** - The Address Lease Time is the amount of time a network user will be allowed to connect to the access point with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120.
- **Default Gateway (Optional)** - It is suggested to input the IP address of the LAN port of the access point. The default value is 192.168.0.254.
- **Default Domain (Optional)** - Input the domain name of your network.
- **DNS Server (Optional)** - Input the DNS IP address provided by your ISP.
- **Secondary DNS Server (Optional)** - Input the IP address of another DNS server if your ISP provides two DNS servers.

■ Note:

- To use the DHCP server function of the access point, you must configure all computers on the LAN as [Obtain an IP Address automatically](#).
- When you choose [Smart IP \(DHCP\)](#) in [Network > LAN](#), the DHCP Server function will be disabled. You will see the page as below.

DHCP Settings

DHCP Server: ☐ Disable ☒ Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1~2880 minutes, the default value is 120)

Default Gateway: (optional)

Default Domain: (optional)

DNS Server: (optional)

Secondary DNS Server: (optional)

4. 4. 2. DHCP Client List

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **DHCP > DHCP Client List** to view the information of the clients connected to the access point.

DHCP Clients List

This page displays information of all DHCP clients on the network.

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Camille	40:8D:5C:89:74:B5	192.168.0.100	00:00:37

- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the access point has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

You cannot change any of the values on this page. To update this page and show the current attached devices, click [Refresh](#).

4. 4. 3. Address Reservation

You can reserve an IP address for a specific client. When you specify a reserved IP address for a PC on the LAN, this PC will always receive the same IP address each time when it accesses the DHCP server.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the access point.

2. Go to [DHCP > Address Reservation](#).
3. Click [Add New](#) and fill in the blank.

DHCP Address Reservation

This page displays the static IP address assigned by the DHCP Server and allows you to adjust these configurations by clicking the corresponding fields.

☐	MAC Address	IP Address	Status	Edit
☐	40:8D:5C:89:74:B5	192.168.0.100	Disabled	Edit

Add NewEnable SelectedDisable SelectedDelete Selected

Refresh

- 1) Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) of the client for which you want to reserve an IP address.
- 2) Enter the IP address (in dotted-decimal notation) which you want to reserve for the client.
- 3) Leave the [Status](#) as [Enabled](#).
- 4) Click [Save](#).

4. 5. System Tools

4. 5. 1. Diagnostic

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

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to [System Tools > Diagnostic](#).

- **Diagnostic Tool** - Select one diagnostic tool.
 - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
 - **Tracerouter** - This diagnostic tool tests the performance of a connection.

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name** - Enter the destination IP address (such as 192.168.0.254) or Domain name (such as www.tp-link.com).
- **Pings Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

3. Click **Start** to check the connectivity of the Internet.

4. The **Diagnostic Results** page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the Internet is fine.

```

Diagnostic Results

Pinging 192.168.0.254 with 64 bytes of data:

Reply from 192.168.0.254: bytes=64 time=1 TTL=64 seq=1
Reply from 192.168.0.254: bytes=64 time=1 TTL=64 seq=2
Reply from 192.168.0.254: bytes=64 time=1 TTL=64 seq=3
Reply from 192.168.0.254: bytes=64 time=1 TTL=64 seq=4

Ping statistics for 192.168.0.254
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milliseconds:
Minimum = 1, Maximum = 1, Average = 1

```

Note:

Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for the Ping function. Option "Tracert Hops" is used for the Tracert function.

4.5.2. SNMP Settings

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol.

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

SNMP Settings

Simple Network Management Protocol(SNMP) allows management applications to retrieve status updates and statistics from the SNMP agent within this device.

SNMP Agent: ☐ Disable ☒ Enable

Read Community:

Set Community:

System Name:

System Description:

System Location:

System Contact:

Trap Manager IP:

- **Read Community** - Enter the community name that allows Read-Only access to the Device's SNMP information. The community name can be considered a group password. The default setting is "public".
- **Set Community** - Enter the community name that allows Read/Write access to the Device's SNMP information. The community name can be considered a group password. The default setting is "private".
- **System Name** - An administratively-assigned name for this managed node.
- **System Description** - The software version information for this managed node.
- **System Location** - The physical location of this node.

- **System Contact** - The textual identification of the contact person for this managed node.

■ **Note:**

If you are not familiar with the setting items on this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

- **Trap Management IP** - Displays the IP address of the host to receive the traps.

4. 5. 3. Ping Watch Dog

The Ping Watch Dog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. It makes the access point continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the access point will automatically reboot.

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **System Tools > Ping Watch Dog**. Configure the settings and click **Save**.

Ping WatchDog Settings

Ping WatchDog will be the monitor to detect AP's network, reboot device while AP disconnected.

Switch: ☐ Disable ☒ Enable

Destination IP:

Interval: (10-300)s

Startup Delay: (60-300)s

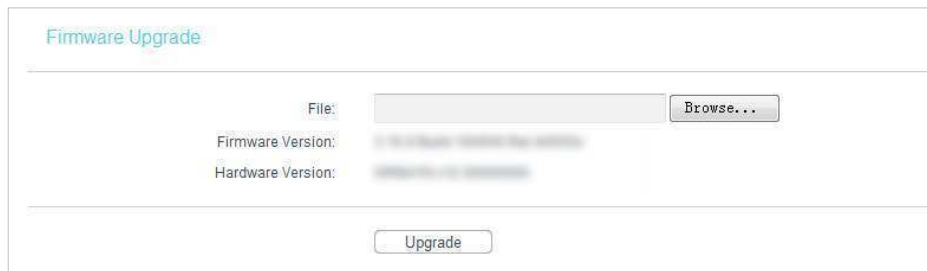
Fail Count: (1-65535)

- **Enable** - Turn on/off Ping Watch Dog.
- **Destination IP** - The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- **Interval** - Time interval between two ping packets which are sent out continuously.
- **Startup Delay** - Time delay before first ping packet is sent out when the access point is restarted.
- **Fail Count** - Upper limit of the ping packets the access point can drop continuously. If this value is overrun, the access point will restart automatically.

4. 5. 4. Firmware Upgrade

TP-Link is dedicated to improving and enriching the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website. You can download the latest firmware file from the [Support](#) page of our website www.tp-link.com and upgrade the firmware to the latest version.

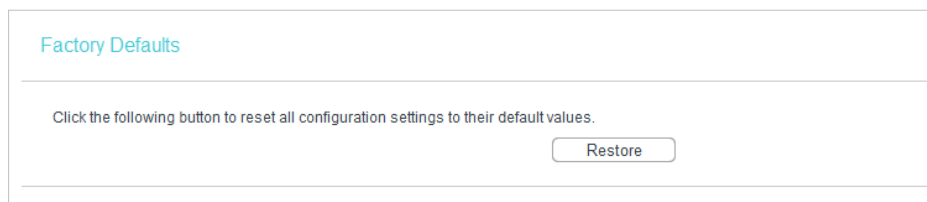
1. Download the latest firmware file for the access point from our website www.tp-link.com.
2. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
3. Go to [System Tools](#) > [Firmware Upgrade](#).
4. Click [Browse](#) to locate the downloaded firmware file, and click [Upgrade](#).



The screenshot shows the 'Firmware Upgrade' page. It has a title 'Firmware Upgrade' in teal. Below the title, there is a 'File:' label next to a text input field, and a 'Browse...' button to its right. Below this, there are two labels: 'Firmware Version:' and 'Hardware Version:', each followed by a text input field. At the bottom of the form, there is an 'Upgrade' button.

4. 5. 5. Factory Defaults

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to [System Tools](#) > [Factory Defaults](#). Click [Restore](#) to reset all settings to the default values.



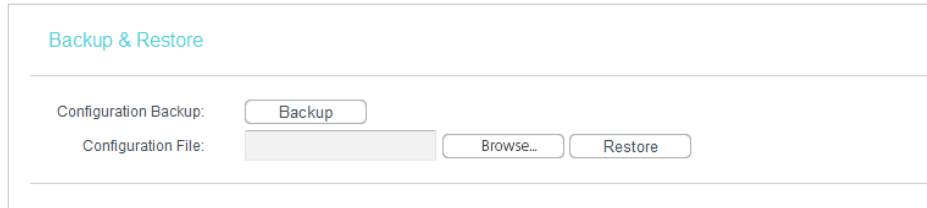
The screenshot shows the 'Factory Defaults' page. It has a title 'Factory Defaults' in teal. Below the title, there is a message: 'Click the following button to reset all configuration settings to their default values.' At the bottom of the form, there is a 'Restore' button.

- The default [username](#): admin
- The default [password](#): admin
- The default [IP Address](#): 192.168.0.254
- The default [Subnet Mask](#): 255.255.255.0

4. 5. 6. Backup & Restore

The configuration settings are stored as a configuration file in the access point. You can backup the configuration file in your computer for future use and restore the access point to the previous settings from the backup file when needed.

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to [System Tools > Backup & Restore](#).

The screenshot shows the 'Backup & Restore' web interface. At the top, the title 'Backup & Restore' is displayed in blue. Below the title, there are two main sections. The first section, 'Configuration Backup:', contains a 'Backup' button. The second section, 'Configuration File:', contains a text input field, a 'Browse...' button, and a 'Restore' button.

➤ **To backup configuration settings:**

Click [Backup](#) to save a copy of the current settings in your local computer. A ".bin" file of the current settings will be stored in your computer.

➤ **To restore configuration settings:**

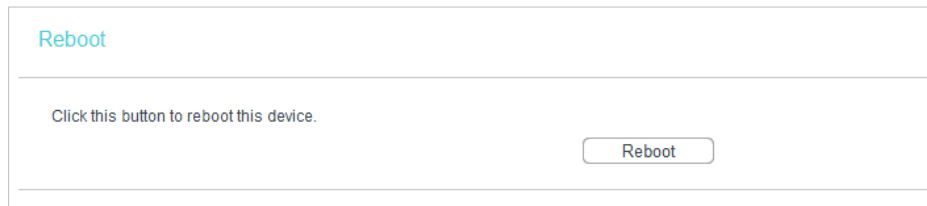
1. Click [Choose File](#) to locate the backup configuration file stored in your computer, and click [Restore](#).
2. Wait a few minutes for the restoring and rebooting.

■ **Note:**

During the restoring process, do not power off or reset the access point.

4. 5. 7. Reboot

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to [System Tools > Reboot](#), and you can restart your access point.

The screenshot shows the 'Reboot' web interface. At the top, the title 'Reboot' is displayed in blue. Below the title, there is a text instruction: 'Click this button to reboot this device.' At the bottom right of the page, there is a 'Reboot' button.

Some settings of the access point will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.

- Upgrade the firmware of the access point (system will reboot automatically).
- Restore the access point to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

4.5.8. Password

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **System Tools** > **password**, and you can change the factory default username and password of the access point.

Username and password can contain between 1 - 15 characters and may not include spaces.

Old User Name:

Old Password:

New User Name:

New Password:

Confirm New Password:

Save Clear All

It is strongly recommended that you change the default username and password of the access point, for all users that try to access the access point's web-based utility or Quick Setup will be prompted for the access point's username and password.

Note:

The new username and password must not exceed 15 characters and not include any spacing.

3. Click **Save**.

4.5.9. System Log

1. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.
2. Go to **System Tools** > **System Log**, and you can view the logs of the access point.

Log Type: **ALL** Log Level: **Debug**

Index	Time	Type	Level	Content
1	1970-01-01 00:00:08	DHCPD	Notice	Send ACK to 192.168.0.100
2	1970-01-01 00:00:08	DHCPD	Notice	Recv REQUEST from 40:8D:5C:89:74:B5

Refresh Clear Log Save Log Log Settings

- **Loge Type** -By selecting the log type, only logs of this type will be shown.

- [Log Level](#) - By selecting the log level, only logs of this level will be shown.
- [Refresh](#) - Refresh the page to show the latest log list.
- [Clear Log](#) - All the logs will be deleted from the access point permanently, not just from the page.

4. 6. [Log Out](#)

Click [Logout](#) at the bottom of the main menu, and you will log out of the web page and return to the login window.

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 all the LEDs turn on momentarily, then release the button.

Note:

Upon resetting, all previous configurations will be cleared, and the access point will reset to the default Access Point Mode.

Q2. 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 username and password you set for the access point.
2. Go to [Wireless](#) > [Wireless Security](#) to retrieve or reset your wireless password.

Q3. What should I do if I forget my login password of the web management page?

The default username and password of the web management page are [admin](#) (in lowercase).

If you have altered the username and password but Password Recovery is disabled:

1. Reset the access point to its factory default settings: use a pin to press and hold the Reset button until the Power LED starts blinking, then release the button.
2. Visit <http://tplinkap.net>, and log in with the username and password you set for the access point.

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.

Q4. What should I do if my wireless is not stable?

It may be caused by too much interference, you can try the following:

- 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.

Q5. What should I do to maximize my signal strength in Repeater/Bridge mode?

When choosing an ideal location to optimize wireless signal in Repeater/Bridge mode, please refer to the following recommendations.

- The Best Way is Halfway

Generally, the ideal location for the repeater 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.

- Less Obstacles Ensure Better Performance

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

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.  is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2017 TP-Link Technologies Co., Ltd. All rights reserved.

FCC STATEMENT



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."

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.

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 and 2011/65/EU.

The original EU declaration of conformity may be found at

<https://www.tp-link.com/en/ce>

OPERATING FREQUENCY(the maximum transmitted power)

2400 MHz -2483.5 MHz(20dBm)

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.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

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

Le présent appareil est conforme aux CNR d'Industrie 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'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This radio transmitter (IC:8853A-WA801NDV5/ Model:TL-WA801ND) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list below, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (IC: 8853A-WA801NDV5/ Model: TL-WA801ND) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans

cette liste ci-dessous et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Antenna	Two deattachable antennas
---------	---------------------------

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！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，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或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通行；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。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

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。



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



Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.
- Adapter shall be installed near the equipment and shall be easily accessible.
- The plug considered as disconnect device of adapter.
-  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.

Explanations of the symbols on the product label

Symbol	Explanation
	DC voltage
	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.
	Indoor use only