AX3000 Wi-Fi 6 Long-Range Access Point

User Guide

V1.0

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! Please read this user guide before you start.

This user guide walks you through all functions on the AX3000 Wi-Fi 6 long-range access point.

Conventions

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	Internet Settings > LAN Setup
Parameter and value	Bold	Set **SSID** to **Tom**.
Variable	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
UI control	Bold	On the **Quick Setup** page, click the **Save** button.

The symbols that may be found in this document are defined as follows.

Symbol	Meaning
NOTE	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
TIP	This format is used to supplement or explain a procedure.

For more documents

AP support central management either by Tenda Access Point Controller (AC) or Tenda router that supports AP management. For detailed information, refer to user guides of target ACs or routers.

Search target product models on our official website www.tendacn.com to obtain the latest product documents.

Product document overview

Document	Description
Data Sheet	It introduces the basic information of the device, including product overview, selling points, and specifications.
Quick Installation Guide	It introduces how to set up the device quickly for internet access, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on.
User Guide	Walks you through detailed functions and configurations of APs, including all the functions on the web UI.

Technical Support

If you need more help, contact us by any of the following means. We will be glad to assist you as soon as possible.

Hotline	Global: (86) 755-27657180 (China Time Zone) United States: 1-800-570-5892 (Toll Free: 7 x 24 hours) Canada: 1-888-998-8966 (Toll Free: Mon - Fri 9 am - 6 pm PST) Hong Kong: 00852-81931998	Email	support@tenda.com.cn
Website	www.tendacn.com		

Revision History

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the i29 was introduced.

Version	Date	Description
V1.0	2022-05-01	Original publication.

Contents

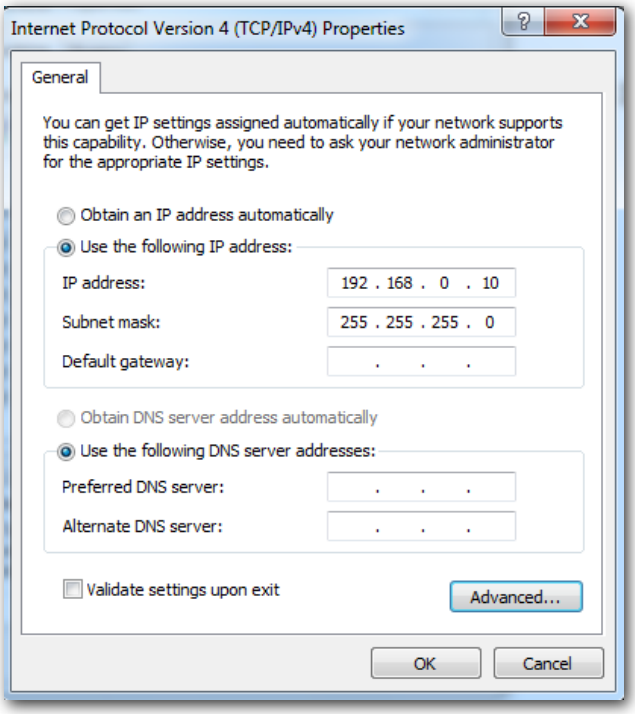
1 Log in to the Web UI

1.1 Login

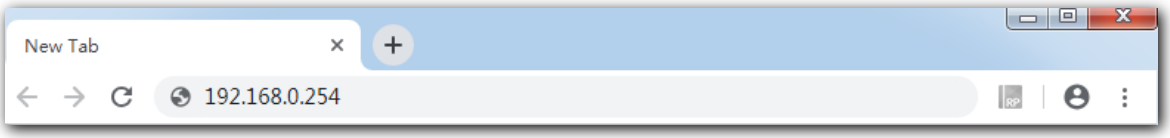
Step 1 Connect your computer to the AP or the switch connected to the AP with an Ethernet cable.

Step 2 Ensure that the IP address of the management computer is in the same network segment of the AP.

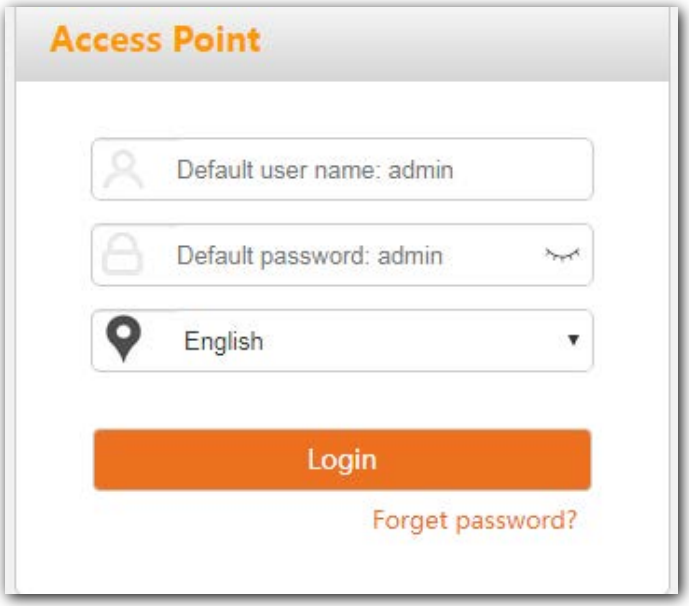
For example, if the IP address of the AP is **192.168.0.254**, the management computer should be configured with an IP address of **192.168.0.*X*** (*X*: 2~253).



Step 3 Start a web browser on the computer, enter the IP address of the AP (default: **192.168.0.254**) in the address bar.



Step 4 Enter the login user name and password (default: **admin**/**admin**), and click **Login**.



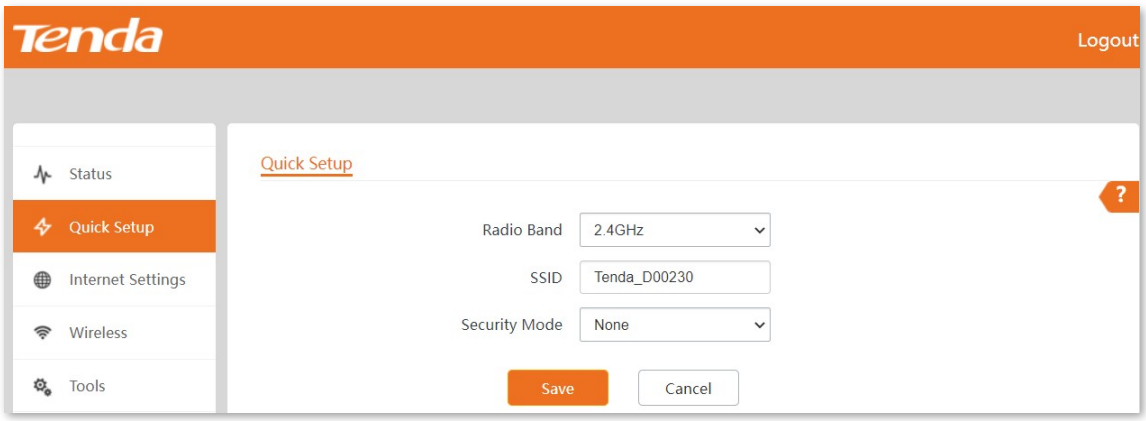
---- End

TIP

If the login page does not appear, please try the following solutions:

- If there is a DHCP server in the LAN where the AP is deployed, AP automatically obtains IP address from the DHCP server. Under such circumstance, check the new IP address of the AP at the client list of the DHCP server first, and use the new IP address to log in to the web UI of the AP.
- If an Tenda AC (including Tenda router that supports AP management) has already been deployed in the network, AP may have been managed by the AC and its IP address has changed. Please log in to the Web UI of the AC and check the new IP address of the AP, and log in again using the new IP address.
- If more than one AP are deployed in the network, IP address conflicts may occur, causing web UI login errors. Verify that the IP address of the AP is not occupied before being integrated into the network.
- Reset the AP and try logging in using the default IP address. How to reset: After the AP is started, hold down the Reset button for about 8 seconds and release it. Wait about 8 seconds, AP is restored to factory settings and restarted.

Log in to the web UI of the AP. You can configure the AP now.



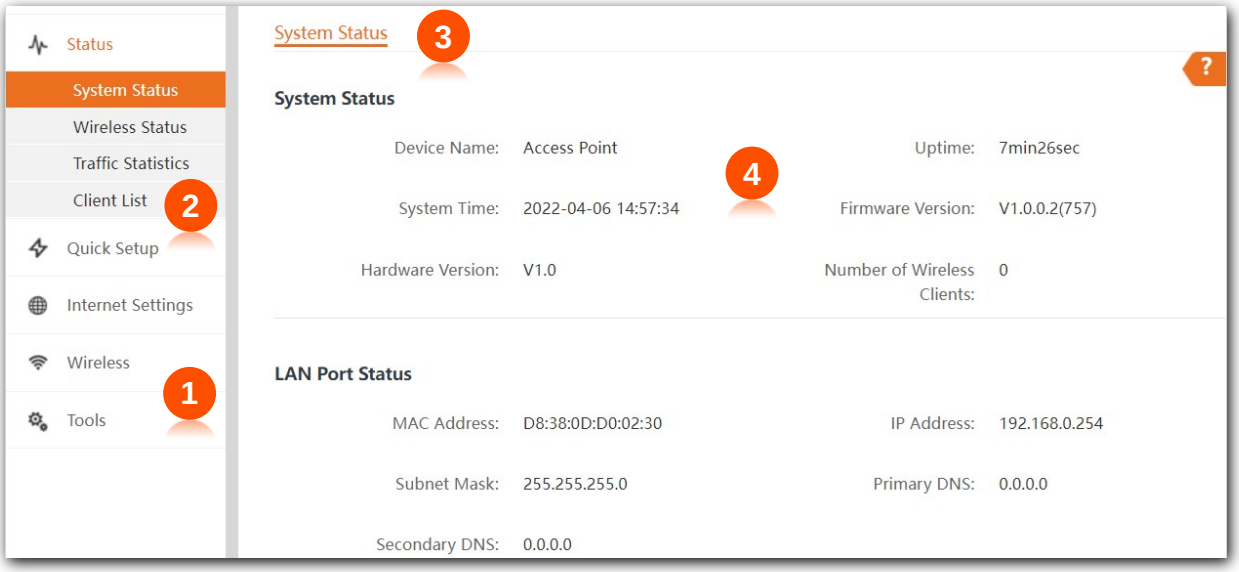
1.2 Logout

After logging in to the web UI of the AP, if no operations are performed during the **Login Timeout Interval**, the system will log out automatically. In addition, you can click **Logout** on the upper right corner to safely exit from the web UI.

2 Web UI operations

2.1 Layout

The web UI of the AP consists of four sections, including the level-1, and level-2 navigation bars, tab page area, and the configuration area. See the following figure.



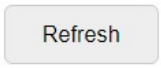
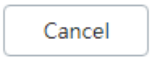
TIP

Functions or parameters displayed in gray on the web UI are not supported yet or cannot be modified under the current configurations.

No.	Name	Description
1	Level-1 navigation bar	Used to display the function menu of the AP. Users can select functions in the navigation bars and the configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Tab page area	
4	Configuration area	Used to modify or view your configuration.

2.2 Frequently-used buttons

The following table describes the frequently-used buttons available on the web UI of the AP.

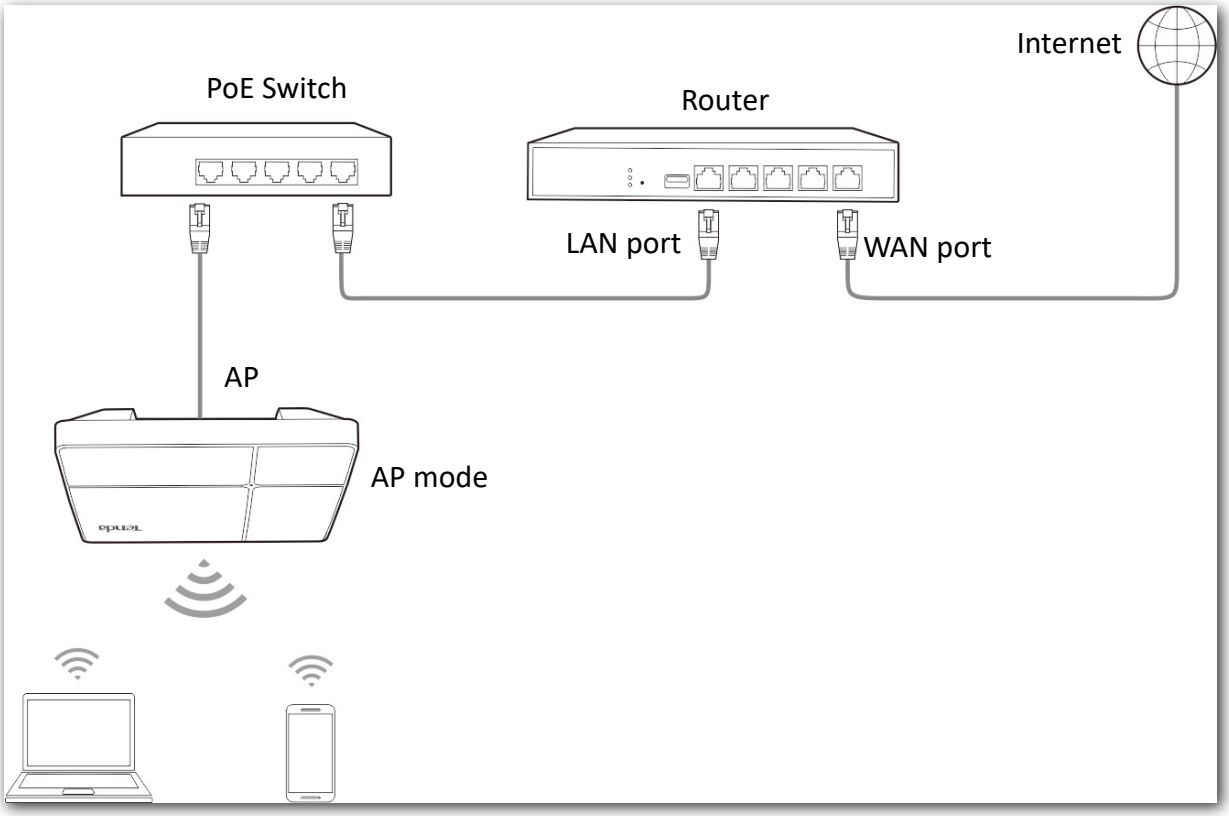
Button	Description
	Used to refresh the current page.
	Used to save the configuration on the current page and enable the configuration to take effect.
	Used to modify the current configuration on the current page back to the original configuration.
	Used to get the online help.

3 Quick setup

3.1 Overview

In the **Quick Setup** module, you can set up the AP in a quick way to enable internet access for your wireless devices such as smart phones and tablets.

AP supports only the AP mode. In this mode, AP connects to the internet using Ethernet cables and transforms wired signals to wireless signals for wireless coverage. See the following topology.



3.2 Quick setup

TIP

Before configuration, ensure that the upstream router has connected to the internet.

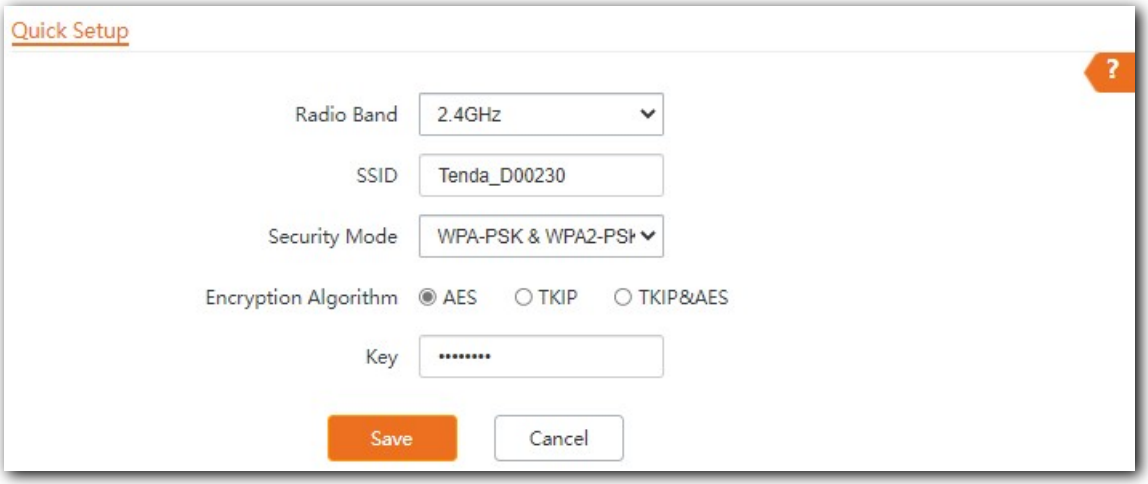
Step 1 Choose **Quick Setup**.

Step 2 Choose the **Radio Band** you wish to configure, for example, **2.4 GHz**.

Step 3 Set a wireless network name (primary SSID) in the **SSID** box.

Step 4 Select a **Security Mode** and configure the incurred parameters.

Step 5 Click **Save**.



Step 6 If you need to set other wireless networks in another radio band, please select another wireless radio band and perform step 2 to 5 again.

---- End

Search and connect your wireless devices such as smart phones to the **SSID** you set. Enter the wireless password (the **Key** you set) and you will be able to access the internet.

Parameter description

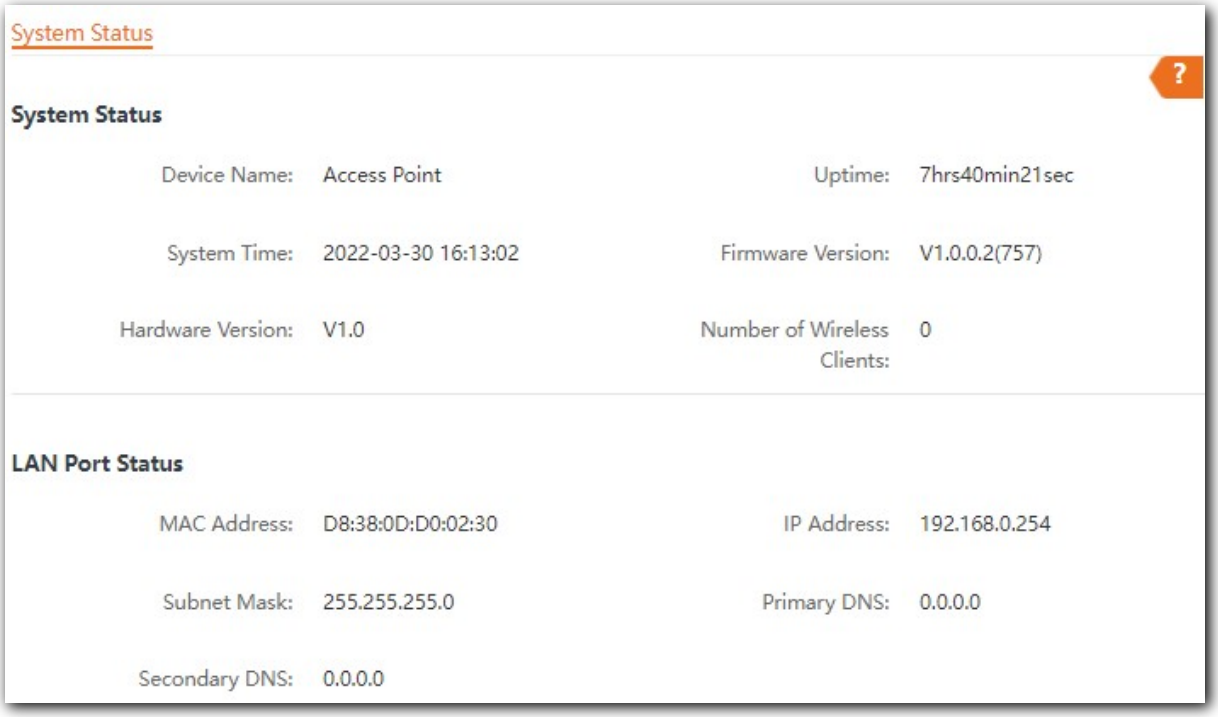
Parameter	Description
Radio Band	It is used to select the radio band for configurations.
SSID	Click to modify the WiFi name of the primary network under the selected radio band.
Security Mode	Select the security modes for target wireless networks, including **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA3-SAE**, **WPA3-SAE/WPA2-PSK**, **WPA-PSK & WPA2-PSK**, **WPA** and **WPA2**.

4 Status

4.1 System status

The **System Status** page allows you to check the **System Status** and **LAN Port Status** of the AP.

To access the page, choose **Status** > **System Status**.



Parameter description

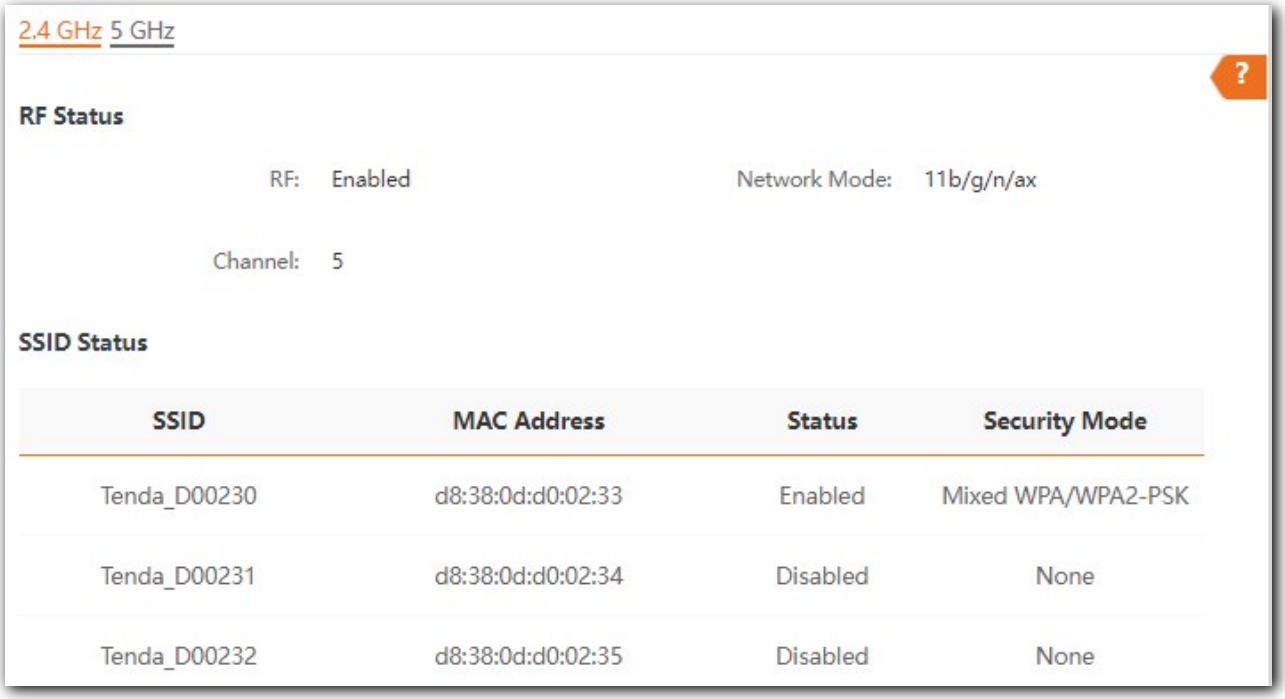
Parameter		Description
System Status	Device Name	It specifies the name of the AP. You can modify it on LAN Setup page.
	Uptime	It specifies the time that has elapsed since the AP starts up last time.
	System Time	It specifies the current system time of the AP.
	Firmware Version	It specifies the current firmware version number of the AP.
	Hardware Version	It specifies the current hardware version number of the AP.
	Number of Wireless Clients	It specifies the quantity of wireless devices currently connected to the AP.

Parameter		Description
LAN Port Status	MAC Address	It specifies the physical address of the AP's LAN port.
	IP Address	It specifies the IP address of the AP and it is also the management IP address of the AP, which can be used to log in to the web UI. You can modify it on **LAN Setup** page.
	Subnet Mask	It specifies the subnet mask of the AP.
	Primary DNS	It specifies the primary DNS server of the AP.
	Secondary DNS	It specifies the secondary DNS server of the AP.

4.2 Wireless status

The **Wireless Status** page allows you to check **RF Status** and **SSID Status** of the AP.

To access the page, choose **Status** > **Wireless Status**.



Parameter description

Parameter		Description
RF Status	RF	It specifies whether the wireless function of the AP is enabled.
	Network Mode	It specifies the network mode currently enabled by the AP on each radio band.
	Channel	It specifies the current working channel of the AP.
SSID Status	SSID	It specifies the names of all the wireless networks of the AP.
	MAC Address	It specifies the physical address of the corresponding wireless network.
	Status	It specifies whether or not the corresponding WiFi network is enabled.
	Security Mode	It specifies the security modes of the wireless networks corresponding to the SSIDs of the AP.

4.3 Traffic statistics

The Traffic Statistics page allows you to check statistical information about traffic based on SSIDs.

To access the page, choose **Status** > **Traffic Statistics**.

SSID	Received Traffic	Received Packets (Qty.)	Transmitted Traffic	Transmitted Packets (Qty.)
Tenda_D00230	0.00MB	0	0.00MB	0
Tenda_D00231	0.00MB	0	0.00MB	0
Tenda_D00232	0.00MB	0	0.00MB	0
Tenda_D00233	0.00MB	0	0.00MB	0
Tenda_D00234	0.00MB	0	0.00MB	0
Tenda_D00235	0.00MB	0	0.00MB	0
Tenda_D00236	0.00MB	0	0.00MB	0

Parameter description

Parameter	Description
SSID	It specifies the wireless network name.
Received Traffic	It specifies the total number of bytes received by a wireless network.
Received Packets (Qty.)	It specifies the total number of packets received by a wireless network.
Transmitted Traffic	It specifies the total number of bytes transmitted by a wireless network.
Transmitted Packets (Qty.)	It specifies the total number of packets transmitted by a wireless network.

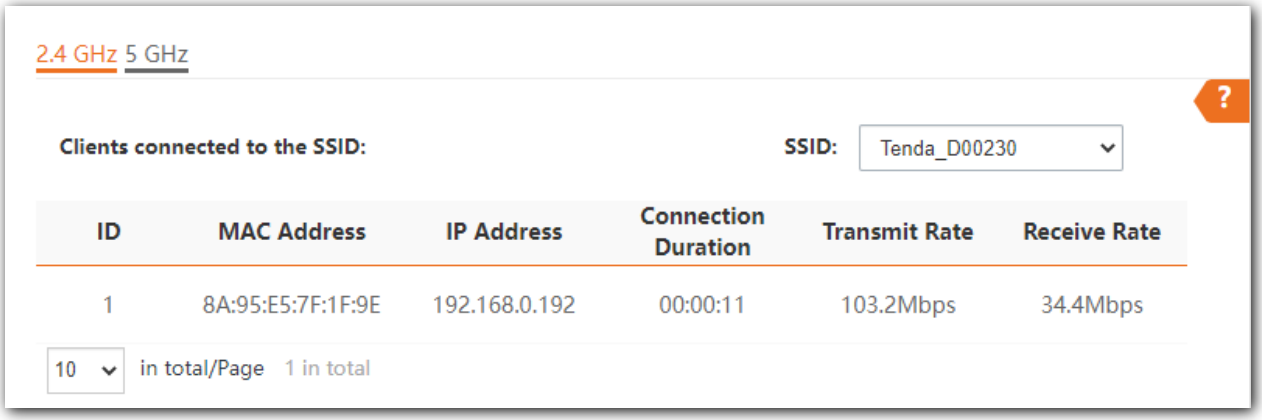
NOTE

All the statistics are cleared when the wireless function is disabled or this device is rebooted. All the wireless network statistics of an SSID are cleared when the SSID is disabled.

4.4 Client list

The **Client List** page allows you to view wireless clients connected to each SSID of the AP and their basic information.

To access the page, choose **Status** > **Client List**.



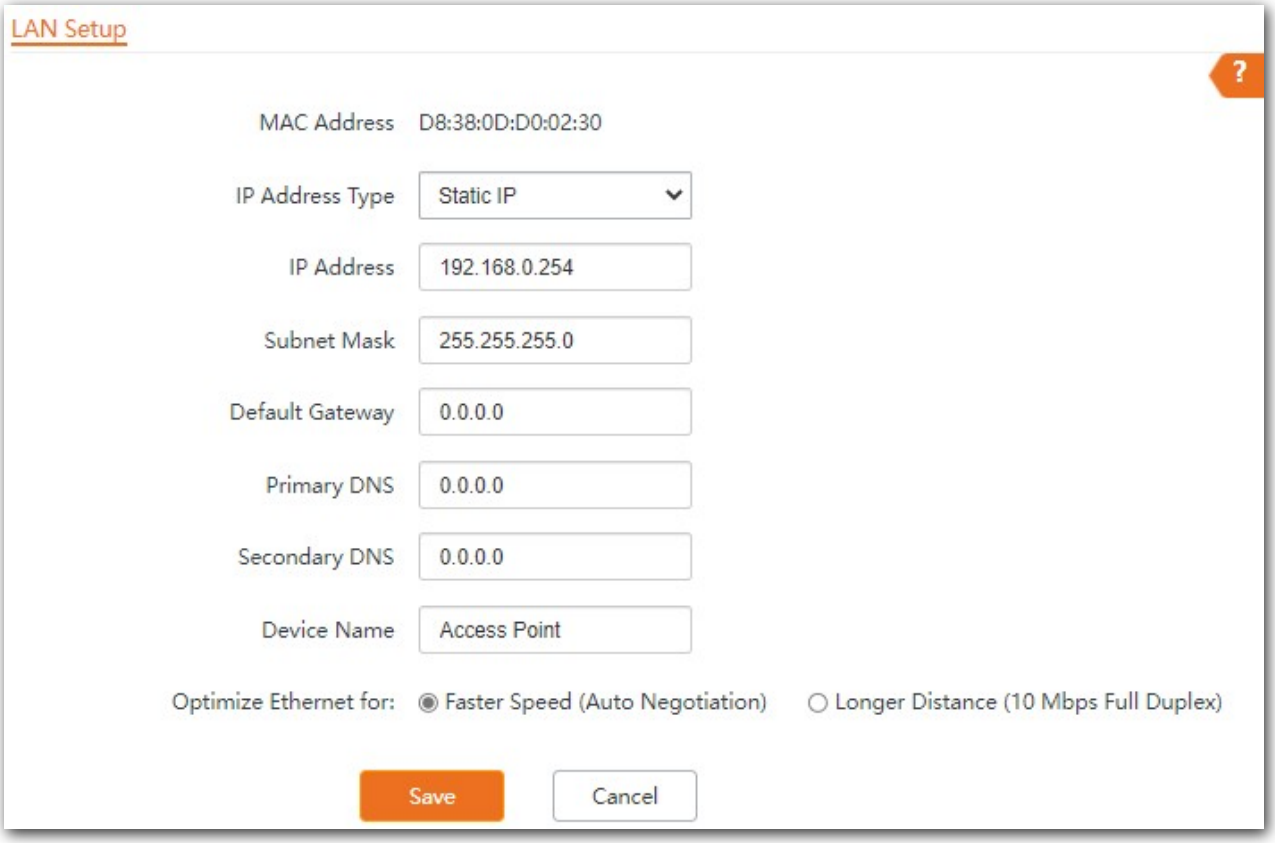
Parameter description

Parameter	Description
SSID	Select the SSID from the drop-down list menu to view client information connected to it.
MAC Address	It specifies the physical address of the wireless client.
IP Address	It specifies the IP address of the wireless client.
Connection Duration	It specifies the duration of a connection between a wireless client and a wireless network with a specified SSID.
Transmit Rate	It specifies the real time traffic the client has transmitted.
Receive Rate	It specifies the real time traffic the client has received.

5 Internet settings

The **LAN Setup** page allows you to check the MAC address of the LAN port of AP, modify the IP address obtaining method of the AP, modify device name, and modify Ethernet mode.

To access the page, choose **Internet Settings** > **LAN Setup**.



Parameter description

Parameter	Description
MAC Address	It specifies the MAC address of the AP's LAN port.
IP Address Type	It specifies IP address obtaining method of the AP. • **Static IP**: You are required to set related parameters manually. This method is suitable for scenarios where only one or several APs are deployed. • **DHCP (Dynamic IP Address)**: The AP automatically obtains related parameters from a DHCP server on your LAN network. This method is suitable for scenarios where a great number of APs are deployed.  After setting the IP address obtaining method to **DHCP (Dynamic IP Address)**, before logging in to the web UI of the AP next time, check the IP address obtained by the AP in the client list of the DHCP server in the network first, then use the IP address to log in.
IP Address	It specifies the LAN IP address (also the login IP address) of the AP. The web UI of the AP is accessible at this IP address.
Subnet Mask	It specifies the subnet mask of the AP. Default: **255.255.255.0**.
Default Gateway	It specifies the gateway IP address of the AP. Generally, enter the LAN IP address of the router connected to the internet.
Primary DNS	It specifies the IP address of the primary DNS server of the AP. If DNS proxy function is supported on your router connected to the internet, you can set the IP address of the primary DNS server to the LAN IP address of your router. Otherwise, enter a correct DNS server IP address.
Secondary DNS	It specifies the IP address of the secondary DNS server of the AP. This parameter is optional. If you have two DNS server IP addresses, you can enter the other one here.
Device Name	It specifies the name of the AP. You are recommended to change the name of the AP to indicate the location of the AP (such as Living Room), so that you can easily identify the AP when managing many APs.
Optimize Ethernet for	It specifies the Ethernet mode of the PoE power-supply port of the AP. • **Faster Speed (Auto Negotiation)**: This option features a high data rate but short transmission distance. Generally, you are advised to select this option. • **Longer Distance (10 Mbps Full Duplex)**: This option features long transmission distance but low data rate. Generally, the negotiated speed is 10 Mbps. If the Ethernet cable connecting the PoE Ethernet port of the AP to the peer device is longer than 100 meters, the Longer Distance (10 Mbps Full Duplex) mode is recommended. In this case, ensure that the peer device adopts auto negotiation option.

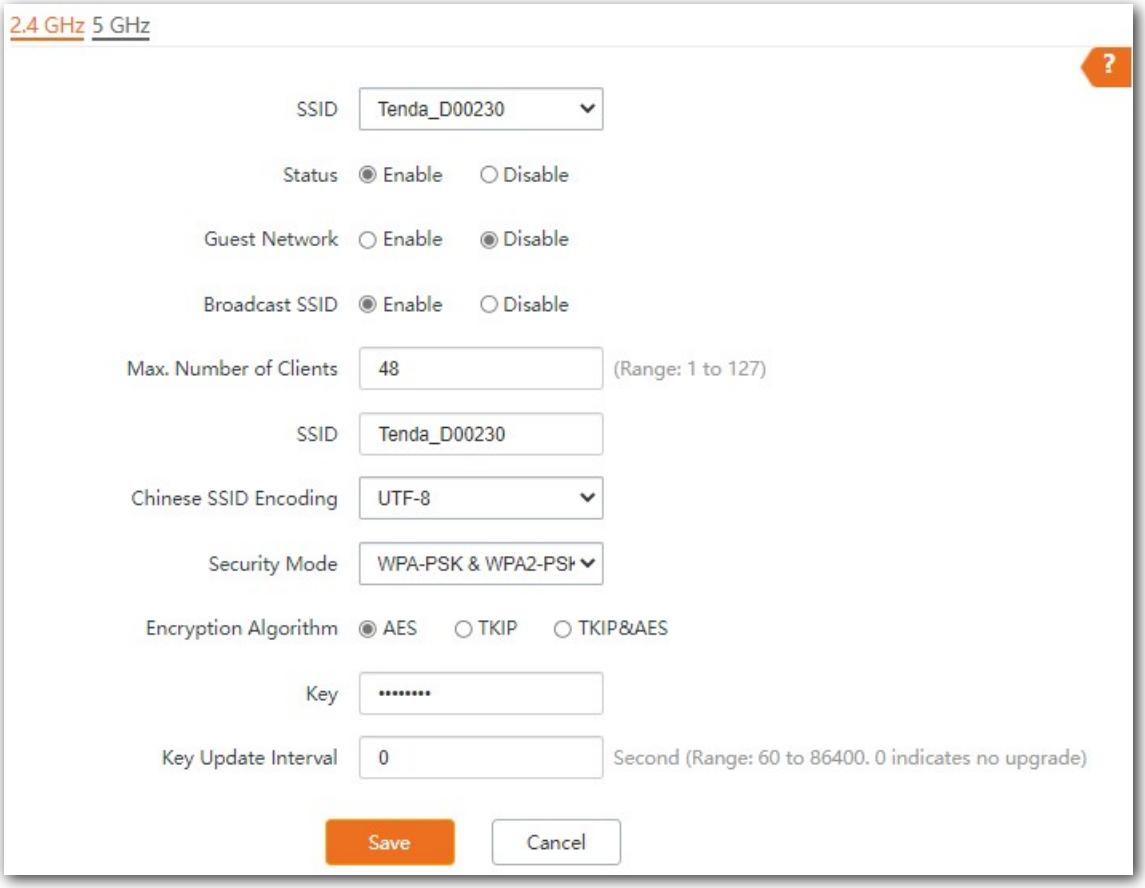
6 Wireless

6.1 SSID

6.1.1 Overview

The **SSID** page allows you to set SSID-related parameters of the AP.

To access the page, choose **Wireless** > **SSID**.



Parameter description

Parameter	Description
SSID	It specifies the SSID to be configured. On each band, the first displayed SSID is the primary SSID.

Parameter	Description
Status	It specifies the status of the selected SSID. The primary SSID is enabled by default and you can enable other SSIDs manually.
Guest Network	After this function is enabled, users can access only the internet but cannot access the LAN.
Broadcast SSID	After this function is disabled, AP stops broadcasting SSID and nearby wireless clients cannot detect the SSID. Users need to enter the SSID manually on the wireless client to access the wireless network, enhancing the security of the wireless network.
Max. Number of Clients	It specifies the maximum number of devices that can connect to the WiFi network corresponding to an SSID. If the number is reached, new devices cannot connect to the SSID unless some devices cut off their connections.
SSID	Click this field to modify the selected SSID (the name of the wireless network).
Chinese SSID Encoding	It specifies the character encoding format. By default, **UTF-8** is selected. If you want to configure multiple Chinese SSIDs for the AP, you are recommended to select the UTF-8 encoding format for some SSIDs and the GB2312 encoding format for other SSIDs so as to ensure compatibility for different wireless clients.
Security Mode	It specifies the security modes supported by the AP, including: **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA3-SAE**, **WPA3-SAE/WPA2-PSK**, **WPA-PSK & WPA2-PSK**, **WPA** and **WPA2**.

Security Mode

A wireless network uses radio, which is open to the public, as its data transmission medium. If the wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network. To ensure communication security, transmission links of wireless networks must be encrypted for protection.

The AP supports various security modes for network encryption, including **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA3-SAE**, **WPA3-SAE/WPA2-PSK**, **WPA-PSK & WPA2-PSK**, **WPA** and **WPA2**.

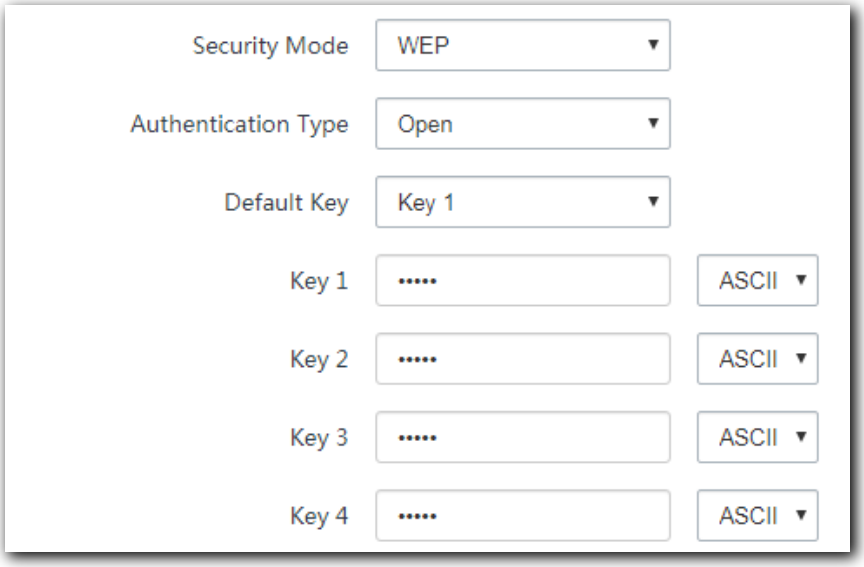
None

It indicates that any wireless device can connect to the WiFi network. This option is not recommended because it leads to network insecurity.

WEP

It is abbreviated for Wired Equivalent Privacy. It uses a static key to encrypt all exchanged data, and ensures that a WLAN has the same level of security as a wired LAN. However, data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum WiFi network throughput of

only 54 Mbps. Therefore, this security mode is not recommended.



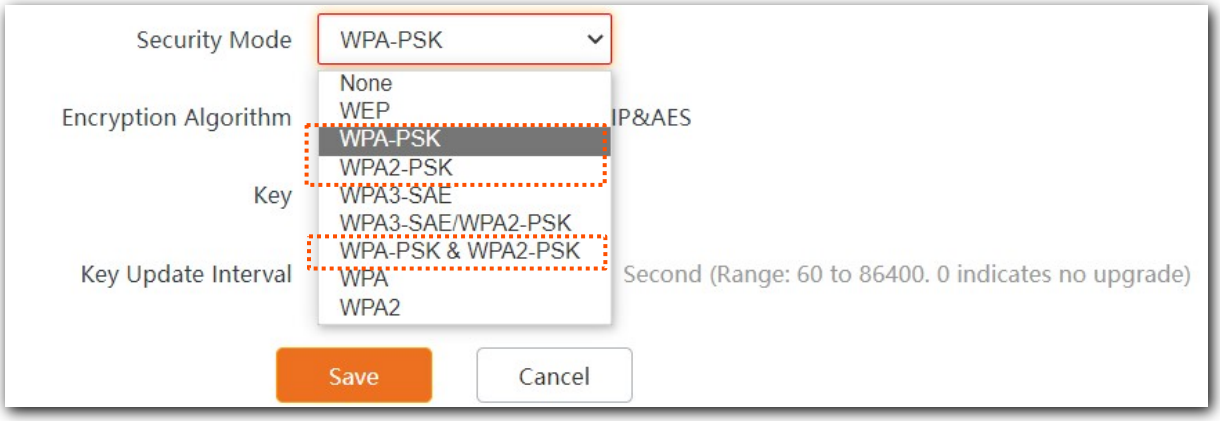
Parameter description

Parameter	Description
Authentication Type	It specifies the authentication type for the WEP security mode. The options include **Open** and **Shared**. The options share the same encryption process. • **Open**: It specifies that authentication is not required and data exchanged is encrypted with WEP. In this case, a wireless client can connect to the wireless network corresponding to the selected SSID without being authenticated, and the data exchanged between the client and the network is encrypted in WEP security mode. • **Shared**: It specifies that a shared key is used for authentication and data exchanged is encrypted with WEP. In this case, a wireless client must use a preset WEP key to connect to the wireless network corresponding to the selected SSID. The wireless client can be connected to the wireless network only if they use the same WEP key.
Default Key	It specifies the WEP key for the current SSID. For example, if **Default Key** is set to **Key 2**, a wireless client can connect to the wireless network corresponding to the selected SSID only with the password specified by Key 2.
Key 1/2/3/4	4 WEP keys are allowed at the same time, but only the one specified by the **Default Key** is valid. The key type includes ASCII and Hex. • ASCII: 5 or 13 ASCII characters are allowed in the key. • Hex: 10 or 26 hexadecimal characters are allowed in the key (0-9, a-f, A-F).

WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK

They belong to pre-shared key or personal key modes, where WPA-PSK & WPA2-PSK supports both WPA-PSK and WPA2-PSK.

WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK adopt a pre-shared key for authentication, while the AP generates another key for data encryption. This prevents the vulnerability caused by static WEP keys, and makes the three security modes suitable for ensuring security of home WiFi networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all devices use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.

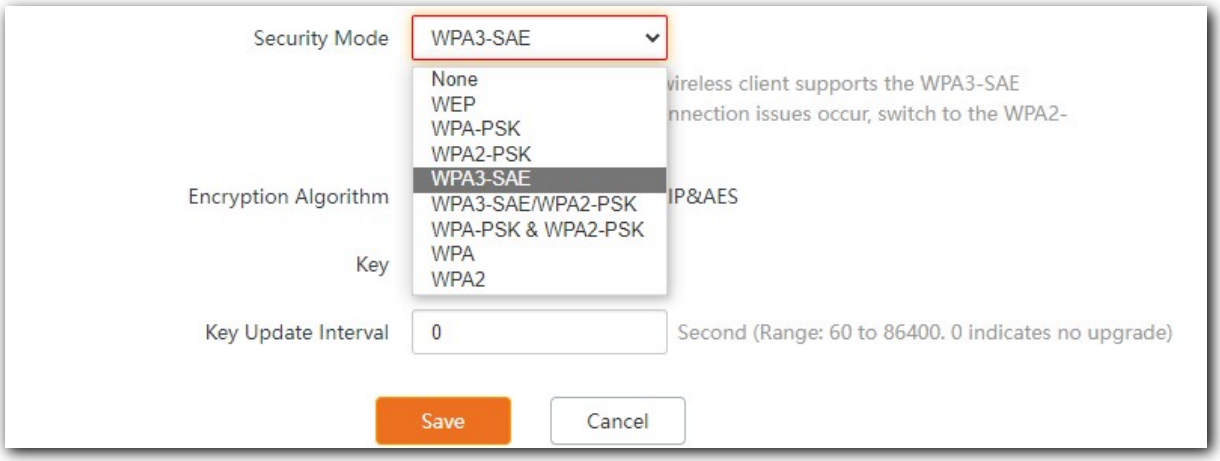


WPA3-SAE

It is an upgraded version of WPA2-PSK. With Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF), this security mode provides protection against dictionary attacks and information disclosure, saving you the trouble to set a complicated password.

TIP

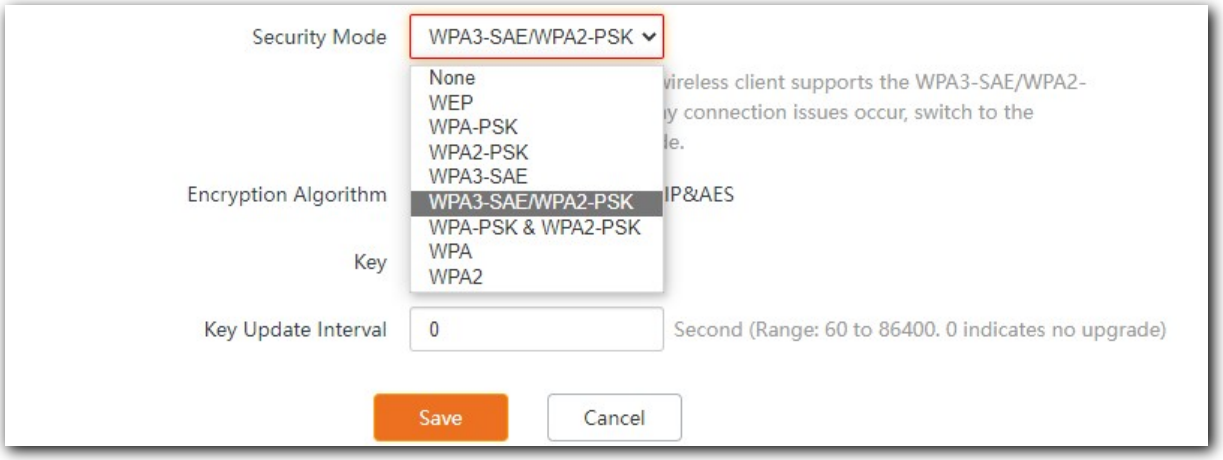
If your wireless clients do not support WPA3-SAE or the WiFi experience is unsatisfying, you are recommended to set the security mode to WPA2-PSK.



WPA3-SAE/WPA2-PSK

It indicates that the AP is compatible with both WPA3-SAE and WPA2-PSK security modes. WPA2 is

still widely used currently. In order to allow wireless devices that do not support WPA3 to access the WPA3 network, the AP supports the WPA3-SAE transition mode, which means that the mixed encryption mode of WPA2-PSK and WPA3-SAE is adopted to ensure both compatibility and security.



Parameter description

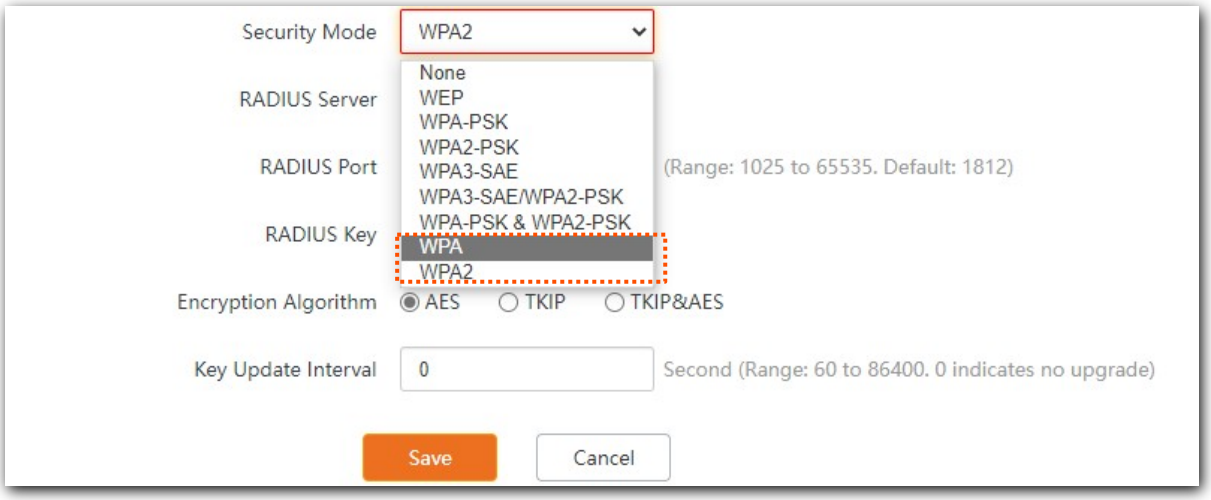
Parameter	Description
Security Mode	Select security mode. • WPA-PSK: The wireless network adopts the WPA-PSK security mode, which has better compatibility. • WPA2-PSK: The wireless network adopts the WPA2-PSK security mode, which has a higher security level. • WPA-PSK & WPA2-PSK: Compatible with WPA-PSK and WPA2-PSK. At this time, wireless devices can connect to the corresponding wireless network using both WPA-PSK and WPA2-PSK. • WPA3-SAE: The wireless network adopts the WPA3-SAE security mode, which is an upgraded version of WPA2-PSK. • WPA3-SAE/WPA2-PSK: Compatible with WPA3-SAE and WPA2-PSK. At this time, wireless devices can connect to the corresponding wireless network using both WPA3-SAE and WPA2-PSK.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. You can refer to the following instructions to select an appropriate encryption algorithm. • **AES**: It indicates the Advanced Encryption Standard. • **TKIP**: It indicates the Temporal Key Integrity Protocol. If **TKIP** is used, the maximum wireless throughput of the AP is limited to 54 Mbps. • **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key	It specifies a pre-shared WPA key, that is, the password clients use to connect to the wireless network.

Parameter	Description
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value **0** indicates that a WPA key is not updated.

WPA and WPA2

To address the key management weakness of WPA-PSK and WPA2-PSK, the WiFi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate devices and generate data encryption–oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.

WPA and WPA2 uses 802.1x to authenticate devices and the login information of a device is managed by the device. This effectively reduces the probability of information leakage. In addition, each time a device connects to an AP that adopts the WPA or WPA2 security mode, the RADIUS server generates a data encryption key and assigns it to the device, which makes it difficult for attackers to obtain the key. These features of WPA and WPA2 security modes help increase network security significantly, making WPA and WPA2 the preferred security modes of WiFi networks that require high security.



Parameter description

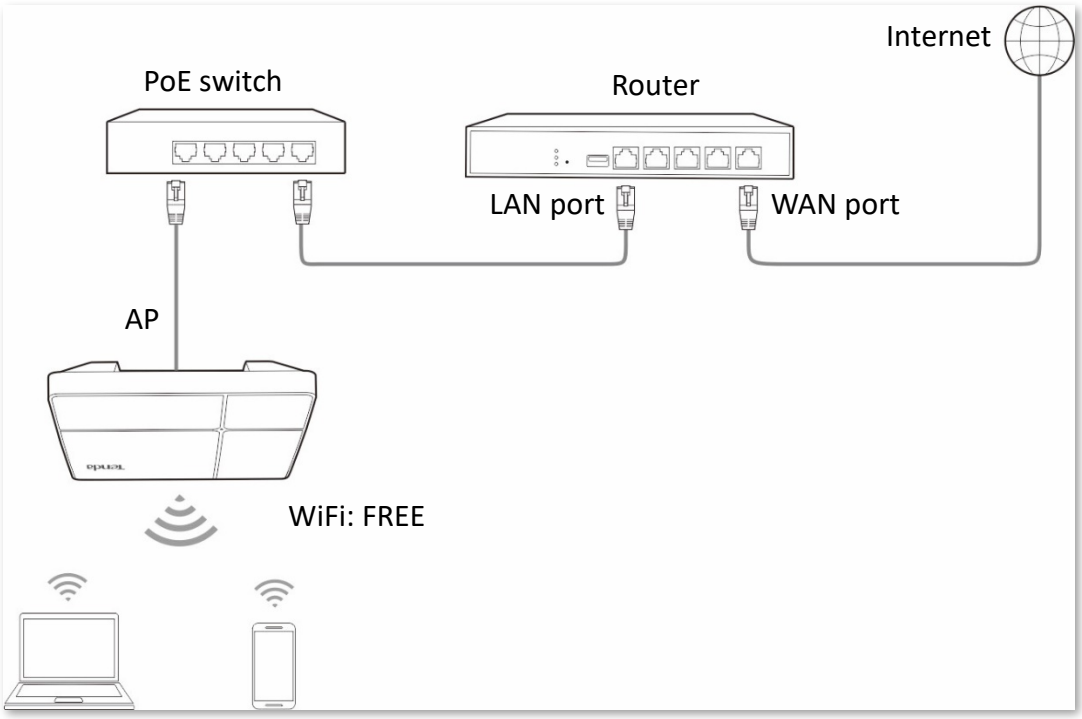
Parameter	Description
Security Mode	Select security mode. • WPA: The wireless network adopts the WPA enterprise security mode. • WPA2: The wireless network adopts the WPA2 enterprise security mode.
RADIUS Server	It specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	It specifies the port number of the RADIUS server for client authentication.
RADIUS Key	It specifies the shared key of the RADIUS server.
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. • **AES**: It indicates the Advanced Encryption Standard. • **TKIP**: It indicates the Temporal Key Integrity Protocol. • **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES.
Key Update Interval	It specifies the automatic update interval of a WPA key for data encryption. A shorter interval results in higher data security. The value **0** indicates that a WPA key is not updated.

6.1.2 Example of SSID configurations

Example of setting up an open wireless network

■ Networking requirement

In a hotel lounge, guests can connect to the wireless network without a password and access the internet through the WiFi network.



■ Configuration procedure

Assume that the first SSID of the 2.4 GHz radio band of the AP is to be configured.

Step 1 Choose **Wireless** > **SSID**.

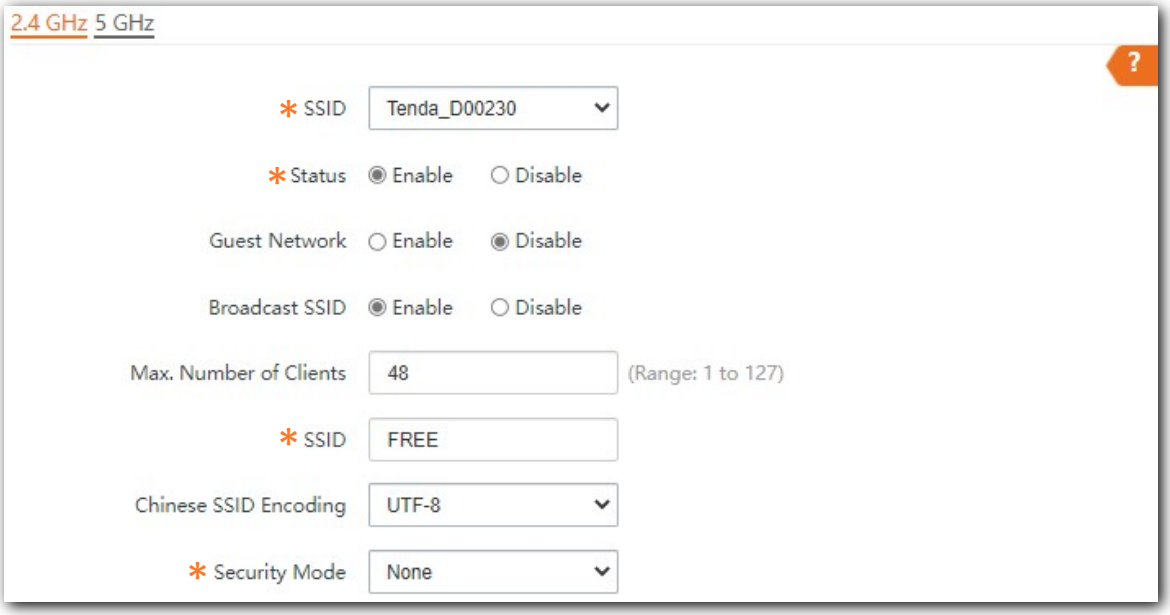
Step 2 Select the first SSID from the **SSID** drop-down list menu.

Step 3 Set **Status** to **Enable**.

Step 4 Change the value of the **SSID** text box to **FREE**.

Step 5 Set **Security Mode** to **None**.

Step 6 Click **Save**.



---- End

Verification

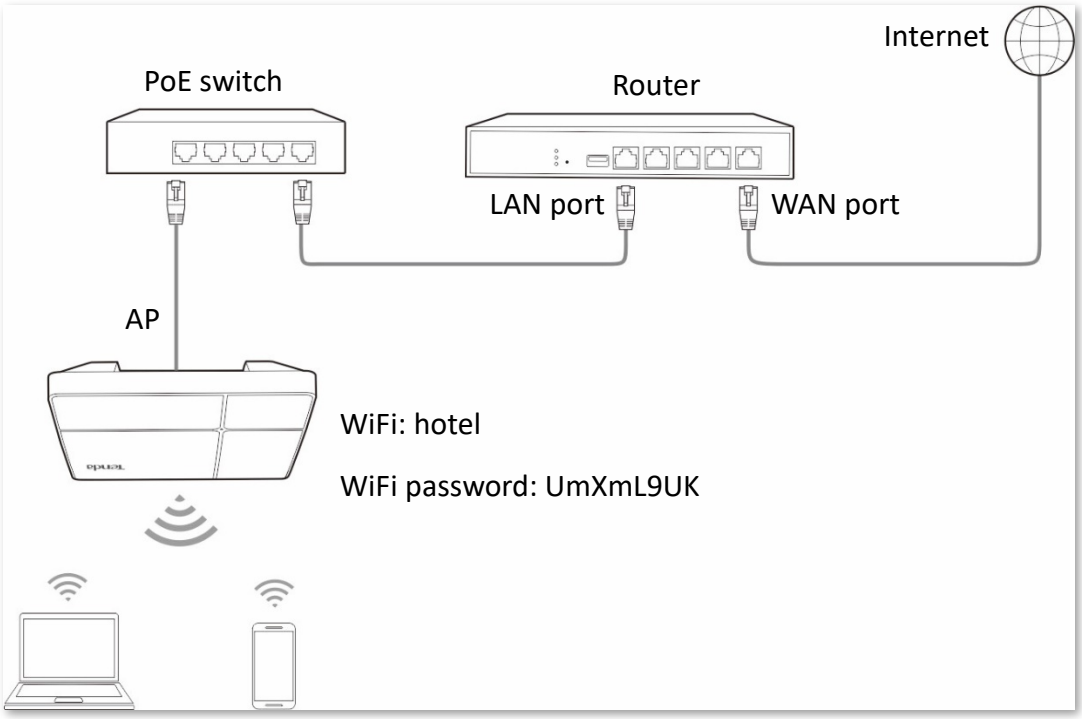
Wireless devices can connect to the **FREE** wireless network without a password.

Example of setting up a wireless network encrypted with PSK

Networking requirement

A hotel wireless network with a certain level of security must be set up through a simply procedure. In this case, WPA, WPA2-PSK or WPA-PSK & WPA2-PSK security mode is recommended.

Assume that the SSID is **hotel**, the Wifi password is **UmXmL9UK**. See the following figure.



Configuration procedure

Assume that the first SSID of the 2.4 GHz radio band of the AP is to be configured.

Step 1 Choose **Wireless** > **SSID**.

Step 2 Select the first SSID from the **SSID** drop-down list menu.

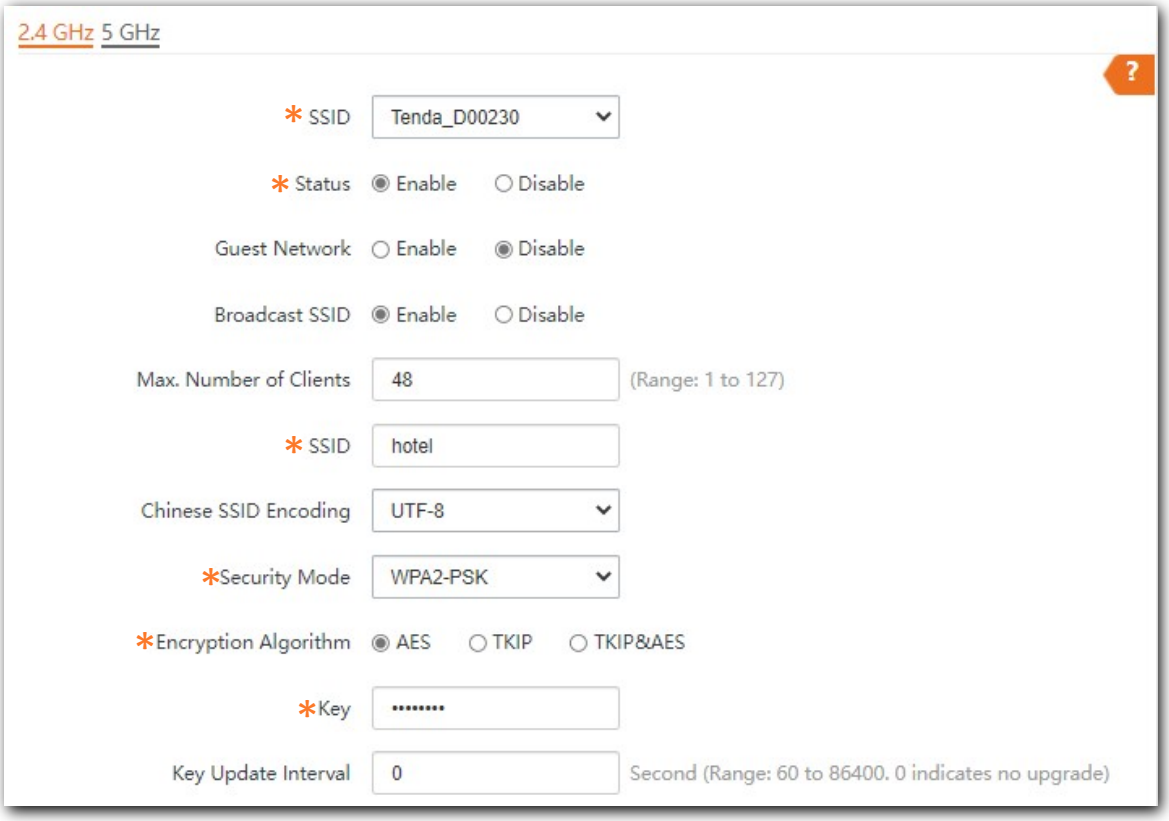
Step 3 Set **Status** to **Enable**.

Step 4 Change the value of the **SSID** text box to **hotel**.

Step 5 Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.

Step 6 Set **Key** to **UmXmL9UK**.

Step 7 Click **Save**.



---- End

Verification

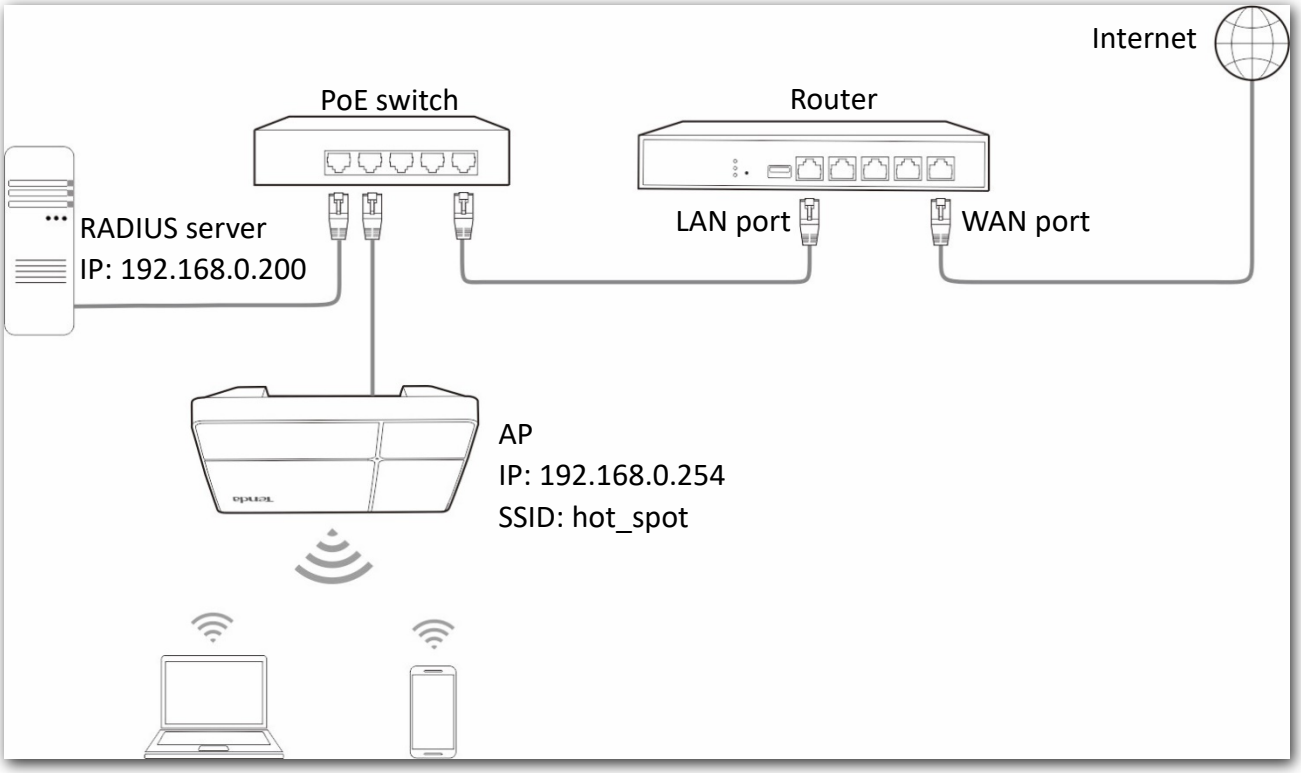
Wireless devices can connect to the **hotel** wireless network with the password **UmXmL9UK**.

Example of setting up a wireless network encrypted with WPA or WPA2

Networking requirement

A highly secure wireless network is required and a RADIUS server is available. In this case, WPA or WPA2 mode is recommended.

Assume that the IP address of the RADIUS server is **192.168.0.200**, the RADIUS password is **12345678**, the port number for authentication is **1812**, and the SSID is **hot_spot**. See the following figure.



Configuration procedure

Configure the AP.

Assume that the first SSID of the 2.4 GHz radio band of the AP is to be configured.

Step 1 Choose **Wireless** > **SSID**.

Step 2 Select the first SSID from the **SSID** drop-down list menu

Step 3 Set **Status** to **Enable**.

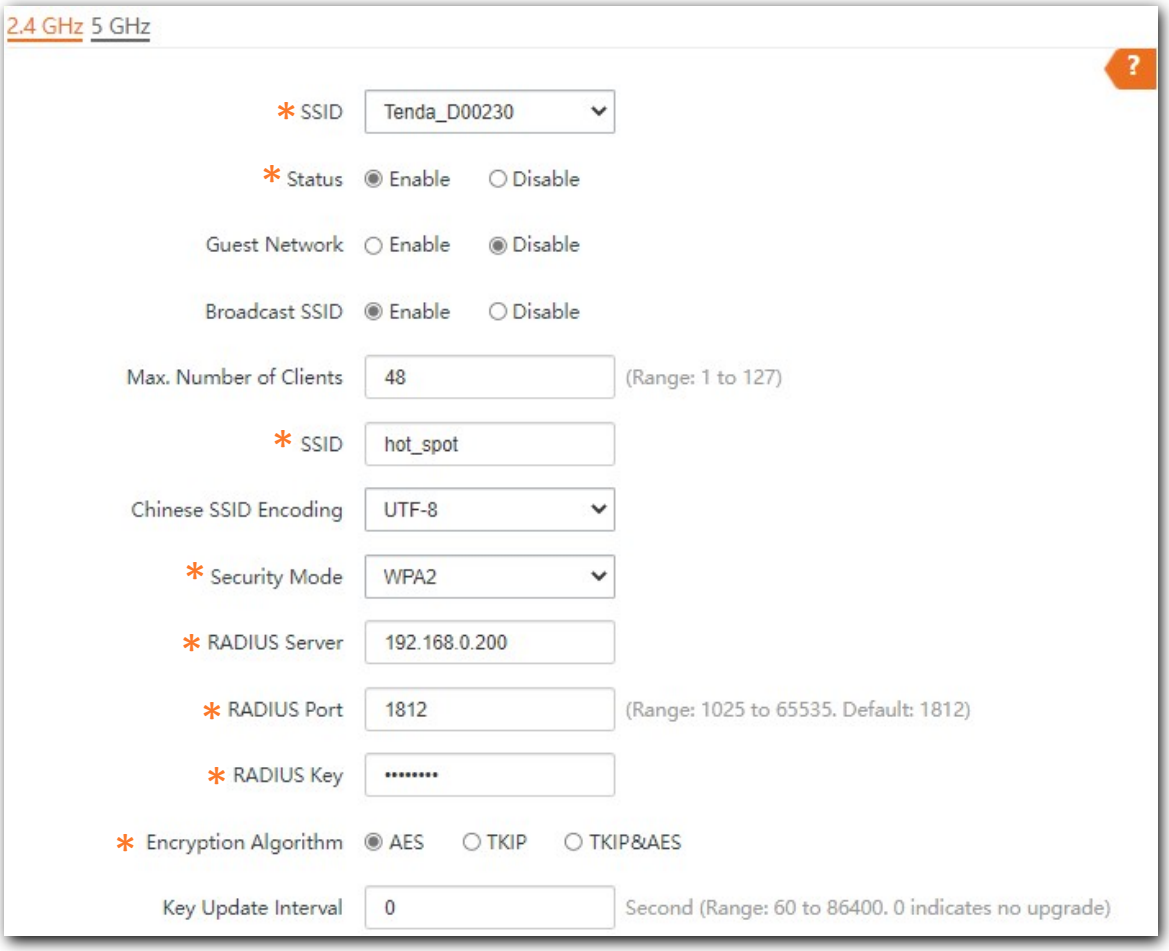
Step 4 Change the value of the SSID text box to **hot_spot**.

Step 5 Set **Security Mode** to **WPA2**.

Step 6 Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Key** to **192.168.0.200**, **1812**, and **12345678** respectively.

Step 7 Set **Encryption Algorithm** to **AES**.

Step 8 Click **Save** to apply your settings.



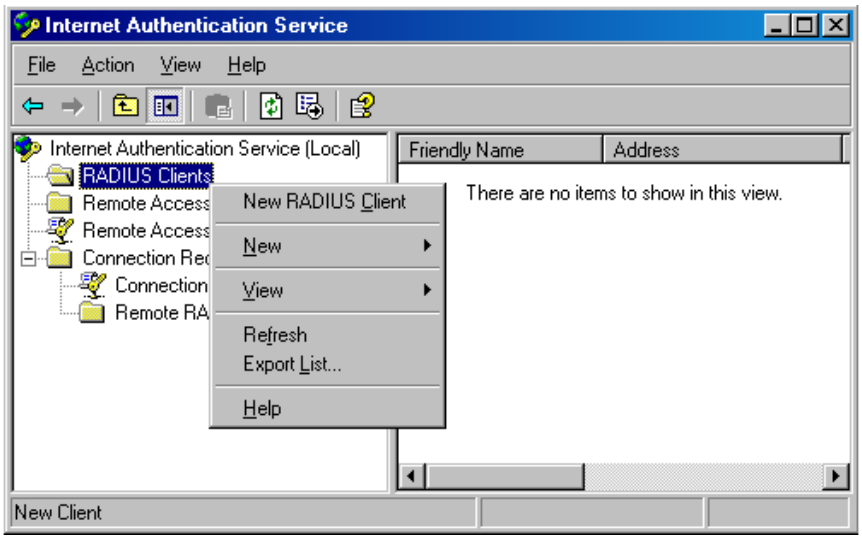
Configure the RADIUS client.

TIP

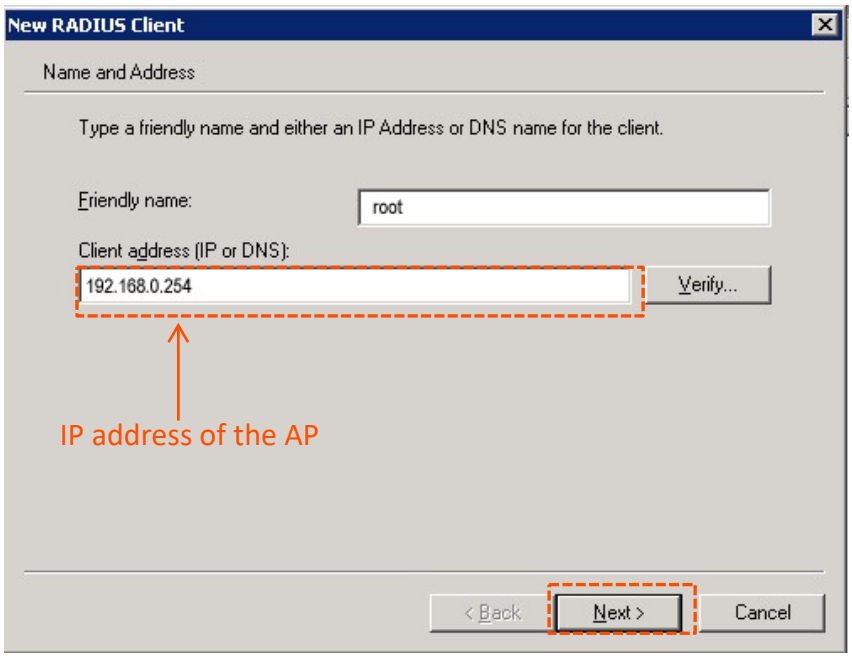
Windows 2003 is used as an example to describe how to configure the RADIUS client.

Step 1 Configure RADIUS client

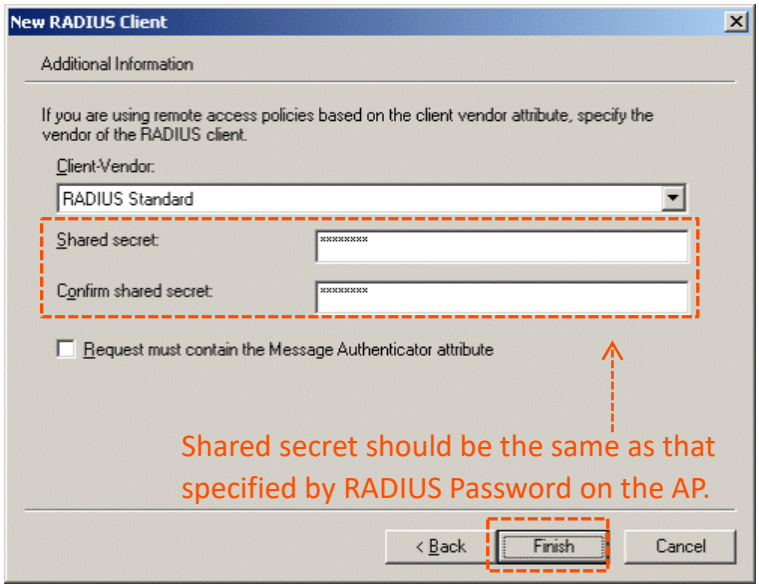
1. In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



2. Enter a RADIUS client name (device name of the AP is recommended) and the IP address of the AP, and click **Next**.

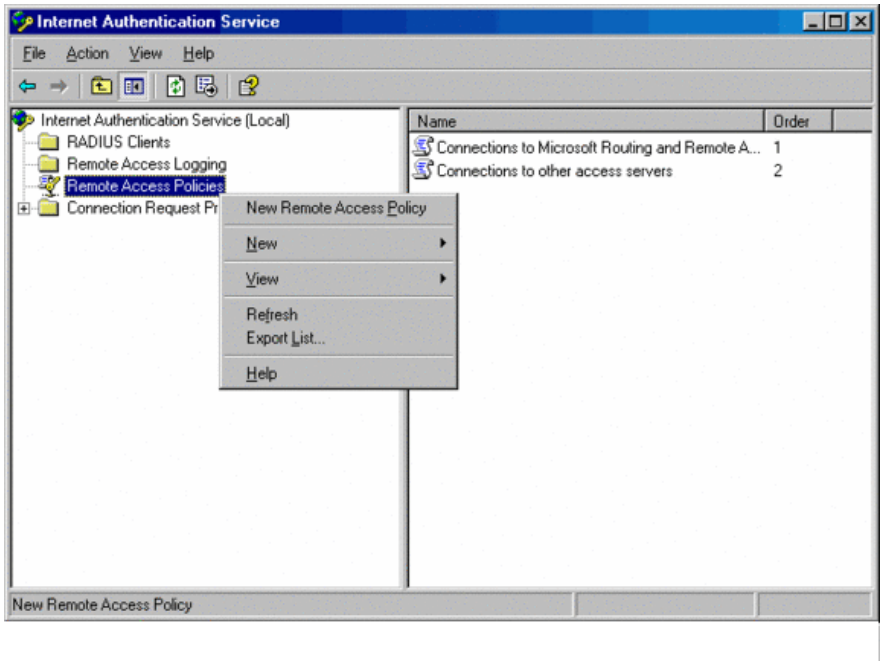


3. Enter **12345678** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.

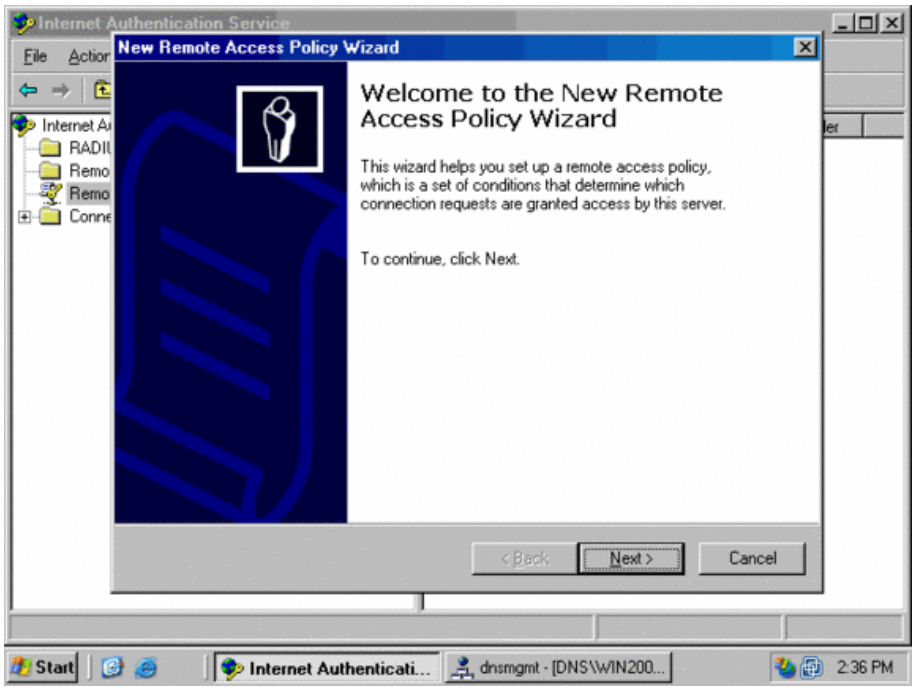


Step 2 Configure a remote access policy.

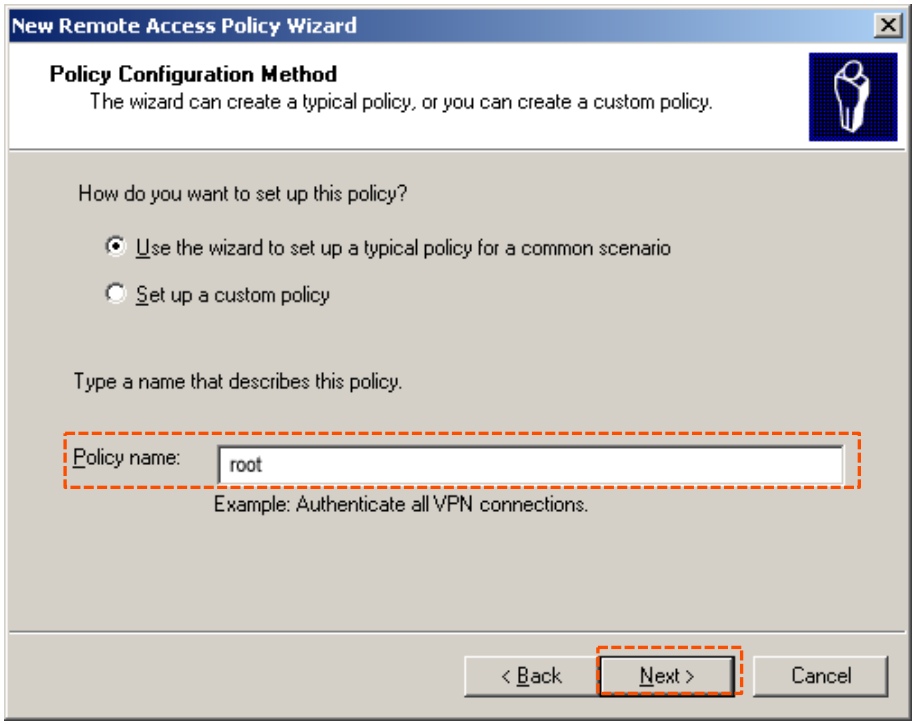
1. Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



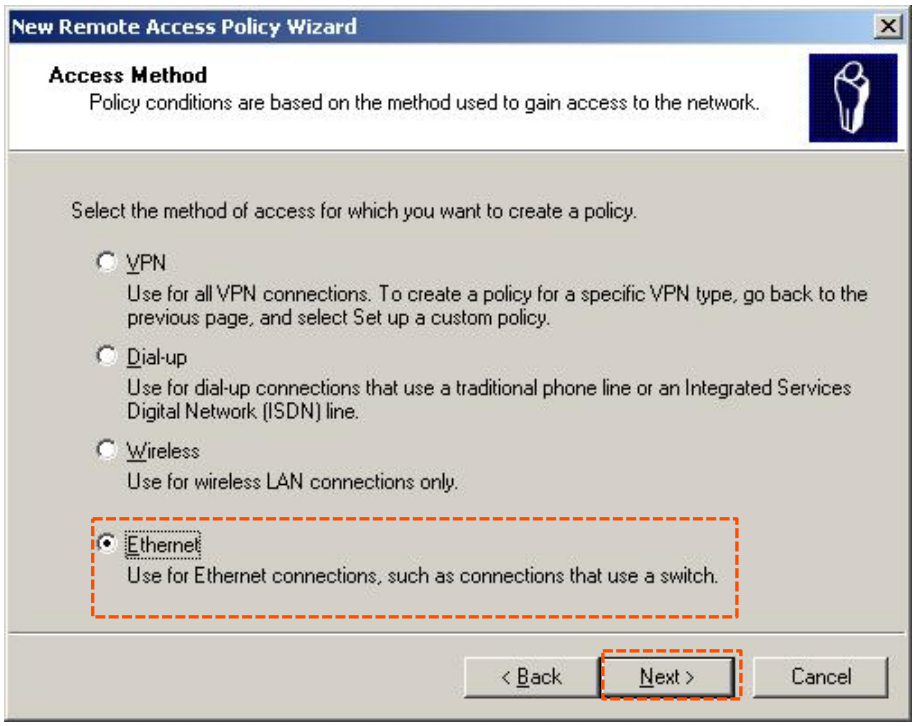
2. In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.



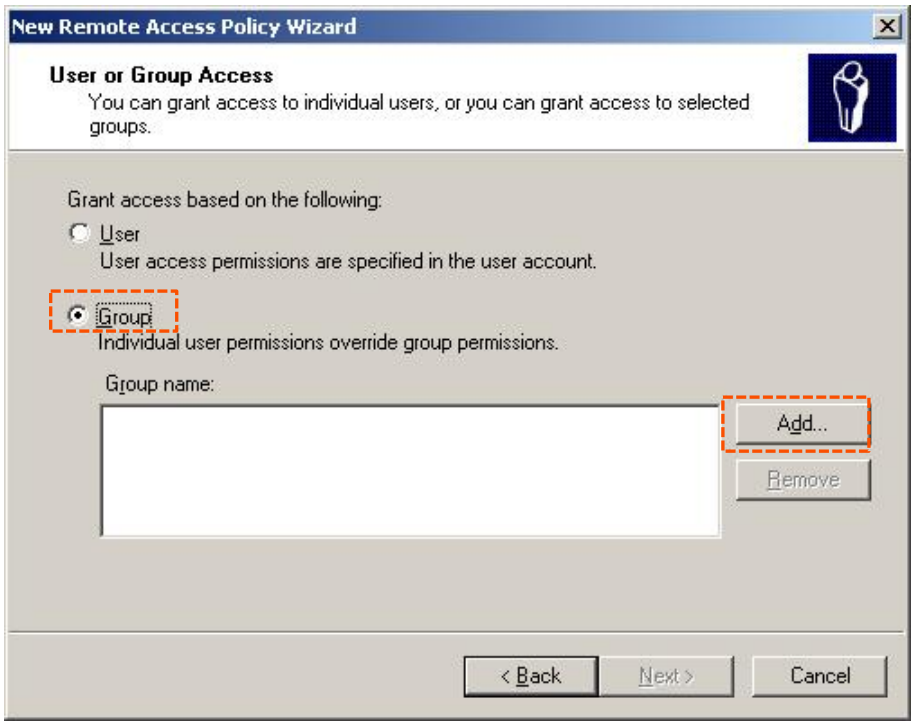
3. Enter a policy name and click **Next**.



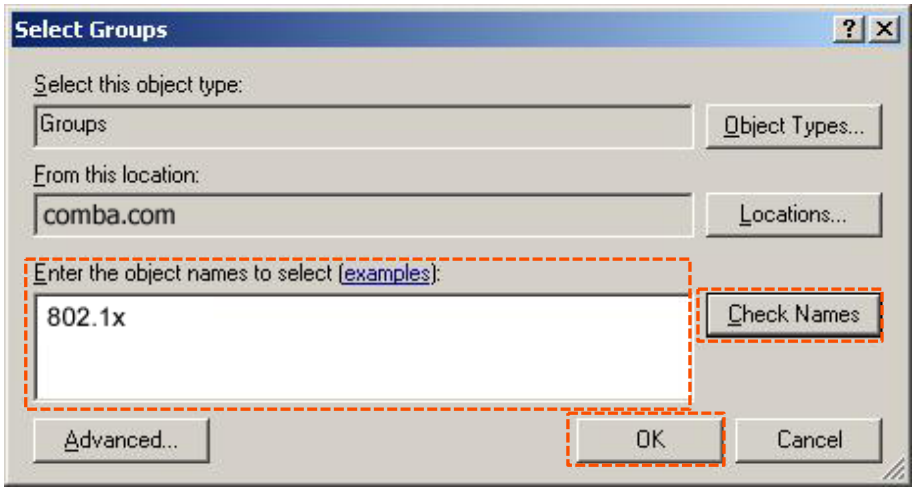
4. Select **Ethernet** and click **Next**.



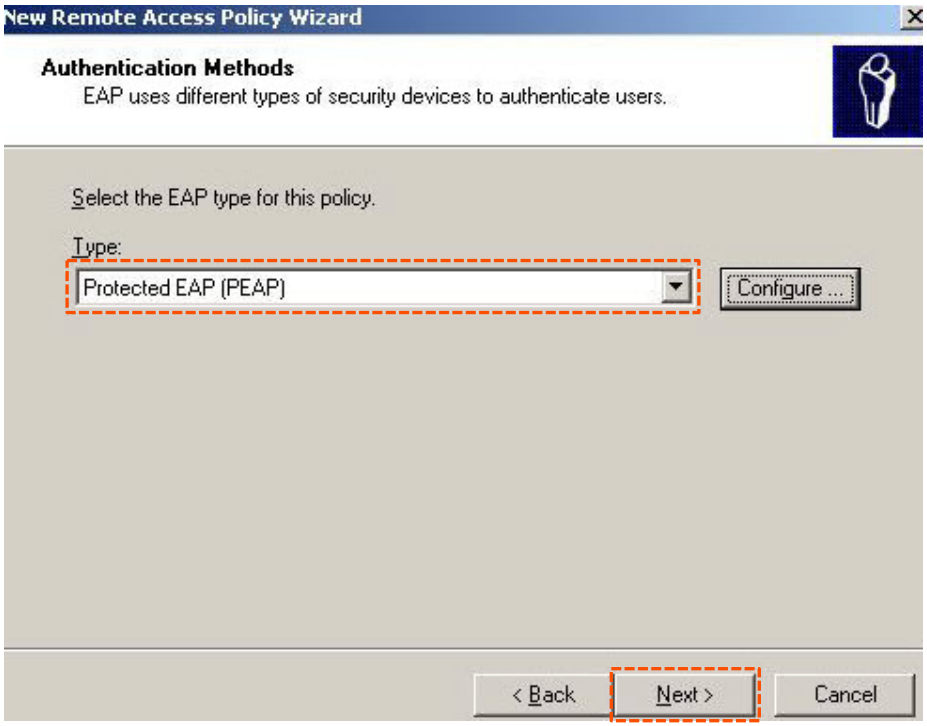
5. Select **Group** and click **Add**.



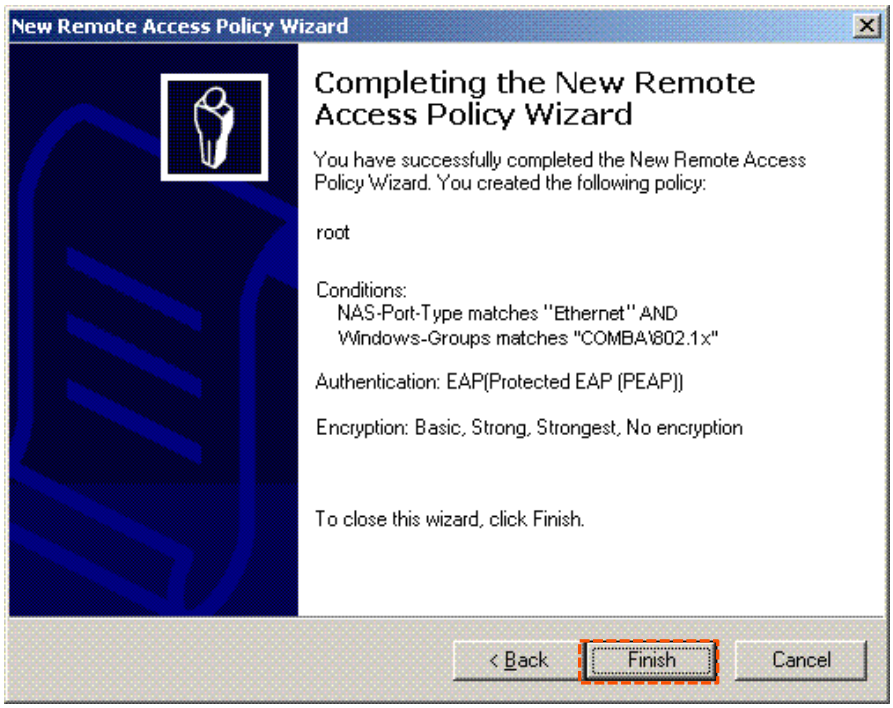
6. Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



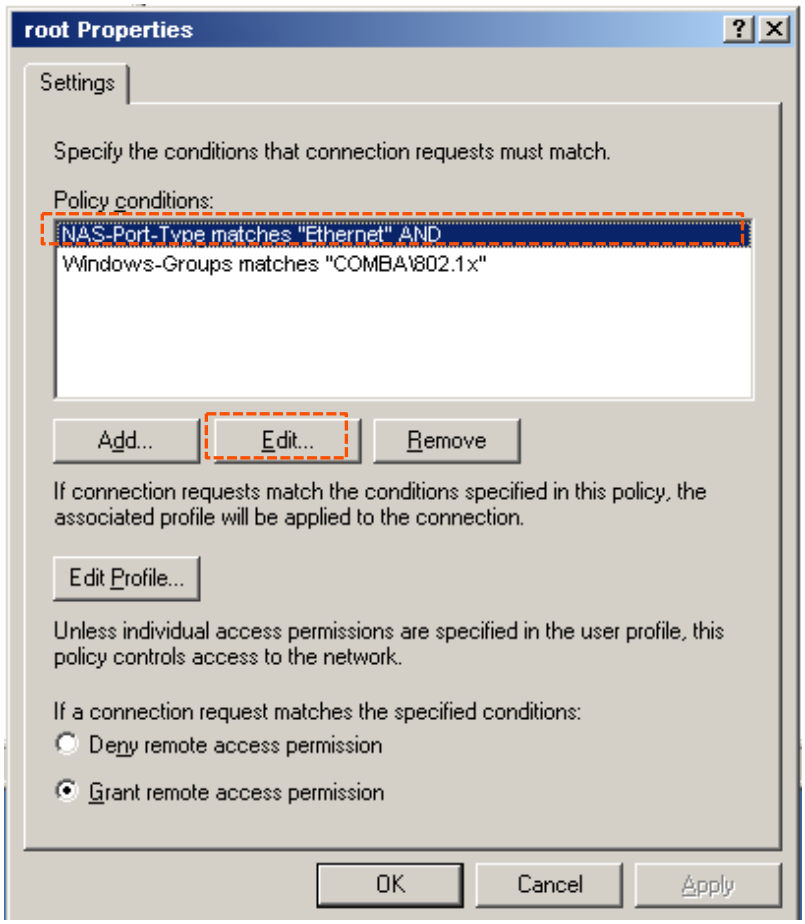
7. Select **Protected EAP (PEAP)** and click **Next**.



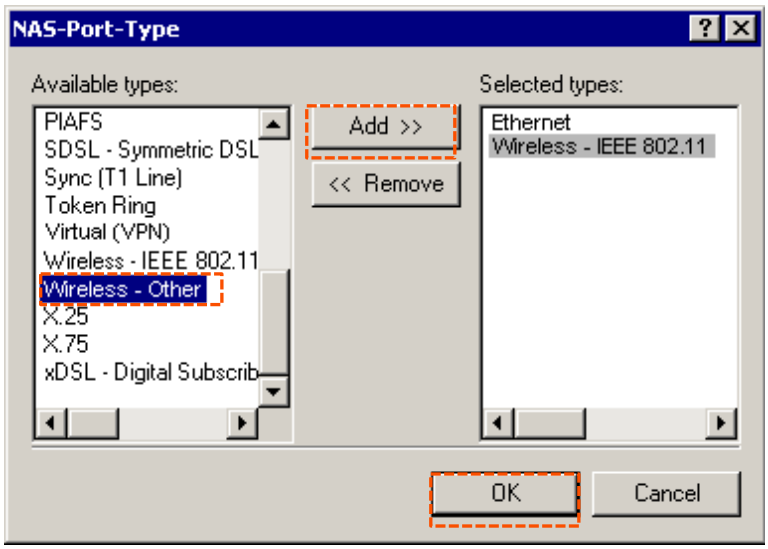
8. Click **Finish**. The remote access policy is created.



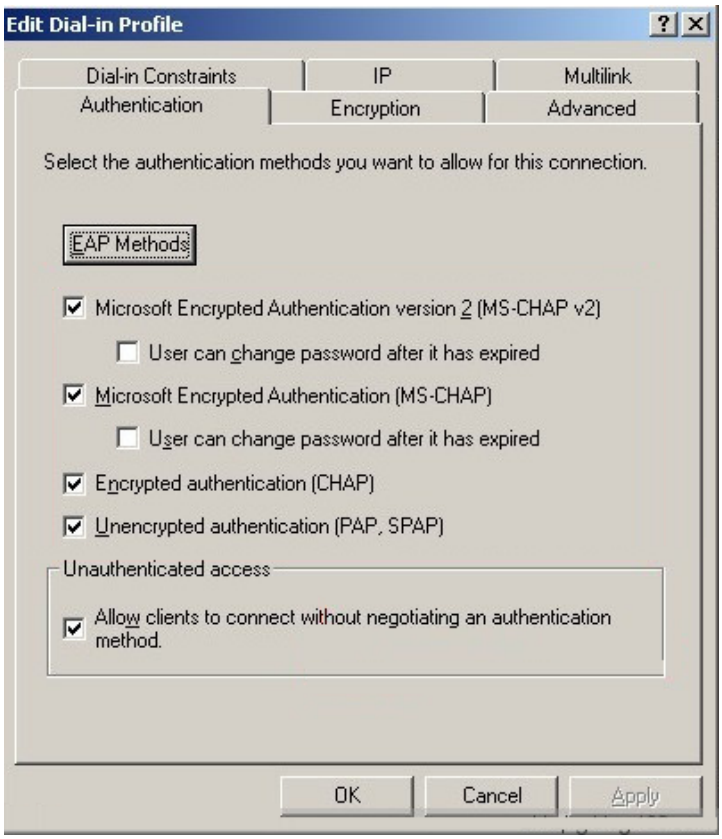
9. Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



10. Select **Wireless – Other**, click **Add**, and click **OK**.



11. Click **Edit Dial-in Profile**, click the **Authentication** tab, configure settings as shown in the following figure, and click **OK**.



12. When a message appears, click **No**.

Step 3 Configure user information.

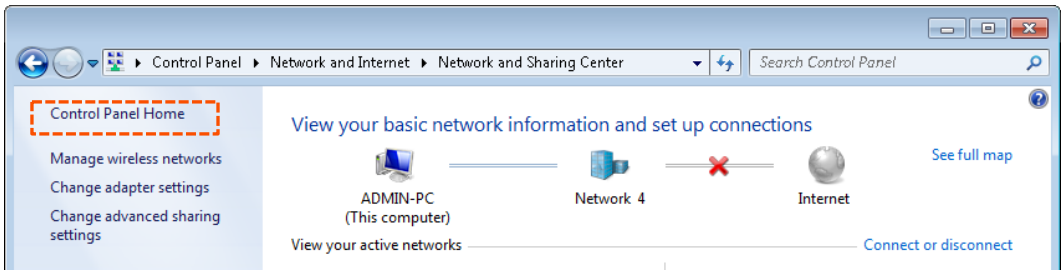
Create a user and add the user to group **802.1x**.

Configure your wireless device.

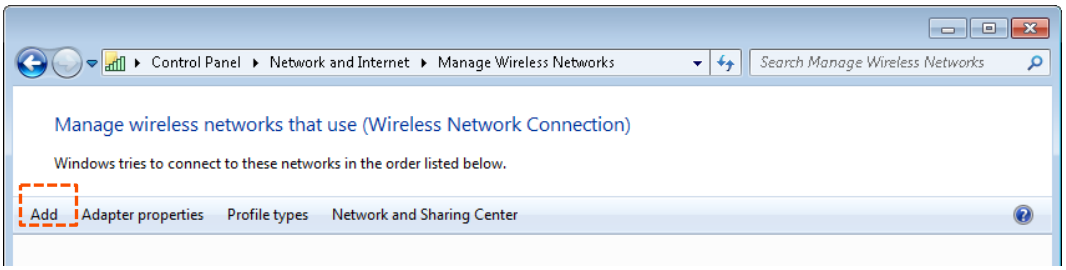
TIP

Windows 7 is taken as an example to describe the procedure.

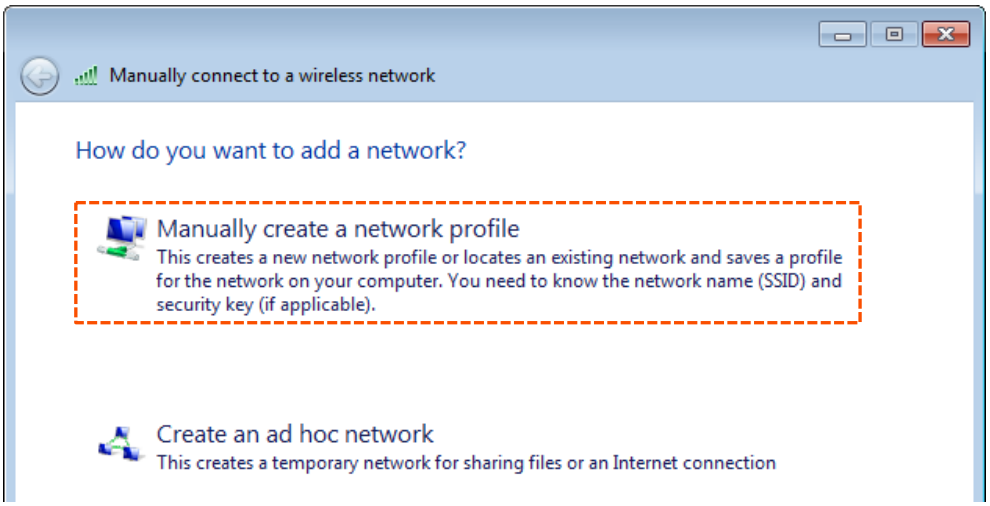
Step 1 Choose **Start** > **Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



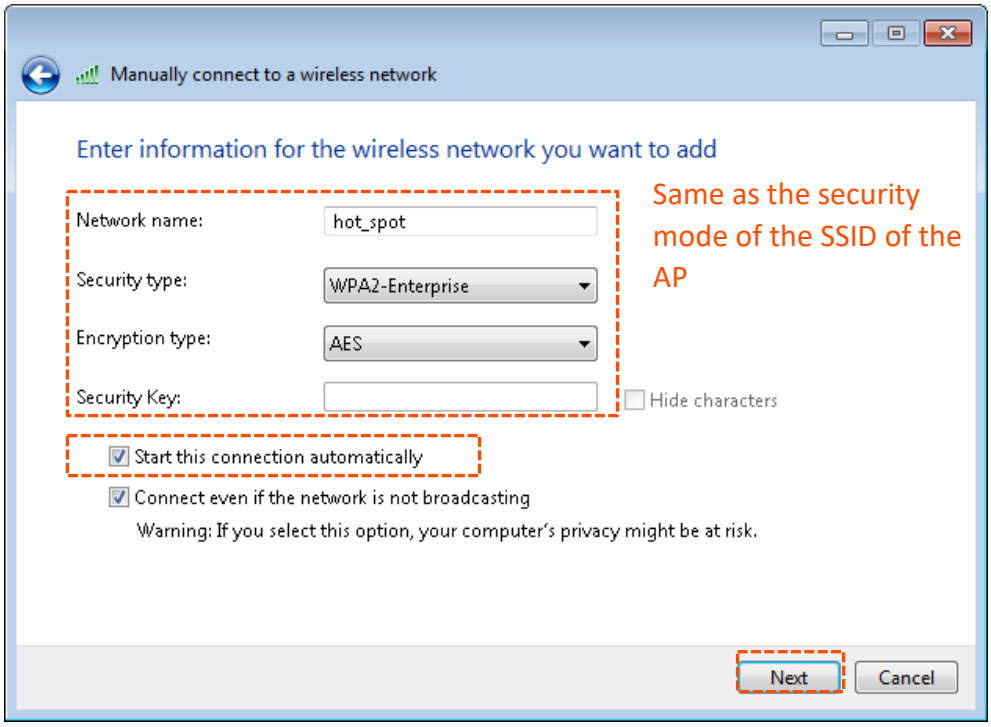
Step 2 Click **Add**.



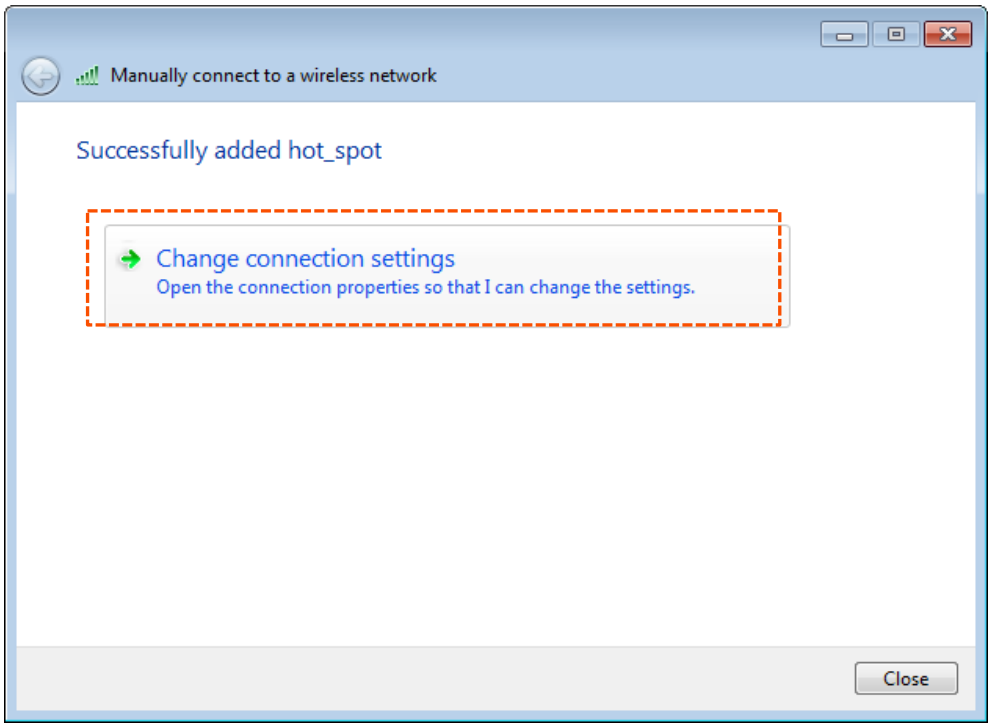
Step 3 Click **Manually create a network profile**.



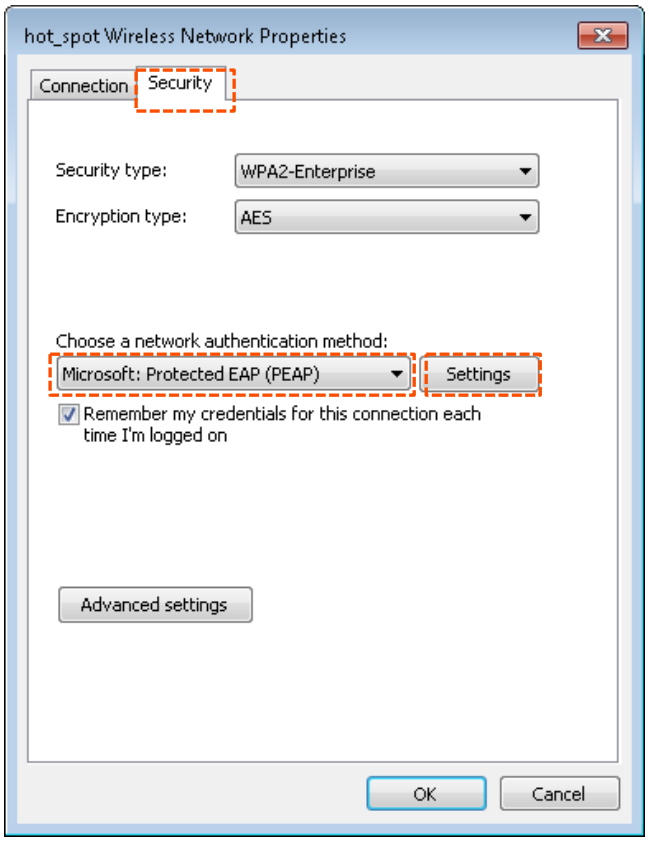
Step 4 Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.



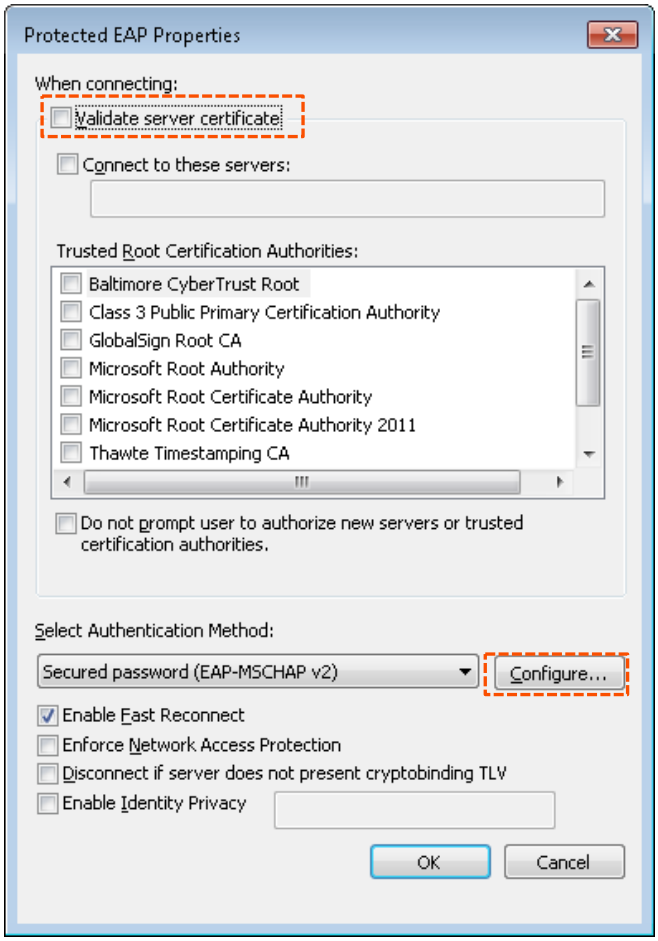
Step 5 Click **Change connection settings**.



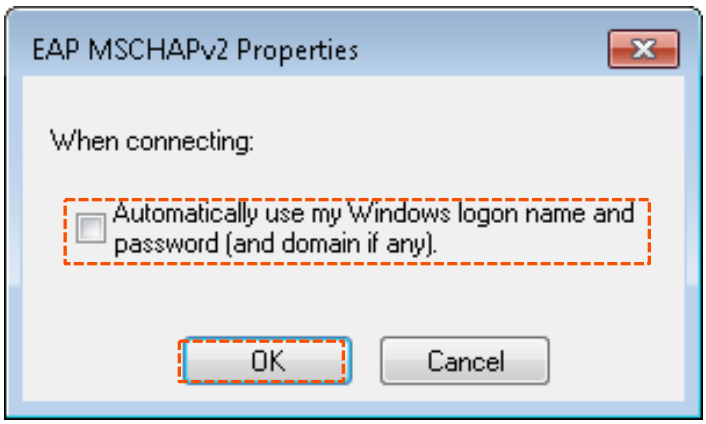
Step 6 Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



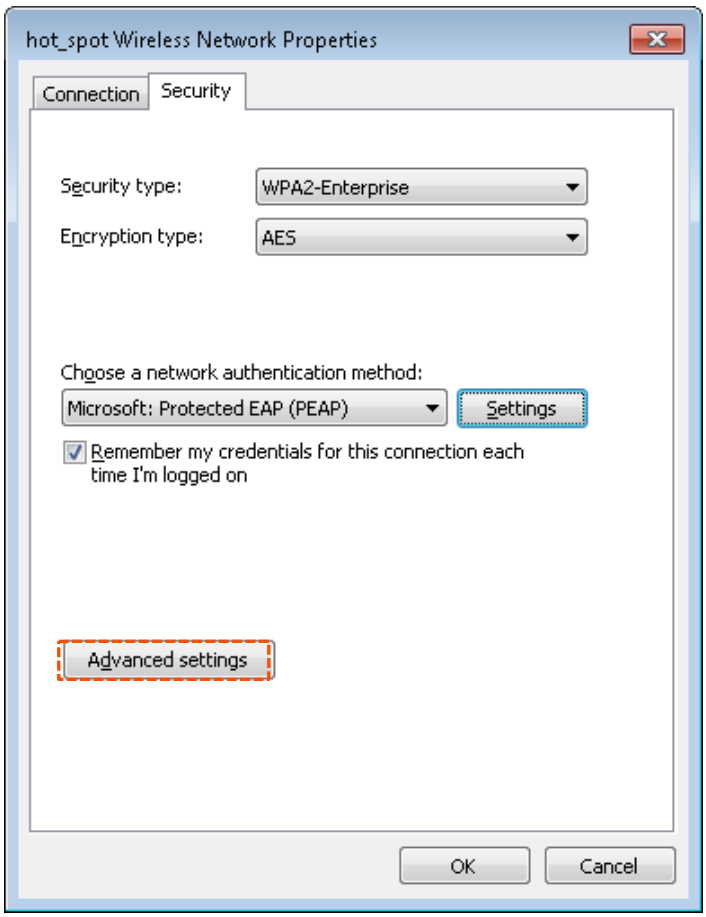
Step 7 Deselect **Validate server certificate** and click **Configure**.



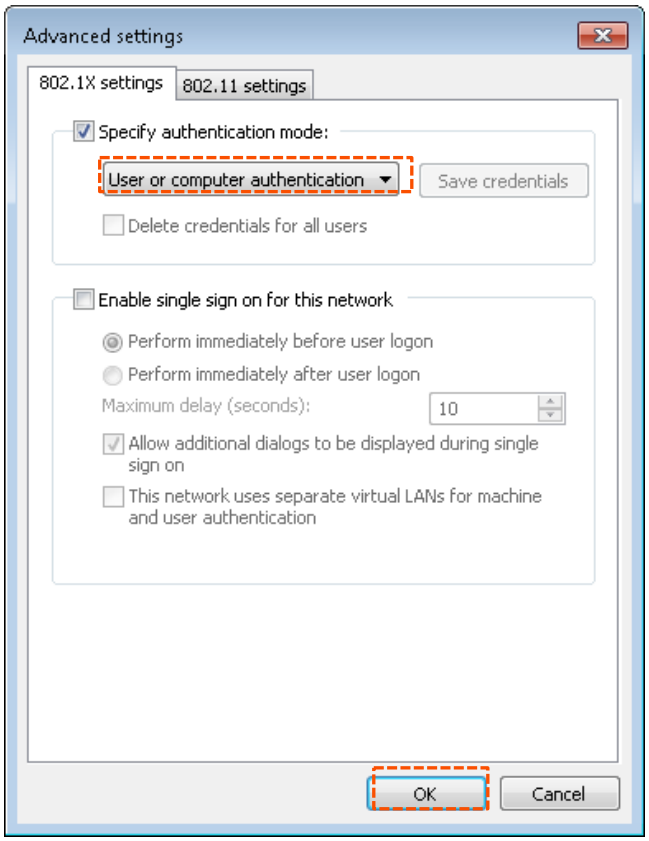
Step 8 Deselect A**utomatically use my Windows logon name and password (and domain if any)** and click **OK**.



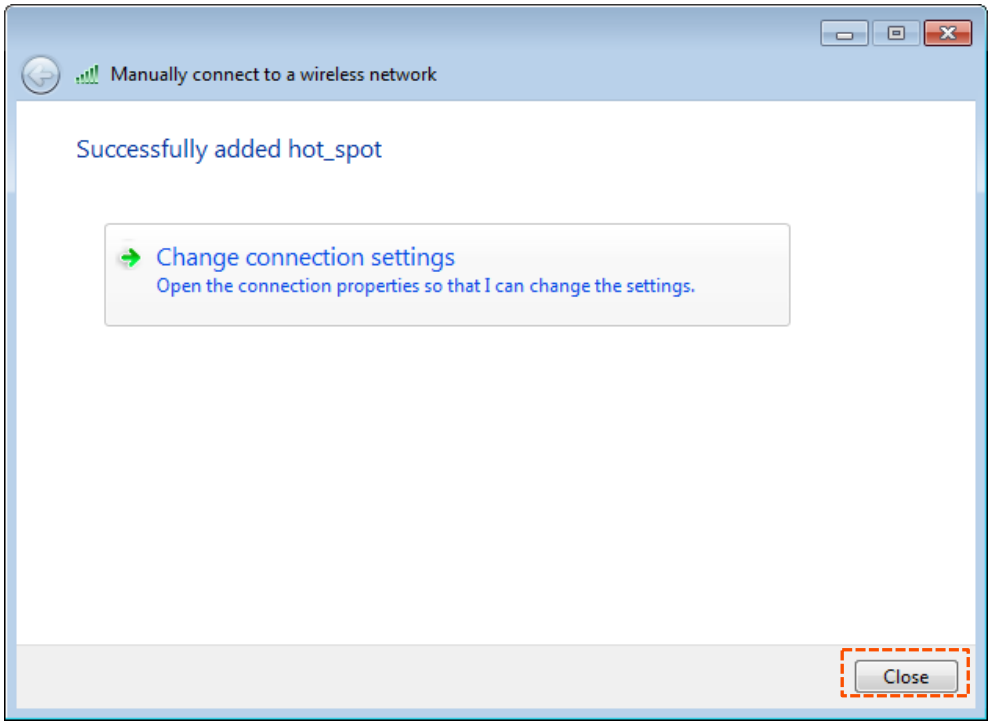
Step 9 Click **Advanced settings**.

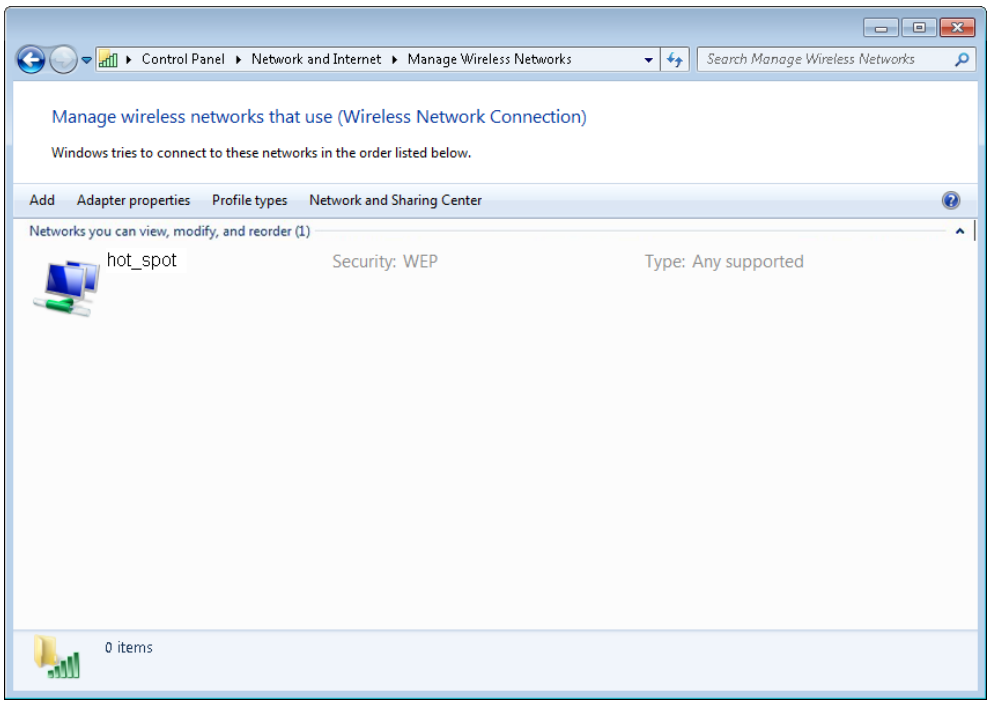


Step 10 Select **User or computer authentication** and click **OK**.

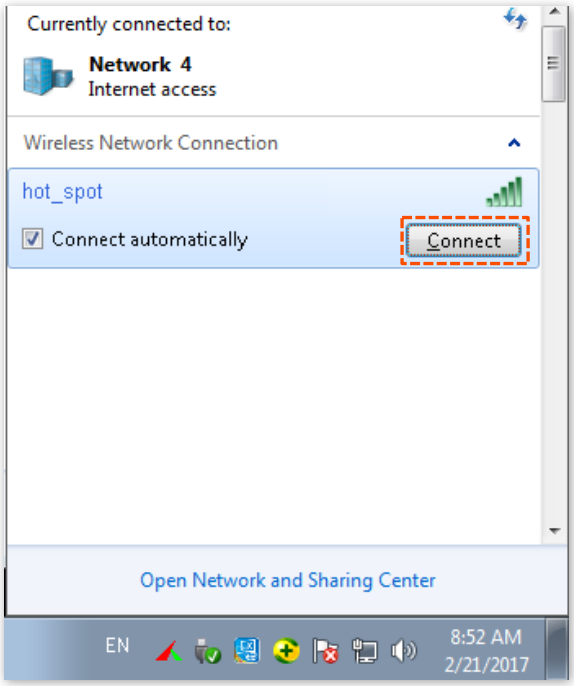


Step 11 Click **Close**.

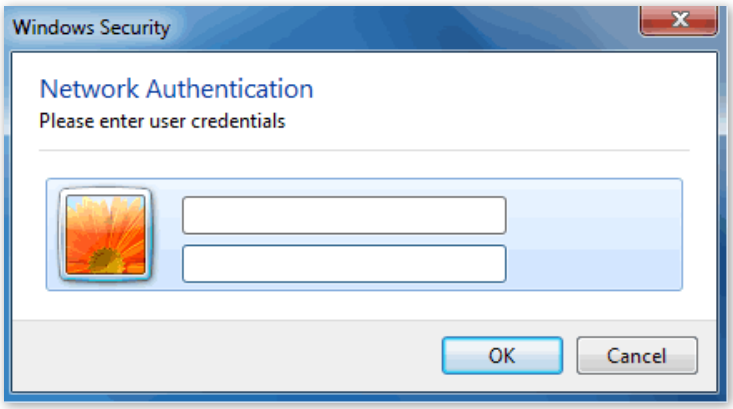




Step 12 Click the network icon in the lower-right corner of the desktop and choose the wireless network of the AP, such as **hot_spot** in this example.



Step 13 In the **Windows Security** dialog box that appears, enter the user name and password set on the RADIUS server and click **OK**.



---- End

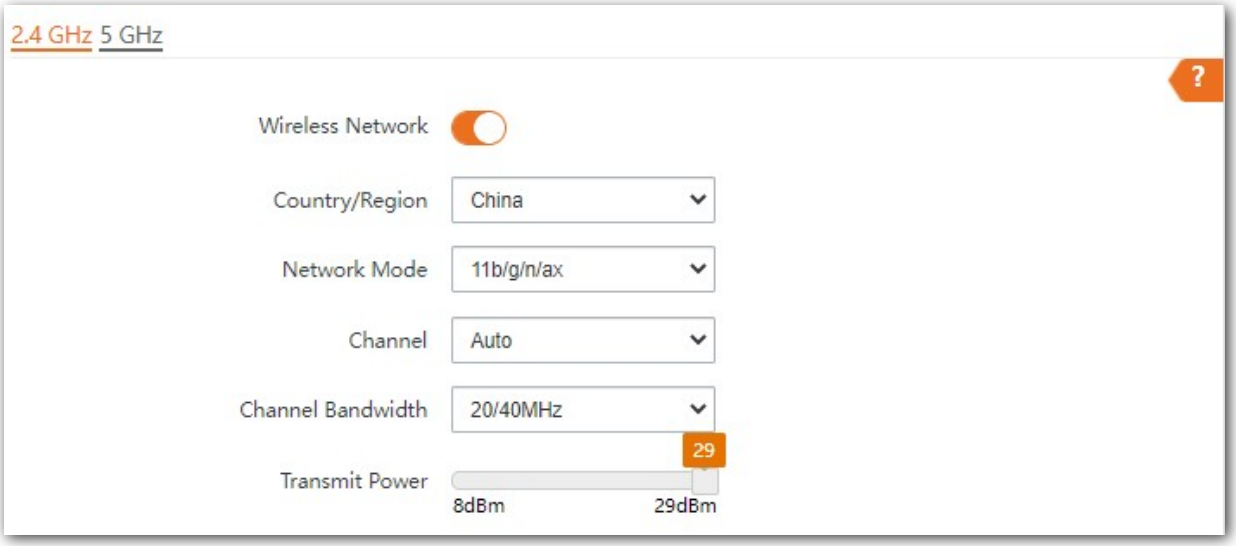
- **Verification**

Wireless devices can connect to the wireless network named **hot_spot**.

6.2 RF settings

The **RF Settings** page allows you to configure advanced settings about the AP.

To access the page, choose **Wireless** > **RF settings**.



Parameter description

Parameter	Description
Wireless Network	It specifies whether to enable the wireless function of the AP.
Country/Region	It specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region.
Network Mode	It specifies the wireless network mode of the AP. Available options for 2.4 GHz are **11b**, **11g**, **11b/g**, **11b/g/n, 11b/g/n/ax**. • 11b: The AP works in 802.11b mode and only wireless devices compliant with 802.11b can connect to the 2.4 GHz wireless networks of the AP. • 11g: The AP works in 802.11g mode and only wireless devices compliant with 802.11g can connect to the 2.4 GHz wireless networks of the AP. • 11b/g: The AP works in 802.11b/g mode and only wireless devices compliant with 802.11b or 802.11g can connect to the 2.4 GHz wireless networks of the AP. • 11b/g/n: The AP works in 802.11b/g/n mode. Wireless devices compliant with 802.11b or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n can connect to the 2.4 GHz wireless networks of the AP. • 11b/g/n/ax: The AP works in 11b/g/n/ax mode. Wireless devices compliant with 802.11b, or 802.11g and wireless devices working at 2.4 GHz and compliant with 802.11n or 802.11ax can connect to the 2.4 GHz wireless networks of the AP. Available options for 5 GHz are **11a, 11ac, 11a/n, and 11a/n/ac/ax.** • 11a: The AP works in 802.11a mode and only wireless devices compliant with 802.11a can connect to the 5 GHz wireless networks of the AP. • 11ac: The AP works in 802.11ac mode and only wireless devices compliant with 802.11ac can connect to the 5 GHz wireless networks of the AP. • 11a/n: The AP works in 802.11a/n mode and only wireless devices compliant with 802.11a or 802.11n can connect to the 5 GHz wireless networks of the AP. • 11a/n/ac/ax: The AP works in 11a/n/ac/ax mode. Wireless devices compliant with 802.11a, or 802.11ac and wireless devices working at 5 GHz and compliant with 802.11n or 802.11ax can connect to the 5 GHz wireless networks of the AP.
Channel	It specifies the operating channel of the AP. **Auto**: It indicates that the AP automatically adjusts its operating channel according to the ambient environment.

Parameter	Description
Channel Bandwidth	It specifies the wireless channel bandwidth of the AP. • 20 MHz: It indicates that the AP can use only 20 MHz channel bandwidth. • 40 MHz: It indicates that the AP can use only 40 MHz channel bandwidth. • 20/40 MHz: Only available for 2.4 GHz. It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment. • 80 MHz: Only available for 5 GHz. It indicates that the AP can use only 80 MHz channel bandwidth. • 160 MHz: Only available for 5 GHz. It indicates that the AP can use only 160 MHz channel bandwidth. • 20/40/80/160 MHz: Only available for 5 GHz. It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz, 40 MHz, 80 MHz, or 160 MHz according to the ambient environment.
Transmit Power	It specifies the transmit power of the AP. A higher value leads to wider WiFi coverage. However, decreasing the value properly increases performance and security of the wireless network.

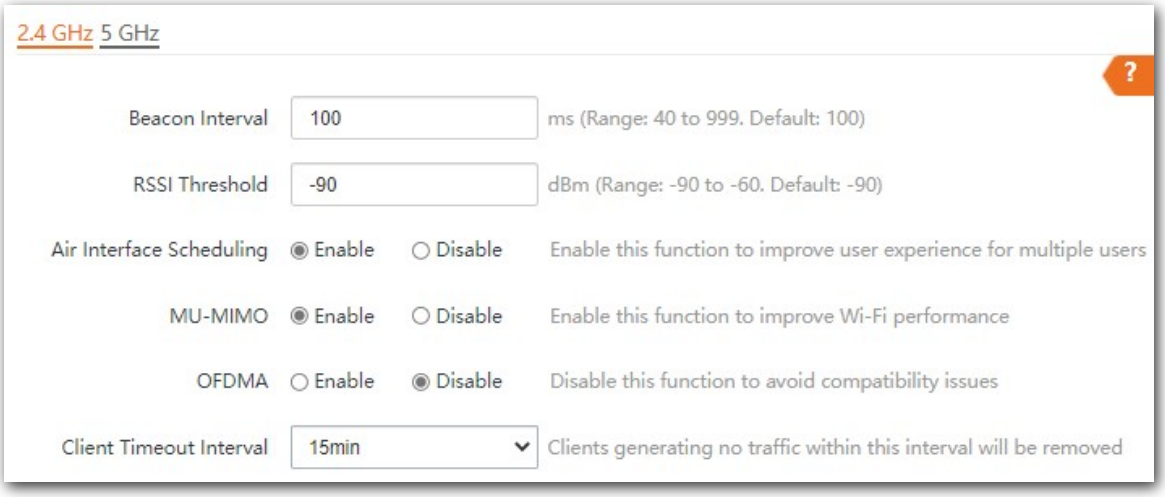
6.3 RF optimization

The **RF Optimization** page allows you to modify the radio parameters to optimize performance.

To access the page, choose **Wireless** > **RF Optimization**.

NOTE

You are recommended to retain the default settings if without the professional guidance to prevent degrading wireless performance of the AP.



Parameter description

Parameter	Description
Beacon Interval	It is used to set the interval at which this device sends Beacon frames. The Beacon frame is transmitted at the specified interval to announce the presence of a wireless network. Generally, a smaller interval enables wireless devices to connect to the AP more quickly, while a larger interval ensures higher data transmission speed for the AP.
RSSI Threshold	It specifies the minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless device is weaker than this threshold, the wireless device cannot connect to this device. A proper value facilitates wireless devices to connect to the AP with stronger signal in case of multiple APs exist.
Prioritize 5 GHz	If this function is enabled, dual band wireless devices prefer the 5 GHz WiFi network of the AP to connect when the 5 GHz signal strength transmitted by devices is stronger than the **Prioritize 5 GHz Threshold**.
Prioritize 5 GHz Threshold	With Prioritize 5 GHz function enabled, if the strength of the signals transmitted by a wireless device is stronger than this threshold, the wireless device connects to the 5 GHz WiFi network. Otherwise, it connects to the 2.4 GHz WiFi network.

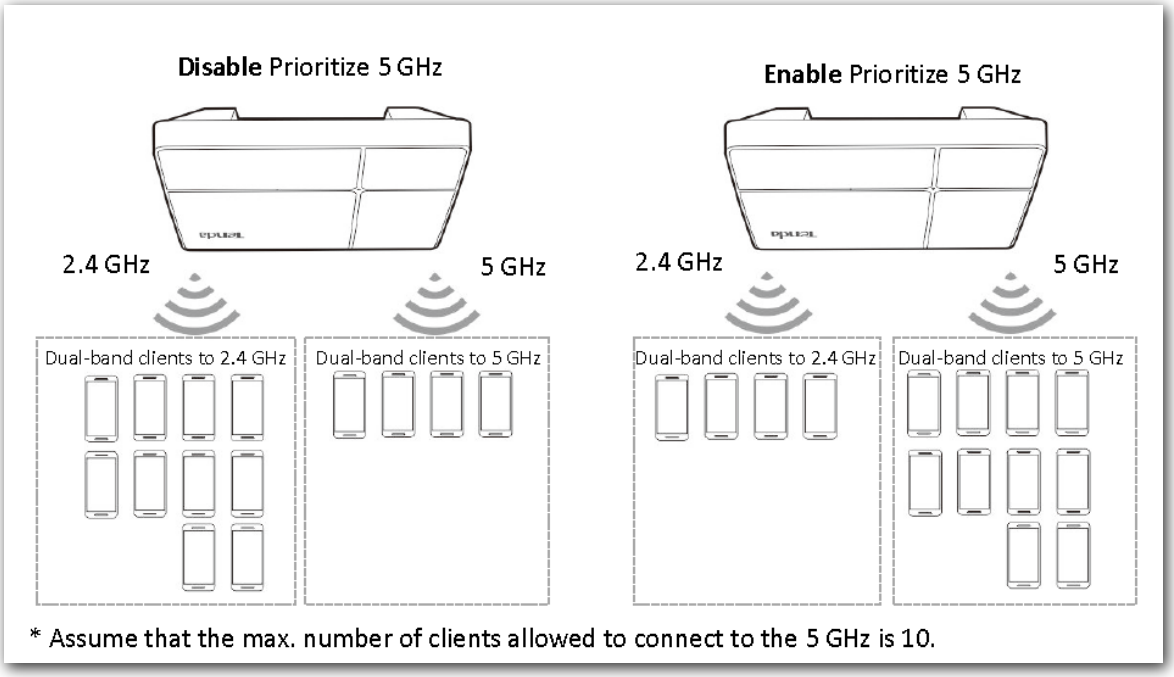
Parameter	Description
Air Interface Scheduling	It specifies whether to enable the air interface scheduling function of the AP. If this function is enabled, the same download time is assigned to users experiencing different download rates, ensuring a better experience for high-rate users.
MU-MIMO	Multi-User Multiple-Input Multiple-Output. If enabled, AP can communicate with multiple users concurrently, avoiding WiFi network congestion and improving communication.
OFDMA	Orthogonal Frequency Division Multiple Access. If this function is enabled, multiple clients can transmit data at the same time, so that the transmission efficiency is improved, delay is reduced, and user experience is enhanced.
Client Timeout Interval	It is used to set the wireless client disconnection interval of this device. The device disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.

- **Prioritize 5 GHz**

Although the 2.4 GHz band is more widely used than the 5 GHz band in actual wireless networks application, channels and signals on 2.4 GHz suffer more serious congestion and interference since there are only 3 non-overlapped communication channels on this band. The 5 GHz band could provide more non-overlapped communication channels. The quantity could reach more than 20 in some countries.

With the evolvement of the wireless networks, wireless clients that support both the 2.4 GHz and 5 GHz are more popular. However, by default, such dual-band wireless clients choose the 2.4 GHz to connect, resulting in even worse congestion of the 2.4 GHz band and the waste of the 5 GHz band.

The prioritize 5 GHz function enables such dual-band wireless clients to connect the 5 GHz band on network initialization if the 5 GHz signal strength the AP received reaches or exceeds the 5 GHz threshold so as to improve the utilization of the 5 GHz band, reduce the load and interference on the 2.4 GHz band, thus bettering user experience.



NOTE

The prioritize 5 GHz function takes effect only on the condition that the wireless both of the 2.4 GHz and 5 GHz are enabled, and the two bands share the same SSID, security mode and password.

- **Air Interface Scheduling**

In mixed wireless rates environment, the traditional FIFO (First-in First-out) allocates more air interface time to clients with low transmission capacity and low spectrum efficiency, reducing the system throughput of each AP then the system utilization.

The air interface scheduling function evenly allocates downlink transmission time to clients so that clients with high transmission rate could transmit more data, improving the throughput of each AP and number of clients allowed to be connected.

6.4 WMM

6.4.1 Overview

802.11 networks offer wireless access services based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) channel competition mechanism, which allows all wireless clients to fairly compete for channels. All the services implemented over wireless networks share the same channel competition parameters. Nevertheless, different services usually have different requirements for bandwidth, delay, and jitter. This requires wireless networks to offer accessibility based on the services implemented over the networks.

WMM is a wireless QoS protocol used to ensure that packets with high priorities are transmitted first. This ensures better experience of voice and video service over WiFi networks.

WMM involves the following terms:

- Enhanced Distributed Channel Access (EDCA): It is a channel competition mechanism to ensure that packets with higher priorities are assigned more bandwidth and transmitted earlier.
- Access Category (AC): The WMM mechanism divides WLAN traffic by priority in descending order into the voice stream (AC-VO), video stream (AC-VI), best effort (AC-BE), and background (AC-BK) access categories. The access categories use queues with different priorities to send packets. The WMM mechanism ensures that packets in queues with higher priorities have more opportunities to access channels.

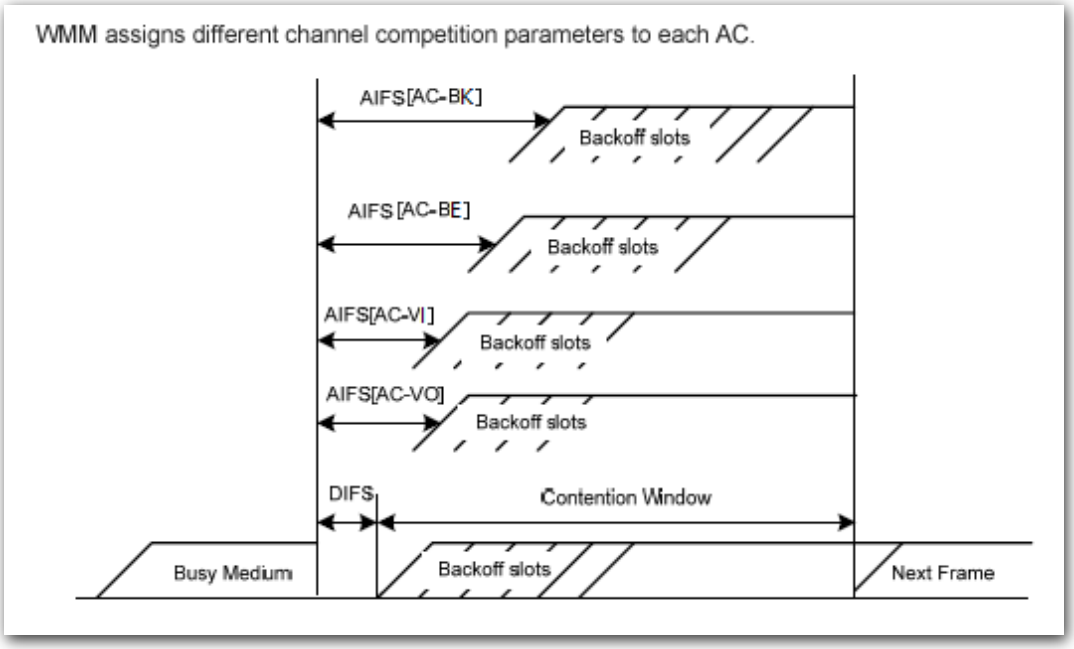
According to the 802.11 protocol family, all devices listen on a channel before using the channel to send data. If the channel stays idle for or longer than a specified period, the devices wait a random backoff period within the contention window. The device whose backoff period expires first can use the channel. The 802.11 protocol family applies the same backoff period and contention window to all devices across a network to ensure that the devices have the same channel contention opportunity.

- **EDCA Parameters**

WMM changes the contention mechanism of 802.11 networks by dividing packets into four ACs, among which the ACs with higher priorities have more opportunities to access channels. The ACs help achieve different service levels.

WMM assigns each AC a set of EDCA parameters for channel contention, including:

- Arbitration Inter Frame Spacing Number (AIFSN): Different from the fixed distributed inter-frame spacing (DIFS) specified in the 802.11 protocol family, AIFSN varies across ACs. A greater AIFSN indicates a longer backoff period. See AIFS in the following figure.
- Contention window minimum (CWmin) and contention window maximum (CWmax) specify the average backoff period. The period increases along with these two values. See the backoff slots in the following figure.
- Transmission Opportunity (TXOP): It specifies the maximum channel use duration after successful channel contention. The duration increases along with this value. The value **0** indicates that a device can send only one packet through a channel after winning contention for the channel.



ACK Policies

WMM specifies the Normal ACK and No ACK policies.

- According to the No ACK policy, no ACK packet is used during wireless packet transmission to acknowledge packet reception. This policy is applicable to scenarios where interference is mild and can effectively improve transmission efficiency. In case of strong interference, lost packets are not sent again if this policy is adopted. This leads a higher packet loss rate and reduces the overall performance.
- According to the Normal ACK policy, each time a receiver receives a packet, it sends back an ACK packet to acknowledge packet reception.

6.4.2 Configuring WMM settings

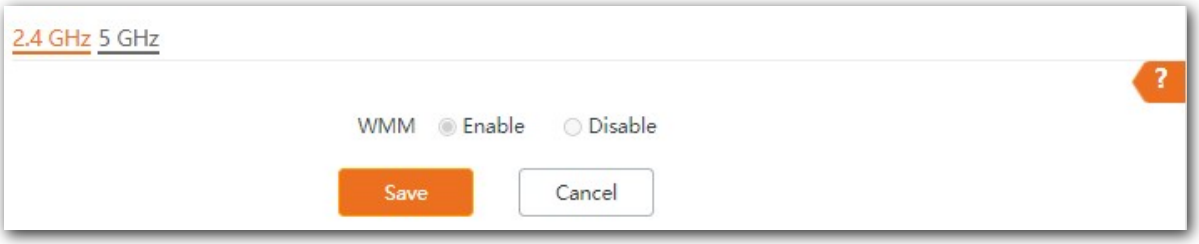
TIP

The WMM function of the corresponding radio band cannot be set to **Disable** in the following cases:

- The network mode of the AP at 2.4 GHz is **11b/g/n** or **11b/g/n/ax**
- The network mode of the AP at 5 GHz is **11a/n**, **11ac** or 1**1a/n/ac/ax**.

The **WMM** page allows you to enable or disable the WMM function of the corresponding radio band of the AP. This function is enabled by default.

To access the page, choose **Wireless** > **WMM**.



6.5 Access control

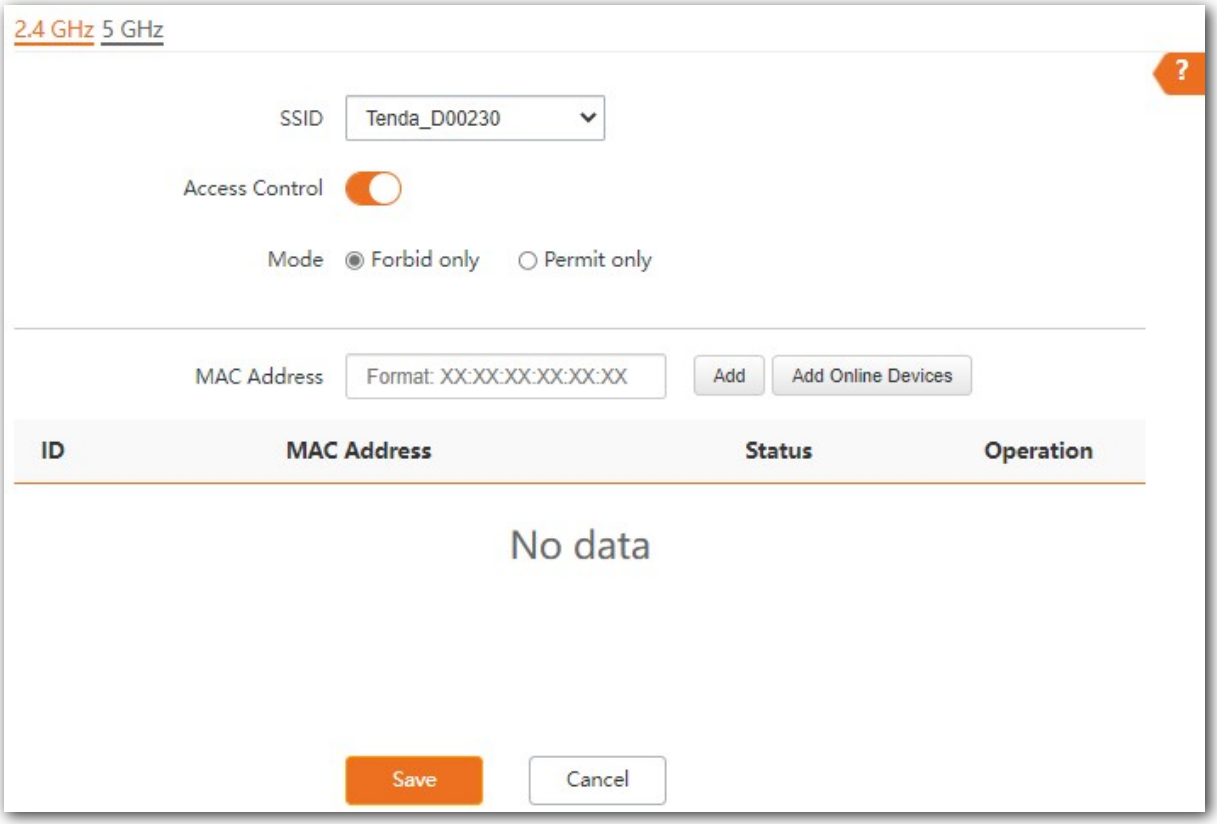
6.5.1 Overview

The access control function enables you to allow or disallow the wireless devices to access the wireless network of the AP based on their MAC addresses.

The AP supports the following 2 filter modes:

- **Forbid only**: It indicates that only the wireless devices with the specified MAC addresses cannot access the wireless networks of the AP.
- **Permit only**: It indicates that only the wireless devices with the specified MAC addresses can access the wireless networks of the AP.

Access Control is disabled by default. The following figure displays the page when Access Control is enabled.



Parameter description

Parameter	Description
SSID	It specifies the wireless network to which the rule applies.
Access Control	It specifies whether to enable this function.
Mode	Set access control mode. • **Forbid only**: It indicates that only the wireless clients on the wireless access control list cannot connect to the AP with the selected SSID. • **Permit only**: It indicates that only the wireless clients on the wireless access control list can connect to the AP with the selected SSID.
MAC Address	It specifies the MAC address of client.
Add	Manually add the device with the MAC address you specified to the access control list.
Add Online Devices	Add the online wireless clients to the access control list conveniently.
Status	It specifies the status of the rule. You can enable or disable it as required.
Operation	Click to delete the rule.

6.5.2 Configuring access control

Step 1 Choose **Wireless** > **Access Control**. Choose a wireless network radio band on which access control is to be configured.

Step 2 Select the SSID to which the access control is applied from the **SSID** drop-down list menu.

Step 3 Enable **Access Control**.

Step 4 Set **Mode** to **Forbid only** or **Permit only**.

Step 5 Enter the MAC address of the wireless device to which the rule applies. Then click **Add**.

TIP

If the wireless device to be controlled has connected to the AP, click **Add Online Devices** to quickly add the MAC address of the device to the access control client list.

Step 6 Click **Save**.

---- End

6.5.3 Example of configuring access control

Networking requirement

A wireless network whose SSID is **VIP** under the 5 GHz radio band has been set up in a company. Only a few members are allowed to connect to the wireless network.

The Access Control function of the AP is recommended. The members have three wireless devices whose MAC addresses are **D8:38:0D:00:00:01**, **D8:38:0D:00:00:02**, and **D8:38:0D:00:00:03**.

Configuration procedure

Step 1 Choose **Wireless** > **Access Control** > **5 GHz**.

Step 2 Select **VIP** from the **SSID** drop-down list.

Step 3 Enable **Access Control** function.

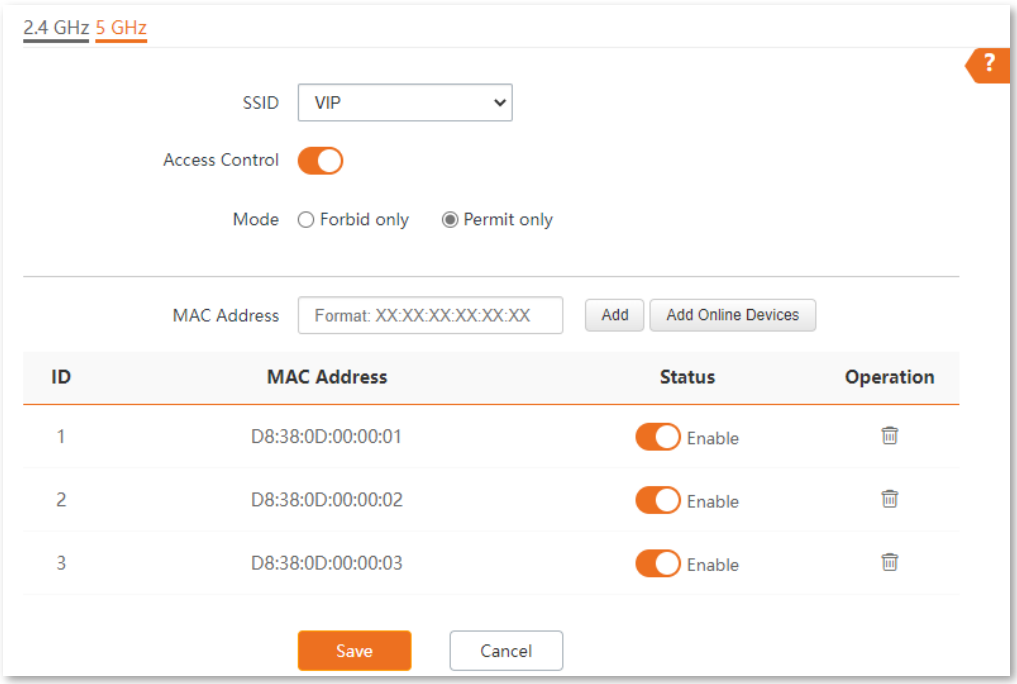
Step 4 Set **Mode** to **Permit only**.

Step 5 Enter **D8:38:0D:00:00:01** in the **MAC Address** text box and click **Add**. Repeat this step to add **D8:38:0D:00:00:02** and **D8:38:0D:00:00:03** as well.

Step 6 Click **Save**.

---End

The following figure shows the configuration.



Verification

Only the specified wireless devices can connect to the **VIP** wireless network.

6.6 QVLAN settings

6.6.1 Overview

The AP supports 802.1Q VLANs and is applicable in a network environment where 802.1Q VLANs have been defined. By default, the QVLAN function is disabled.

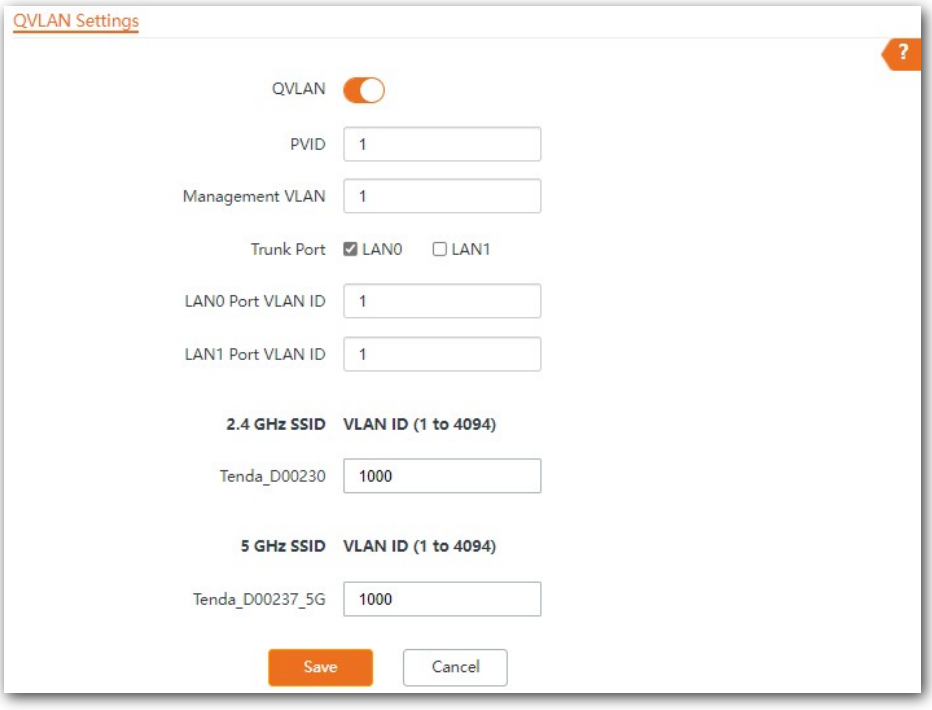
If the QVLAN function is enabled, tagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the VID in the data, whereas untagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the PVID of the port that receives the data.

The following table describes how ports of different link types process transmitted and received data.

Port	Method to process received data		Method to process transmitted data
	Tagged data	Untagged data	
Access	Forward the data to other ports of the VLAN corresponding to the VID in the data.	Forward the data to the other ports of the VLAN corresponding to the PVID of the port that receives the data.	Transmit data after removing tags from the data.
Trunk			Transmit data without removing tags from the data.

The **QVLAN Settings** page allows you to set VLAN IDs of all wireless networks.

To access the page, choose **Wireless** > **QVLAN Settings**.



Parameter description

Parameter	Description
QVLAN	It specifies whether to enable the QVLAN function of the AP.
PVID	It specifies the ID of the default native VLAN of the trunk port of the AP.
Management VLAN	It specifies the ID of the AP management VLAN. After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
Trunk Port	Choose the port which to be set as the trunk mode. By default, LAN0 is chosen. Trunk port allows data of all VLANs to pass. NOTE When you enable the 802.1Q VLAN function, choose at least one LAN port as the trunk port. If the AP has only one Ethernet port, this port serves as the trunk port by default.
LAN0 Port VLAN ID LAN1 Port VLAN ID	It specifies the Ethernet port of the AP and the ID of the VLAN to which a LAN port belongs. • LAN0: The PoE power and data transmission multi-functional port of the AP. • LAN1: The data transmission port of the AP. TIP Ethernet port not set as the trunk port is seen as the access port and you can set its VLAN ID.
2.4 GHz SSID 5 GHz SSID	It specifies the currently enabled SSID(s) over the 2.4 GHz/5 GHz band of the AP, and the VLAN IDs corresponding to SSIDs. TIP
VLAN ID	After the QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID of an access port is the same as its VLAN ID.

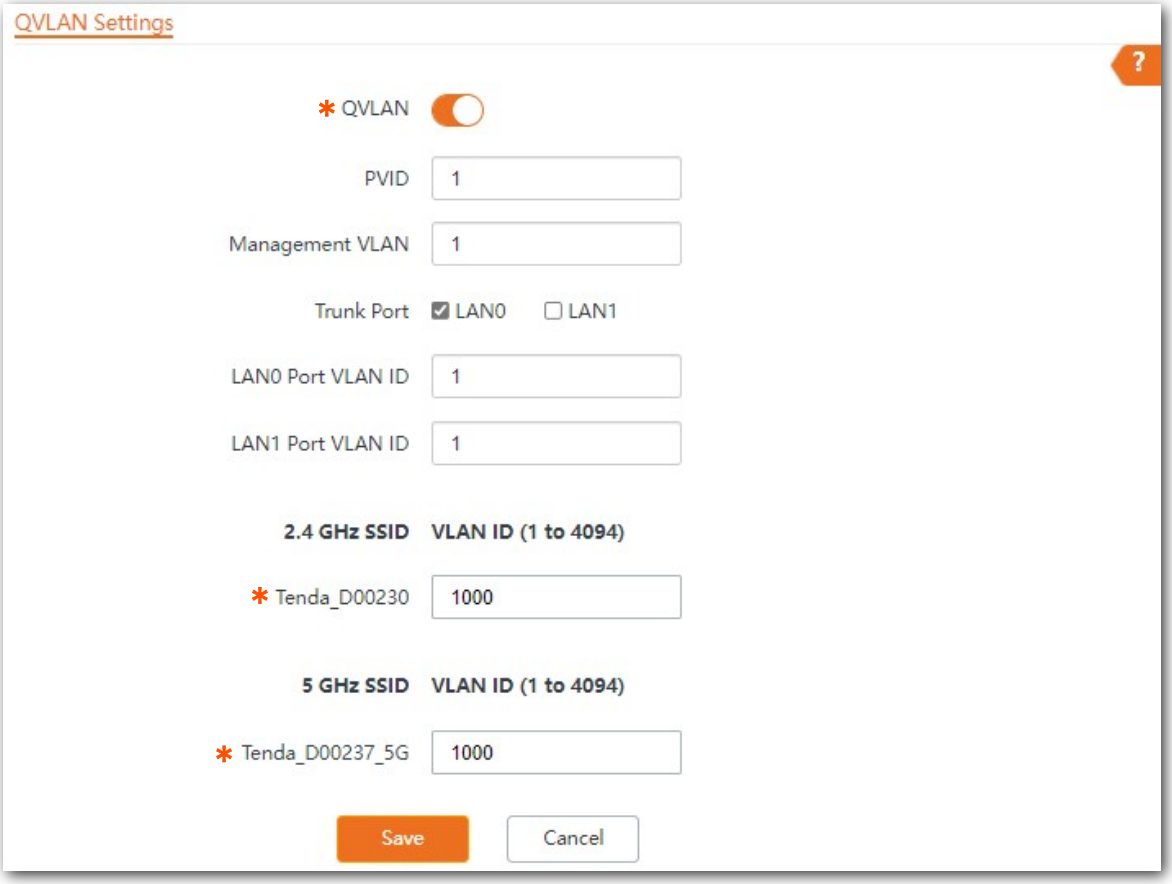
6.6.2 Configure the QVLAN function

Step 1 Choose **Wireless** > **QVLAN Settings**.

Step 2 Enable **QVLAN** function.

Step 3 Change the parameters as required. Generally, you only need to change the **2.4 GHz SSID VLAN ID** and **5 GHz SSID VLAN ID** settings.

Step 4 Click **Save**.



---End

6.6.3 Example of configuring QVLAN

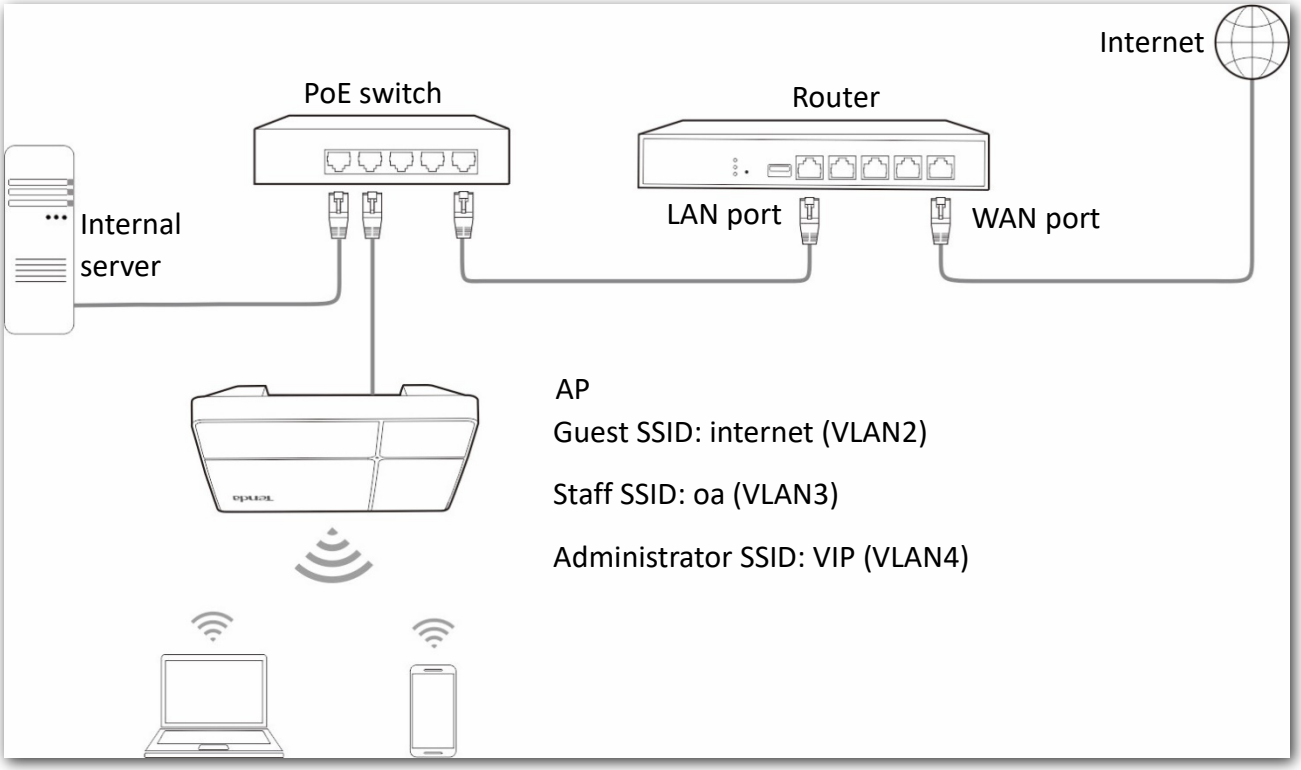
Networking requirement

A hotel has the following WiFi network coverage requirements:

- Guests are allowed to connect to VLAN2 and only able to access the internet.
- Hotel staffs are allowed to connect to VLAN3 and only able to access the intranet.
- Hotel administrators are allowed to connect to VLAN4, able to access both the intranet and the internet.

Network plan

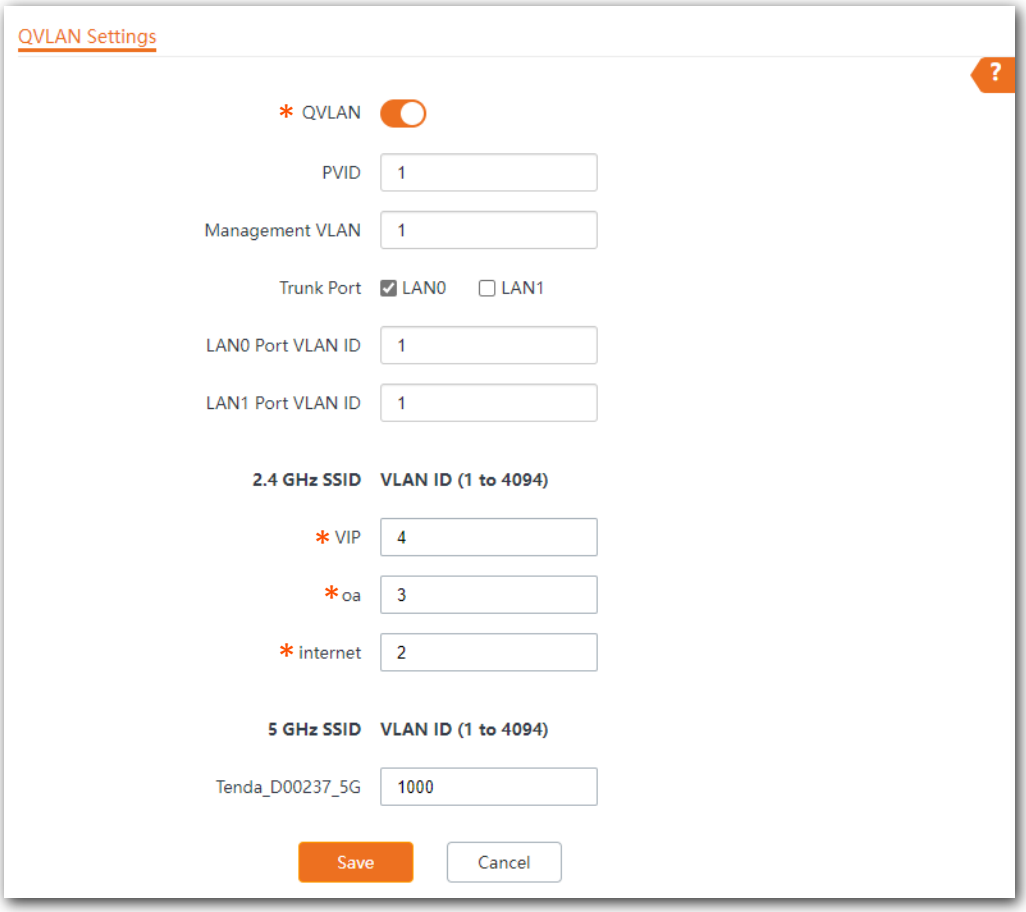
- Set the SSID to **internet** for guests, **oa** for staffs, and **VIP** for managers for 2.4 GHz network.
- Configure VLANs for the three SSIDs on AP.
- Configure VLAN forwarding rules on switch.
- Configure VLAN forwarding rules on router and internal server..



Configuration procedure

Step 1 Configure the AP.

1. Choose **Wireless** > **QVLAN Settings**.
2. Enable **QVLAN**.
3. Modify the VLAN ID of the SSIDs at 2.4 GHz band. Set the VLAN ID of internet to **2**, oa to **3**, and VIP to **4** respectively.
4. Click **Save**.



5. Click **OK** after confirming the prompted message.

Wait for the automatic reboot of the AP.

Step 2 Configure the switch.

Create IEEE 802.1q VLANs described in the following table on the switch.

Port Connected To	Accessible VLAN ID	Port Type	PVID
AP	1, 2, 3, 4	Trunk	1
Internal server	3, 4	Trunk	1
Router	2, 4	Trunk	1

Retain the default settings of other ports. For details, refer to the user guide for the switch.

Step 3 Configure the router and the internal server.

To ensure a normal internet access for wireless clients connected to the AP, the router and internal server must support the QVLAN function and need to be configured. See the following table.

Router:

Port Connected To	Accessible VLAN ID	Port Type	PVID
Switch	2, 4	Trunk	1

Internal server:

Port Connected To	Accessible VLAN ID	Port Type	PVID
Switch	3, 4	Trunk	1

For configuration details, refer to the user guides of your router and internal server.

---- End

Verification

Wireless devices connected to the SSID **internet** can access only the internet. Wireless devices connected to the SSID **oa** can access only the intranet. Wireless devices connected to the SSID **VIP** can access both the internet and the intranet.

7 Tools

7.1 Date & time

This section allows you to set the system time and login timeout interval of your AP.

7.1.1 System time

The **System Time** page allows you to set the system time.

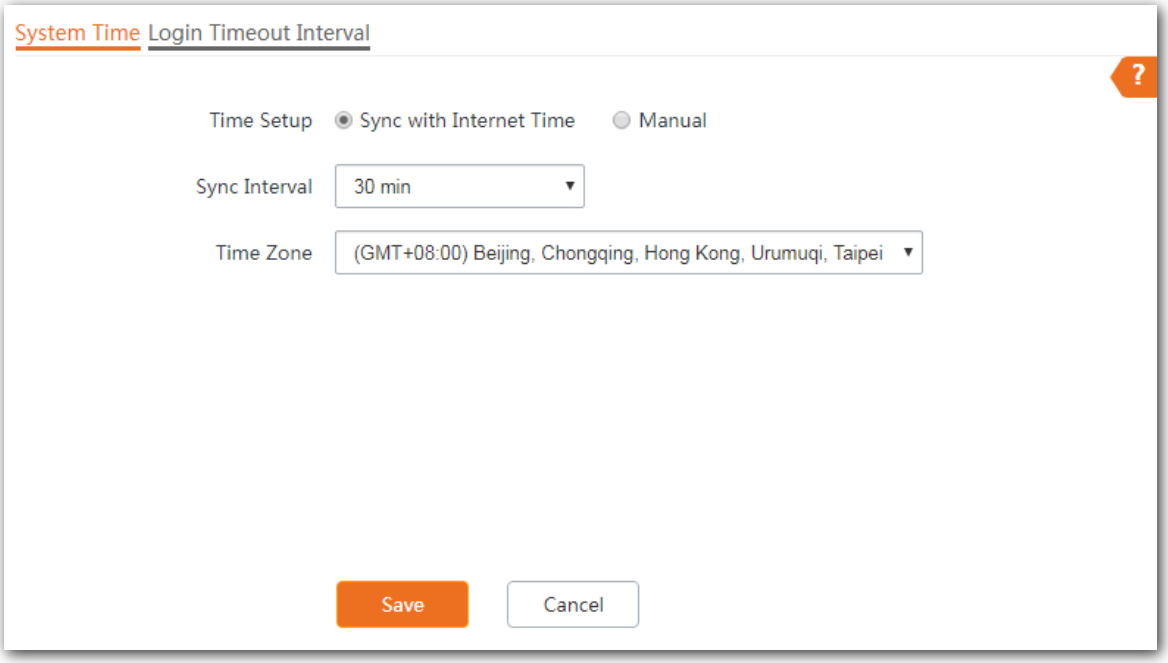
To access the page, choose **Tools** > **Date & Time** > **System Time**.

Ensure that the system time of the AP is correct, so that time-based functions can take effect properly. The AP supports **Sync with Internet Time** and **Manual** to correct the system time.

Sync with Internet Time

The AP automatically synchronizes its system time with a time server of the internet. This enables the AP to automatically correct its system time after being connected to the internet. The AP can also self-calibrate after restarting without setting again.

For details about how to connect the AP to the internet, refer to LAN Setup.



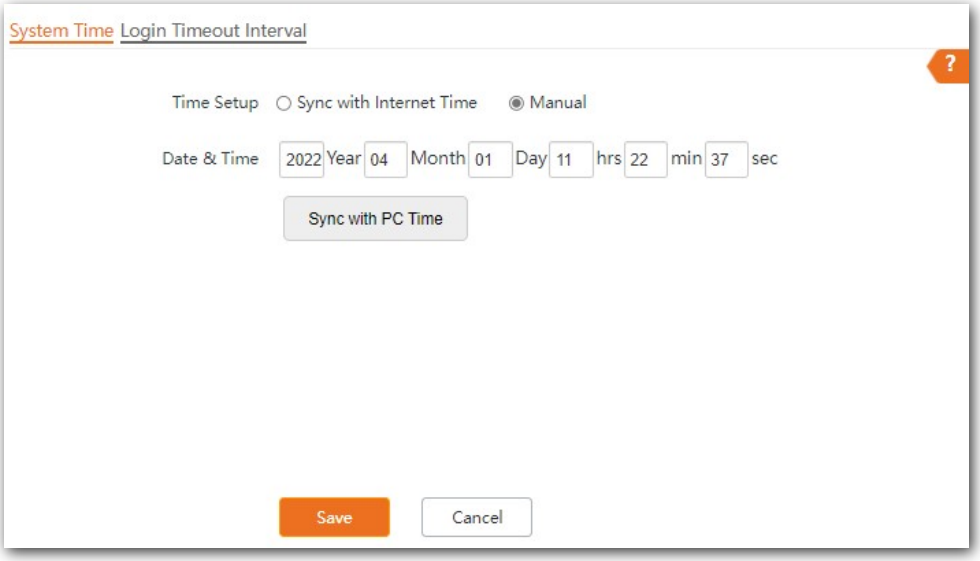
Parameter description

Parameter	Description
Time Setup	It specifies the modes to set the system time.
Time Zone	It specifies the standard time zone of the region in which the AP locates.

Manual

You can manually set the system time of the AP. If you choose this option, you need to set the system time each time after the AP reboots.

Enter a correct date and time, or click **Sync with PC Time** to synchronize the system time of the AP with the system time (ensure that it is correct) of the management computer.

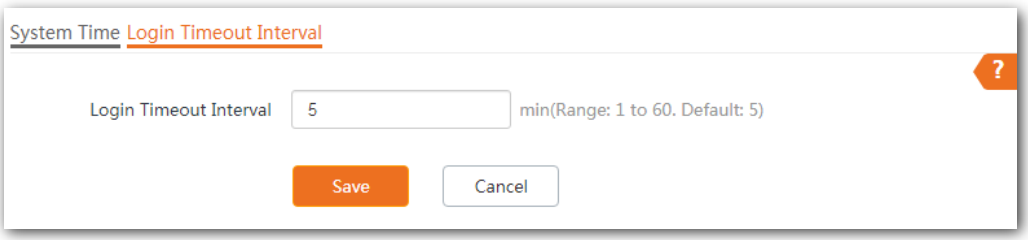


7.1.2 Login timeout interval

If you log in to the web UI of the AP and perform no operation within the login timeout interval, the AP logs you out automatically for network security.

The Login Timeout Interval page allows you to modify the login timeout interval. The default login timeout interval is **5** minutes.

To access the page, choose **Tools** > **Date & Time** > **Login Timeout Interval**.



7.2 Maintenance

The Maintenance page allows you to reboot and reset AP, upgrade firmware, back up or restore settings, and control LED indicator.

7.2.1 Reboot

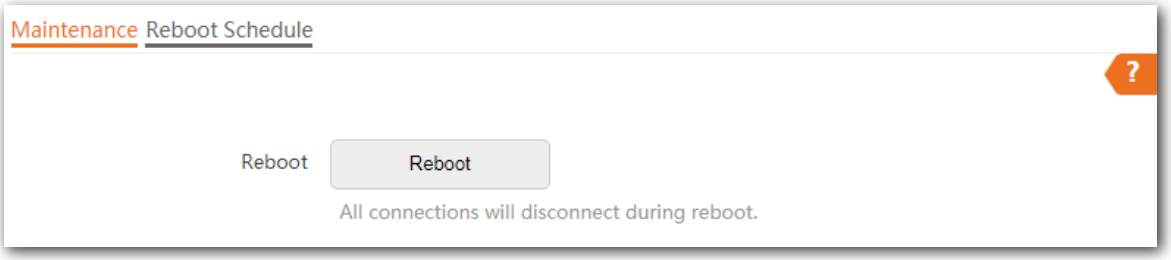
TIP

Rebooting the AP disconnects all connections. You are recommended to reboot the AP in spare time.

Manual reboot

If a parameter does not take effect or the AP does not work properly, you can try rebooting the AP manually to resolve the problem.

Method: on the **Tools** > **Maintenance** > **Maintenance** page, click **Reboot**.



Reboot schedule

This function allows the AP to automatically reboot as scheduled. You can use this function to prevent wireless performance degradation or network instability that occurs after a long AP uptime. The AP supports the following two types of scheduled reboot:

- Reboot Interval: The AP reboots at the interval you set.
- Reboot Schedule: The AP reboots regularly at the time you set.

■ **Configuring the AP to Reboot Interval**

TIP

Rebooting at intervals is based on the system time. To avoid reboot time error, ensure that the system time is correct.

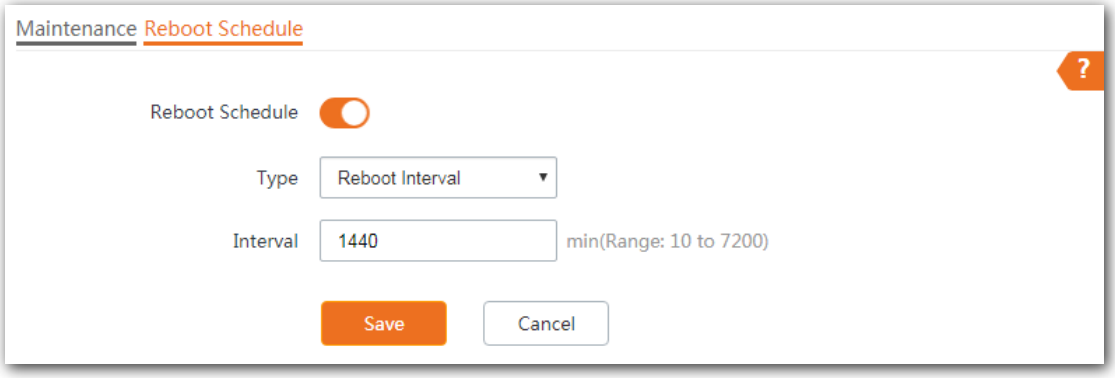
Step 1 Click **Tools** > **Maintenance** > **Reboot Schedule**.

Step 2 Enable **Reboot Schedule**.

Step 3 Set **Type** to **Reboot Interval**.

Step 4 Set **Interval** as required, which is **1440** minutes in this example.

Step 5 Click **Save**.



---- End

After the configurations, the AP will automatically reboot in a day.

- **Configuring the AP to Reboot Schedule**

Step 1 Click **Tools** > **Maintenance** > **Reboot Schedule**.

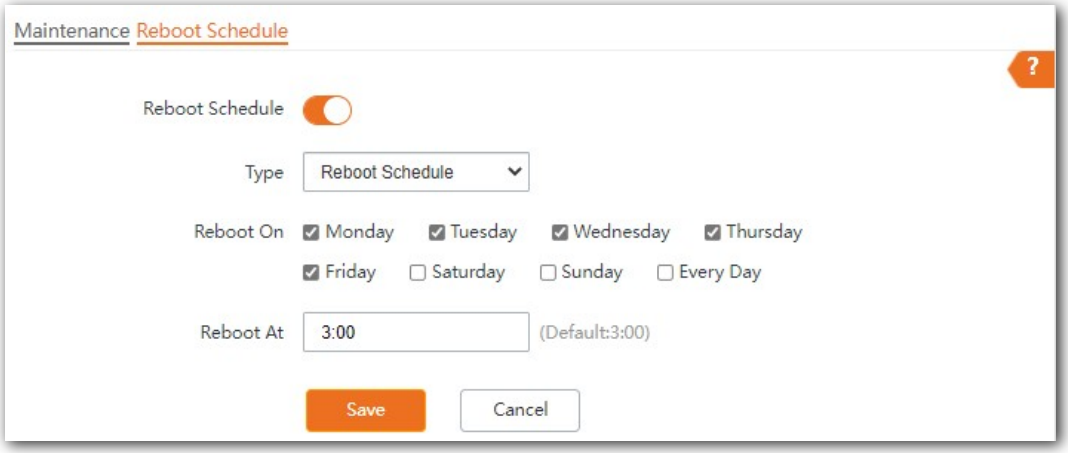
Step 2 Enable **Reboot Schedule**.

Step 3 Set **Type** to **Reboot Schedule**.

Step 4 Select the day or days when the AP reboots, such as **Monday** to **Friday**.

Step 5 Set the time when the AP reboots, such as **3:00**.

Step 6 Click **Save**.



---- End

After the configurations, the AP will automatically reboot at 3 a.m. every Monday to Friday.

7.2.2 Reset

If you cannot locate a fault of the AP or forget the password of the web UI of the AP, you can reset the AP to restore its factory settings and then configure it again.

NOTE

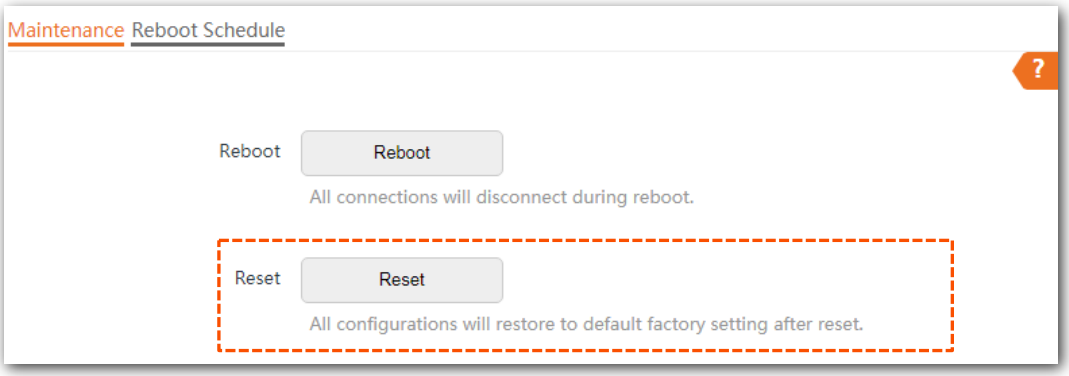
- When the factory settings are restored, your configuration is lost. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.
- After the factory settings are restored, the login IP address of the AP is changed to **192.168.0.254**, and the user name and password of the AP are changed to **admin**.

Method 1:

After AP completes startup, hold down the reset button (**RESET** or **Reset**) for about 8 seconds.

Method 2:

Log in to the web UI of the AP, on the **Tools** > **Maintenance** > **Maintenance** page, click **Reset**.



7.2.3 Upgrade firmware

This function enables you to upgrade the AP's firmware to get more functions and higher stability.

NOTE

To ensure a correct upgrade and avoid damage:

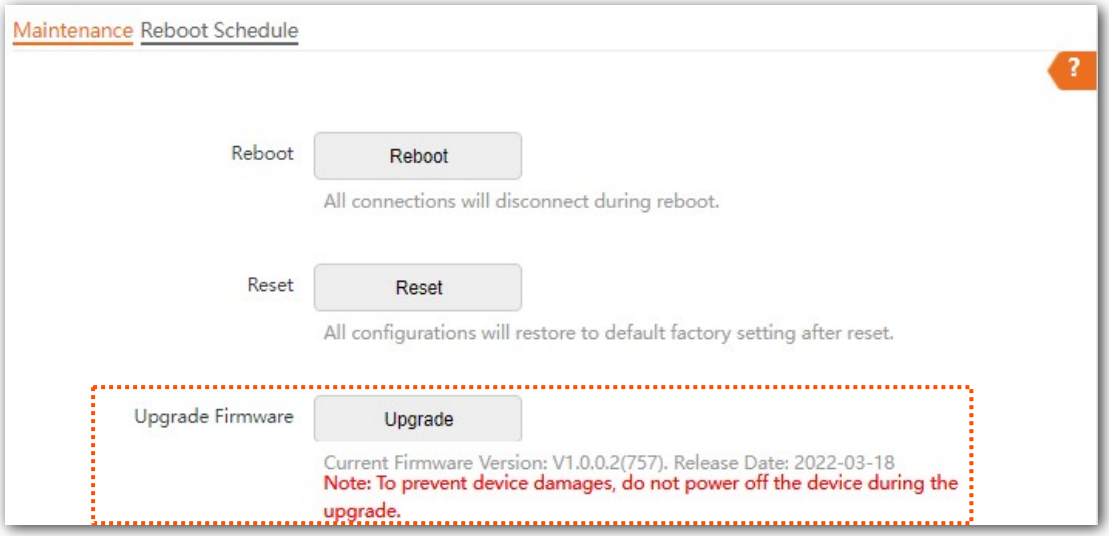
- Make sure the new firmware is applicable to the AP.
- Keep a proper power supply to the AP during the upgrade.

Configuration procedure:

Step 1 Download the latest firmware version for the AP from www.tendacn.com to your local computer and decompress the package. Generally, the package is in the format of .bin.

Step 2 Log in to the web UI of the AP and choose **Tools** > **Maintenance** > **Maintenance**.

Step 3 Click **Upgrade**.



Step 4 Choose and upload the upgrade file in the popped window.

---- End

Wait until the progress bar completes. Then log in to the web UI of the AP again. Click **Status** > **System Status** and check whether the upgrade is successful according to the **Firmware Version** parameter.

TIP

After the firmware is upgraded, you are recommended to restore the factory settings of the AP and configure the AP again, so as to ensure stability of the AP and proper operation of new functions.

7.2.4 Backup/restore

The backup function allows you to back up the current configuration of the AP to a local computer. The restore function allows you to restore the AP to a previous configuration.

If the AP enters the optimum condition after you greatly change the configuration of the AP, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the AP.

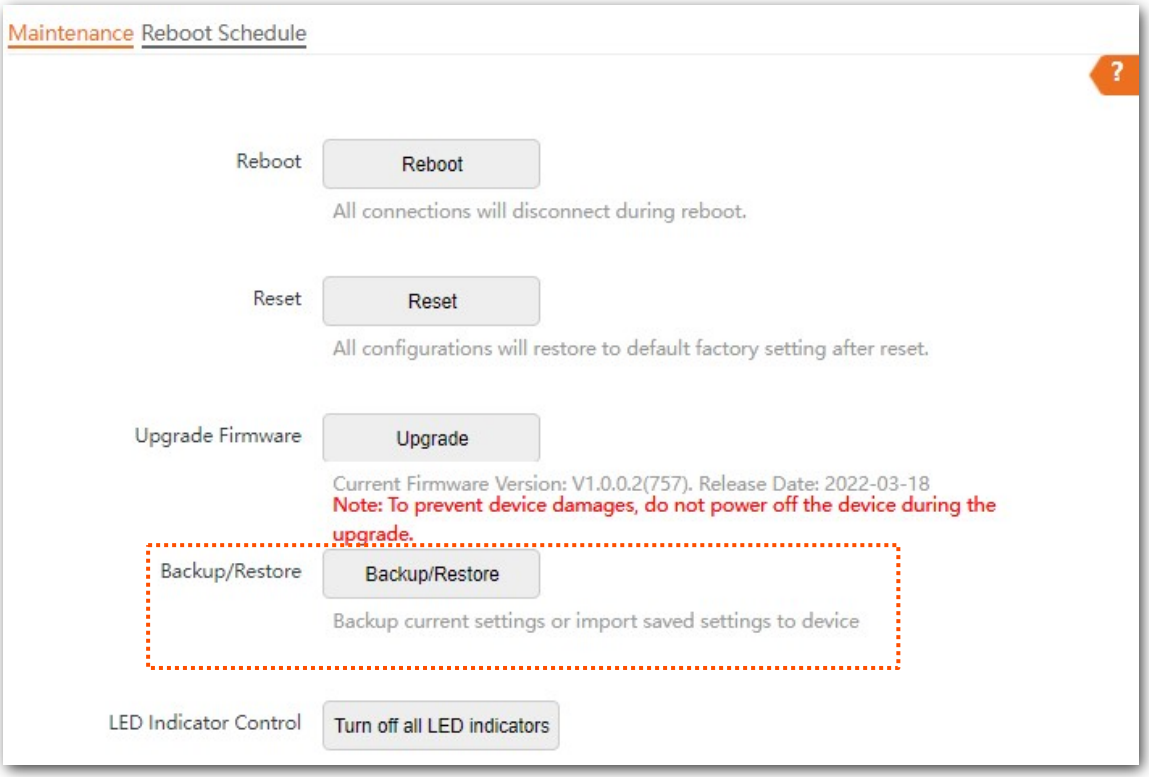
TIP

If you need to apply same or similar configurations to many APs, you can configure one of the APs, back up the configuration of the AP, and use the backup to restore the configuration on the other APs. This improves configuration efficiency.

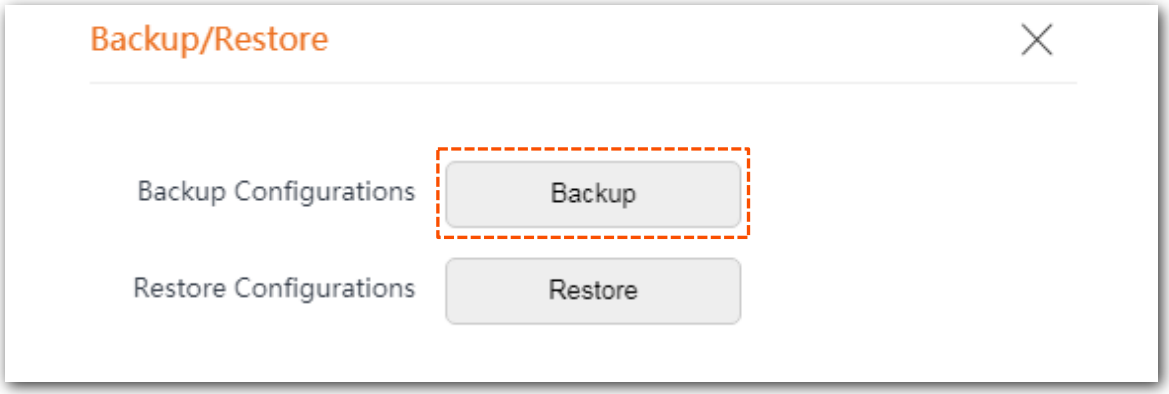
Backup the current configuration

Step 1 Choose **Tools** > **Maintenance** > **Maintenance**.

Step 2 Click **Backup/Restore**.



Step 3 Click **Backup**.



---- End

A configuration file named **APCfm.cfg** will be downloaded.

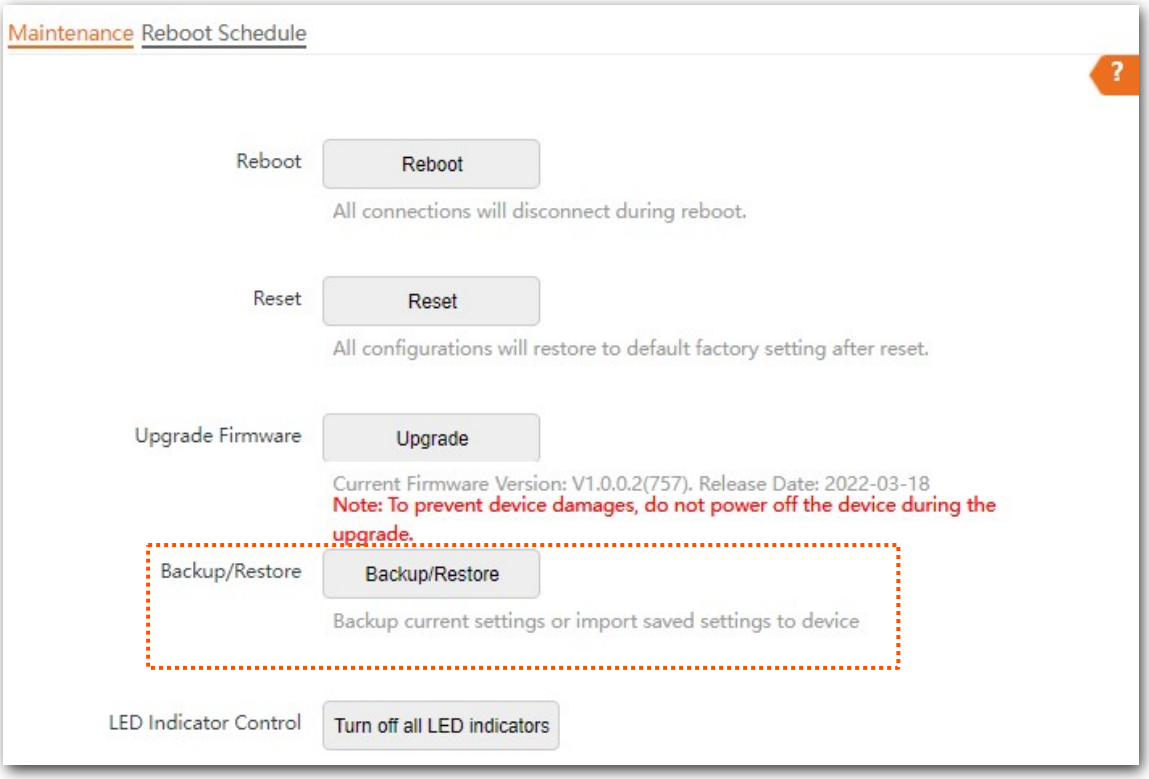
TIP

If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click “Keep”.

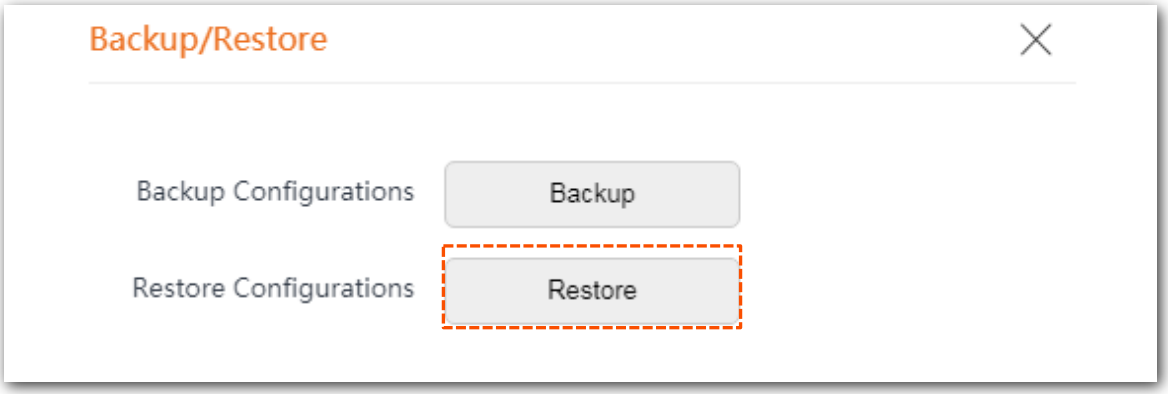
Restoring a configuration

Step 1 Click **Tools** > **Maintenance** > **Maintenance**.

Step 2 Click **Backup/Restore**.



Step 3 Click **Restore**.



Step 4 Choose the configuration file you backed up.

---- End

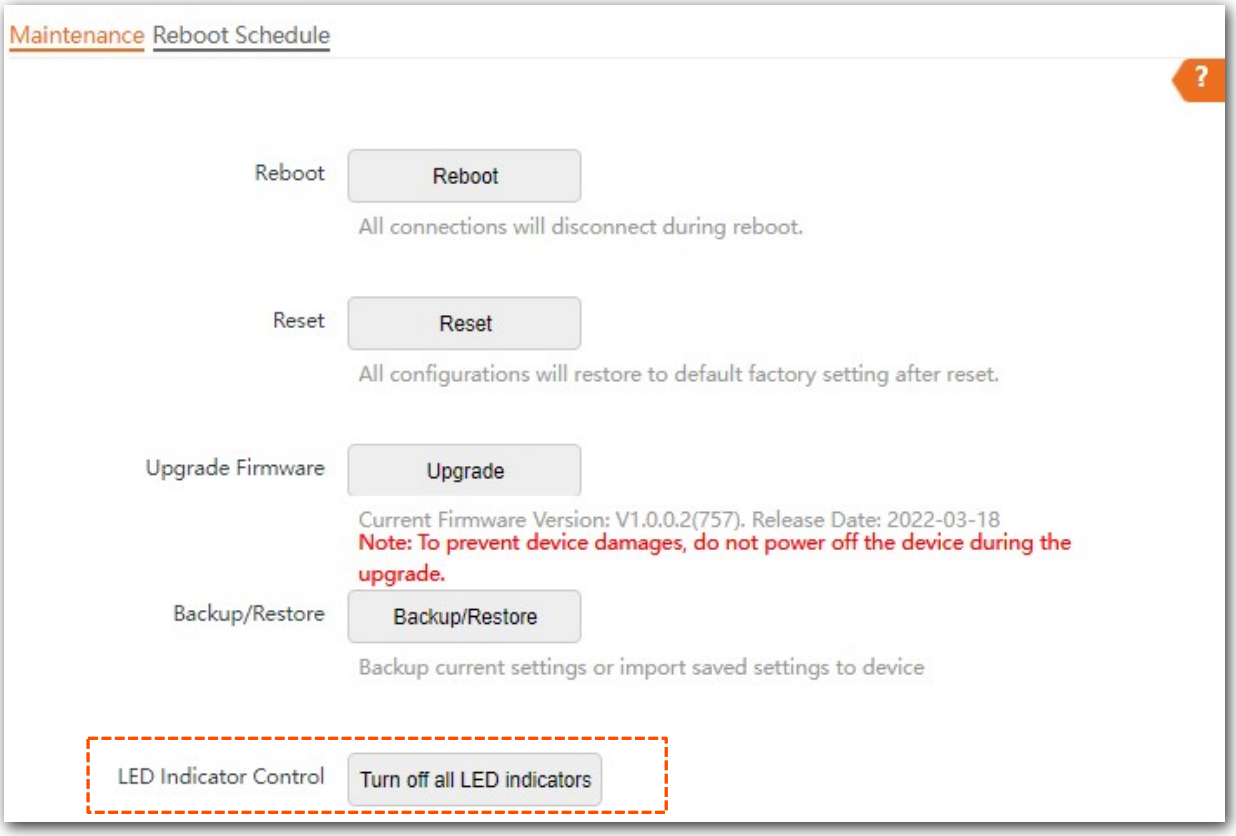
The AP restores the configurations successfully when the progress bar is done.

7.2.5 LED indicator control

This function enables you to turn on/off the LED indicator of the AP. By default, the LED indicator is turned on.

Turn off the LED indicator

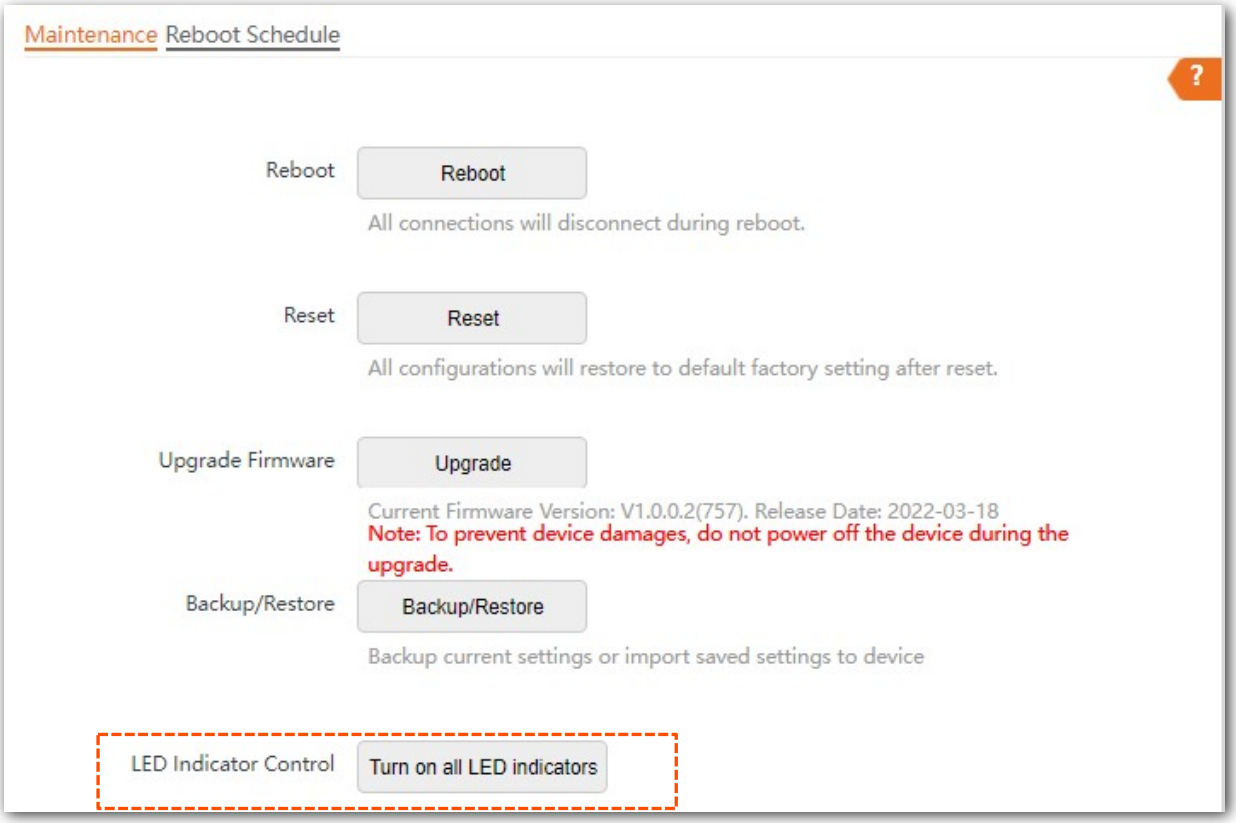
On the **Tools** > **Maintenance** > **Maintenance** page, click **Turn off all LED indicators**.



After the configurations, the LED indicator is turned off and no longer displays the working status of the AP.

Turn on the LED indicator

On the **Tools** > **Maintenance** > **Maintenance** page, click **Turn on all LED indicators**.



After the configurations, the LED indicator lights up again and you can judge the working status of the AP.

7.3 Account

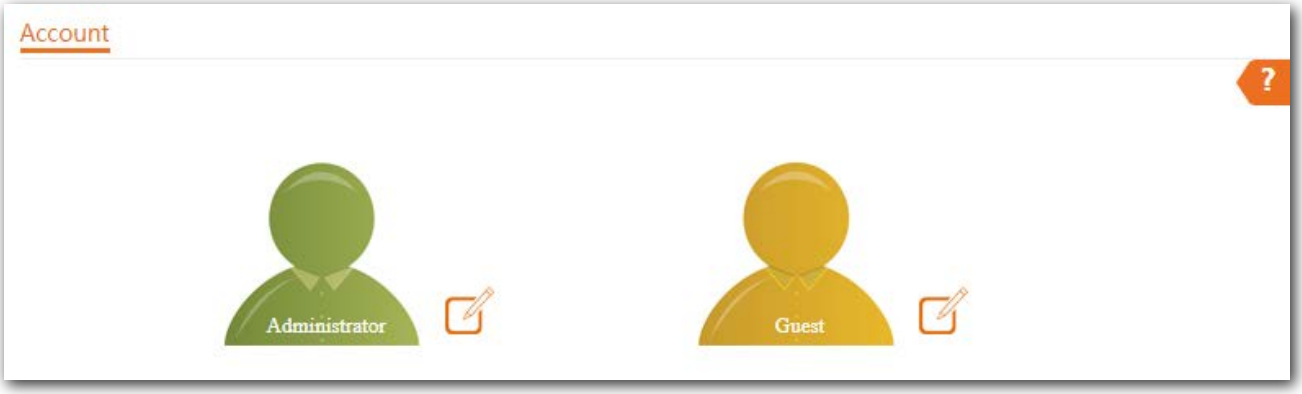
7.3.1 Overview

The Account page allows you to modify the information of the login account to keep unauthorized users from entering the web UI and modifying configurations, thus protecting the wireless network.

To access the configuration page, choose **Tools** > **Account**.

AP supports two account types: **Administrator** and **Guest**.

- **Administrator**: This account type has permission to view and modify the settings. The default username and password for this account are **admin**/**admin** (both are case-sensitive).
- **Guest**: This account type can only view other than modifying the settings. The default username and password for this account are **user**/**user** (both are case-sensitive). This account type is disabled by default.



7.3.2 Modifying the password and user name of login account

Step 1 Click **Tools** > **Account**.

Step 2 Click beside the account to be modified.

Step 3 If the account to be modified is a Guest, enable the **Guest Account** first. Otherwise, go to the next step.

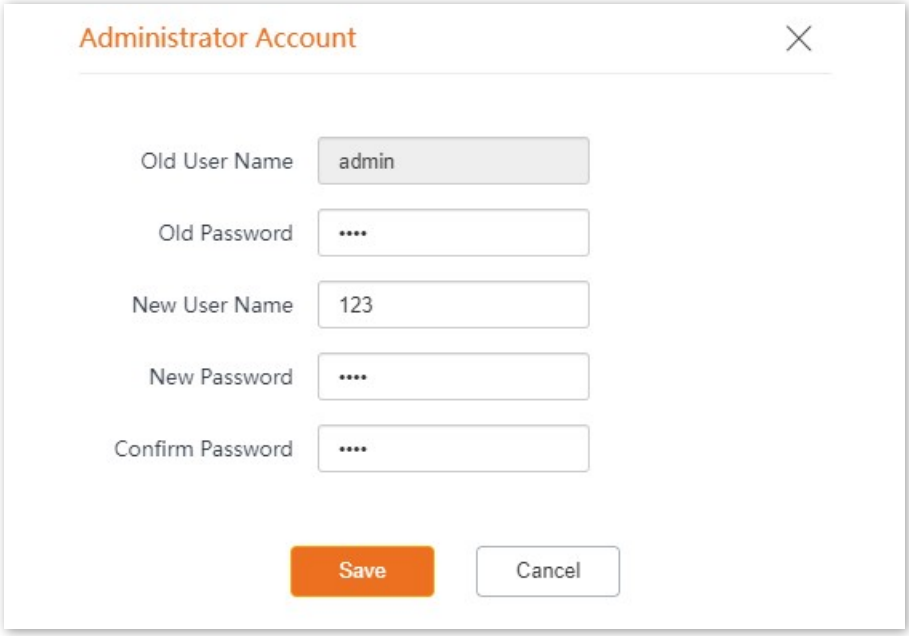
Step 4 Enter the current password in **Old Password**.

Step 5 Enter the new account name, for example, **123**, in **New User Name**.

Step 6 Enter the new password in **New Password**.

Step 7 Enter again the new password in **Confirm Password**.

Step 8 Click **Save**.



---- End

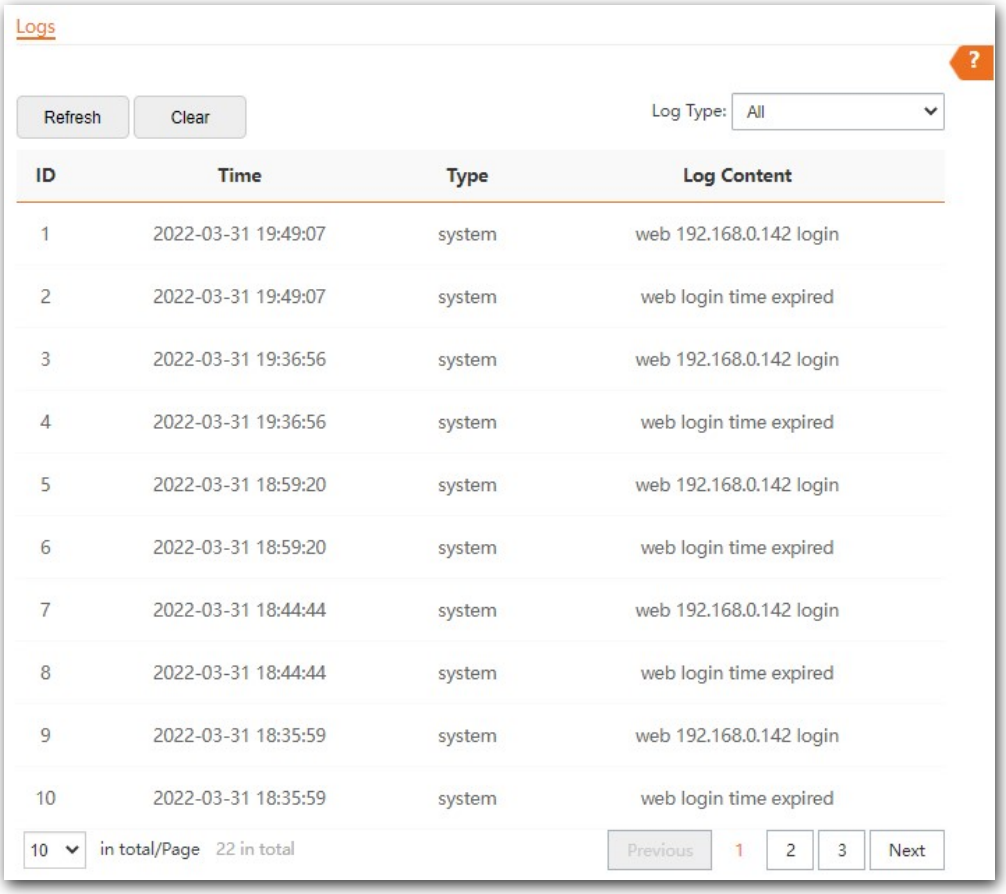
Then you will be redirected to the login page. Enter the new password and click **Login** to log in to the AP.

7.4 System Log

The logs of the AP record various events that occur and the operations that users perform after the AP starts. In case of a system fault, you can refer to the logs during troubleshooting.

The **Logs** page allows you to view system logs.

To access the page, choose **Tools** > **System Log** > **Logs**.



To ensure that the logs are recorded correctly, verify that the system time of the AP is correct. You can correct the system time of the AP by choosing **Tools** > **Date & Time** > **System Time**.

By default, AP saves the latest 500 logs. The older logs will be automatically deleted if more than 500 logs are generated. To view the latest logs of the AP, click **Refresh**. To clear the existing logs of the AP, click **Clear**.

NOTE

- When the AP reboots, the previous logs are lost.
- The AP reboots when the AP is powered on after a power failure, the QVLAN function is configured, the firmware is upgraded, an AP configuration is restored, or the factory settings are restored.

7.5 Diagnostic tool

With the diagnostic tool, you can detect the connection status and connection quality of a network.

Assume that you need to check the connection quality between the AP and its upstream router (IP address: **192.168.1.1**).

Procedure:

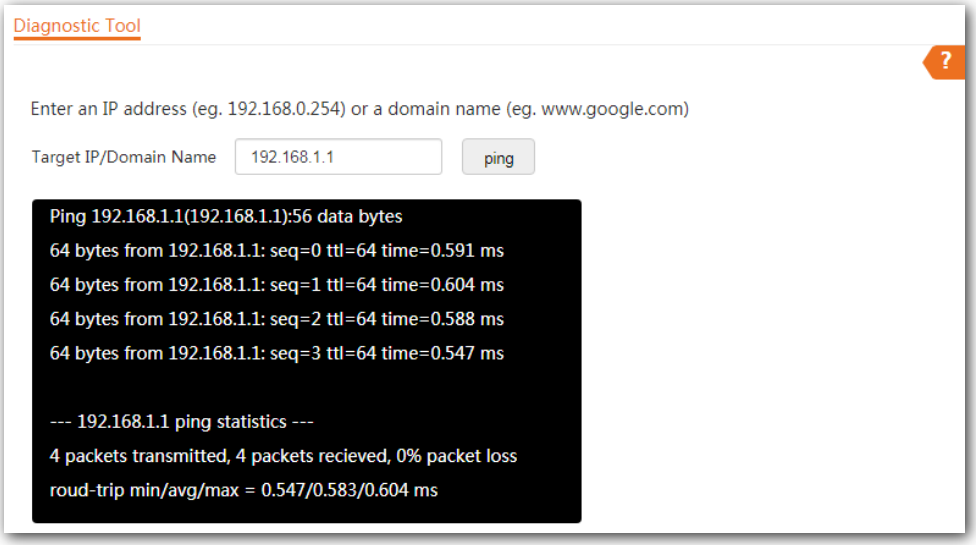
Step 1 Choose **Tools** > **Diagnostic Tool** to enter the configuration page.

Step 2 Enter the IP address of its upstream router in the **Target IP/Domain Name** box, which is **192.168.1.1** in this example.

Step 3 Click **ping**.

---- End

Wait a moment. The Ping result is displayed in the black square. See the following figure:



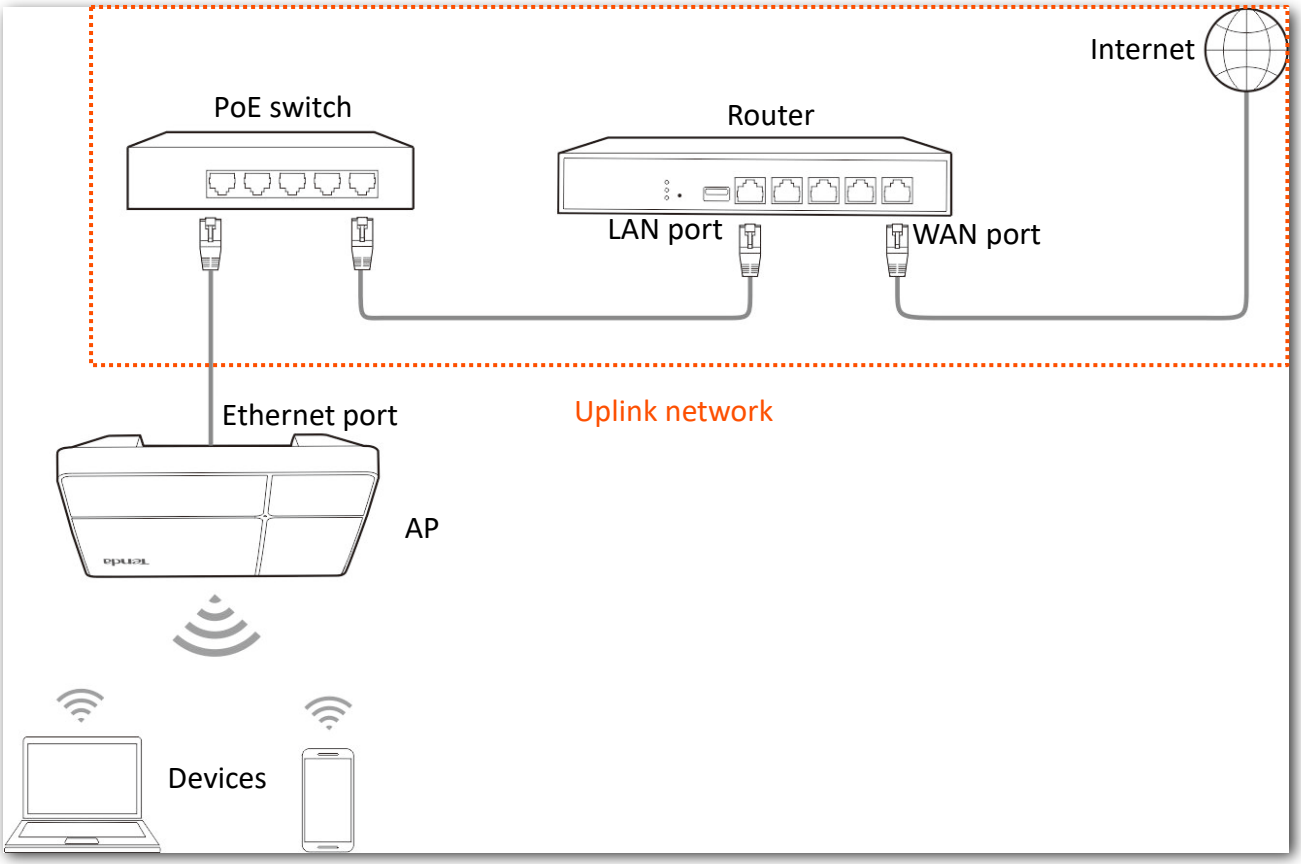
7.6 Uplink check

7.6.1 Overview

In AP mode, the AP connects to its upstream network using the Ethernet port (LAN port). If a critical node between the LAN port and the upstream network fails, the AP as well as the wireless devices connected to the AP cannot access the upstream network. If uplink detection is enabled, the AP regularly pings specified hosts through the LAN port. If all the hosts are not reachable, the AP performs the action of disabling RF or device reboot.

- If the AP performs the actions of disabling RF, wireless devices cannot find the SSIDs of the AP. The device can reconnect to the AP only after the connection between the AP and the upstream networks is recovered, and the AP stops performing the action of disabling RF. This ensures that if the uplink of the AP with uplink check enabled is faulty, wireless devices can connect to the upstream network through another nearby AP that works properly.
- If the AP performs the action of device reboot, after the device restarts, it will check whether the uplink network is back to normal. If the device does not recover, it will restart in the next detection cycle until the uplink network connection of the faulty AP returns to normal, and the AP stops restarting. In this way, the problem that the uplink is faulty due to device failure is solved by device reboot to a certain extent.

See the following topology (The LAN port serves as the uplink port).



7.6.2 Configuring uplink detection

Step 1 Choose **Tools** > **Uplink Detection**.

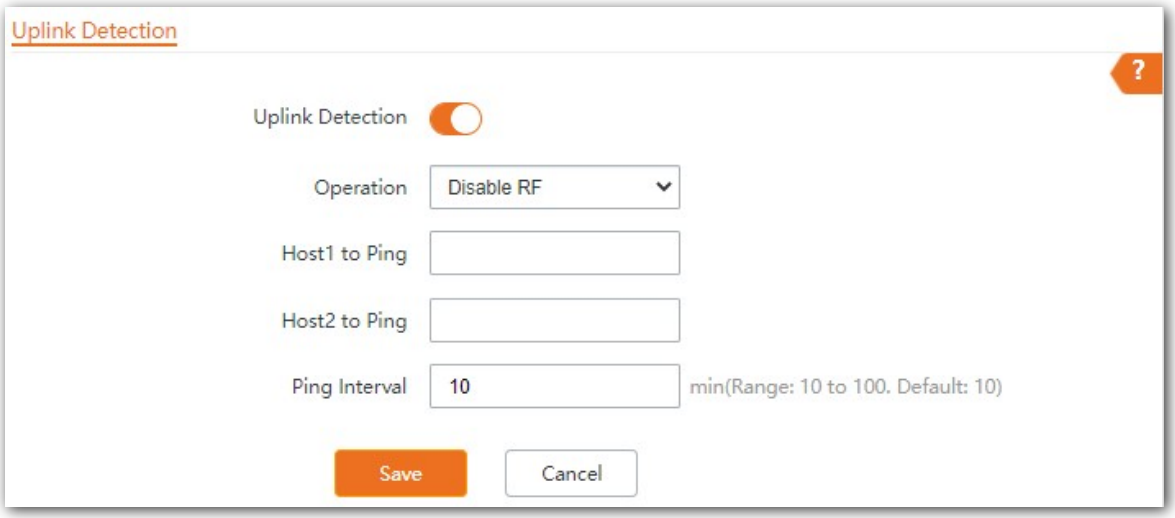
Step 2 Enable **Uplink Detection**.

Step 3 Select an operation you want the AP to perform.

Step 4 Enter the IP address of the host to be pinged in **Host1 to Ping** or **Host2 to Ping**, such as the IP address of the switch or router directly connected to the Ethernet port of the AP.

Step 5 Enter the interval at which the AP detects its uplink in **Ping Interval** box. The default value is **10** minutes.

Step 6 Click **Save**.



---- End

Parameter description

Parameter	Description
Uplink Detection	It specifies whether to enable the Uplink Detection function of the AP.
Operation	Set the operation of uplink detection. This parameter can be set if **Uplink Detection** is enabled. • Disable RF: The AP performs the action of disabling RF. • Reboot: The AP performs the device reboot action.
Host1 to Ping	Enter the IP address of the host to be pinged. This parameter can be set if **Uplink Detection** is enabled.
Host2 to Ping	
Ping Interval	Set the interval at which this device detects the uplink. This parameter can be set if **Uplink Detection** is enabled.

Appendix

A.1 Default parameter values

The following table lists the default parameter values of the AP.

Parameter			Default Value
Login	Login IP address		192.168.0.254
	User Name | Password	Administrator	admin|admin
Quick Setup	Working Mode		AP
LAN Setup	IP Address Type		The default IP address of the LAN port is 192.168.0.254. If the LAN where the AP is located has a DHCP server, the AP may automatically obtain a new IP address from the DHCP server. In this case, go to the client list of the DHCP server to check the IP address obtained by the AP.
SSID	SSID	2.4 GHz	The AP allows 7 SSIDs. SSID is Tenda_*XXXXXX*. *XXXXXX* indicates the last 6 digits of the AP's LAN MAC address with a range of *XXXXXX~XXXXXX+6.* By default, the primary SSID is enabled, and the other SSIDs are disabled.
		5 GHz	The AP allows 4 SSIDs. SSID is Tenda_*XXXXXX*_5G. *XXXXXX* indicates the last 6 digits of the AP's LAN MAC address with a range of *XXXXXX*+6~*XXXXXX*+9. By default, the primary SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network		Enable

A.2 Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AC	Access Point Controller (Network Equipment)
AC	Access Category (WMM settings)
ACK	Acknowledge
AES	Advanced Encryption Standard
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
BE	Best Effort
BK	Background
CAT5e	Category 5 Ethernet
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
Cwmax	Contention Window Maximum
Cwmin	Contention Window Minimum
DHCP	Dynamic Host Configuration Protocol
DIFS	Distributed Inter-Frame Spacing
DNS	Domain Name Server
DTIM	Delivery Traffic Indication Message
EDCA	Enhanced Distributed Channel Access
GI	Guard Interval
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Medium Access Control

Acronym or Abbreviation	Full Spelling
MIB	Management Information Base
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NMS	Network Management System
NTS	Network Time Server
OID	Object Identifier
PoE	Power-over-Ethernet
PPP	Point to Point Protocol
PVID	Port-based VLAN ID
QVLAN	IEEE 802.11q VLAN
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTS	Request To Send
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
STA	Station
SYS	System
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
UI	User Interface
UTF-8	8-bit Unicode Transformation Format
VI	Video Stream
VID	Virtual ID
VLAN	Virtual Local Area Network
VO	Voice Stream
WAN	Wide Area Network

Acronym or Abbreviation	Full Spelling
WEP	Wired Equivalent Privacy
WMF	Wireless Multicast Forwarding
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WPA-PSK	Wi-Fi Protected Access-Pre-shared Key