www.ip-com.com.cn

User Guide

ProFi Series AP

IP-COM
World Wide Wireless

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) 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 the warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM! Please read this user guide before you start.

This user guide walks you through all functions on the web UI of ProFi series APs. All screenshots herein, unless otherwise specified, are taken from iUAP-AC-M.

Tip

Web UI of different models may differ. The web UI of your model shall prevail.

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 highlight a procedure that will save time or resources.

For More Documents

APs of this series can all be managed by ProFi Software Controller in a unified manner. For detailed information, refer to the user guide of ProFi Software Controller.

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

Product document overview

Document	Overview
Datasheet	Walks you through basic parameters of AP, including product overview, product features, product specifications and so on.
Quick Installation Guide	Walks you through a rapid AP network establishment, including AP installation, network configuration, LED/Port/Button description, FAQ, 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.



+86-755-27653089	info@ip-com.com.cn	www.ip-com.com.cn

Revision History

IP-COM is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the ProFi Series APs were introduced.

Version	Date	Description
V1.0	2021-09-01	Original publication.

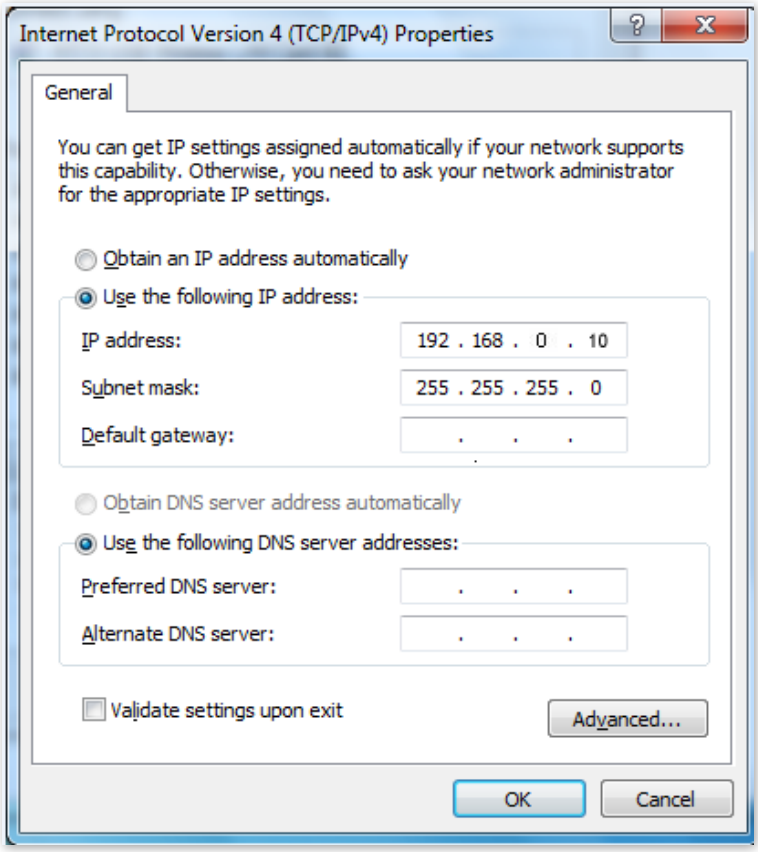
Contents

1 Log in to the Web UI

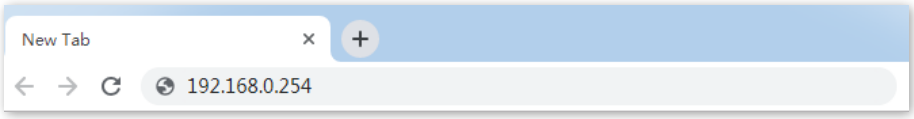
1.1 Login

1. Use an Ethernet cable to connect the management computer to AP or the switch to which AP is connected.
2. Configure the IP address of the management computer to ensure that its IP address is in the same network segment with AP.

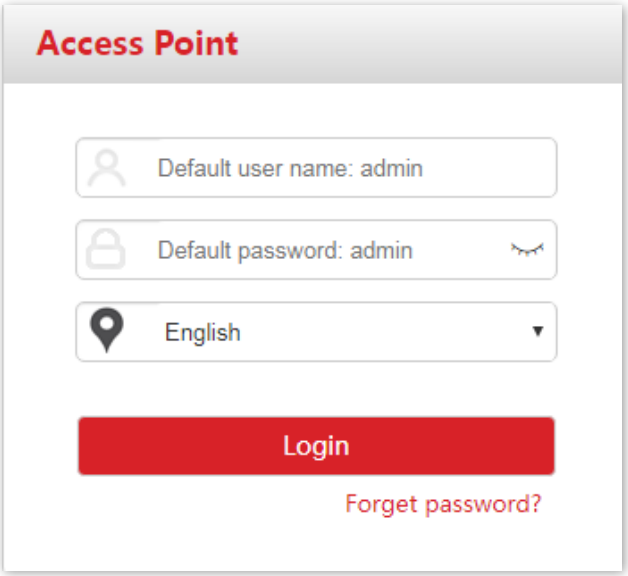
   For example, if IP address of the AP is **192.168.0.254**, then the IP address of the computer can be configured to **192.168.0.*X*** (*X* ranges from 2 to 253 and is not occupied by other devices) and subnet mask should be configured to **255.255.255.0**.



3. Start a browser on the computer and visit the IP address of AP (**192.168.0.254** by default).



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



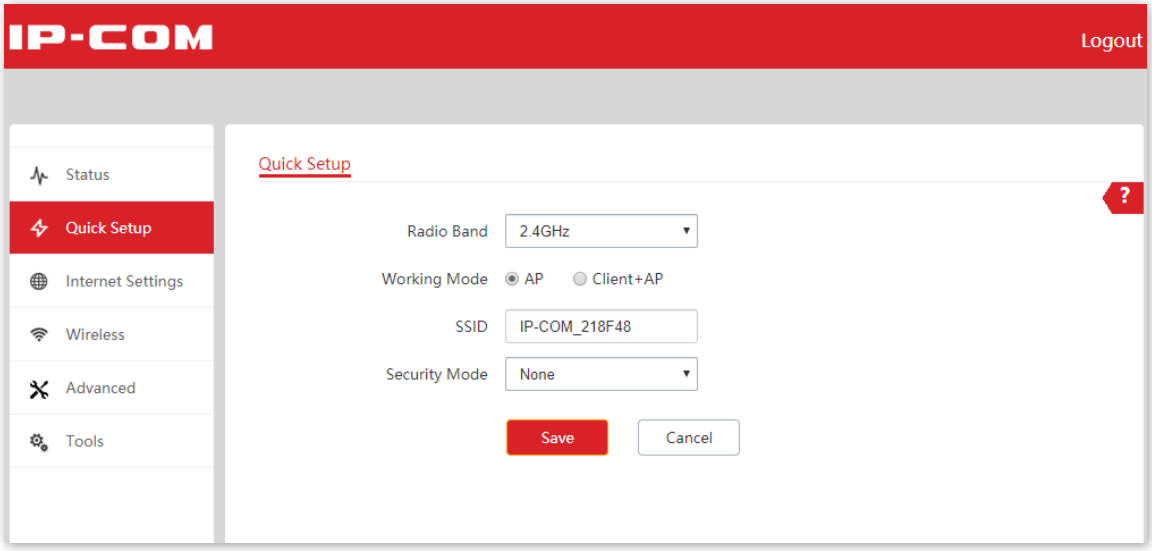
---End

Tip

If the above page does not appear, 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 ProFi Software Controller is deployed in the network, AP may be managed and therefore its IP address is no longer **192.168.0.254**. In this case, go to the web UI of the ProFi Software Controller to view the new IP address of the AP, and then log in to the AP's web UI using the new IP address.
- If two or more APs are connected in the network, IP address conflicts may occur. Please ensure that the IP address of the AP has been changed to one that is different from other APs.
- Reset the AP and try logging in using the default IP address. How to reset: When the **SYS** LED indicator of the AP blinks, hold down the **Reset** button for about 8 seconds and release it. When the **SYS** LED indicator lights solid on, AP is restored to factory settings.

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


IP-COM
Logout
Status
Quick Setup
Internet Settings
Wireless
Advanced
Tools
Quick Setup
Radio Band
2.4GHz
Working Mode
AP
Client+AP
SSID
IP-COM_218F48
Security Mode
None
Save
Cancel

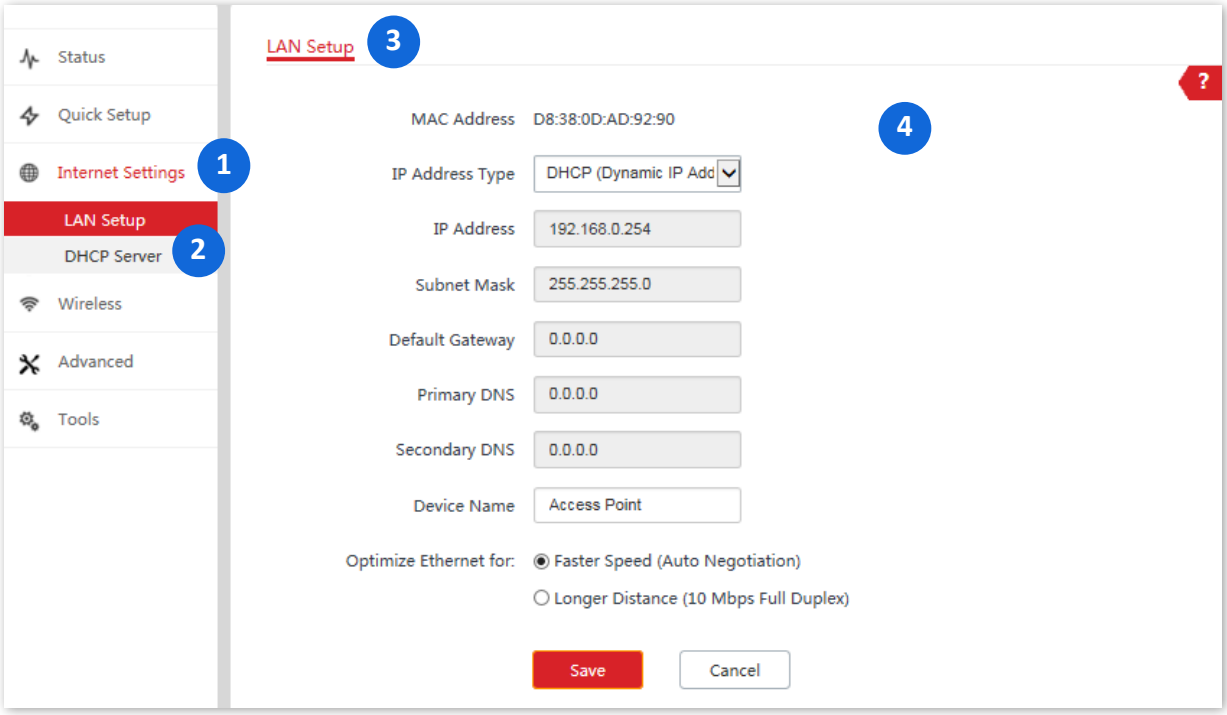
1.2 Logout

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

2.1 Layout

The web UI of the AP consists of four sections, including the first-level navigation bar, second-level navigation bar, tab, 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	First-level 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	Second-level navigation bar	

No.	Name	Description
3	Tab	
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
Refresh	Used to refresh the current page.
Save	Used to save the configuration on the current page and enable the configuration to take effect.
Cancel	Used to modify the current configuration on the current page back to the original configuration.
?	Check the help information of the current page.

3 Quick Setup

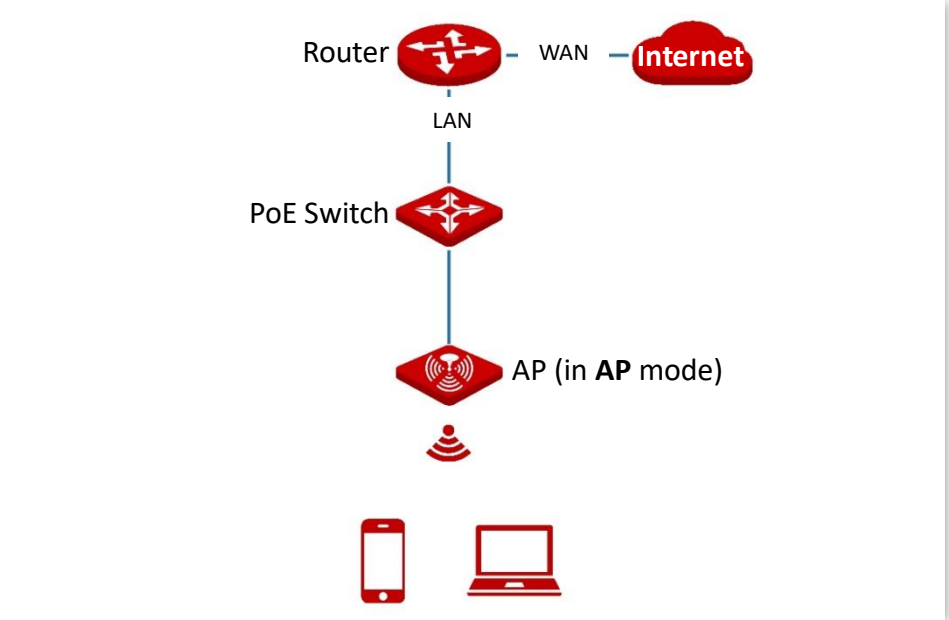
In the **Quick Setup** module, you can set up the AP in a quick way to enable internet access for your wireless devices such as smart phones and tablets.

Some models support only the AP mode (their quick setup page does not have a working mode option). The web UI of the target model prevails.

3.1 AP Mode

3.1.1 Overview

In this mode, the AP connects to the internet in a wired manner, and converts wired network into wireless network. AP works in this mode by default. See the following typical network topology.



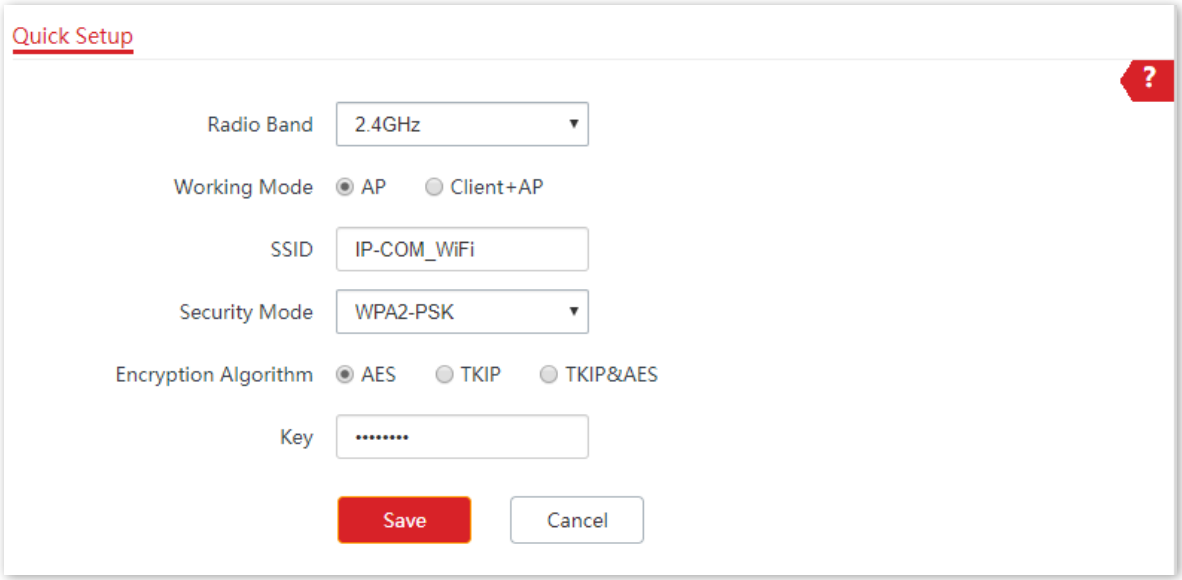
3.1.2 Quick Setup

Tip

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

1. Click **Quick Setup**.
2. Select **2.4 GHz** from the **Radio Band** drop-down list menu.
3. Set **Working Mode** to **AP**.
4. Customize an SSID (wireless network name) in the **SSID** box, which is **IP-COM_WiFi** in this example.

   This SSID is also your primary SSID on 2.4 GHz band.
5. Select the security mode from the **Security Mode** drop-down list menu, which is **WPA2-PSK** in this example.
6. Select the **Encryption Algorithm**, which is **AES** in this example.
7. Set a WiFi password in the **Key** box.
8. Click **Save** to apply your settings.



9. If you need to configure the **5GHz** radio band as well, repeat steps 2 to 8.

---End

After configuration, you can connect wireless devices to the WiFi network of your AP using the SSID and WiFi password you set.

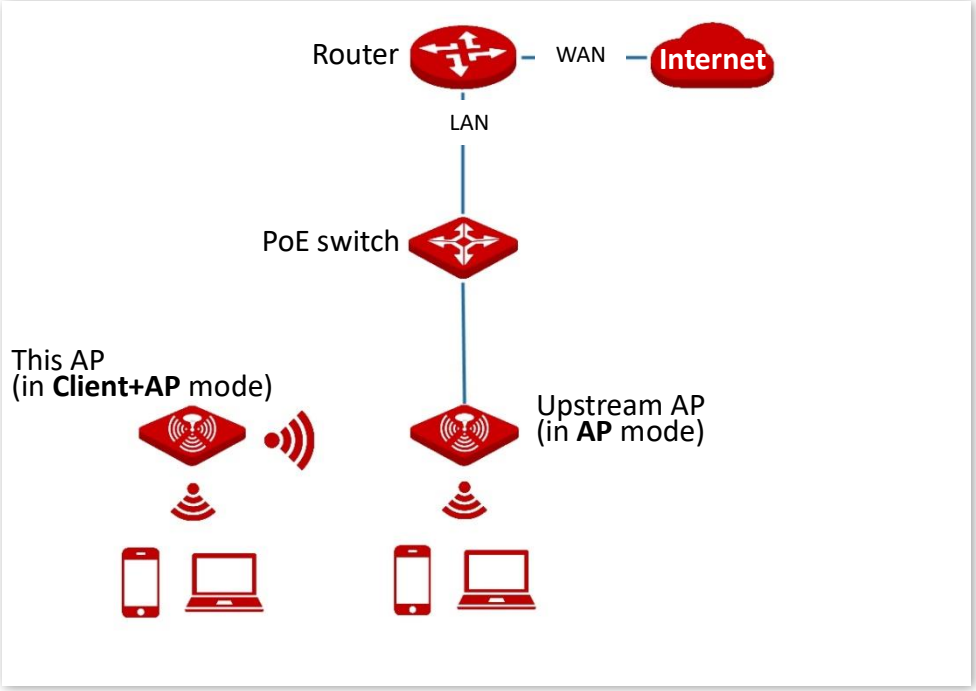
Parameter description

Parameter	Description
Radio Band	It is used to select the radio band for configurations.
Working Mode	It specifies the working modes supported by the device. – **AP** mode (default mode): This mode is used to convert wired networks into wireless networks. – **Client+AP** mode: This mode is used to bridge the upstream WiFi network.
SSID	Click it to modify the primary network name of the selected radio band.
Security Mode	It specifies the security mode you set for your AP's WiFi network. You can select the proper security mode by referring to the following description. – **None**: It indicates that the WiFi network is not encrypted. This option is not recommended because it leads to network insecurity. – **WEP:** 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. – **WPA-PSK, WPA2-PSK**, and **Mixed WPA/WPA2-PSK:** They belong to pre-shared key or personal key modes, where Mixed WPA/WPA2-PSK supports both WPA-PSK and WPA2-PSK. WPA-PSK, WPA2-PSK, and Mixed WPA/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. – (For Pro-6-LR) **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. (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.) – (For Pro-6-LR) **WPA3-SAE/WPA2-PSK**: You are recommended to select this security mode. This mode adopts a mixed encryption mode to ensure both compatibility and security. – **WPA and WPA2**: 802.1x is used to authenticate users and generate root key for encrypting data instead of using pre-shared key you set manually. Data encryption key is automatically generated by AP based on encryption rule TKIP or AES, which is proper for wireless networks with high security requirements such as enterprises.

3.2 Client+AP Mode

3.2.1 Overview

In this mode, the AP extends the existing wireless network by bridging the upstream wireless signals. See the following typical network topology.

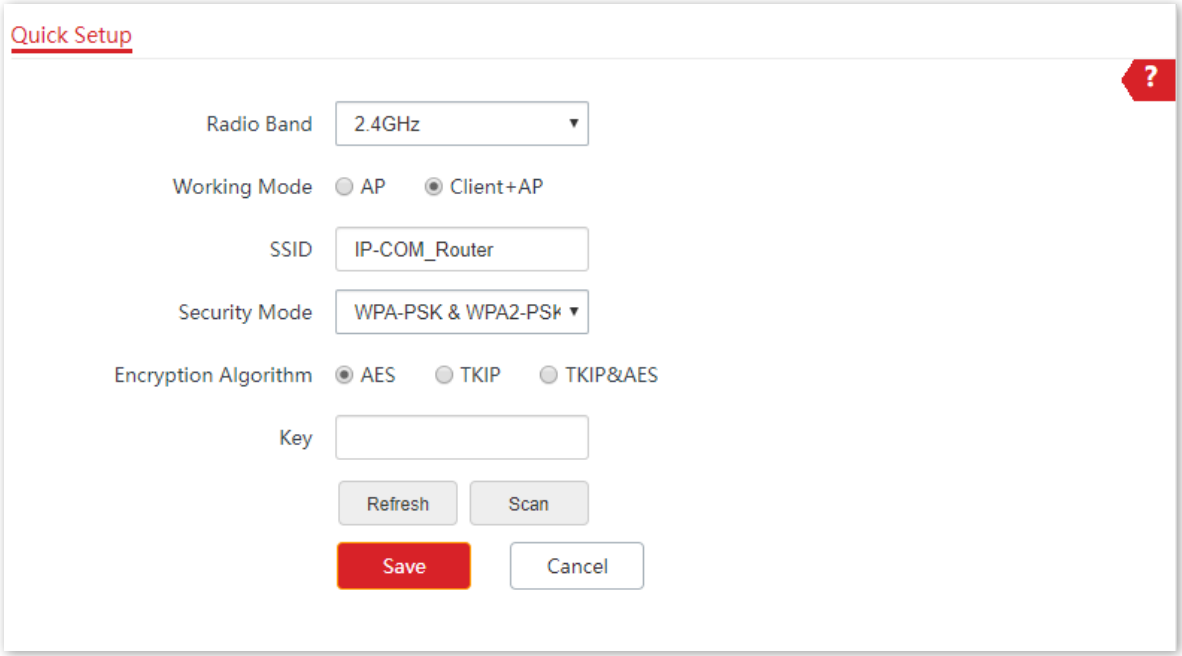


3.2.2 Quick Setup

Tip

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

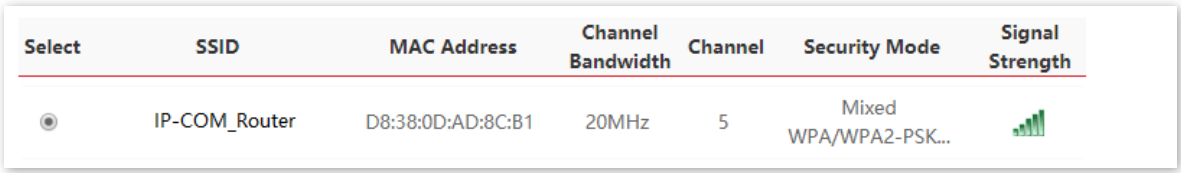
1. Click **Quick Setup**.
2. Select the radio band to be configured from the **Radio Band** drop-down list menu, which is **2.4 GHz** in this example.
3. Set **Working Mode** to **Client+AP**.
4. Click **Scan**. The nearby available radio signals appear on the lower page.



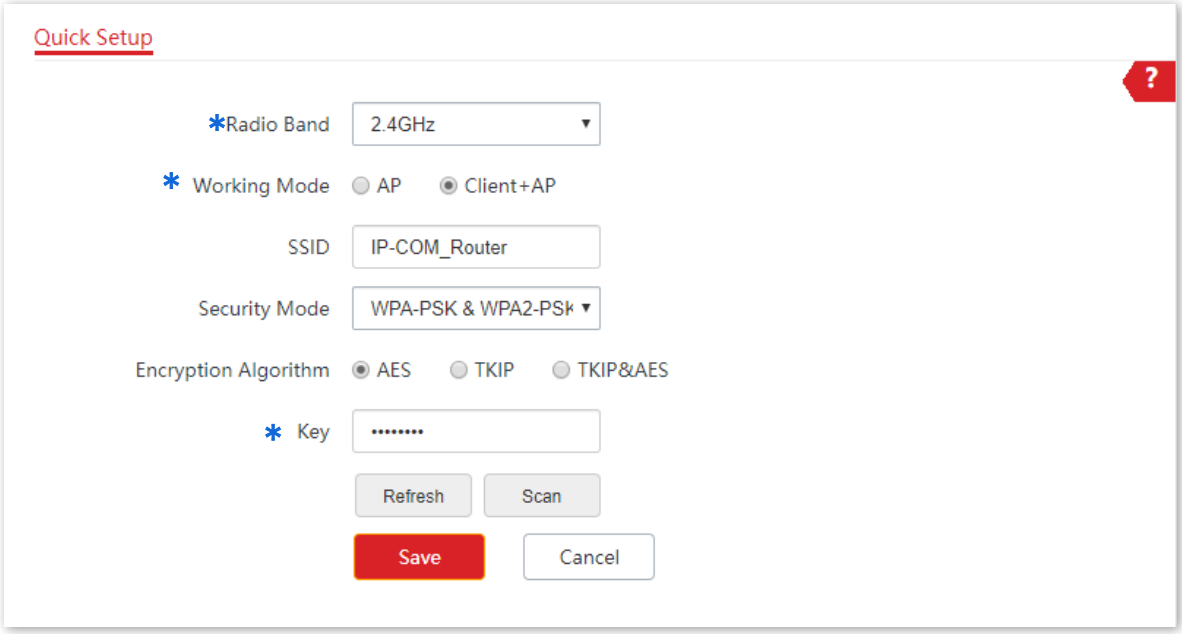
5. Select the WiFi network to bridge, which is **IP-COM_Router** in this example.

Tip

- If the SSID for bridging is not displayed, check if your upstream **Wireless Network** is enabled by entering the **Wireless** > **RF Settings** page. If not, enable it. Then refresh the scan result.
- The device detects and auto-fills **SSID, Security Mode**, and **Encryption Algorithm** of the upstream wireless network for you, except the **Key**, which requires you to enter manually.



6. Click **Disable**.
7. If the upstream network is encrypted, enter the **Key**.
8. Click **Save** to apply your settings.



---End

After the configuration, devices connected to the AP can access the upstream wireless network after entering the wireless password (Key).

Tip

You can enter the **Wireless** > **SSID** page to check the SSID and key of AP.

Parameter description

Parameter	Description
Radio Band	It is used to select the radio band for configurations.
Working Mode	It specifies the working modes supported by the device: – **AP** mode (default mode): This mode is used to convert wired networks into wireless networks. – **Client+AP** mode: This mode is used to bridge the upstream WiFi network.
SSID	It specifies the WiFi network name (SSID) of the WiFi network to be bridged. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically.

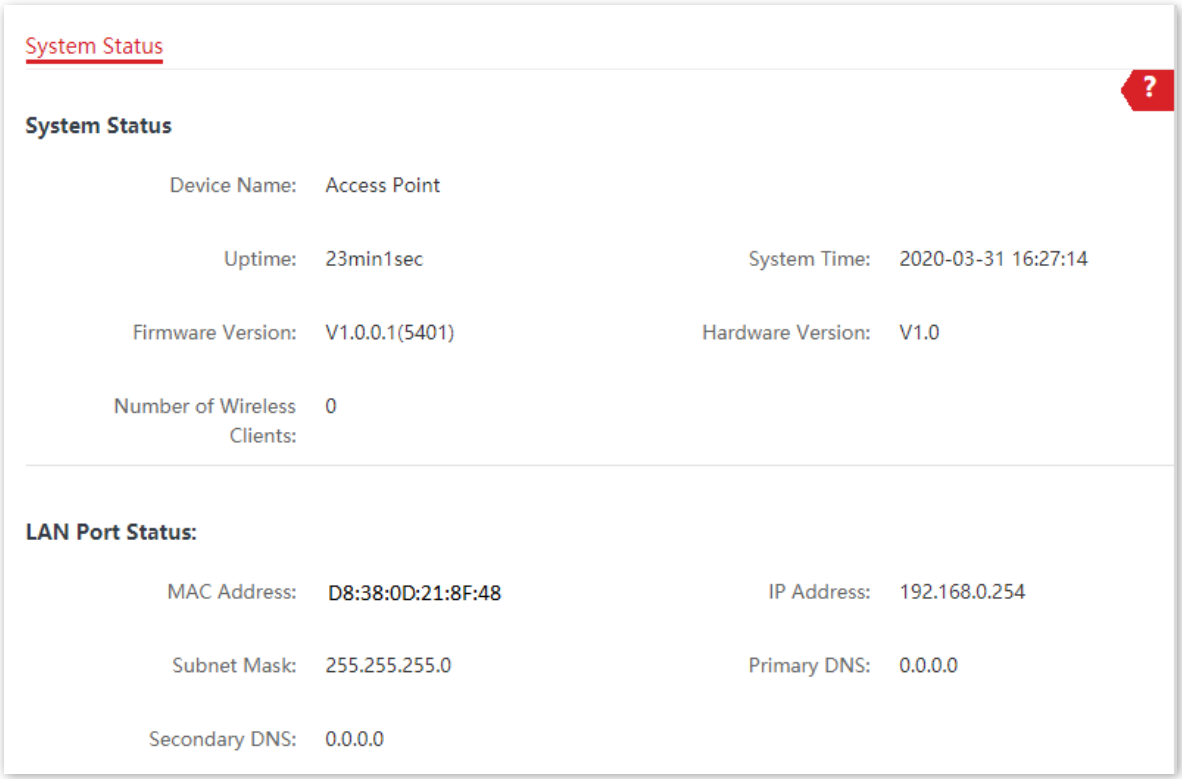
Parameter	Description
Security Mode	It specifies the security mode of which the upstream WiFi network adopted. After you select the upstream WiFi network from the scanned wireless network list, this parameter will be populated automatically. AP can bridge wireless networks adopting security modes of **None**, **WEP**, **WPA-PSK**, **WPA2-PSK**, and **Mixed WPA/WPA2-PSK**. Some models support **WPA3-SAE** and **WPA3-SAE/WPA2-PSK** as well. The web UI of the target model prevails. – **None**: It indicates that the WiFi network is not encrypted. This option is not recommended because it leads to network insecurity. – **WEP:** 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. – **WPA-PSK, WPA2-PSK,** and **Mixed WPA/WPA2-PSK:** They belong to pre-shared key or personal key modes, where Mixed WPA/WPA2-PSK supports both WPA-PSK and WPA2-PSK. WPA-PSK, WPA2-PSK, and Mixed WPA/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. – **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. (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**: You are recommended to select this security mode. This mode adopts a mixed encryption mode to ensure both compatibility and security. Note – If the wireless network to be bridged adopts the WEP security mode, you need to enter Key x (x ranges from 1 to 4). – If the wireless network to be bridged adopts the WPA-PSK, WPA2-PSK, or Mixed WPA/WPA2-PSK security mode, the system auto-fills **SSID, Security Mode**, and **Encryption Algorithm** of the upstream wireless network for you, except the **Key**, which requires you to enter manually.
Key	It specifies the WiFi password for the upstream wireless network you selected.
Refresh	Used to refresh the scan results.
Scan/Disable	- **Scan**: Used to scan nearby available wireless networks. The scan results are displayed on the lower page. - **Disable**: The button only appears after you clicked **Scan**. It is used to end the scan operation and collapse the scan result.

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

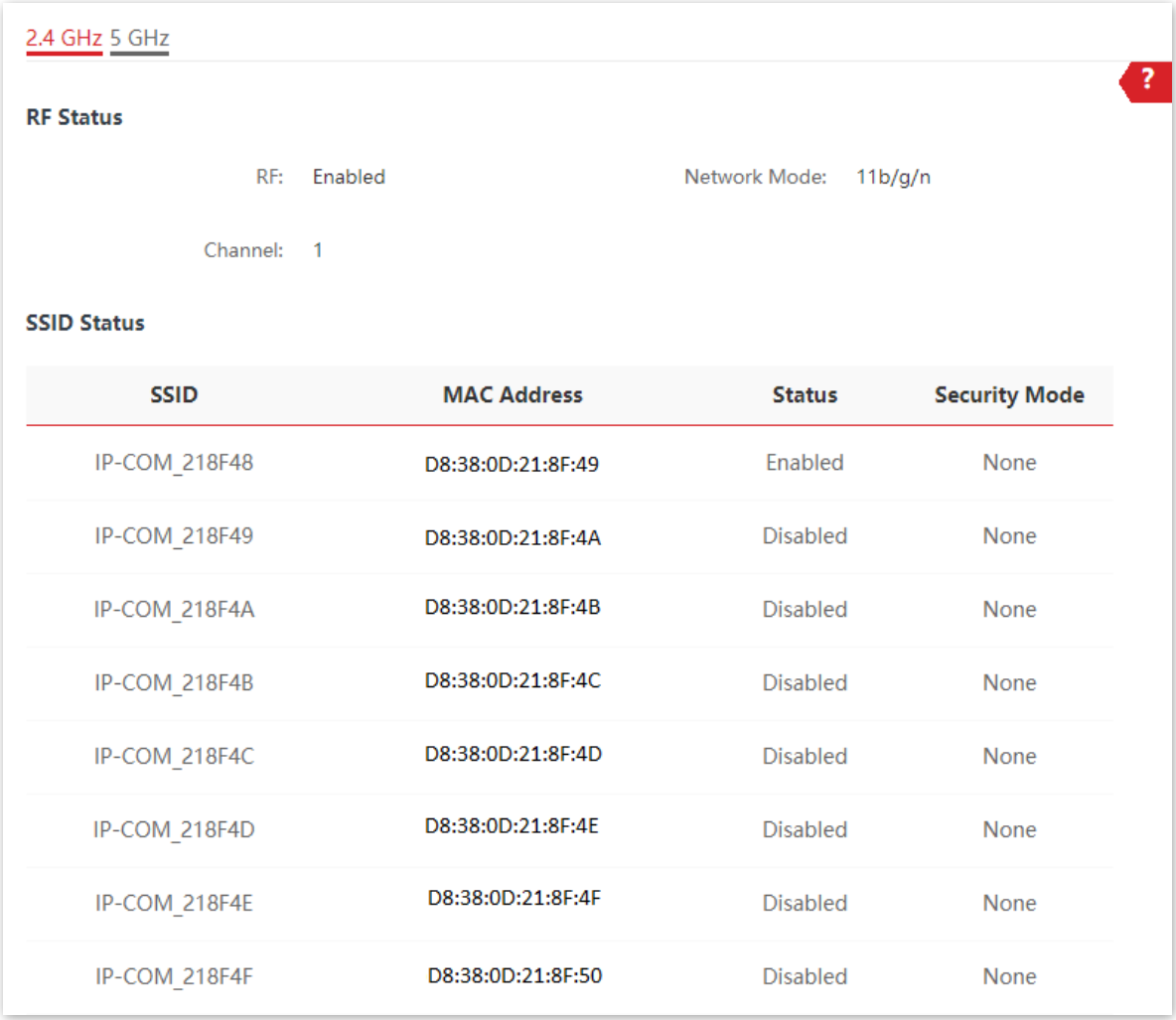
Parameter	Description
Device Name	It specifies the name of the AP. You can modify it on **Internet Settings** > LAN Setup page.
Uptime	It specifies the time that has elapsed since the AP starts up last time.
System Time	It specifies the current system time of the AP.
Firmware Version	It specifies the current firmware version number of the AP.

Parameter	Description
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.
MAC Address	It specifies the physical address of the LAN port of the AP.
IP Address	It specifies the IP address of the LAN port of the AP, which can be used to log in to the web UI. You can modify it on **Internet Settings** > **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**. By default, the page displays the information of 2.4 GHz wireless status. To view the wireless status of 5 GHz, click **5 GHz.**

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



Parameter description

Parameter	Description
RF	It specifies whether the WiFi network at the corresponding band is enabled. – **Enabled**: WiFi network at the corresponding band is enabled. – **Disabled**: WiFi network at the corresponding band is disabled.
Network Mode	It specifies the current network mode of the AP.
Channel	It specifies the current working channel of the AP.

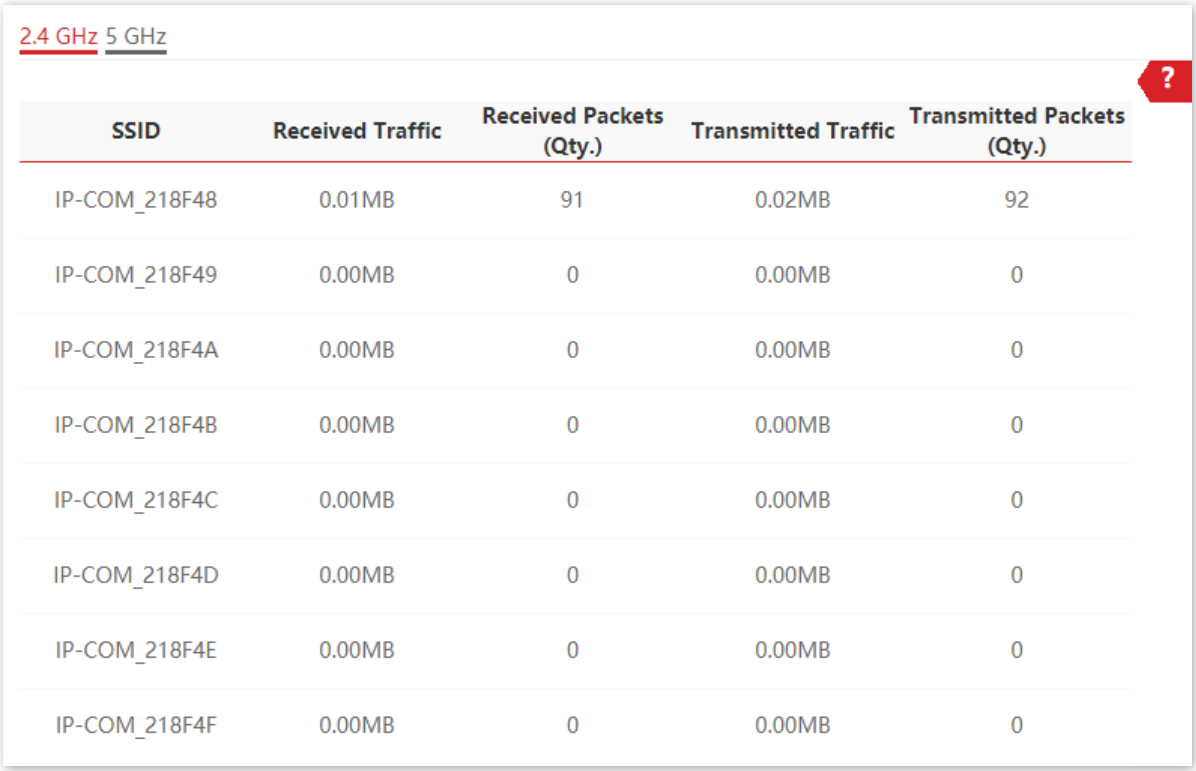
Parameter	Description
SSID	It specifies the wireless network name of the AP.
MAC Address	It specifies the physical address of the corresponding wireless network.
Status	It specifies whether or not the corresponding WiFi network is enabled.
Security Mode	It specifies the security mode adopted by the corresponding WiFi network.

4.3 Traffic Statistics

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

By default, the page displays the traffic statistics information of 2.4 GHz. To view information about 5 GHz, click **5 GHz.**

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

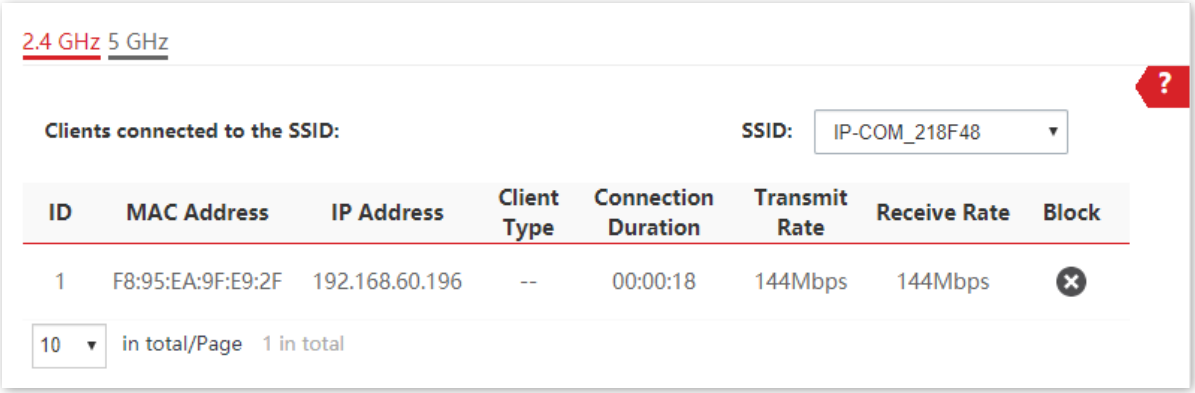


SSID	Received Traffic	Received Packets (Qty.)	Transmitted Traffic	Transmitted Packets (Qty.)
IP-COM_218F48	0.01MB	91	0.02MB	92
IP-COM_218F49	0.00MB	0	0.00MB	0
IP-COM_218F4A	0.00MB	0	0.00MB	0
IP-COM_218F4B	0.00MB	0	0.00MB	0
IP-COM_218F4C	0.00MB	0	0.00MB	0
IP-COM_218F4D	0.00MB	0	0.00MB	0
IP-COM_218F4E	0.00MB	0	0.00MB	0
IP-COM_218F4F	0.00MB	0	0.00MB	0

4.4 Client List

The Client List page allows you to check wireless clients connected to each SSID of the AP and their basic information, and block unknown wireless clients.

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



Parameter description

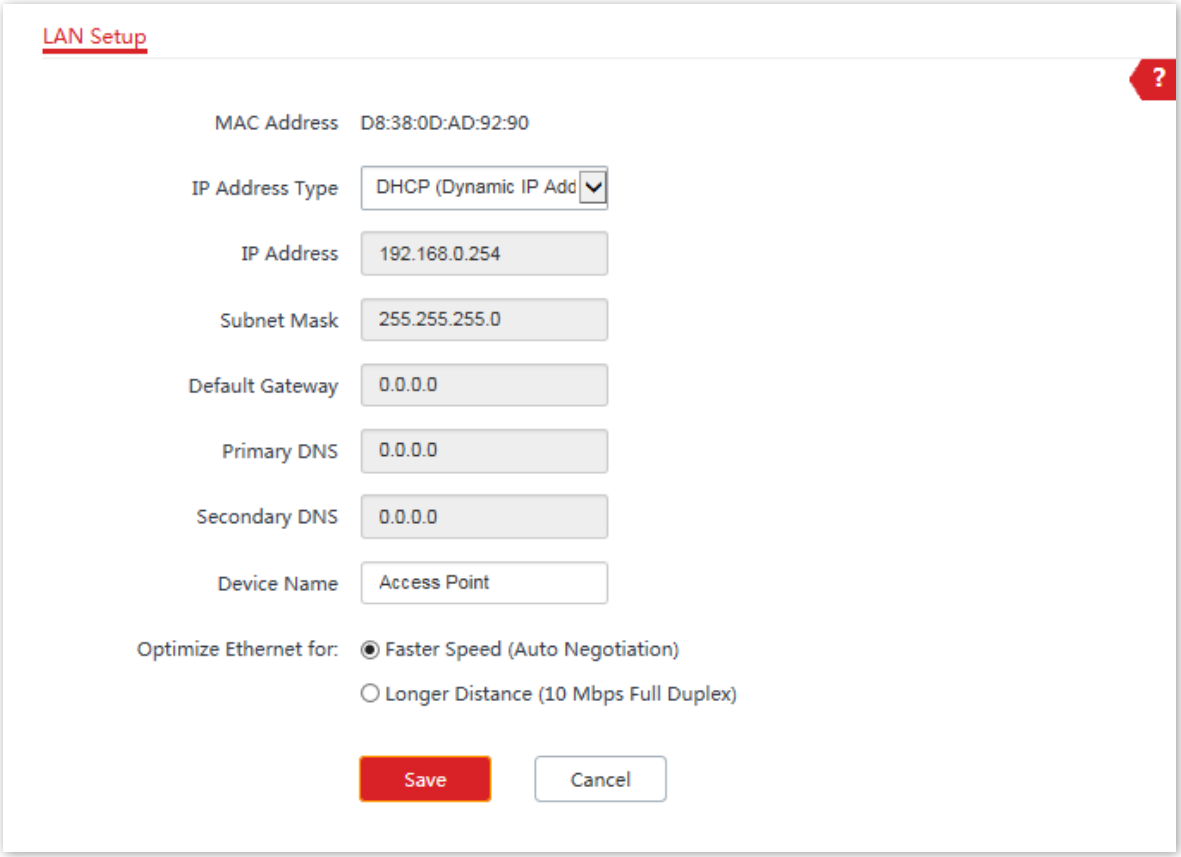
Parameter	Description
SSID	Select the SSID from the drop-down list menu to view client information connected to it.
MAC Address	It specifies the physical address of the client.
IP Address	It specifies the IP address of the client.
Client Type	It specifies the operating system of the client. Tip The AP identities the client type only when both the two conditions are met: – The Identity Client Type function is enabled (To enable it, navigate to **Wireless** > **Advanced Settings**). – The client connected to the AP has accessed an **http:// URL**. Otherwise, -- is displayed.
Connection Duration	It specifies the online duration of the wireless client.
Transmit Rate	It specifies the current transmission rate of the client.
Receive Rate	It specifies the current receiving rate of the client.
Block	Click to block the client from accessing the AP's wireless network. To unblock a client, navigate to **Wireless** > Access Control.

5 Internet Settings

5.1 LAN Setup

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 LAN port of the AP.

Parameter	Description
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)** (default): 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.  If **IP Address Type** is set to **DHCP (Dynamic IP Address)**, you can log in to the web UI of the AP only with the IP address assigned to the AP by the DHCP server. The IP address is specified on the client list of the DHCP server.
IP Address	It specifies the LAN IP address (also the login IP address) of the AP. The default IP address is **192.168.0.254**.
Subnet Mask	It specifies the subnet mask of the AP. The default subnet mask is **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 Bedroom), so that you can easily identify the AP when managing many APs.
Optimize Ethernet for	It specifies the Ethernet mode of the PoE Ethernet 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.

5.2 DHCP Server

5.2.1 Overview

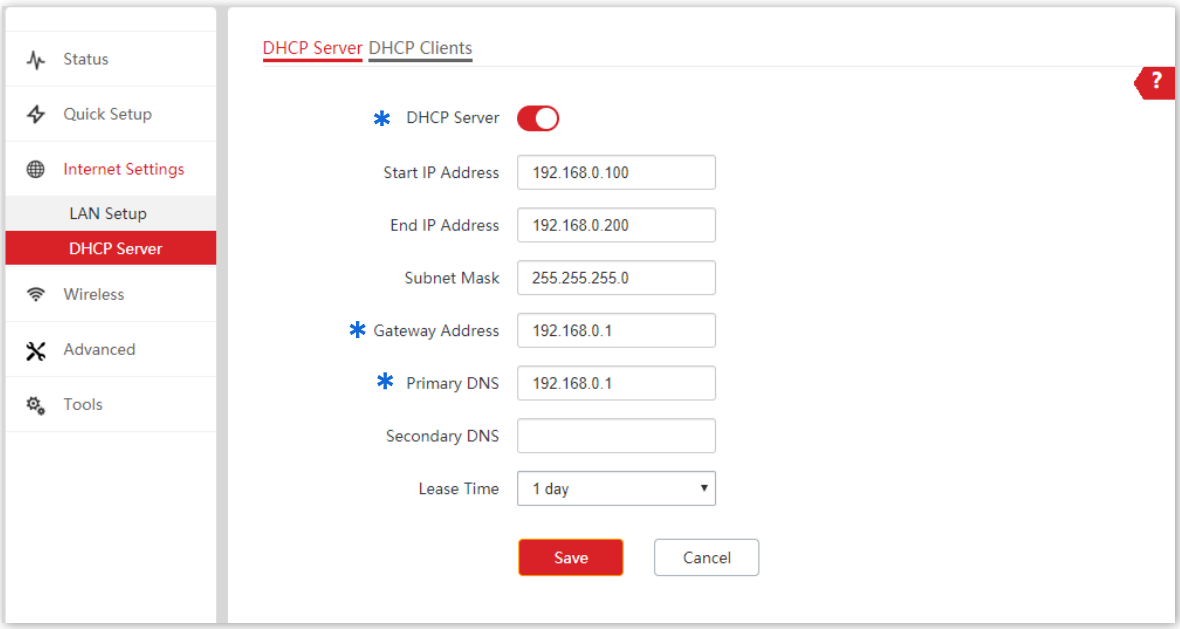
The DHCP Server page allows you to assign IP addresses and other network configuration parameters to devices connected to it. By default, this function is disabled.

Tip

If the modified IP address of the LAN port is not in the same network segment with the original one, the system automatically modifies the DHCP address pool so that the pool is in the same network segment with the new IP address of the LAN port.

5.2.2 Configure DHCP Server

1. Choose **Internet Settings** > **DHCP Server** > **DHCP Server**.
2. Enable **DHCP Server** function.
3. Customize required parameters (Generally, you only need to modify **Gateway Address** and **Primary DNS**).
4. Click **Save** to apply your settings.



---End

Note

If another DHCP server is available in your LAN, ensure that the IP address pool of the AP does not overlap with the IP address pool of that DHCP server. Otherwise, IP address conflicts may occur.

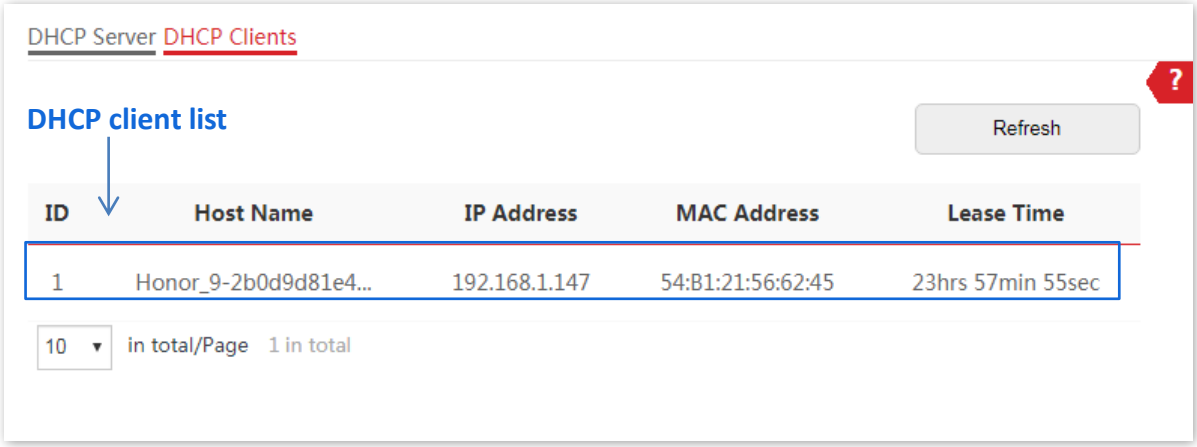
Parameter description

Parameter	Description
DHCP Server	It specifies whether or not to enable the DHCP server function of the AP. By default, it is disabled.
Start IP Address	It specifies the start IP address of the DHCP server's IP address pool. The default value is **192.168.0.100**.
End IP Address	It specifies the end IP address of the DHCP server's IP address pool. The default value is **192.168.0.200**.
Subnet Mask	It specifies the subnet mask assigned by the DHCP server to devices. The default value is **255.255.255.0**.
Gateway Address	It specifies the gateway IP address assigned by the DHCP server to devices. Generally, it is the LAN IP address of the router connected to the internet. The default value is **192.168.0.1**. Tip Only through a gateway can a LAN device access a server or host which is not in the local network segment.
Primary DNS	It specifies the IP address of the primary DNS server assigned by the DHCP server to devices. Tip To enable devices to access the internet, set this parameter to a correct DNS server IP address or DNS proxy IP address.
Secondary DNS	It specifies the IP address of the secondary DNS server assigned by the DHCP server to devices. This parameter is optional, which indicates you can leave it blank if the DHCP server does not assign this parameter.
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a device. By default, it is **1** day. When half of the lease time has elapsed, the device sends a DHCP request to the DHCP server to renew the lease time. If the renewing succeeds, the lease time is extended according to the request. If the renewing fails, the device sends a request again when 7/8 of the lease time has elapsed. If the renewing succeeds, the lease time is extended according to the request. If the renewing fails still, the device must request a new IP address from the DHCP server after the lease time expires. You are recommended to retain the default value.

5.2.3 View DHCP Clients

The DHCP Clients page allows you to view DHCP clients and their connection information.

To access the page, choose **Internet Settings** > **DHCP Server** > **DHCP Clients**.



To view the latest DHCP client list, click **Refresh**.

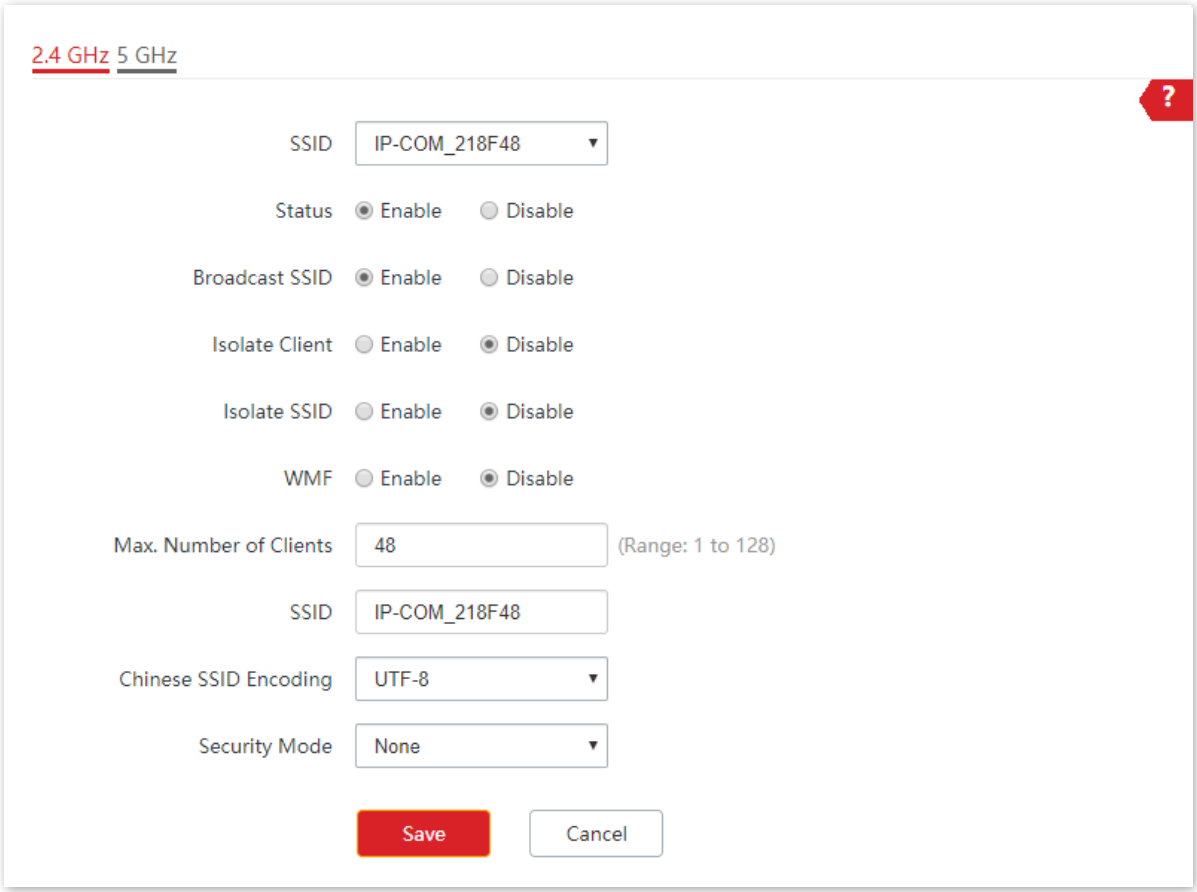
6 Wireless

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.
Status	It specifies the status of the selected SSID. The primary SSID is enabled by default and you can enable other SSIDs manually.
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.
Isolate Client	It isolates the wireless clients connected to the same wireless network corresponding to an SSID, so that the wireless clients can access only the wired network connected to the AP. Applying this function to hotspot setup at public places such as hotels and airports helps increase network security.
Isolate SSID	After this function is enabled, wireless devices connected to different SSIDs of the AP cannot communicate with each other, enhancing the security of the wireless network.
WMF	The WMF function of the AP converts multicast traffic into unicast traffic and forwards the traffic to the multicast traffic destination in the wireless network. This helps save wireless resources, ensure reliable transmission, and reduce delays.
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 it to modify the selected SSID (name of the wireless network).
Chinese SSID Encoding	It specifies the encoding format used by the Chinese characters in the SSID. 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.

Parameter	Description
Security Mode	It specifies the security modes supported by the AP, including: – **None**: This wireless network is open. The security level is the lowest. – **WEP**: Wired Equivalent Privacy. The security level is very low. – **WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK**: Applicable to most scenarios. – (For Pro-6-LR) **WPA3-SAE**: It is an upgraded version of WPA2-PSK and provides protection against dictionary attacks and information disclosure. (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.) – (For Pro-6-LR) **WPA3-SAE/WPA2-PSK**: You are recommended to select this security mode. This mode adopts a mixed encryption mode to ensure both compatibility and security. – **WPA and WPA2:** This mode provides highest security level. It uses 802.1 x RADIUS to encrypt and is applicable to enterprises. Tip See Security Mode for details.

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.

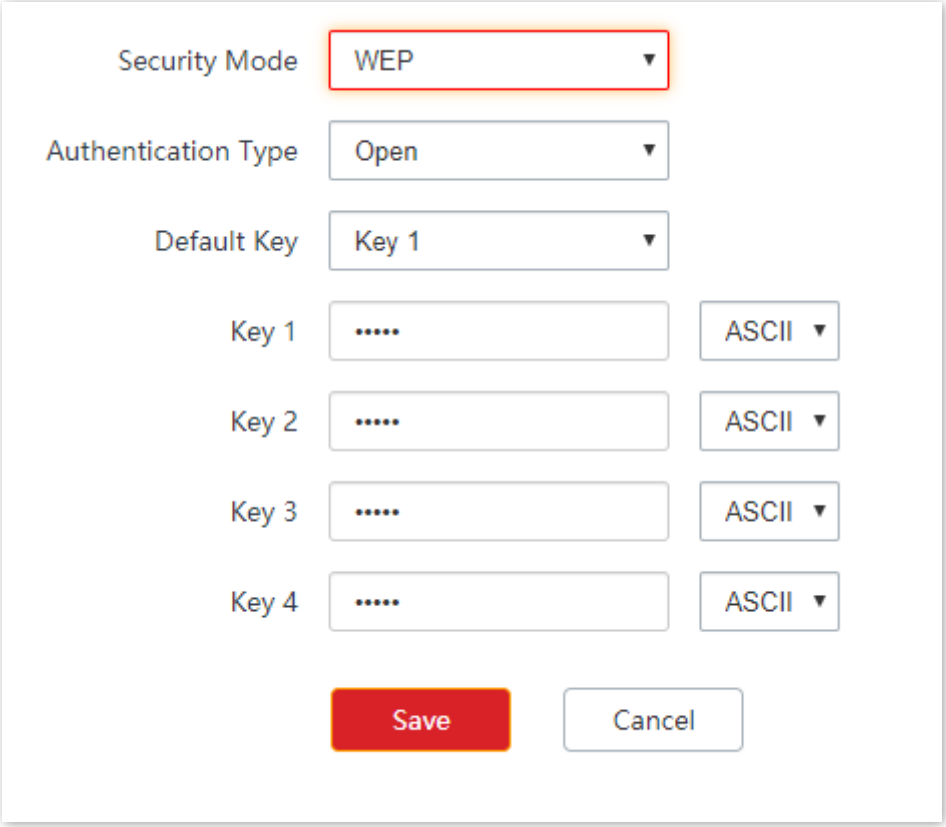
The AP supports various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, WPA3-SAE, WPA3-SAE/WPA2-PSK, Mixed WPA/WPA2-PSK, and WPA/WPA2.

- **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 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.



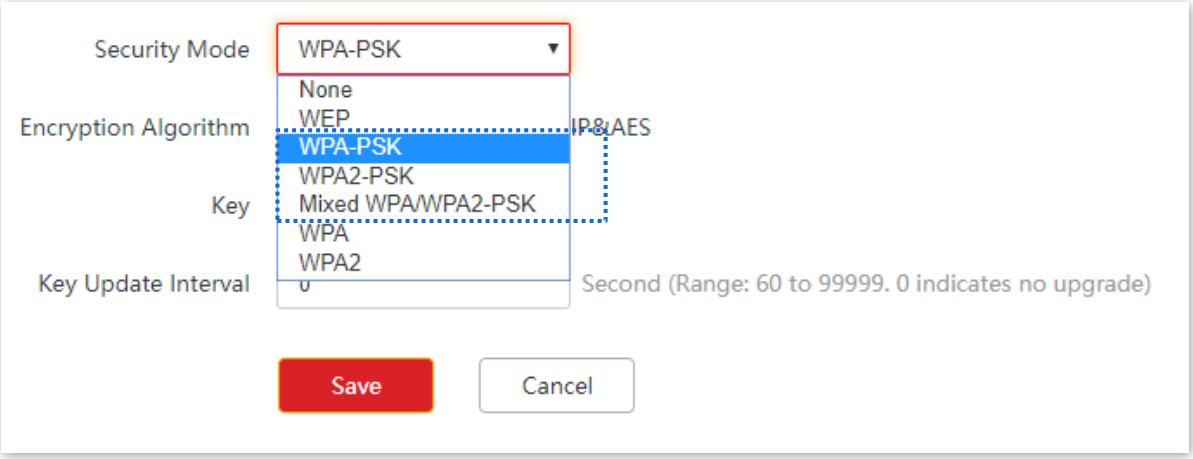
Parameter description

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 Hexadecimal. – **ASCII**: 5 or 13 ASCII characters are allowed in the key. – **Hex**: 10 or 26 hexadecimal characters (range: 0-9, a-f, and A-F) are allowed in the key.

- **WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK**

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

WPA-PSK, WPA2-PSK, and Mixed WPA/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.

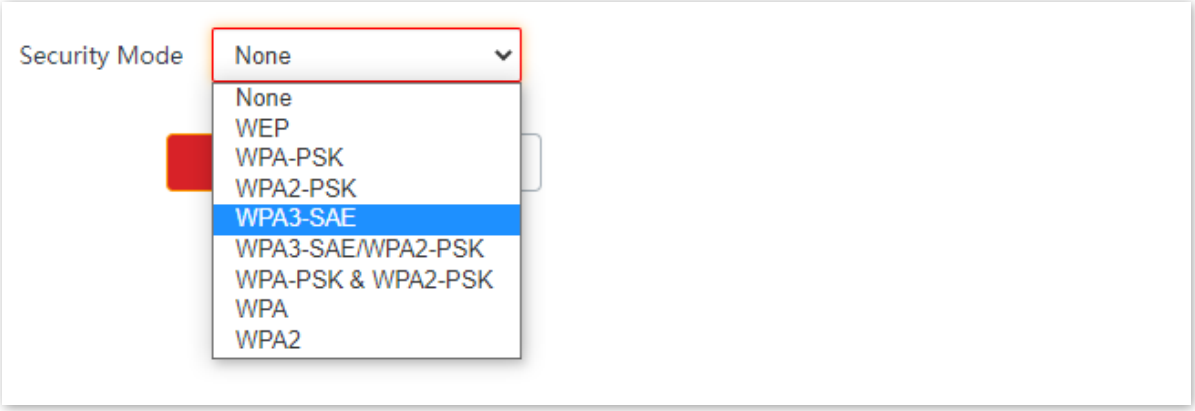


- **WPA3-SAE**

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 mixed encryption mode of WPA2-PSK and WPA3-SAE is adopted to ensure both compatibility and security.

Parameter description

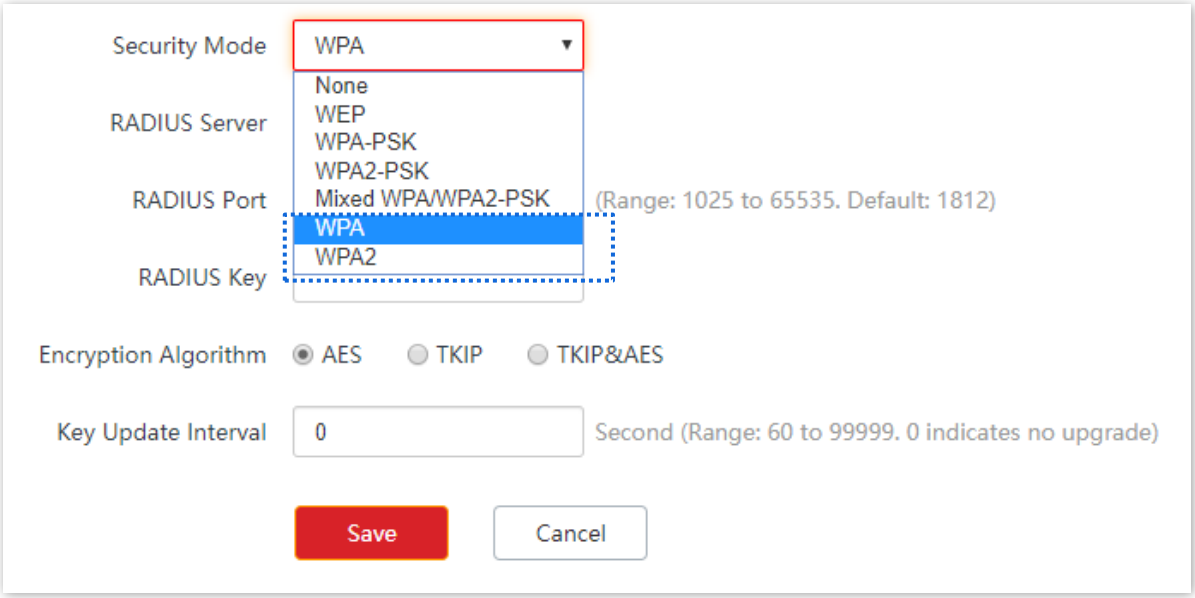
Parameter	Description
Security Mode	It indicates the personal or pre-shared key security mode, including **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK**, **WPA3-SAE**, and **WPA3-SAE/WPA2-PSK**. – **WPA-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA-PSK. – **WPA2-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2-PSK. – **WPA3-SAE**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA3-SAE. – **WPA3-SAE/WPA2-PSK**: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA3-SAE or WPA2-PSK, which can guarantee both compatibility and security. – **Mixed WPA/WPA2-PSK**: It indicates that wireless clients can connect to the wireless network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK. Tip WPA3-SAE is an upgraded version of WPA2-PSK. If your wireless clients do not support WPA3-SAE or the WiFi experience is unsatisfying, you are recommended to set the security mode to WPA/WPA2-PSK (recommended).

Parameter	Description
Encryption Algorithm	It specifies the encryption algorithm corresponding to the selected security mode. If **Security Mode** is set to **WPA-PSK**, this parameter has the **AES** and **TKIP** values. If **Security Mode** is set to **WPA3-SAE** or **WPA3-SAE/WPA2-PSK**, this parameter has only the **AES** value. If **Security Mode** is set to **WPA2-PSK** or **Mixed WPA/WPA2-PSK**, this parameter has the **AES**, **TKIP**, and **TKIP&AES** values. – **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.
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 WAP 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 use 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

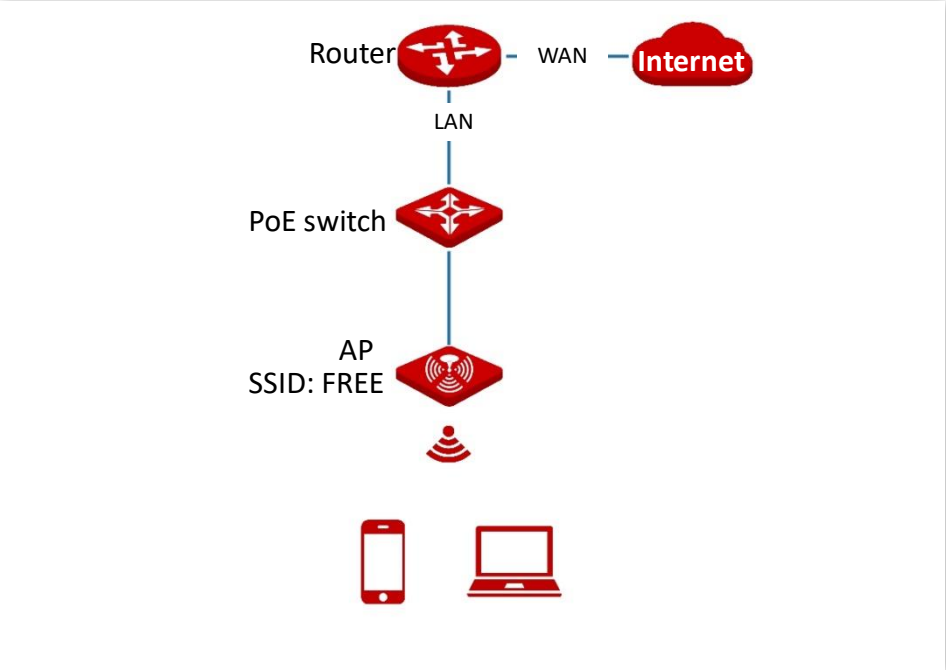
Parameter	Description
Security Mode	The **WPA** and **WPA2** options are available for network protection with a RADIUS server. – **WPA**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA. – **WPA2**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2.
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. The available options include **AES**, **TKIP**, and **TKIP&AES**. – **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 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

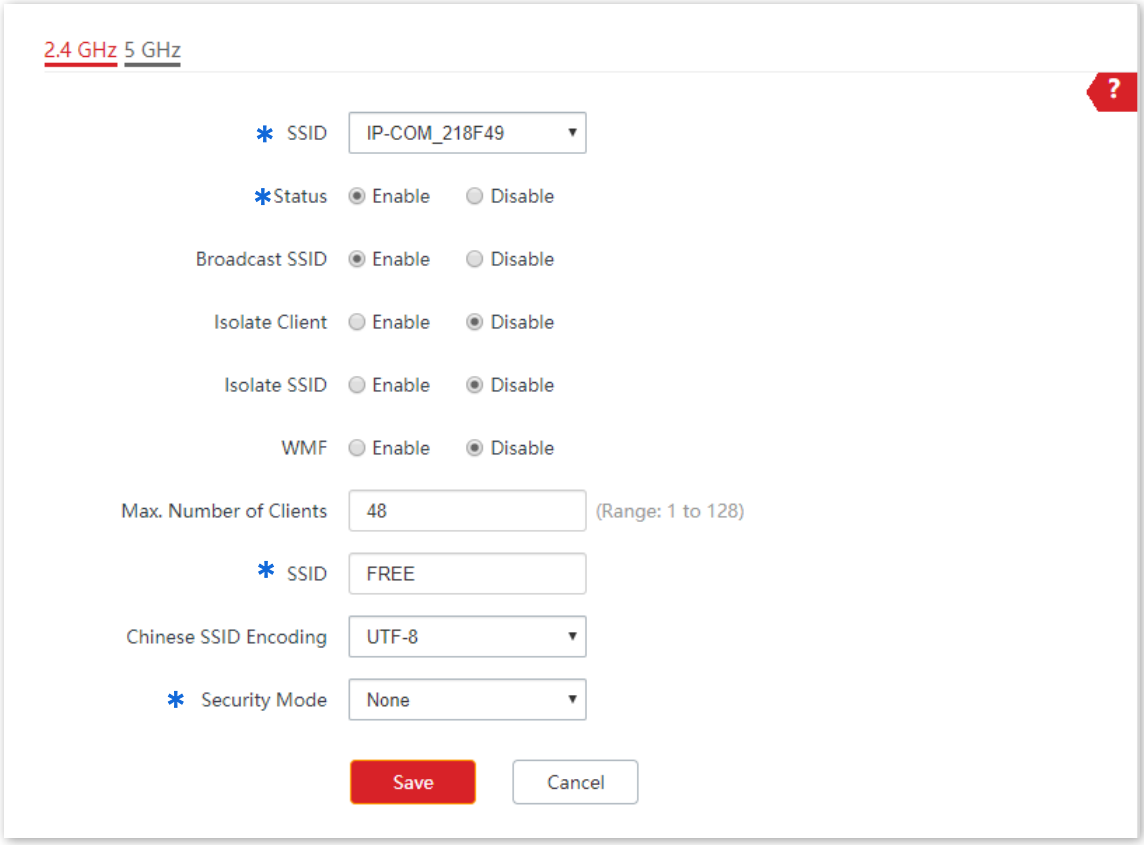
In a hotel lounge, guests can connect to the wireless network without a password and access the internet through the WiFi network.



Configuration procedure

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

1. Choose **Wireless** > **SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Change the value of the **SSID** text box to **FREE**.
5. Set **Security Mode** to **None**.
6. Click **Save**.



---End

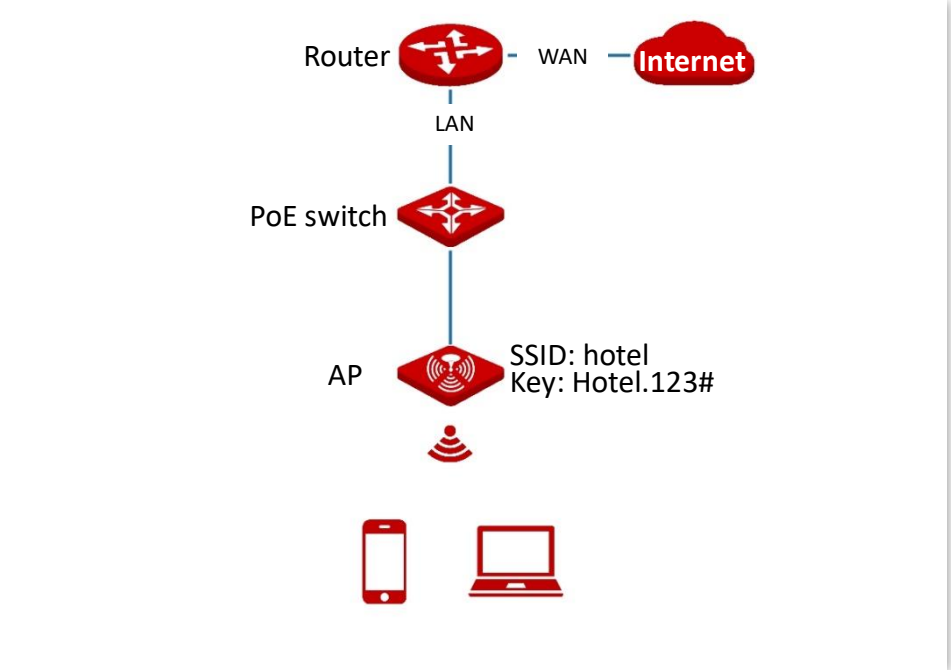
Verification

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

Example of Setting up a Wireless Network Encrypted with PSK

Networking requirement

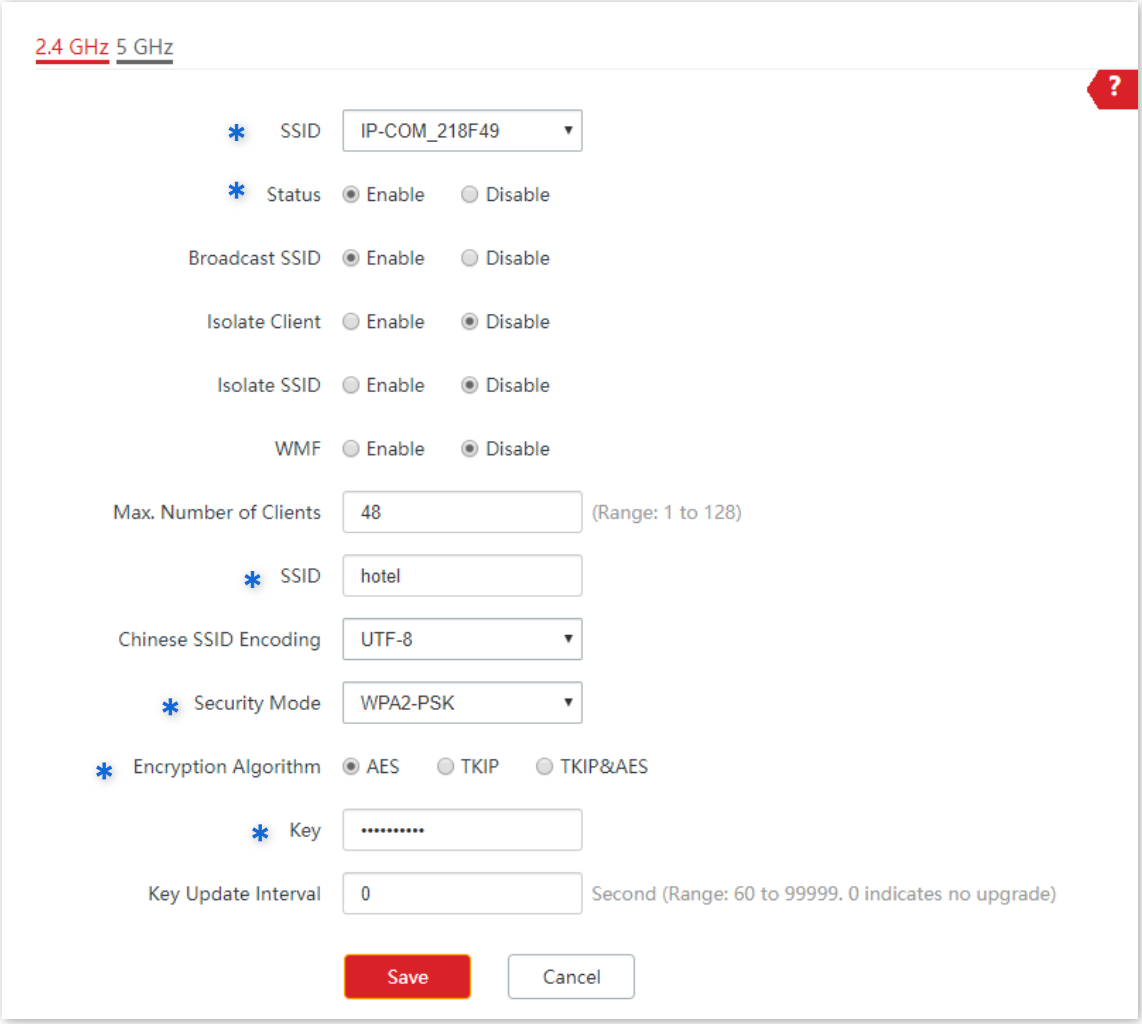
A hotel wireless network with a certain level of security must be set up through a simply procedure. In this case, WPA, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA3-SAE, or WPA3-SAE/WPA2-PSK security mode is recommended. See the following figure.



Configuration procedure

Assume that the second SSID of the AP, the WPA2-PSK security mode, and AES encryption algorithm are used.

1. Choose **Wireless** > **SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Change the value of the **SSID** text box to **hotel**.
5. Set **Security Mode** to **WPA2-PSK** and **Encryption Algorithm** to **AES**.
6. Set **Key** to **Hotel.123#**.
7. Click **Save**.



---End

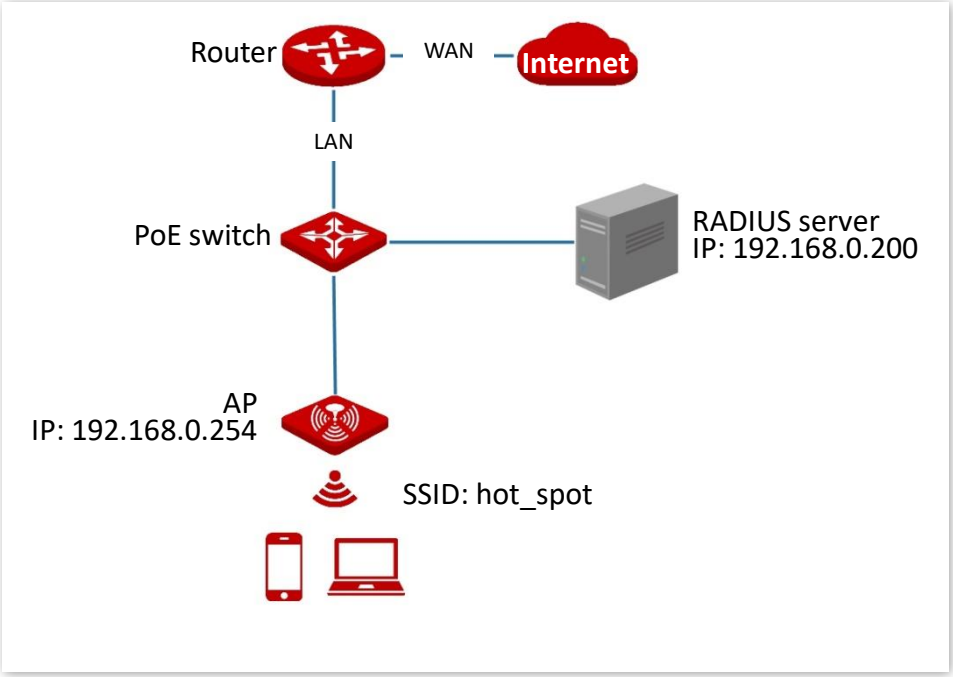
Verification

Wireless devices can connect to the **hotel** wireless network with the password **Hotel.123#**.

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. See the following figure.



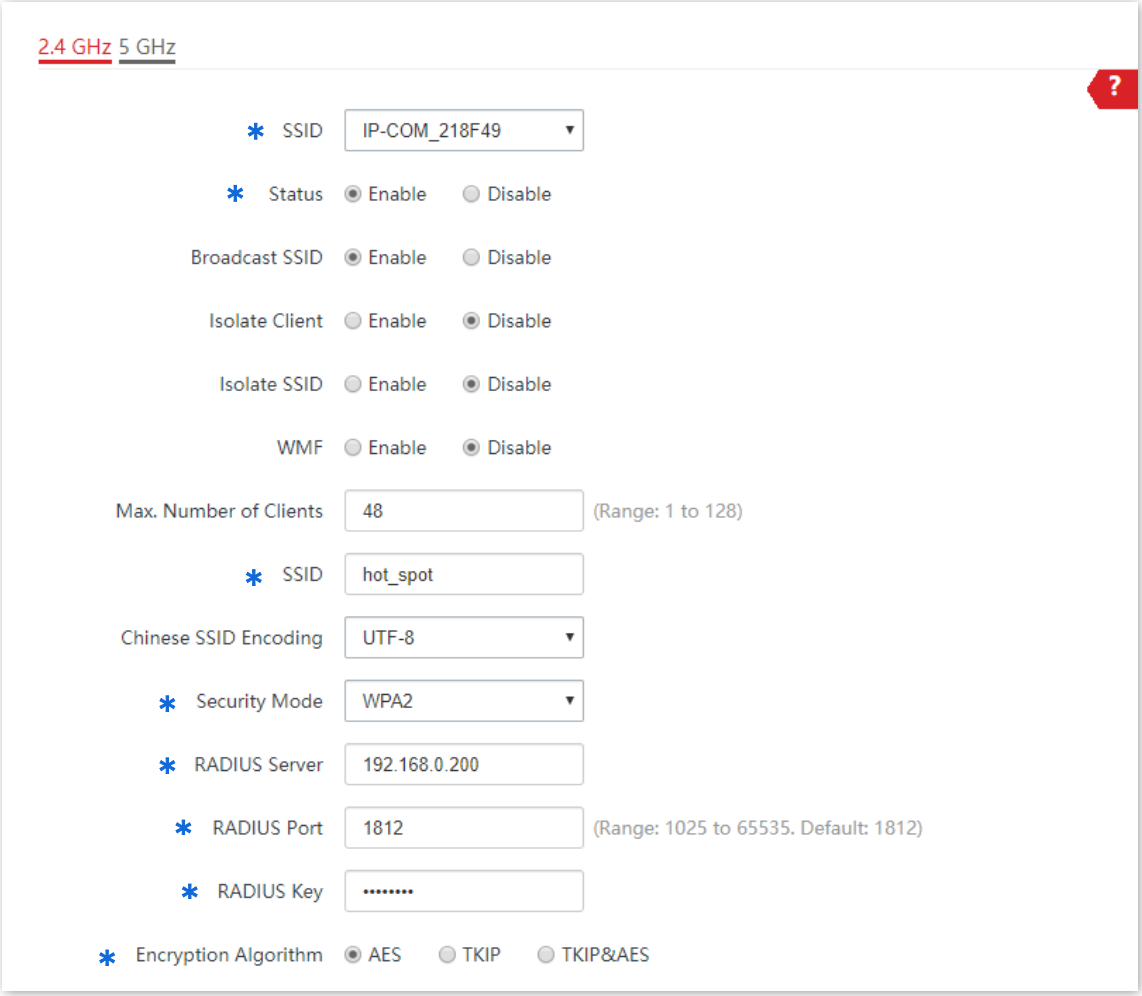
Configuration procedure

I. Configure the AP

Assume that the IP address of the RADIUS server is **192.168.0.200**, the Key is **12345678**, and the port number for authentication is **1812**.

Assume that the second SSID of the AP is used.

1. Choose **Wireless** > **SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Change the value of the **SSID** text box to **hot_spot**.
5. Set **Security Mode** to **WPA2**.
6. Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Password** to **192.168.0.200**, **1812**, and **12345678** respectively.
7. Set **Encryption Algorithm** to **AES**.
8. Click **Save**.



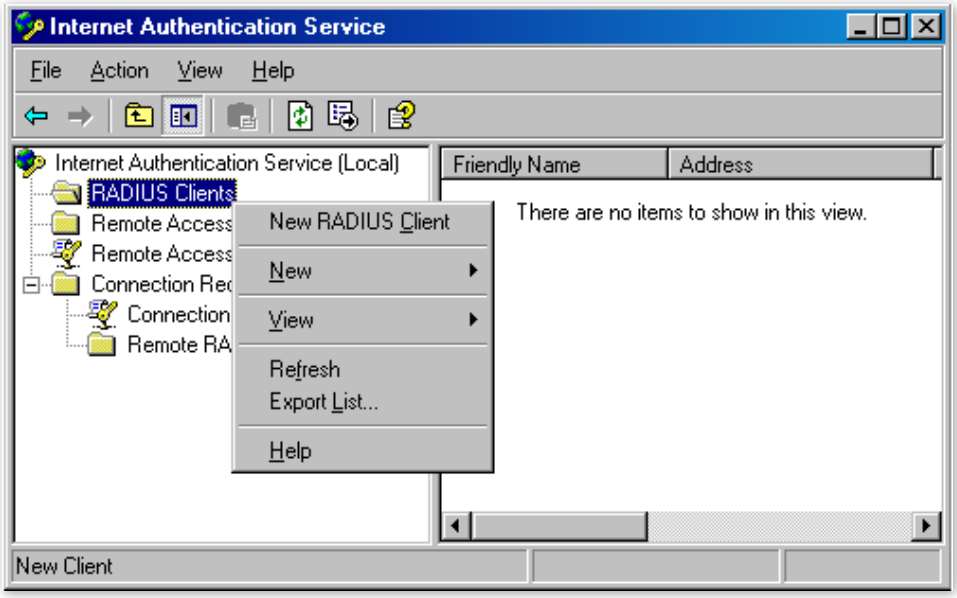
II. Configure the RADIUS server

Tip

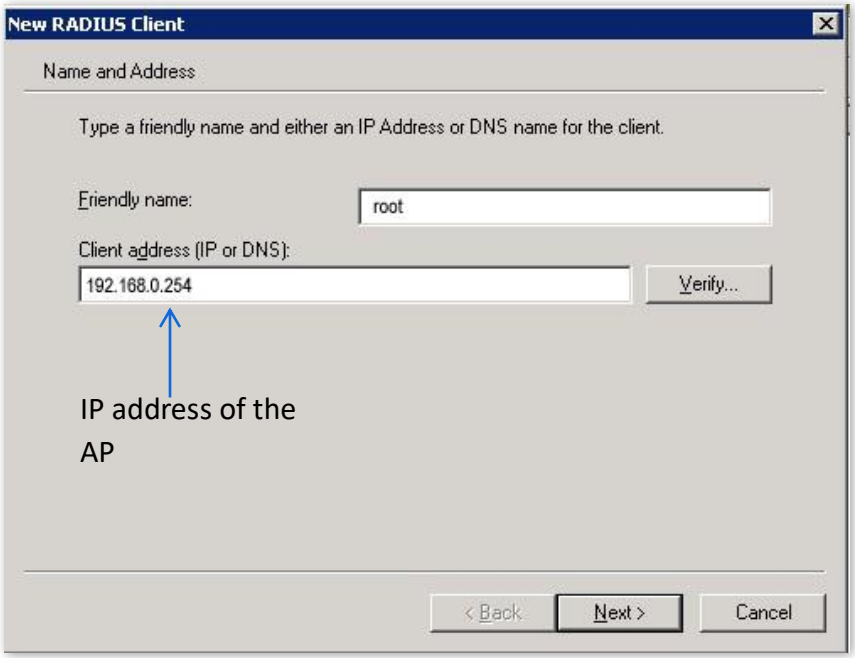
Windows 2003 is used as an example to describe how to configure the RADIUS server.

1. Configure a RADIUS client.

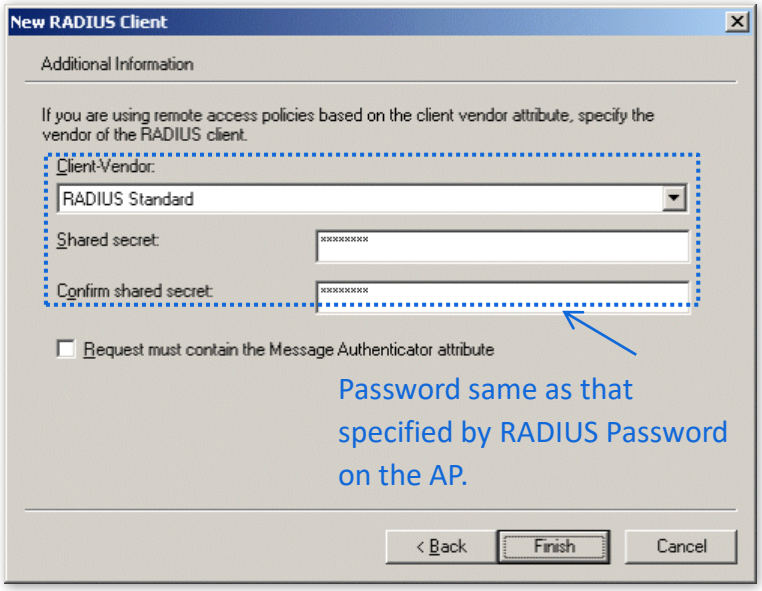
(1) In the **Computer Management** dialog box, double-click **Internet Authentication Service**, right-click **RADIUS Clients**, and choose **New RADIUS Client**.



(2) Enter a RADIUS client name (which can be the name of the AP) and the IP address of the AP, and click **Next**.

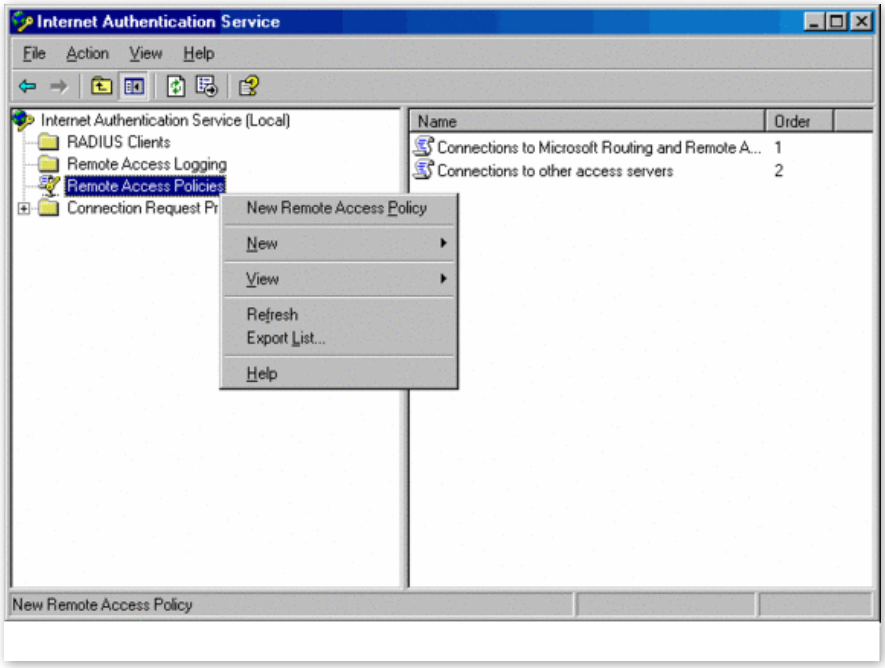


(3) Enter **12345678** in the **Shared secret** and **Confirm shared secret** text boxes, and click **Finish**.

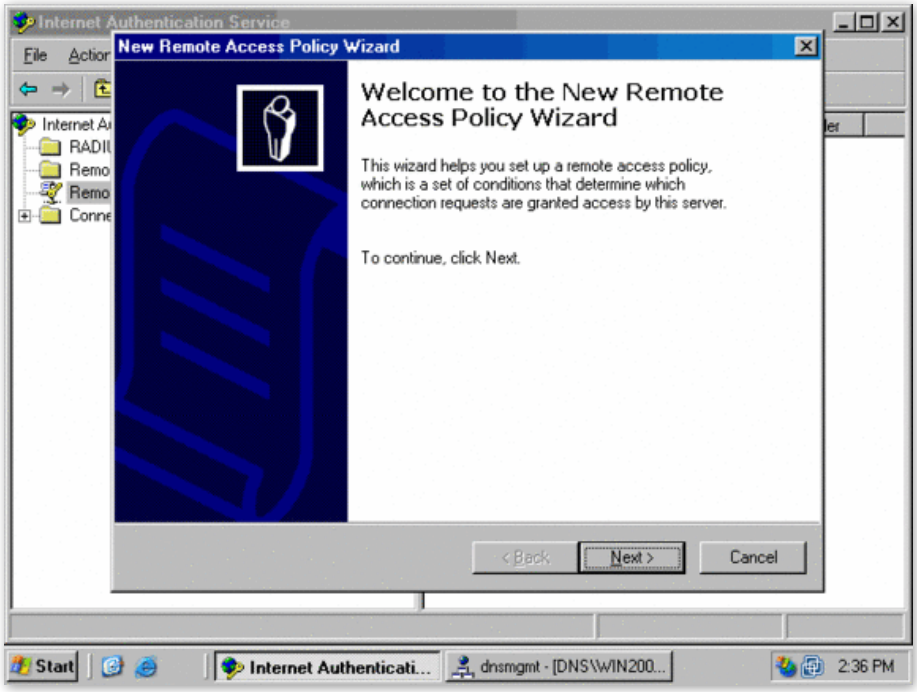


2. Configure a remote access policy.

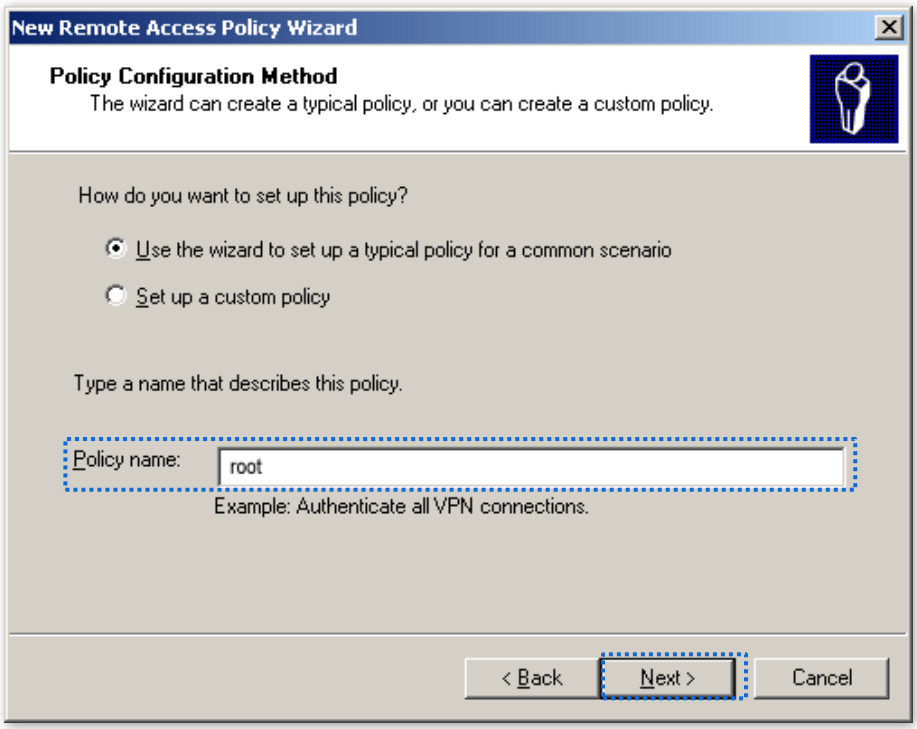
(1) Right-click **Remote Access Policies** and choose **New Remote Access Policy**.



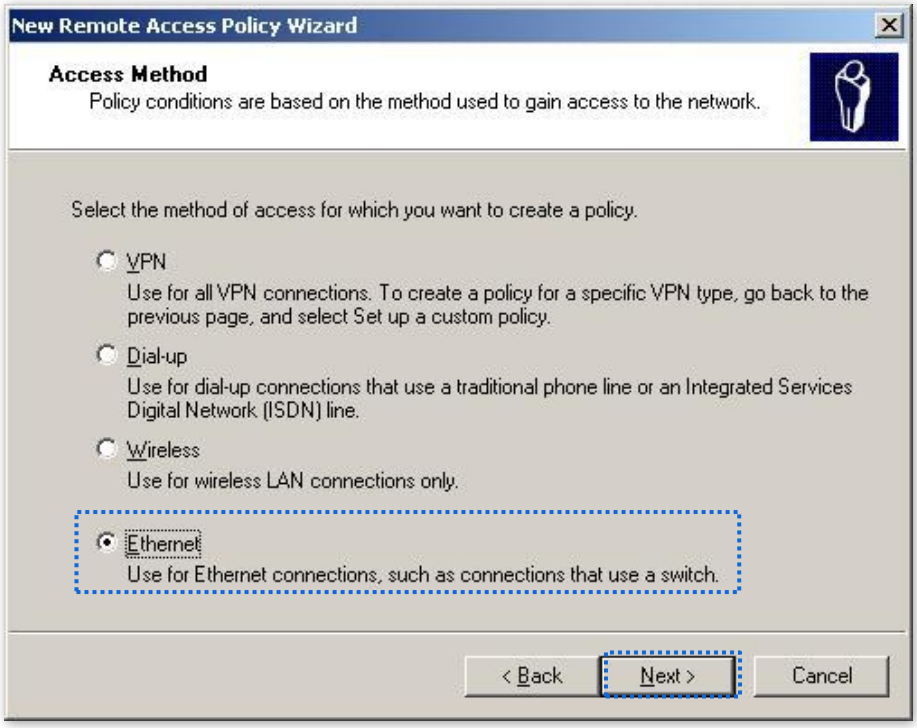
(2) In the **New Remote Access Policy Wizard** dialog box that appears, click **Next**.



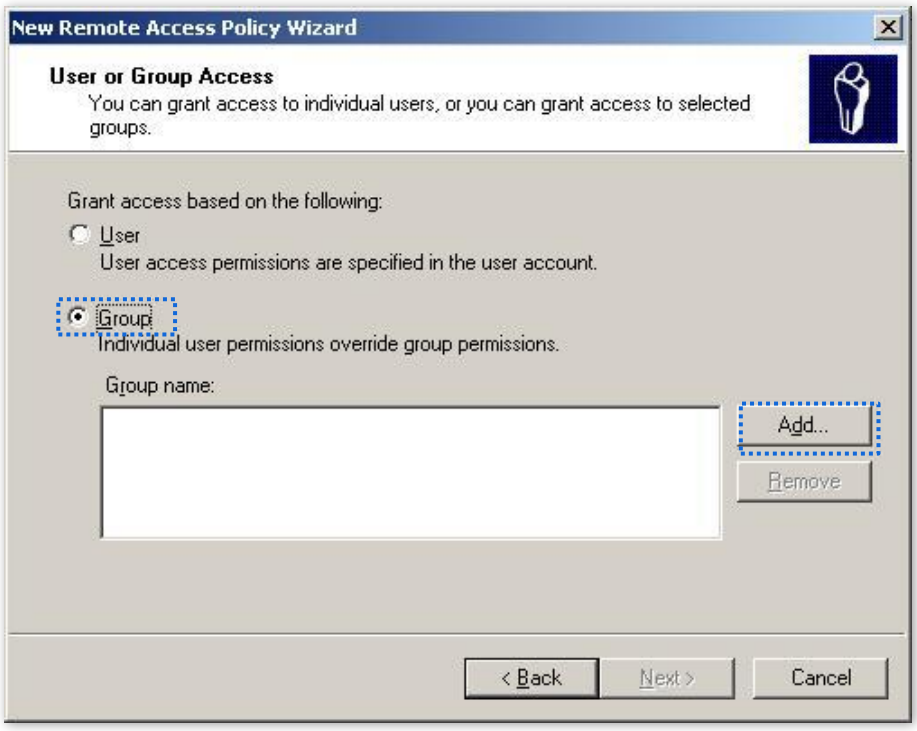
(3) Enter a policy name and click **Next**.



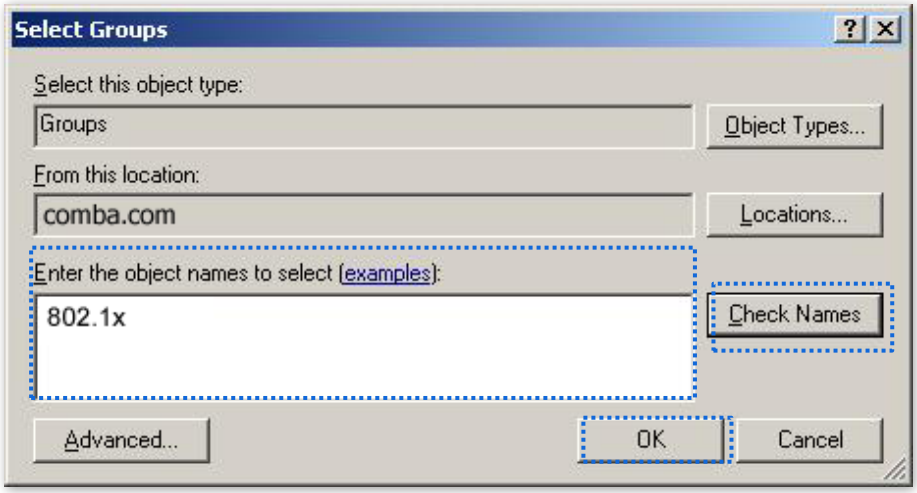
(4) Select **Ethernet** and click **Next**.



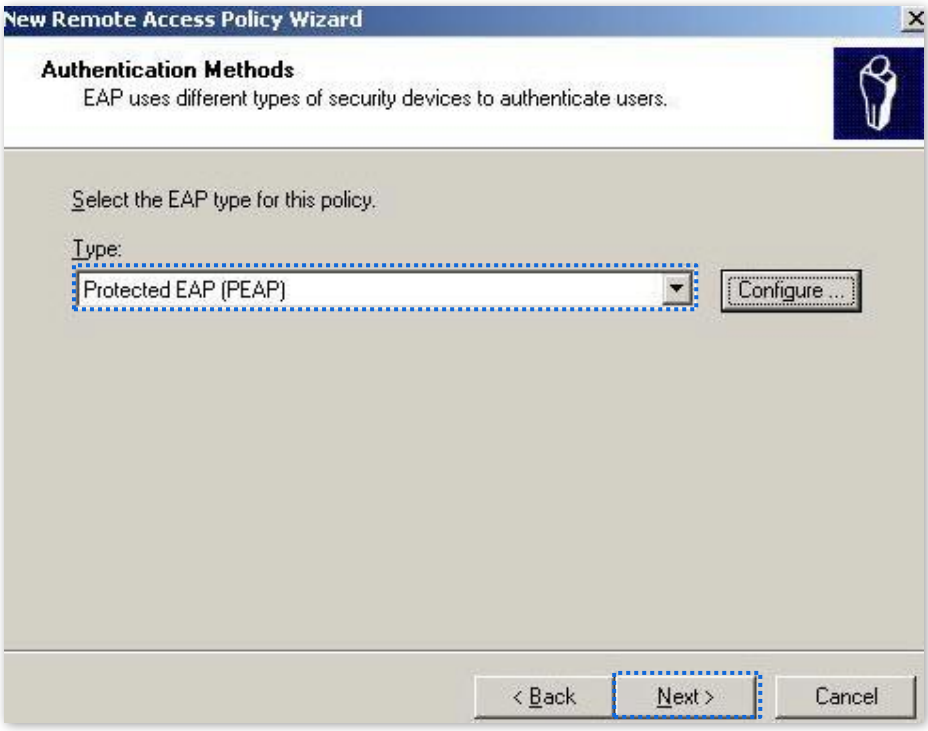
(5) Select **Group** and click **Add**.



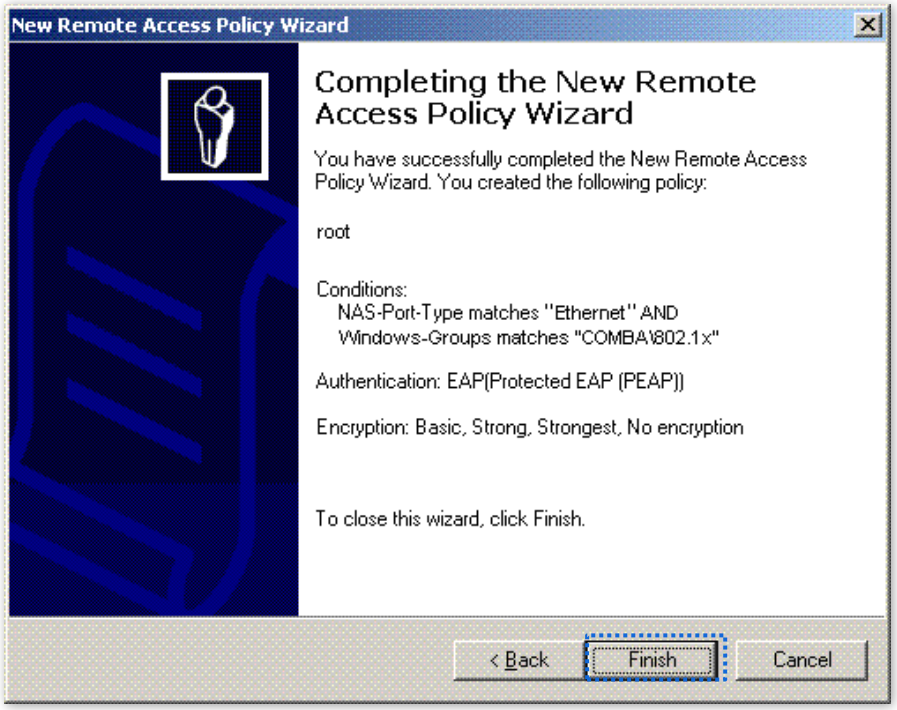
(6) Enter **802.1x** in the **Enter the object names to select** text box, click **Check Names**, and click **OK**.



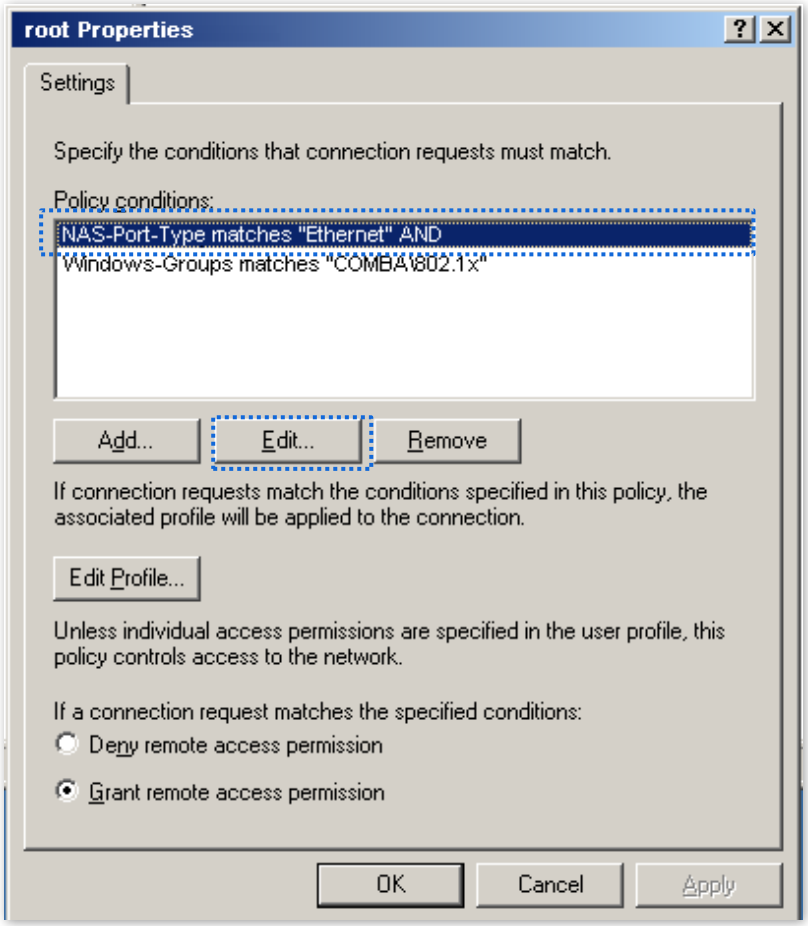
(7) Select **Protected EAP (PEAP)** and click **Next**.



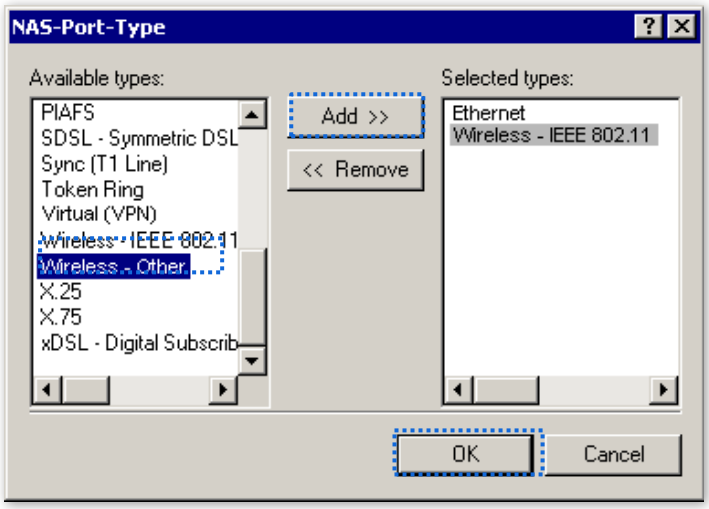
(8) Click **Finish**. The remote access policy is created.



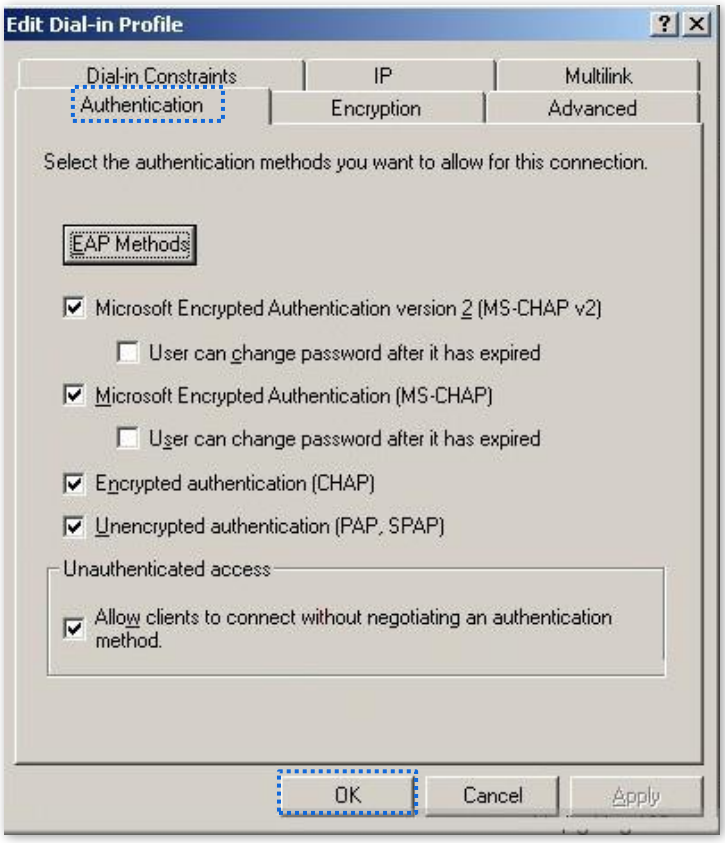
(9) Right-click **root** and choose **Properties**. Select **Grant remote access permission**, select **NAS-Port-Type matches "Ethernet" AND**, and click **Edit**.



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



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



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

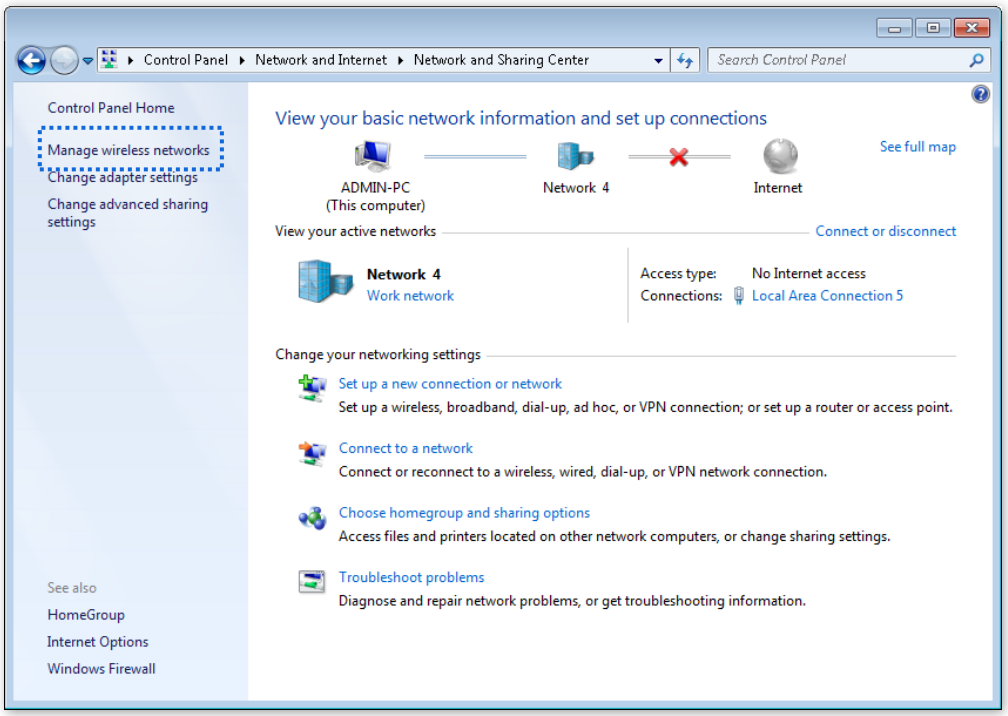
3. Configure user information.
Create a user and add the user to group **802.1x**.

III. Configure your wireless device

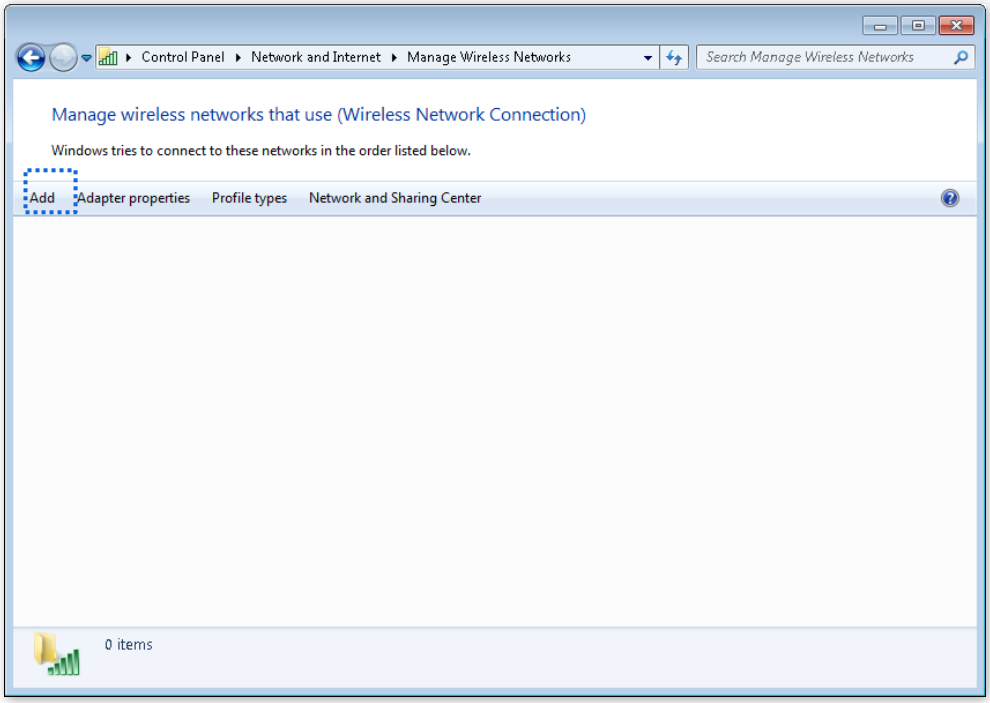
Tip

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

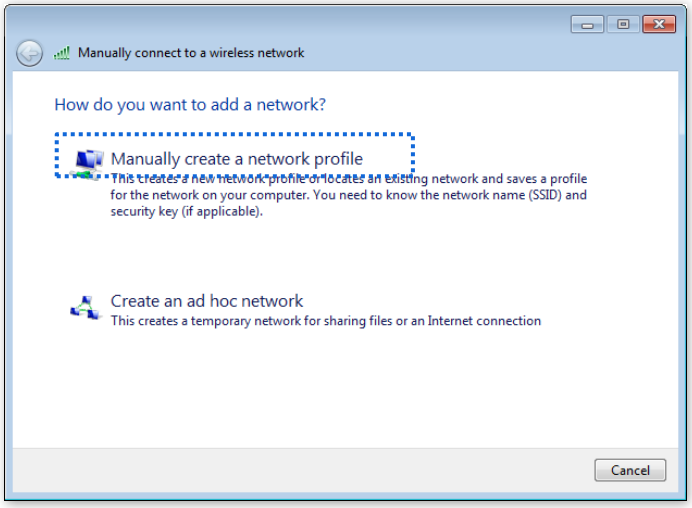
1. Choose **Start** > **Control Panel**, click **Network and Internet**, click **Network and Sharing Center**, and click **Manage wireless networks**.



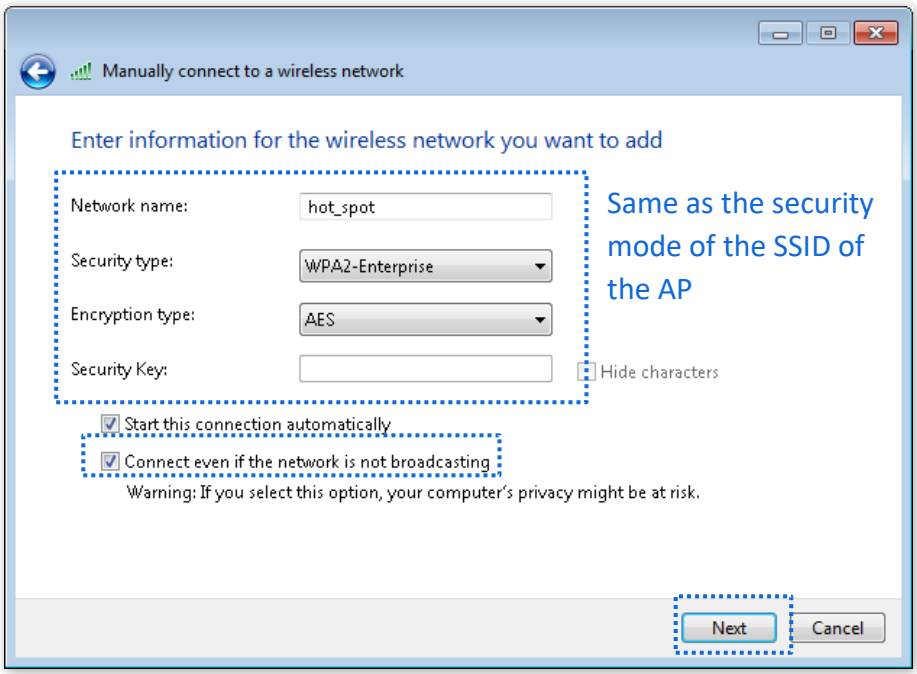
2. Click **Add**.



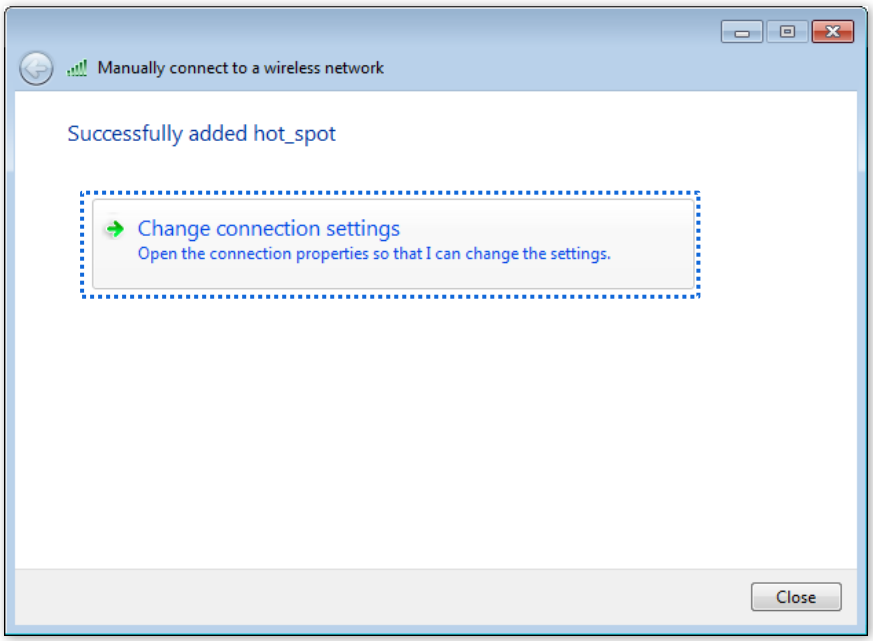
3. Click **Manually create a network profile**.



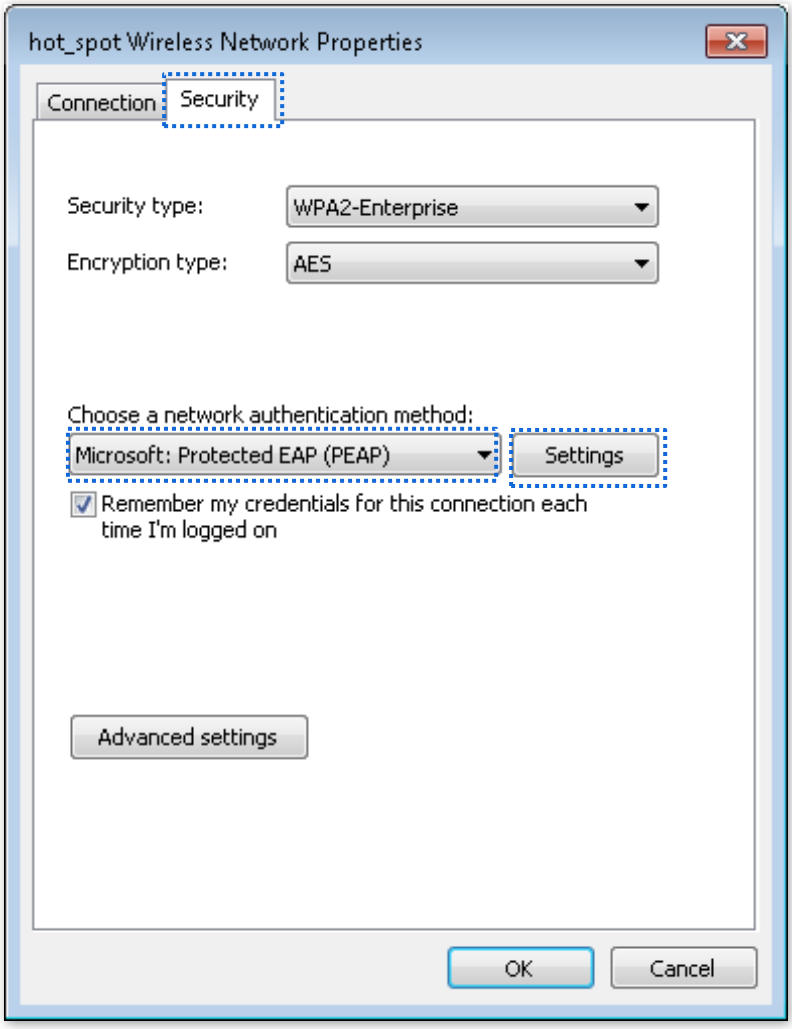
4. Enter wireless network information, select **Connect even if the network is not broadcasting**, and click **Next**.



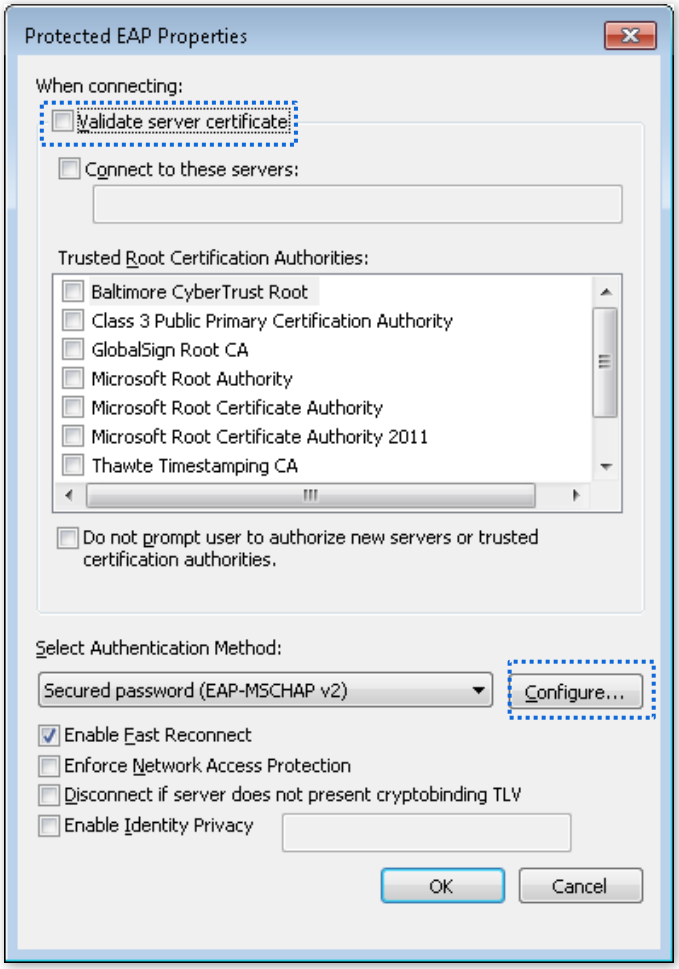
5. Click **Change connection settings**.



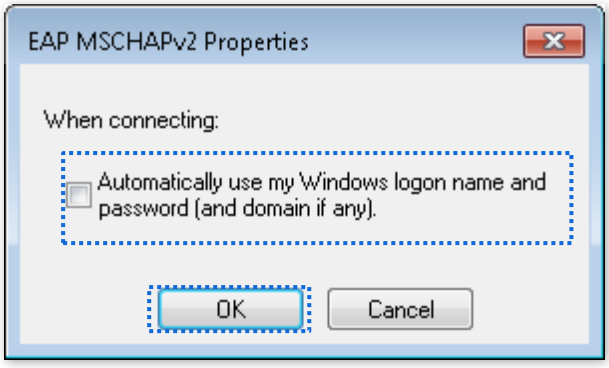
6. Click the **Security** tab, select **Microsoft: Protected EAP (PEAP)**, and click **Settings**.



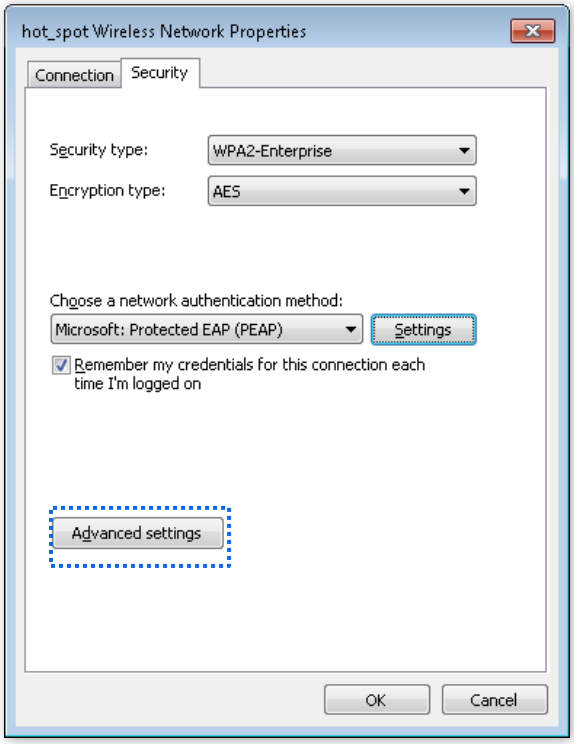
7. Deselect **Validate server certificate** and click **Configure**.



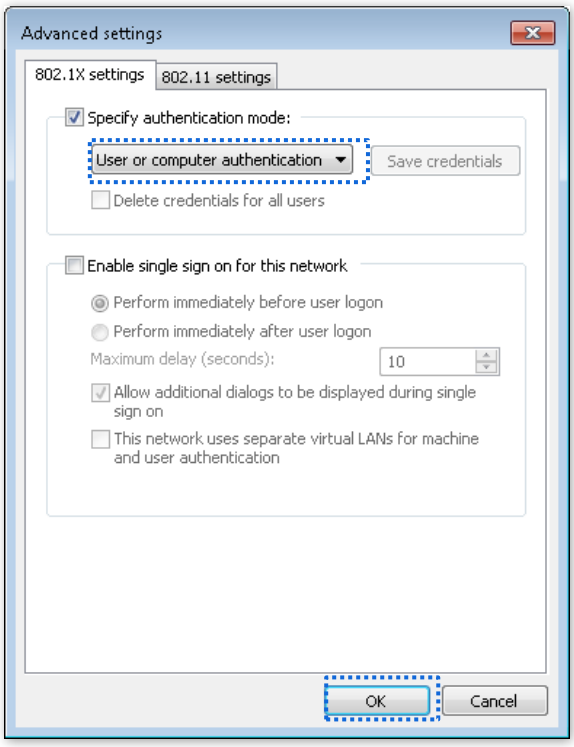
8. Deselect **Automatically use my Windows logon name and password (and domain if any)** and click **OK**.



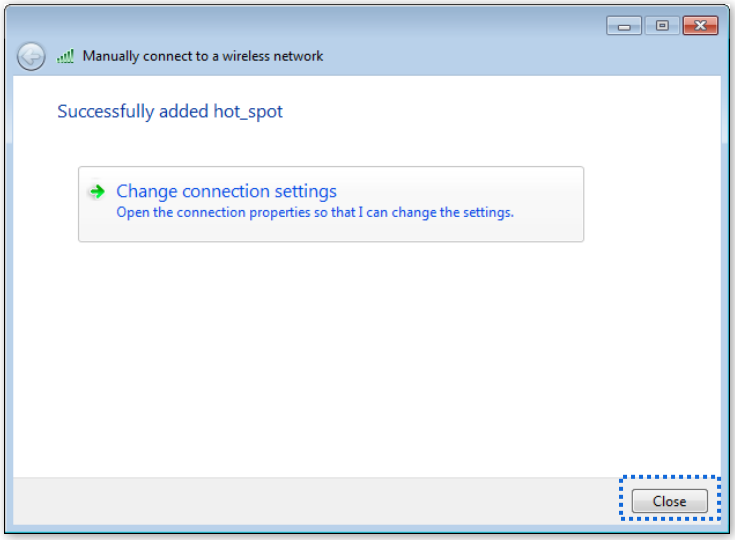
9. Click **Advanced settings**.

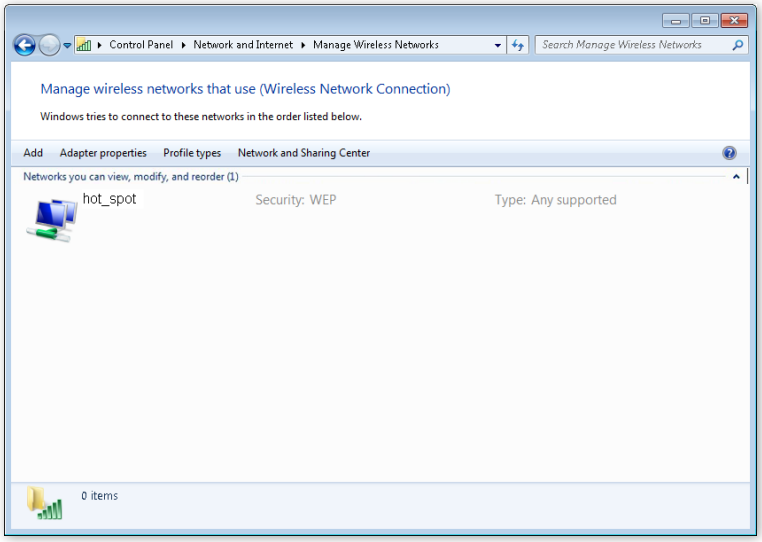


10. Select **User or computer authentication** and click **OK**.

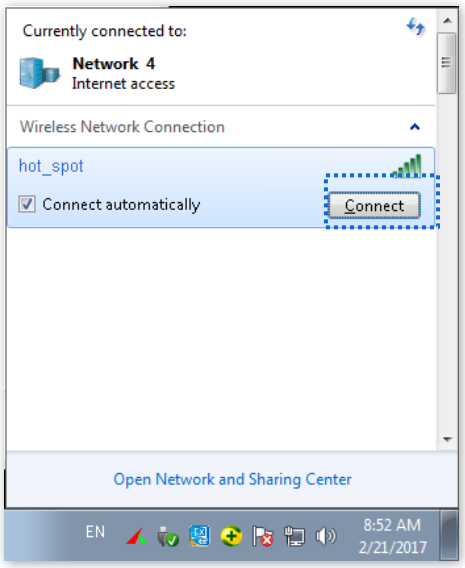


11. Click **Close**.

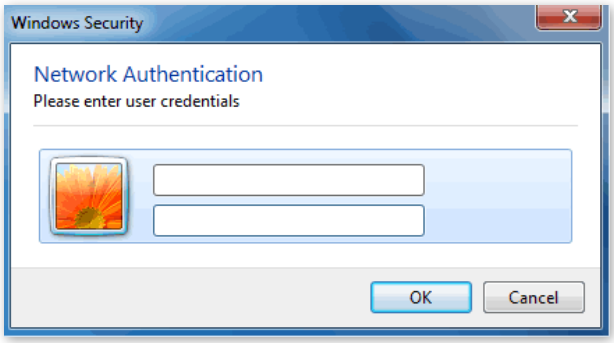




12. Click the network icon in the lower-right corner of the desktop and choose the wireless network of the AP, such as **hot_spot** in this example.



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



---End

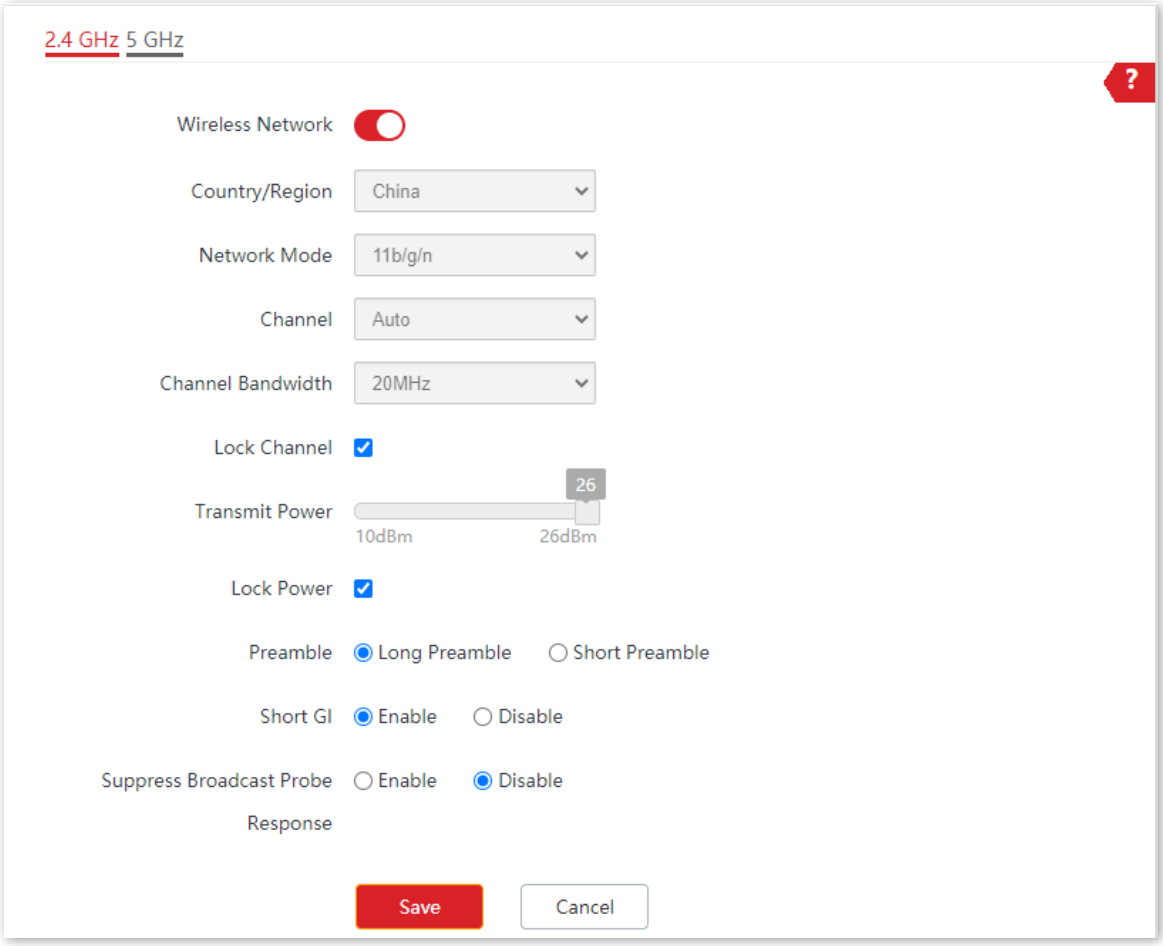
Verification

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, such as channel, power, and short GI.

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



Parameter description

Parameter	Description
Wireless Network	It specifies whether to enable the radio 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. The default value is **China**. This parameter can be set if **Lock Channel** is not selected.

Parameter	Description
Network Mode	It specifies the wireless network mode of the AP. This parameter can be set if **Lock Channel** is not selected. Available options for 2.4 GHz are **11b**, **11g**, **11b/g**, **11b/g/n**, and **11b/g/n/ax**, and available options for 5 GHz are **11a**, **11ac**, **11a/n**, and **11a/n/ac/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. – **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. This parameter can be set if **Lock Channel** is not selected. **Auto**: It indicates that the AP automatically adjusts its operating channel according to the ambient environment.
Channel Bandwidth	It specifies the wireless channel bandwidth of the AP. This parameter can be set if the AP works in 802.11 b/g/n, 802.11b/g/n/ax, 802.11ac, 802.11a/n, or 11a/n/ac/ax mode and **Lock Channel** is not selected. – **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**: It indicates that the AP automatically adjusts its channel bandwidth to 20 MHz or 40 MHz according to the ambient environment. – **80MHz**: It indicates that the AP can use only 80 MHz channel bandwidth. – **160MHz:** It indicates that the AP can use only 160 MHz channel bandwidth. – **20/40/80/160 MHz:** 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.

Parameter	Description
Lock Channel	It is used to lock the channel settings of the AP. If this parameter is selected, channel settings including **Country/Region**, **Network Mode**, **Channel**, **Channel Bandwidth**, and **Expansion Channel** cannot be changed.
Transmit Power	It specifies the transmit power of the AP. A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the wireless network performance and security.
Lock Power	It specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.
Preamble	A preamble is a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. By default, the **Long Preamble** option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the **Short Preamble** option.
Short GI	Short Guard Interval. There is a delay on the receiving side due to multipath and other factors during the wireless signal transmission in space. If the subsequent data block is transmitted too quickly, it will interfere with the previous data block, and the short guard interval can be used to circumvent this interference. Short GI helps to increase the wireless throughput by 10%.
Suppress Broadcast Probe Response	By default, wireless devices keep sending Probe Request packets that include the SSID field to scan their nearby wireless networks. After receiving such packets, this device determines whether the wireless devices are allowed to access its wireless networks based on the packets and responds using the Probe Response packets (including all Beacon frame parameters), which consumes a lot of wireless resources. After this function is enabled, this device does not respond to the requests without an SSID, saving wireless resources.

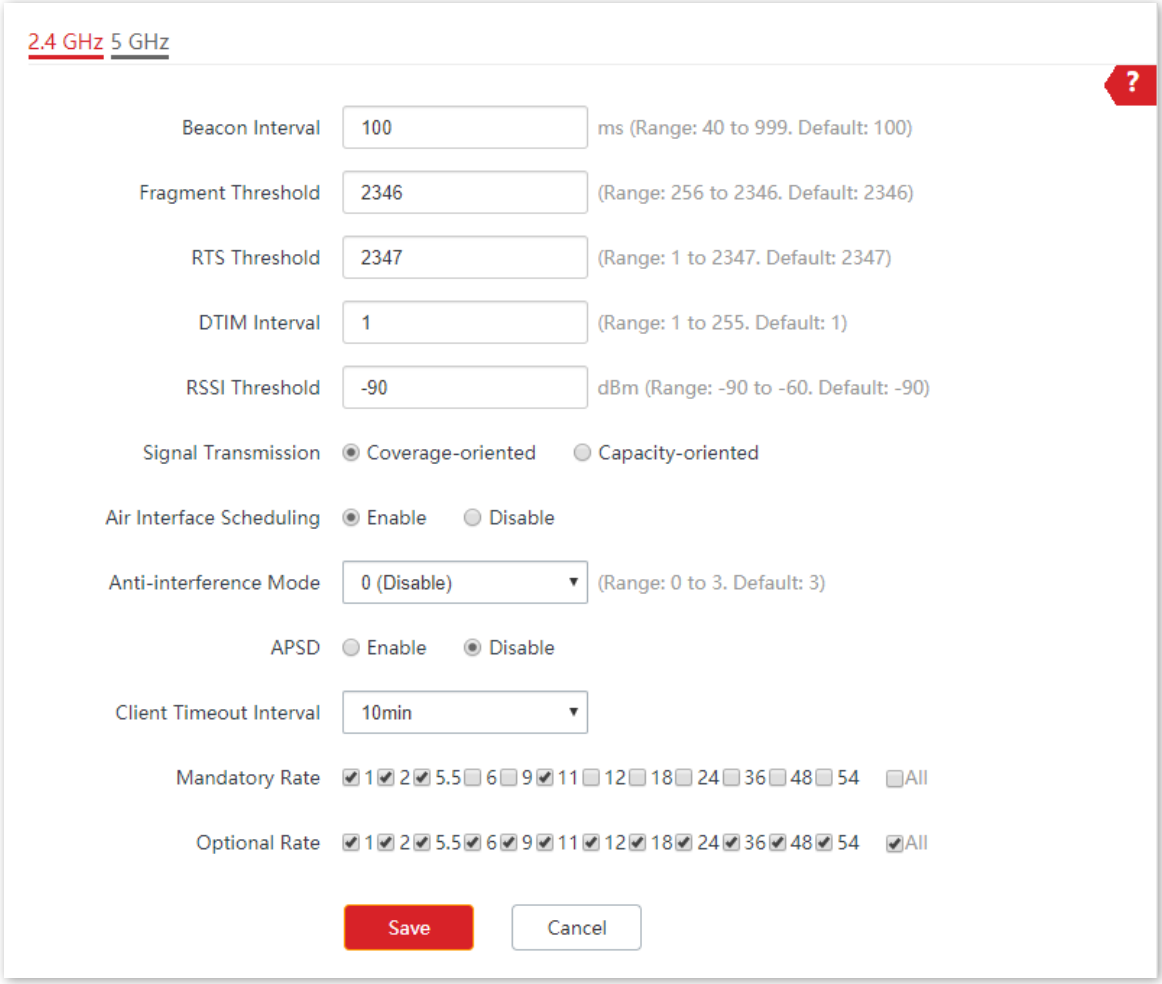
6.3 RF Optimization

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.



Parameter description

Parameter	Description
Beacon Interval	Used to set the interval at which this device sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a wireless network. Generally, a smaller interval allows wireless clients to connect to this device sooner, while a larger interval allows the wireless network to transmit data quicker.

Parameter	Description
Fragment Threshold	It specifies the threshold of a fragment. Fragmenting is a process that divides a frame into several fragments, which are transmitted and acknowledged separately. If the size of a frame exceeds this threshold, the frame is fragmented. In case of a high error rate, you can reduce the threshold to enable this device to resend only the fragments that have not been sent successfully, so as to increase the frame throughput. In an environment with little interference, you can increase the threshold to reduce the number of frames, so as to increase the frame throughput.
RTS Threshold	It specifies the frame length threshold for triggering the RTS/CTS mechanism. The unit is byte. If a frame exceeds this threshold, the RTS/CTS mechanism is triggered to reduce conflicts. Set the RTS threshold based on the actual situation. An excessively small value increases the RTS frame transmission frequency and bandwidth requirement. A higher RTS frame transmission frequency enables a wireless network to recover from conflicts quicker. For a wireless network with high user density, you can reduce this threshold to reduce conflicts. The RTS mechanism requires some network bandwidth. Therefore, it is triggered only when frames exceed this threshold.
DTIM Interval	It specifies the countdown before this device transmits broadcast and multicast frames in its cache. The unit is Beacon interval. For example, if **DTIM Interval** is set to **1**, this device transmits all cached frames at one Beacon interval.
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.
Signal Transmission	- **Coverage-oriented**: This mode broadens WiFi coverage of APs, and is usually used in scenarios deployed with fewer APs, such as offices, warehouses, and hospitals. - **Capacity-oriented**: This mode effectively decreases mutual interference among APs, and is usually used in scenarios deployed with massive APs, such as conferences, exhibition halls, banquet halls, stadiums, classrooms of higher-education institutes, airports and so on.

Parameter	Description
Deployment Mode (for Pro-6-Lite)	- **Default**: This mode is applicable to most application scenarios. - **Coverage-oriented**: This mode broadens WiFi coverage of APs but also increases the interference to APs. It is applicable to such scenarios with low AP deployment density as warehouses and hotel corridors. - **Capacity-oriented**: This mode reduces WiFi coverage of APs but also decreases the interference to APs. It is applicable to such scenarios with high AP deployment density as conference rooms, classrooms, exhibition halls, and banquet halls.
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.
Air Interface Scheduling	Used to enable or disable 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.
Anti-interference Mode	It specifies the anti-interference modes you can select for your AP. - **0 (Disable):** Interference suppression measures are disabled. - **1 (Suppress weak interference):** Suppress mild interference for weak radio environment. - **2 (Suppress moderate interference):** Suppress moderate interference for bad radio environment. - **3 (Suppress critical interference):** Suppress critical interference for heavy loading radio environment.
APSD	Automatic Power Save Delivery. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
MU-MIMO	Multi-User Multiple-Input Multiple-Output. If this function is 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. However, this function may cause compatibility issues; therefore, you are recommended to disable this function to avoid compatibility issues.

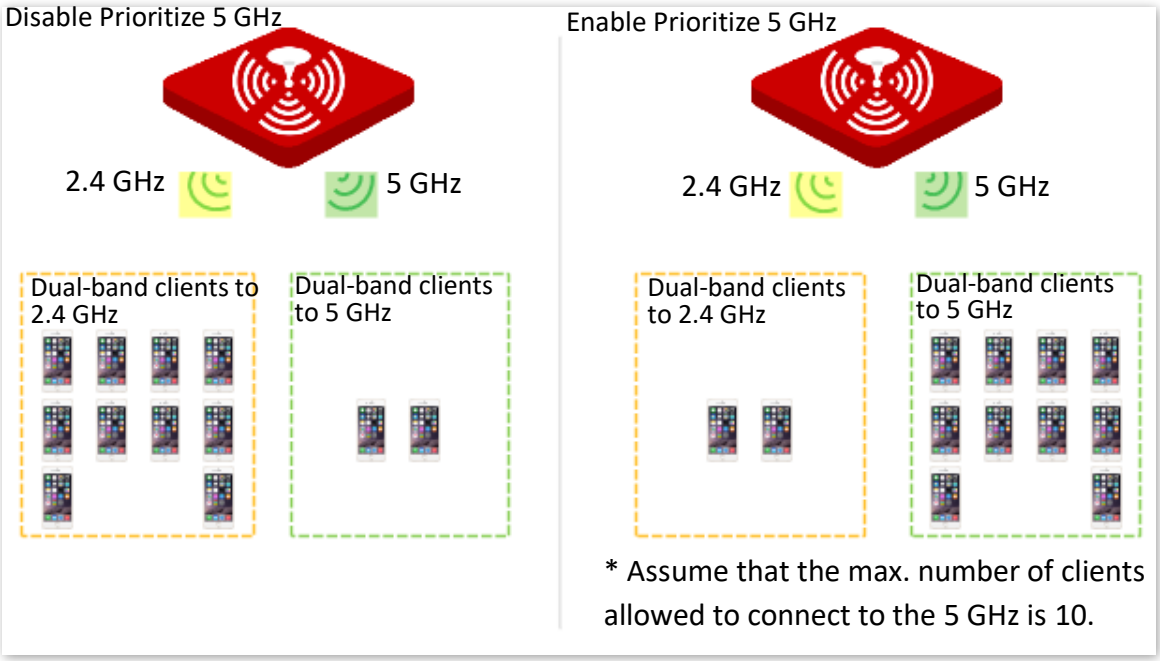
Parameter	Description
Client Timeout Interval	Used to set the wireless client disconnection interval of this device. The device disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.
Mandatory Rate	It specifies rates that wireless clients must support in order to connect to the wireless networks of this device.
Optional Rate	It specifies the additional rates that the AP supports, which are optional to wireless clients. The clients meeting the basic requirement can connect to the AP with higher rate.

- **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.

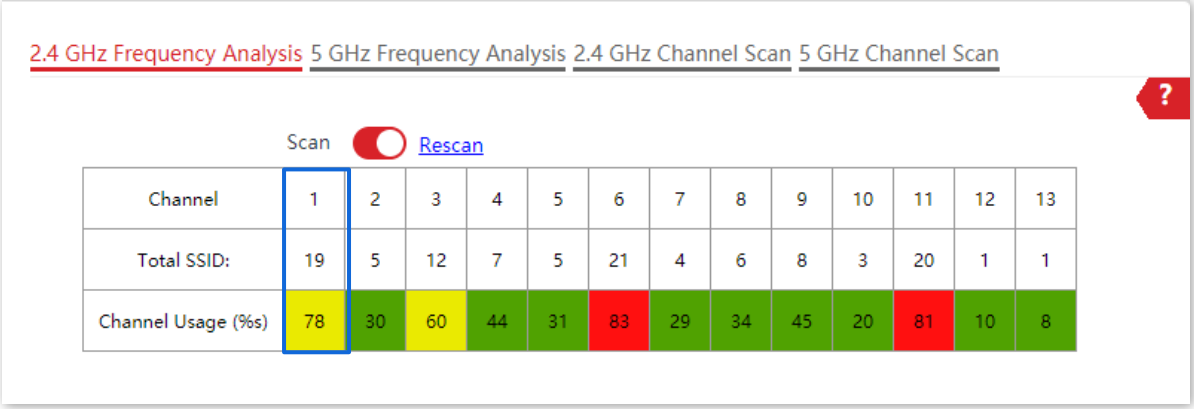
6.4 Frequency Analysis

The Frequency Analysis page allows you to analyze frequency and the Channel Scan page allows you to scan channels.

To access the pages, choose **Wireless** > **Frequency Analysis**.

- **Frequency Analysis**

From the intuitive result, you can check how many wireless networks (total SSID) use the same channel and choose a channel with low usage as the operating channel of the device for better wireless transmission efficiency. See the following figure.

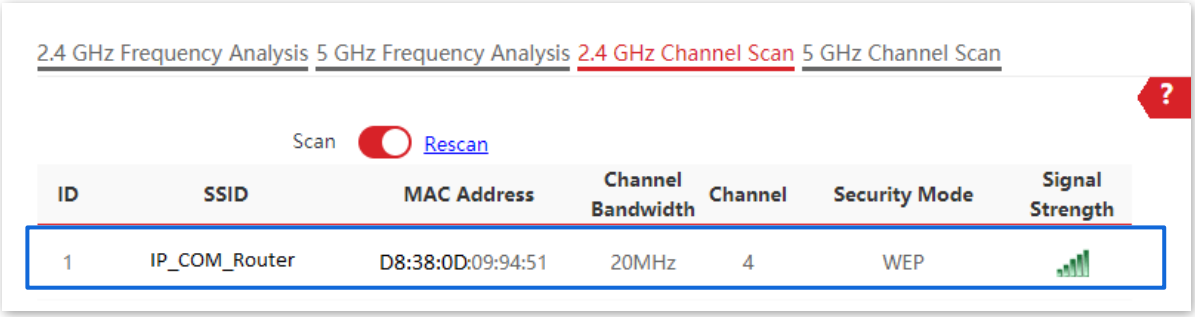


Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Total SSID:	19	5	12	7	5	21	4	6	8	3	20	1	1
Channel Usage (%s)	78	30	60	44	31	83	29	34	45	20	81	10	8

- : High channel usage. The channel is not recommended to use.
- : Moderate channel usage.
- : Low channel usage. The channel is recommended to use.

- **Channel Scan**

The scan result list presents you with information about nearby wireless network, including SSID, MAC address, channel, channel bandwidth, security mode, and signal strength. See the following figure.



6.5 WMM

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 voice and video service experience over wireless 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 AC-VO (voice stream), AC-VI (video stream), AC-BE (best effort), and AC-BK (background) 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.

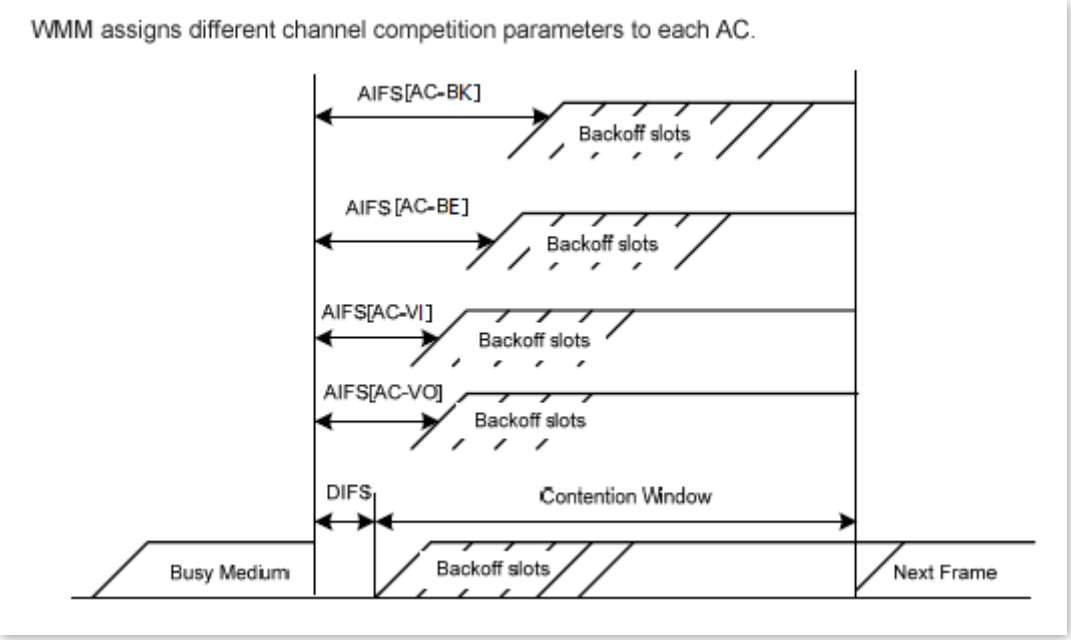
- **EDCA Parameters**

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. This helps achieve different service levels for different ACs.

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**

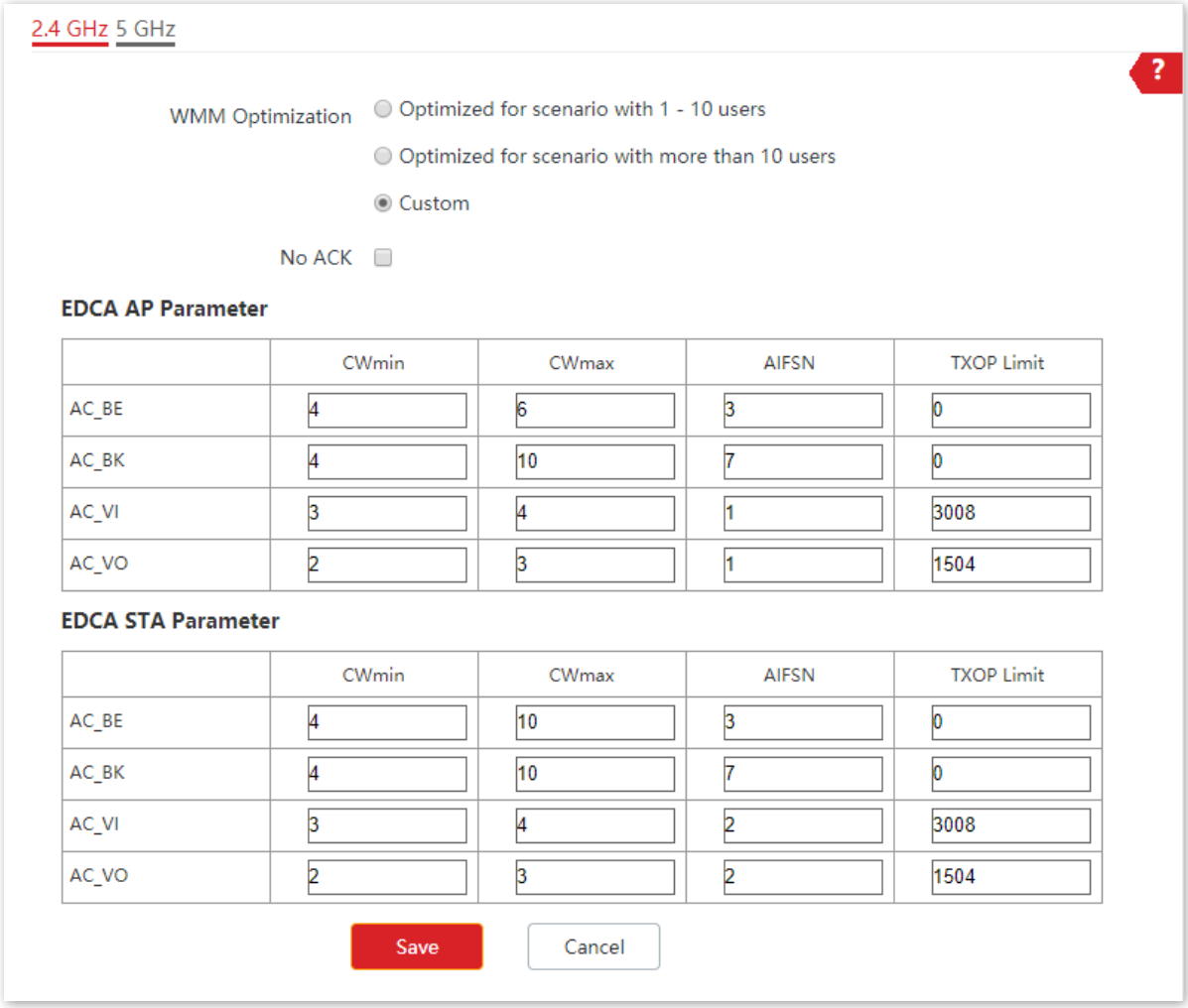
WMM specifies the Normal ACK and No ACK policies.

- 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 will not be resent if this policy is adopted. This leads to 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.

- **WMM Configurations**

The WMM page allows you to configure related WMM parameters.

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



Parameter description

Parameter	Description
WMM Optimization	It specifies the WMM optimization modes supported by the AP: – **Optimized for scenario with 1 - 10 users**: If 10 or less clients are connected to the AP, you are recommended to select this mode to obtain higher client throughput. – **Optimized for scenario with more than 10 users**: If more than 10 clients are connected to the AP, you are recommended to select this mode to ensure client connectivity. – **Custom**: This mode enables you to set the WMM EDCA parameters for manual optimization.
No ACK	If the check box is selected, the No ACK policy is adopted. If the check box is deselected, the Normal ACK policy is adopted.
EDCA Parameters	For details, refer to EDCA Parameters.

6.6 Access Control

6.6.1 Overview

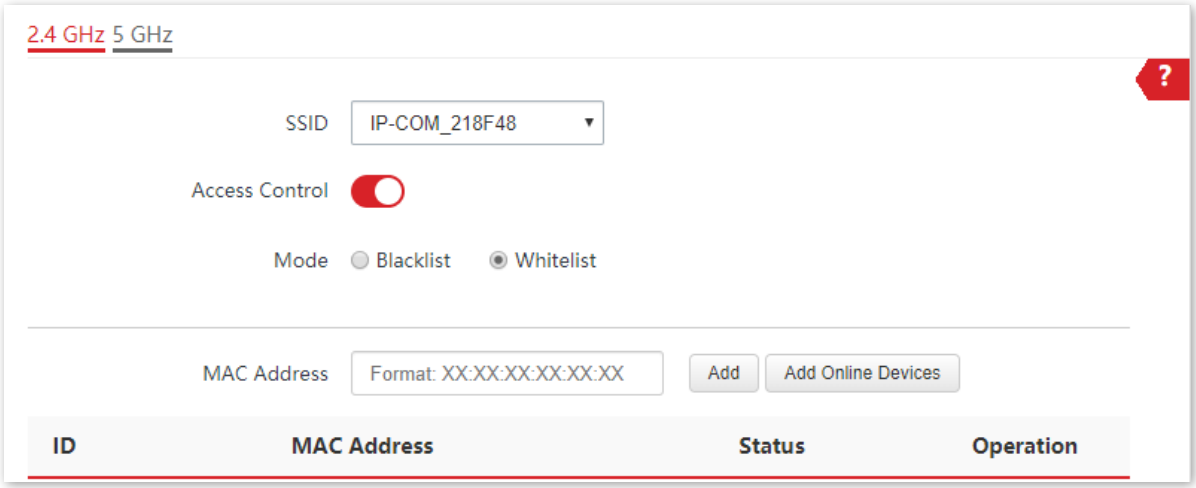
The Access Control page allows you to allow or disallow the wireless devices to access the wireless network of the AP based on their MAC addresses.

To access the page, choose **Wireless** > **Access Control**.

The AP supports the following 2 filter modes:

- **Blacklist (Forbid only)**: It indicates that only the wireless devices with the specified MAC addresses cannot access the wireless networks of the AP.
- **Whitelist (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 (**Whitelist** is taken as an example).



Parameter description

Parameter	Description
SSID	It specifies the SSID on which the MAC address access control is implemented.
Access Control	It specifies whether or not to enable this function.
Mode	- **Blacklist (Forbid only)**: Only clients with MAC addresses on the access control list **cannot** access the wireless network of AP. - **Whitelist (Permit only)**: Only client with MAC addresses on the access control list **can** access the wireless network of AP.
MAC Address	It specifies the MAC address of client.

6.6.2 Configure Access Control

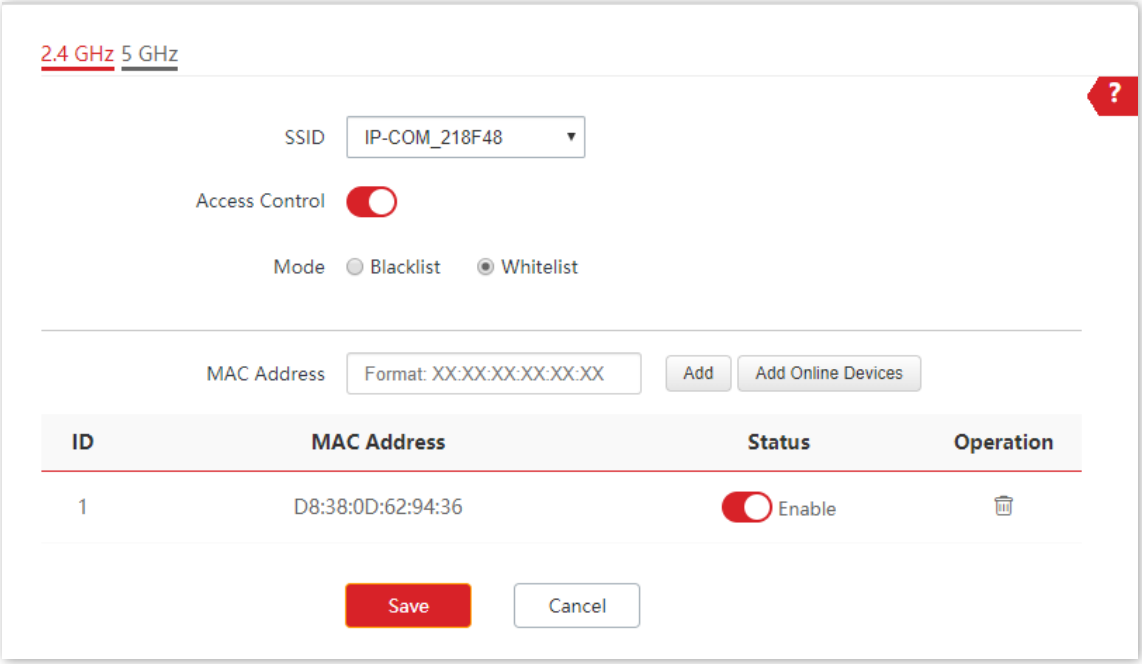
1. Choose **Wireless** > **Access Control**.

2. Choose a wireless network radio band on which access control is to be implemented.
3. From the **SSID** drop-down list box, select an SSID of the wireless network to which the rule applies.
4. Enable **Access Control** function.
5. Set **Mode** to **Blacklist** or **Whitelist**.
6. Enter the MAC address of the wireless device to which the rule applies.
7. 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.

8. Click **Save**.



---End

6.6.3 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.

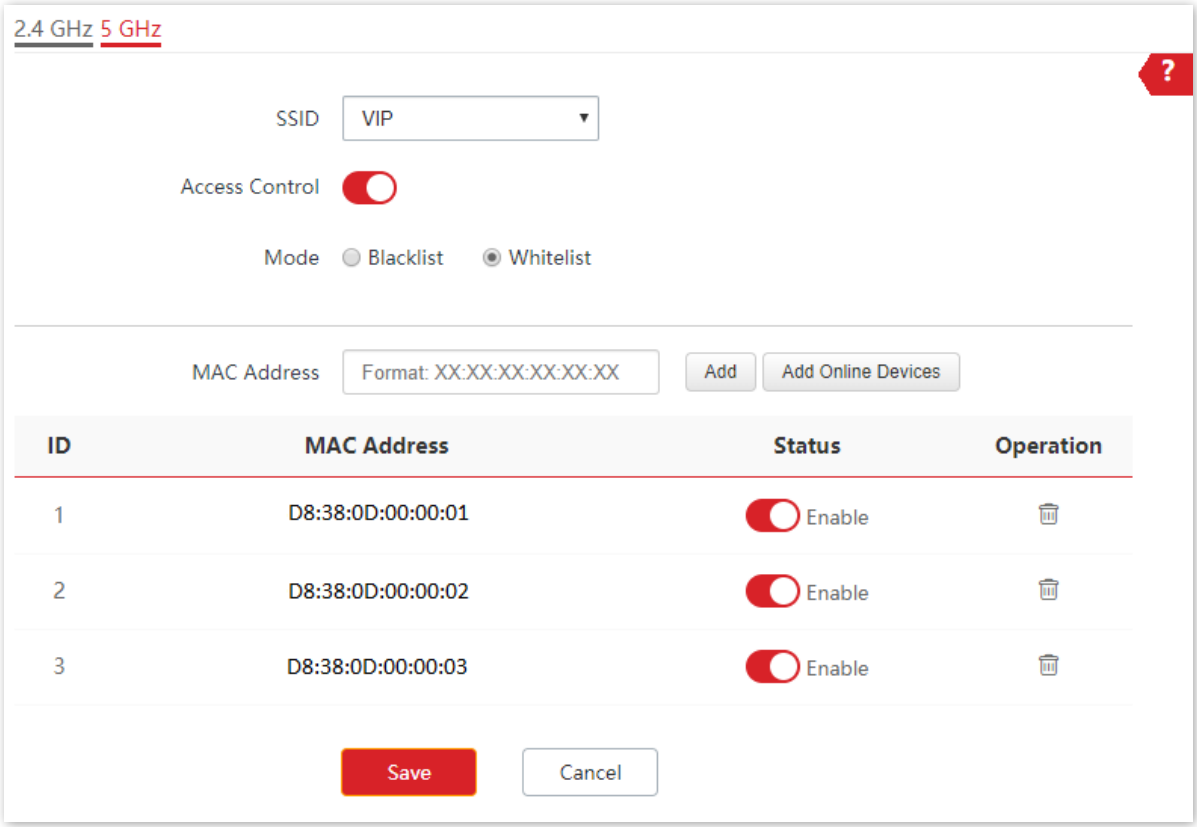
The Access Control function of the AP is recommended. The members have three wireless devices whose MAC addresses are **D8:38:0D:00:00:01**, **D8:38:0D:00:00:02**, and **D8:38:0D:00:00:03**.

Configuration procedure

1. Choose **Wireless** > **Access Control** > **5 GHz**.
2. Select **VIP** from the **SSID** drop-down list.
3. Enable **Access Control** function.
4. Set **Mode** to **Whitelist**.
5. Enter **D8:38:0D:00:00:01** in the **MAC Address** text box and click **Add**.
6. Repeat step 5 to add **D8:38:0D:00:00:02** and **D8:38:0D:00:00:03** as well.
7. Click **Save**.

---End

The following figure shows the configuration.



Verification

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

6.7 Advanced Settings

The Advanced Settings page allows you to set the **Identify Client Type** and **Broadcast Packet Filter** functions of the AP.

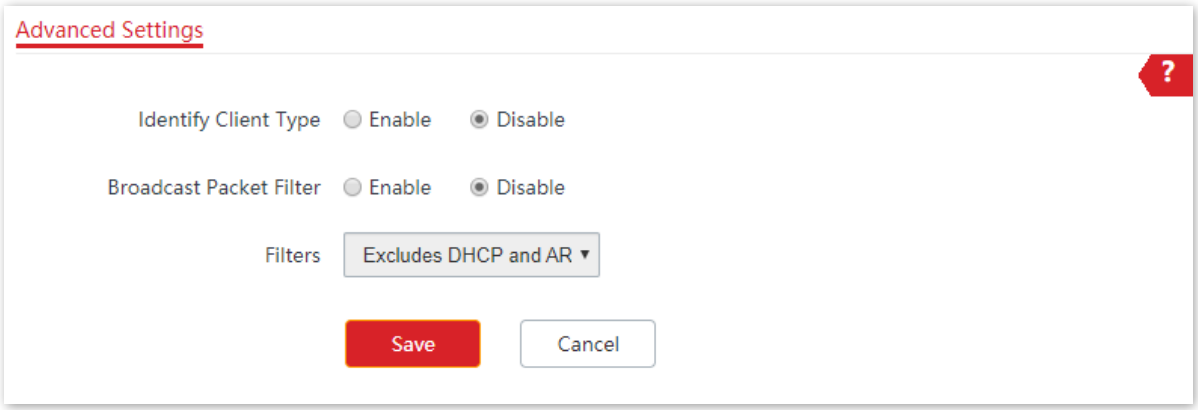
To access the page, choose **Wireless** > **Advanced Settings**.

- **Identify Client Type**

It specifies whether to identify operating system types of wireless clients connected to this device. Terminal types that the AP can identify include: Android, iOS, WPhone, Windows, and macOS.

- **Broadcast Packet Filter**

By default, this device forwards lots of invalid broadcast packets from wired networks, which may affect business data transfer. The broadcast packet filter function allows you to filter broadcast packets by types so that invalid packets are not forwarded. This reduces air interface resources usage and ensures more bandwidth for business data transfer.



Parameter description

Parameter	Description
Identify Client Type	If this function is enabled and the client connected to the AP has accessed an **http:// URL**, the operating system type of the client can be viewed by choosing **Status** > **Client List**.
Broadcast Packet Filter	If this function is enabled, the AP can reduce air interface resources usage and ensure the bandwidth for business data transfer.
Filters	Select a mode after you enable the **Broadcast Packet Filter** function. – **Excludes DHCP and ARP**: Filter out all broadcast or multicast data except DHCP and ARP packets. – **Excludes ARP**: Filter out all broadcast or multicast data except ARP packets.

6.8 QVLAN Settings

6.8.1 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.

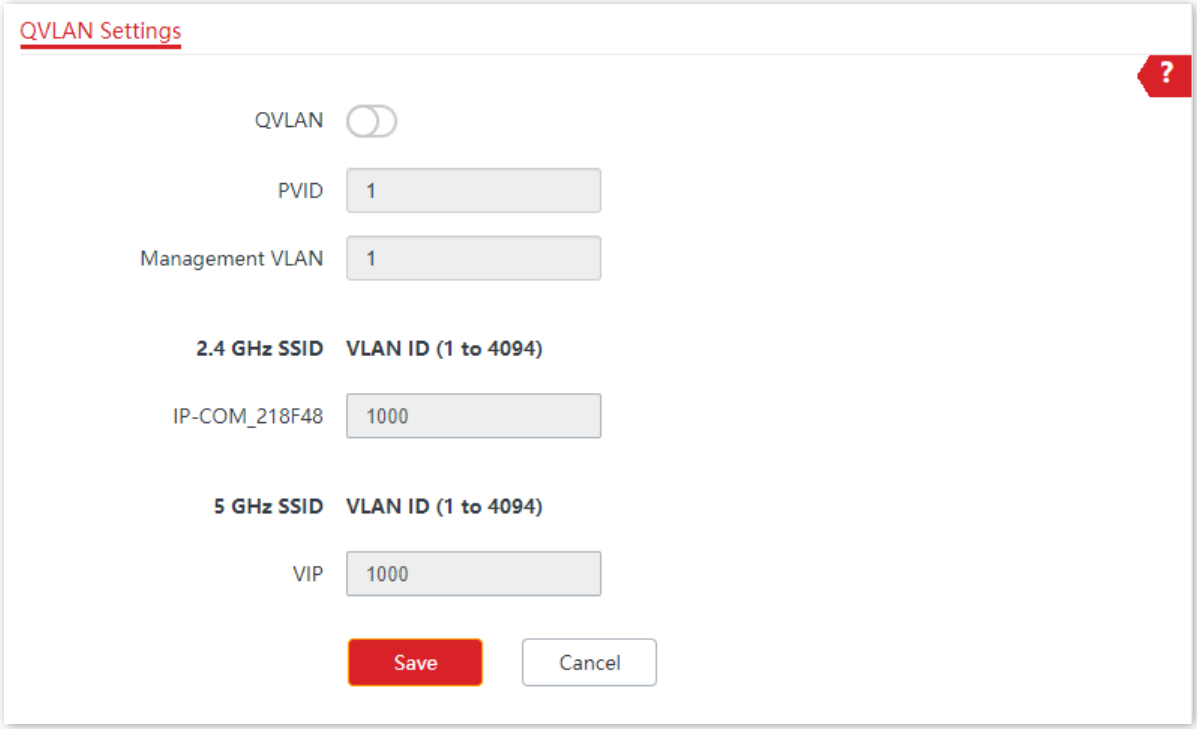
If the QVLAN function is enabled, tagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the VID in the data, whereas untagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the PVID of the port that receives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

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

<table>
<tr><th rowspan="2">Port</th><th colspan="2">Method to Process Received Data</th><th rowspan="2">Method to Process Transmitted Data</th></tr>
<tr><th>Tagged Data</th><th>Untagged Data</th></tr>
<tr><td>Access</td><td rowspan="2">Forward the data to other ports of the VLAN corresponding to the VID in the data.</td><td rowspan="2">Forward the data to the other ports of the VLAN corresponding to the PVID of the port that receives the data</td><td>Transmit data after removing tags from the data.</td></tr>
<tr><td>Trunk</td><td>If the VID and PVID of a port are the same, transmit data after removing tags from the data.
If the VID and PVID of a port are different, transmit data without removing tags from the data.</td></tr>
</table>

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

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



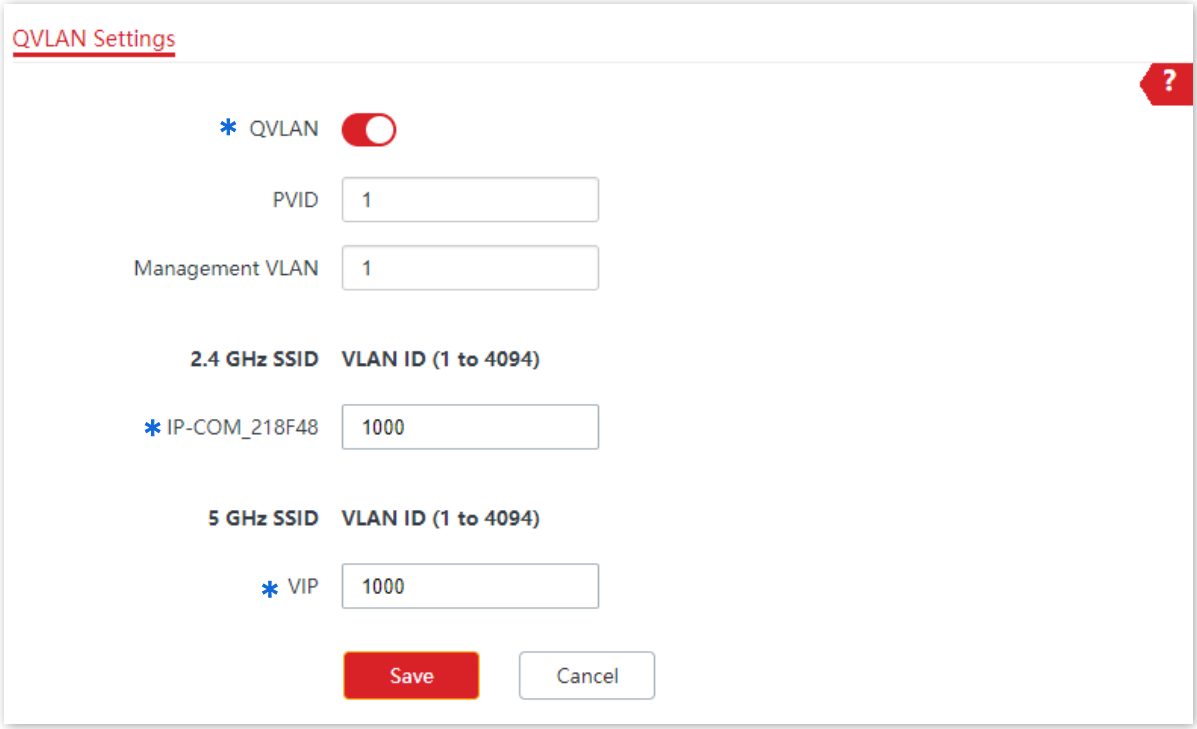
Parameter description

Parameter	Description
QVLAN	It specifies whether to enable the QVLAN function of the AP. By default, it is disabled.
PVID	It specifies the ID of the default native VLAN of the trunk port of the AP. After the QVLAN function is enabled, the LAN port is the trunk port. Traffic of all VLANs can pass through a trunk port. Its default value is **1**.
Management VLAN	It specifies the ID of the AP management VLAN. The default value is **1**. 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.

Parameter	Description
LAN Port VLAN ID	It specifies the Ethernet port of the AP and the ID of the VLAN to which a LAN port belongs. The default ID is **1**. – 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	It specifies the currently enabled SSID of the AP at 2.4 GHz band.
5 GHz SSID	It specifies the currently enabled SSID of the AP at 5 GHz band.
VLAN ID	It specifies VLAN IDs corresponding to SSIDs. The default value is **1000**. After the QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID and VLAN ID of an access port are the same.

6.8.2 Configure the QVLAN Function

1. Choose **Wireless** > **QVLAN Settings**.
2. Enable **QVLAN** function.
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.
4. Click **Save**.



---End

6.8.3 Example of Configuring QVLAN Settings

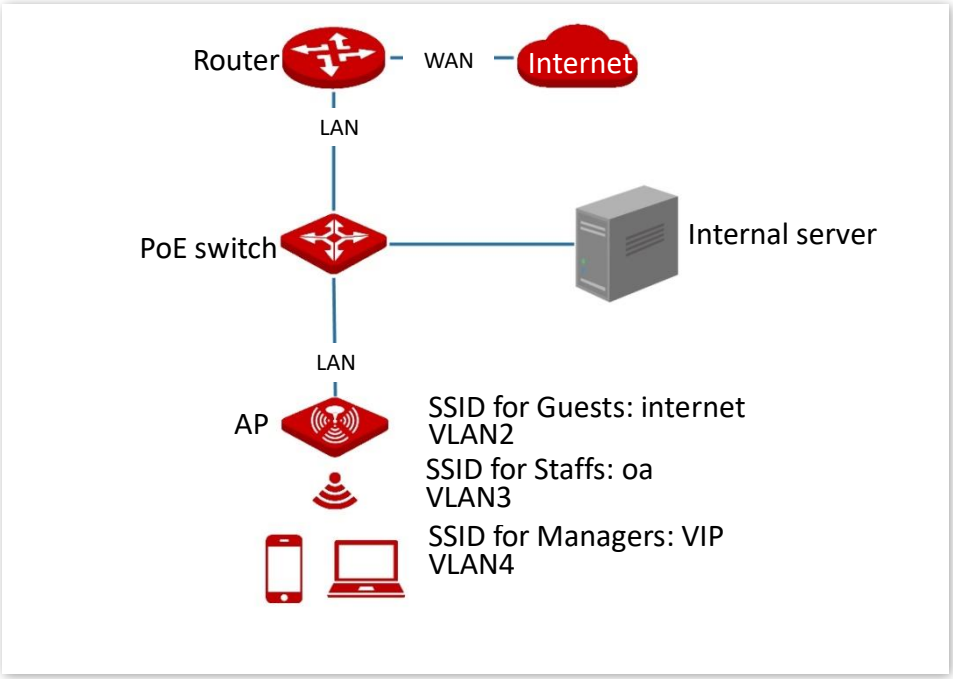
Networking requirement

A hotel has the following wireless network coverage requirements:

- Guests are connected to VLAN2 and can access only the internet.
- Staffs are connected to VLAN3 and can access only the LAN.
- Managers are connected to VLAN4 and can access both the LAN and the internet.

Networking plan

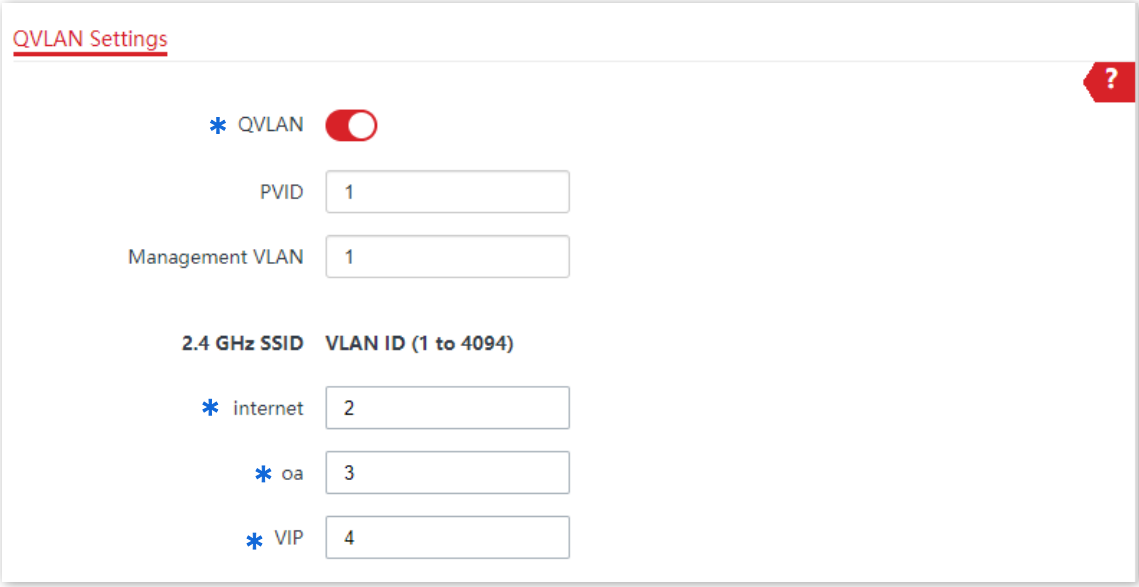
- Set the SSID to **internet** for guests, **oa** for staffs, and **VIP** for managers for 2.4 GHz network.
- Configure VLANs for the three SSIDs on AP.
- Configure VLAN forwarding rules on switch.
- Configure VLAN forwarding rules on router and internal server.



Configuration procedure

I. Configure the AP

1. Choose **Wireless** > **QVLAN Settings**.
2. Enable **QVLAN** function.
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.

II. 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
LAN 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.

III. Configure the router and 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 details, refer to the user guides for the corresponding devices.

---End

Verification

Wireless clients connected to the internet wireless network can only access the internet, wireless clients connected to the oa wireless network can only access the LAN. Wireless clients connected to the VIP wireless network can access both the internet and LAN.

7 Advanced

7.1 SNMP

7.1.1 Overview

The Simple Network Management Protocol (SNMP) is the most widely used network management protocol in TCP/IP networks. SNMP enables you to remotely manage all your network devices compliant with this protocol, such as monitoring the network status, changing network device settings, and receiving network event alarms.

SNMP allows automatic management of devices from various vendors regardless of physical differences among the devices.

SNMP Management Framework

The SNMP management framework consists of SNMP manager, SNMP agent, and Management Information Base (MIB).

- SNMP manager: It is a system that controls and monitors network nodes using the SNMP protocol. The SNMP manager most widely used in network environments is Network Management System (NMS). An NMS can be a dedicated network management server, or an application that implements management functions in a network device.
- SNMP agent: It is a software module in a managed device. The module is used to manage data about the device and report the management data to an SNMP manager.
- MIB: It is a collection of managed objects. It defines a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its MIB. An SNMP manager can read and/or write objects in the MIB based on the permissions assigned to the SNMP manager.

An SNMP manager manages SNMP agents in an SNMP network. The SNMP manager exchanges management information with the SNMP agents using the SNMP protocol.

Basic SNMP Operations

The AP allows the following basic SNMP operations:

- Get: An SNMP manager performs this operation to query the SNMP agent of the AP for values of one or more objects.
- Set: An SNMP manager performs this operation to set values of one or more objects in the MIB of the SNMP agent of the AP.

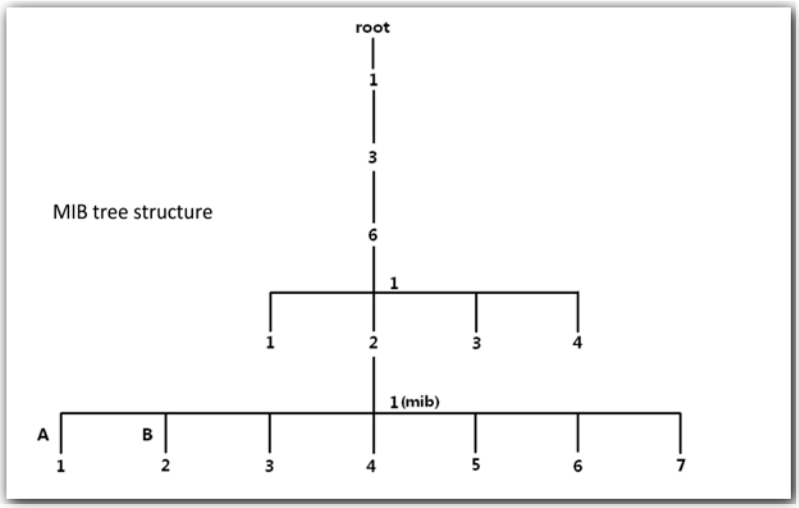
SNMP Protocol Version

The AP is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism. Community name is used to define the relationship between an SNMP agent and an SNMP manager. If the community name contained in an SNMP packet is rejected by a device, the packet is discarded. A community name functions as a password to control SNMP agent access attempts of SNMP managers.

SNMP V2C is compatible with SNMP V1 and provides more functions than SNMP V1. Compared with SNMP V1, SNMP V2C supports more operations (GetBulk and InformRequest) and data types (such as Counter64), and provides more error codes for better distinguishing errors.

MIB Introduction

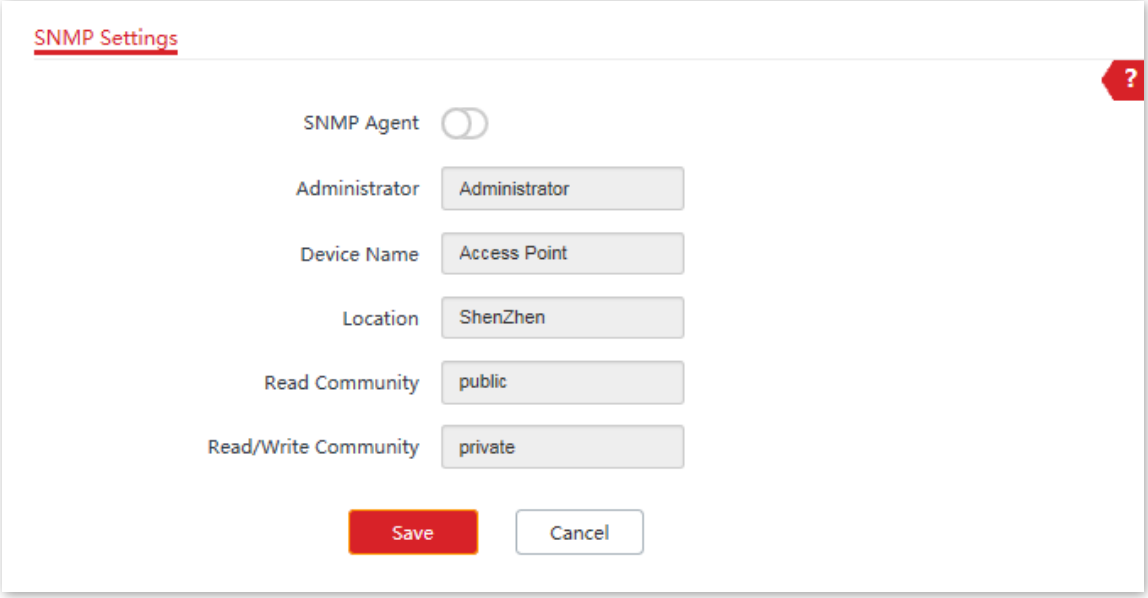
An MIB adopts a tree structure. The nodes of the tree indicate managed objects. A path consisting of digits and starting from the root can be used to uniquely identify a node. This path is calling an object identifier (OID). The following figure shows the structure of an MIB. In the figure, the OID of A is 1.3.6.1.2.1.1, whereas the OID of B is 1.3.6.1.2.1.2.



SNMP Configurations

The SNMP page allows you to configure SNMP agent.

To access the page, choose **Advanced** > **SNMP**.



Parameter description

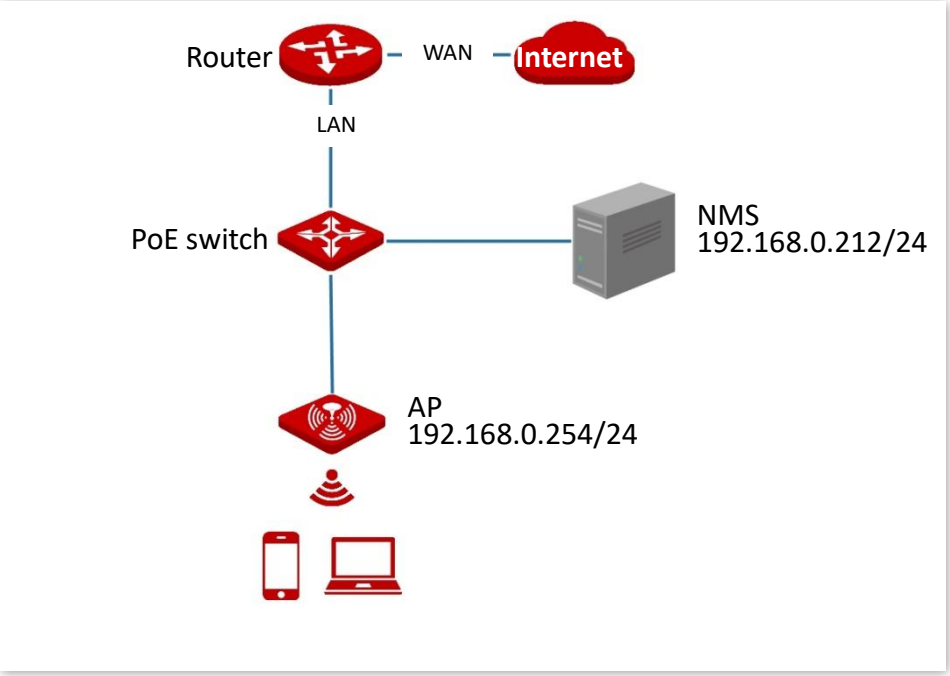
Parameter	Description
SNMP Agent	It specifies whether to enable the SNMP agent function of the AP. By default, it is disabled. An SNMP manager and the SNMP agent can communicate with each other only when their SNMP versions are the same. Currently, the SNMP agent function of the AP supports SNMP V1 and SNMP V2C.
Administrator	It specifies the name of the administrator of the AP. The default name is **Administrator**. You can modify the administrator's name as required.
Device Name	It specifies the device name of the AP. By default, the device name is **Access Point**. You can modify it as required. Tip You are recommended to modify the device name so that you can identify your AP easily when managing the AP using SNMP.
Location	It specifies the location where the AP is used. You can modify the location as required.
Read Community	It specifies the read password shared between SNMP managers and the SNMP agent. The default password is **public**. The SNMP agent function of the AP allows an SNMP manager to use the password to read variables in the MIB of the AP.

Parameter	Description
Read/Write Community	It specifies the read/write password shared between SNMP managers and the SNMP agent. The default password is **private**. The SNMP agent function of the AP allows an SNMP manager to use the password to read/write variables in the MIB of the AP.

7.1.2 Example of Configuring the SNMP Function

Networking requirement

- The AP connects to an NMS over an LAN. This IP address of the AP is **192.168.0.254/24** and the IP address of the NMS is **192.168.0.212/24**.
- The NMS use SNMP V1 or SNMP V2C to monitor and manage the AP.



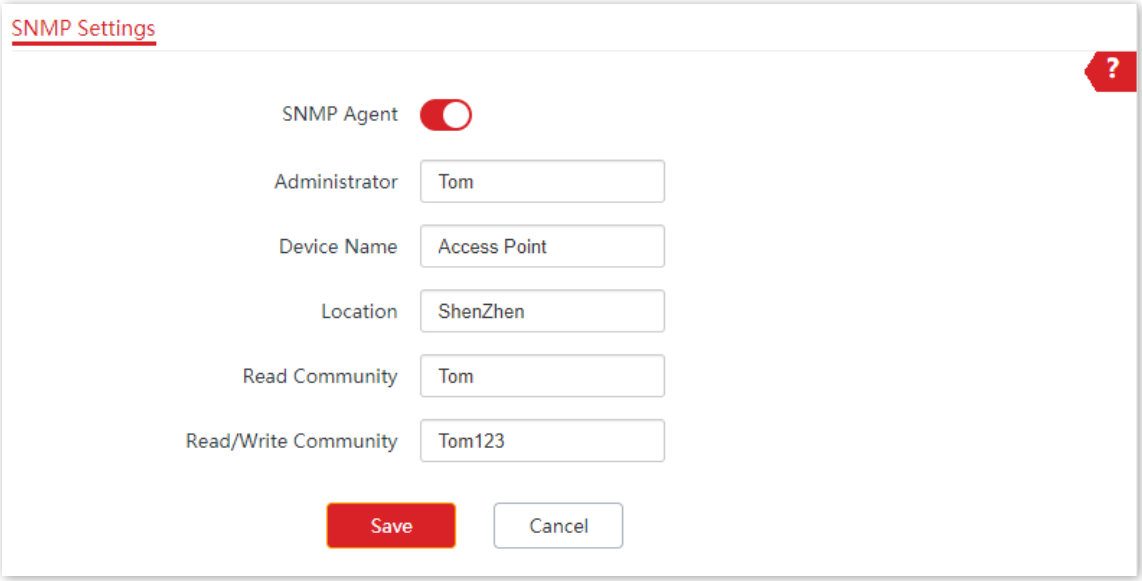
Configuration procedure

I. Configure the AP

Assume that the administrator name is **Tom**, read community is **Tom**, and read/write community is **Tom123**.

1. Choose **Advanced** > **SNMP**.
2. Enable **SNMP** function.
3. Set the SNMP parameters of **Administrator**, **Device Name**, **Location**, **Read Community** and **Read/Write Community**.

4. Click **Save**.



II. Configure the NMS

On an NMS that uses SNMP V1 or SNMP V2C, set the read community to **Tom** and read/write community to **Tom 123**. For details about how to configure the NMS, refer to the configuration guide for the NMS.

---End

Verification

After the configuration, the NMS can connect to the SNMP agent of the AP and query and set some parameters on the SNMP agent through the MIB.

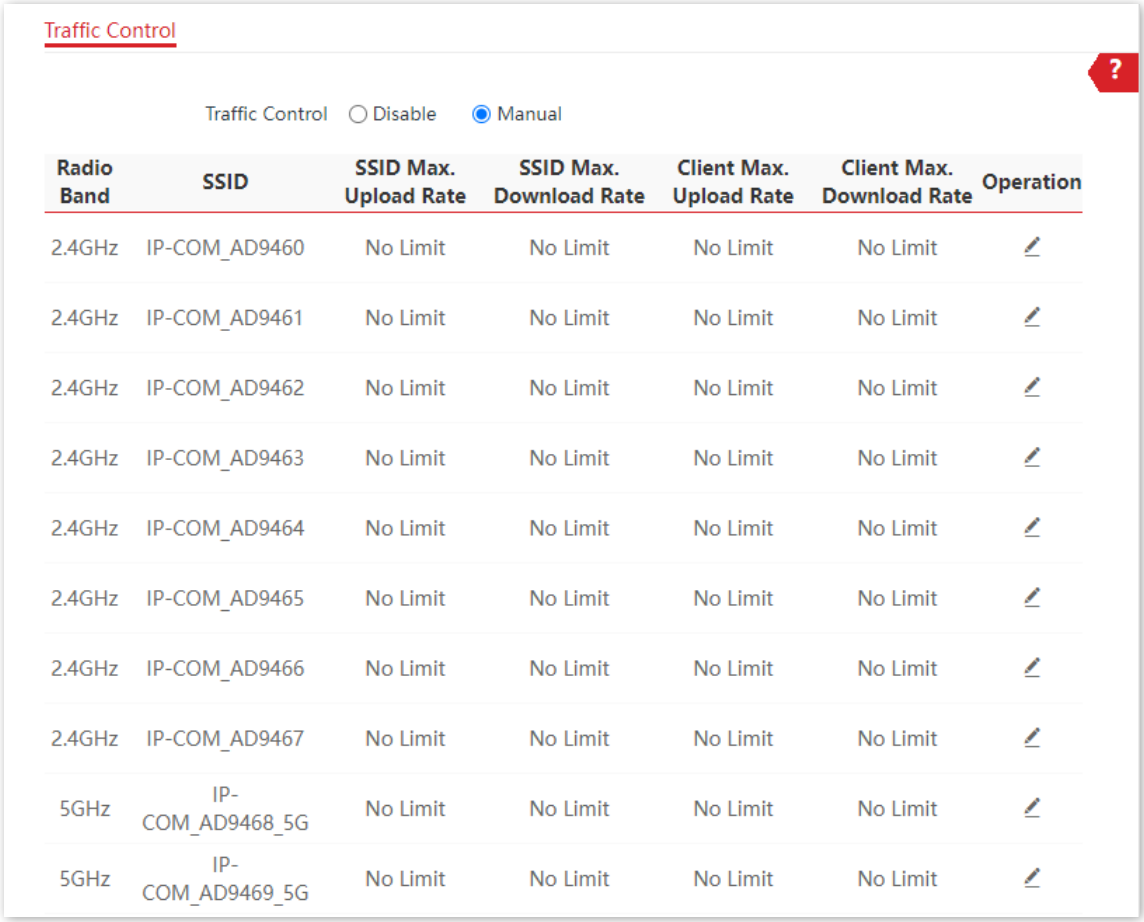
7.2 Traffic Control

7.2.1 Overview

This function is supported only by Pro-6-Lite.

The Traffic Control page allows you to set limits on the internet speed of clients to guarantee a proper allocation of limited broadband resources.

By default, the Traffic Control function is disabled. If you want to use this function, configure it on the **Advanced** > **Traffic Control** page. The following figure displays the page when Traffic Control is enabled.



Parameter description

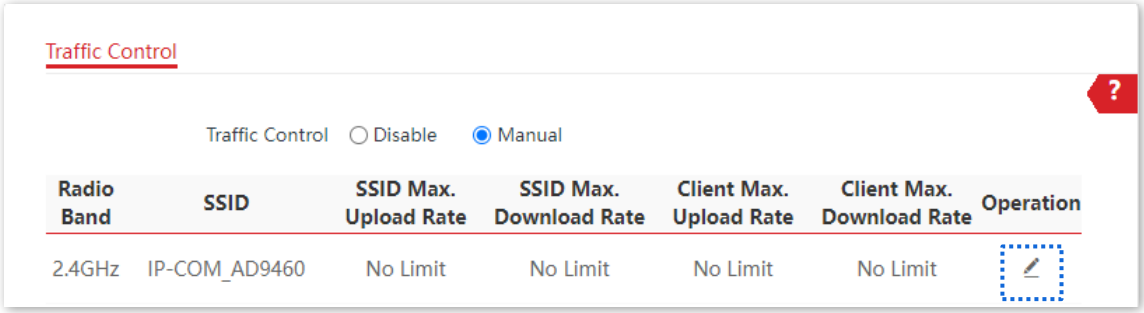
Parameter	Description
Traffic Control	– Disable: The Traffic Control function is disabled. – Manual: The Traffic Control function is enabled. The network administrator manually set SSID and the maximum upload/download speed of user devices to limit the total bandwidth of SSID and evenly allocate bandwidth to users. In this way, if multiple SSIDs are enabled, and a user network with a lower priority (such as guest network) occupies an excessively high internet speed or a user occupies too much bandwidth, such circumstances as excessively low internet speed or even internet unavailability for other users will not occur.
Radio Band	It specifies the radio band of the WiFi network on which you want to set a traffic control rule.
SSID	It specifies the name of the WiFi network on which you want to set a traffic control rule.
SSID Max. Upload Rate SSID Max. Download Rate	It specifies the maximum upload/download rate allowed for a WiFi network. If you leave it blank, the maximum upload/download rate of the target WiFi network are not limited.
Client Max. Upload Rate Client Max. Download Rate	It specifies the maximum upload/download rate allowed for every user device connected to the target WiFi network. If you leave it blank, the maximum upload/download rate of every user device connected to the target WiFi network are not limited.
Operation	Click to set the maximum upload/download rate allowed for the target WiFi network and the maximum upload/download rate allowed for every user device connected to the target WiFi network.

7.2.2 Configure Traffic Control

Tip

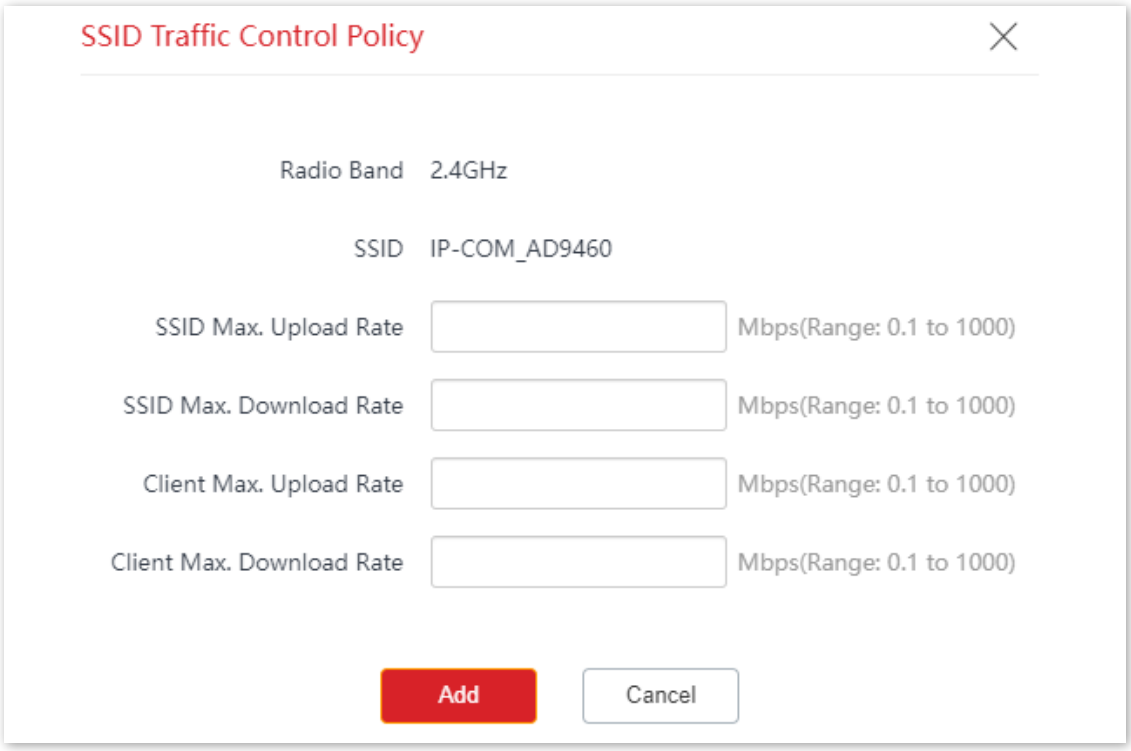
The following web UI screenshots are taken from Pro-6-Lite.

1. Click **Advanced** > **Traffic Control**.
2. Set **Traffic Control** to **Manual**.
3. On the **Traffic Control** list, click on the row where the WiFi network to be controlled resides.



4. In the pop-up window, set the maximum upload/download rate allowed for the WiFi network and the maximum upload/download rate allowed for every user device connected to the WiFi network.

5. Click **Add**.



---End

8 Tools

8.1 Date & Time

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

8.1.1 System Time

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

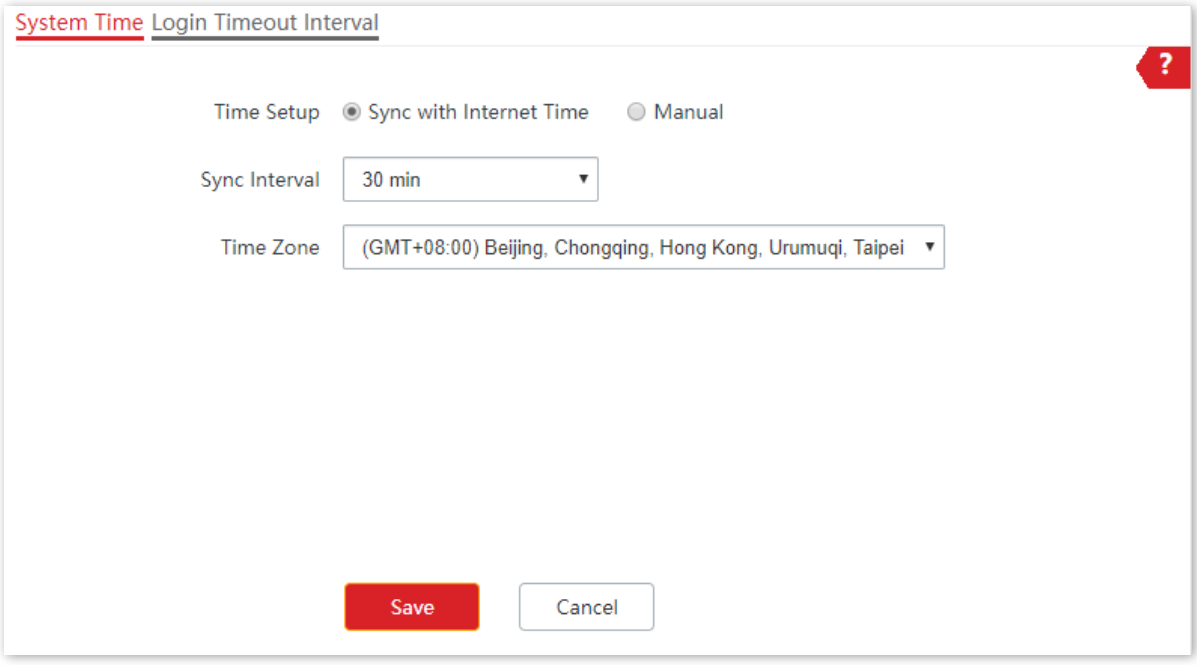
To access the page, choose **Tools** > **Date & Time** > **System Time**.

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.

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



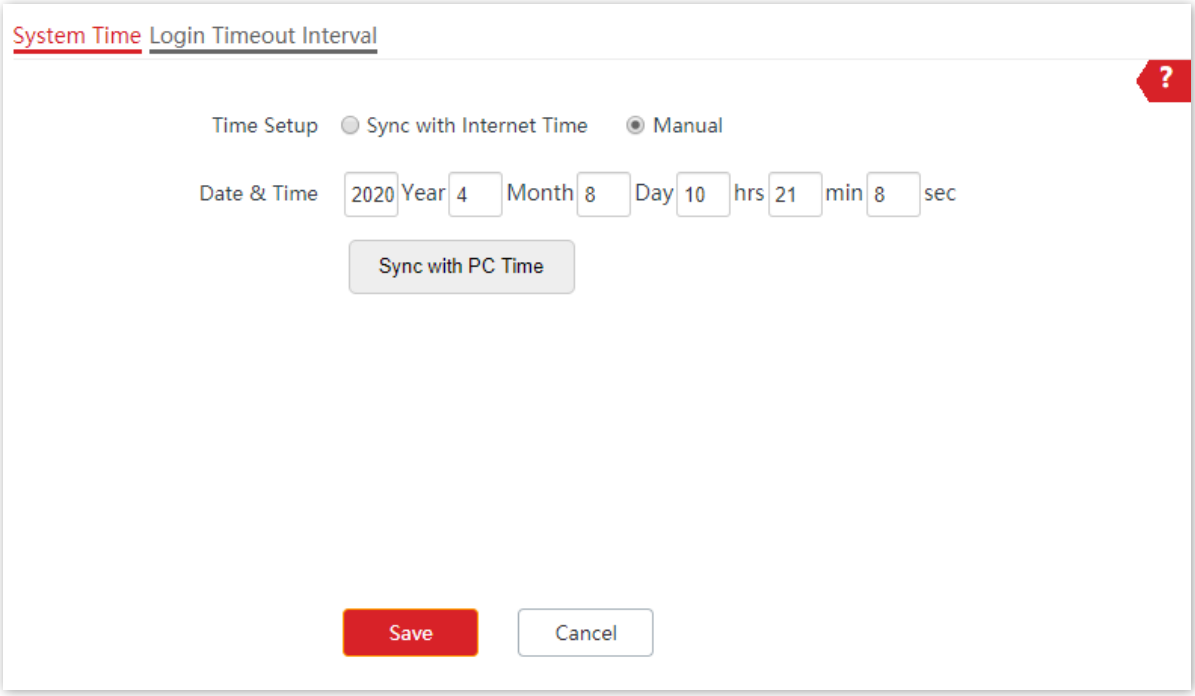
Parameter description

Parameter	Description
Time Setup	It specifies the modes to set the system time.
Sync Interval	It is valid only when **Sync with Internet Time** is chosen. It specifies the interval at which the AP will automatically synchronize with a time server of the internet.
Time Zone	It is valid only when **Sync with Internet Time** is chosen. 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.

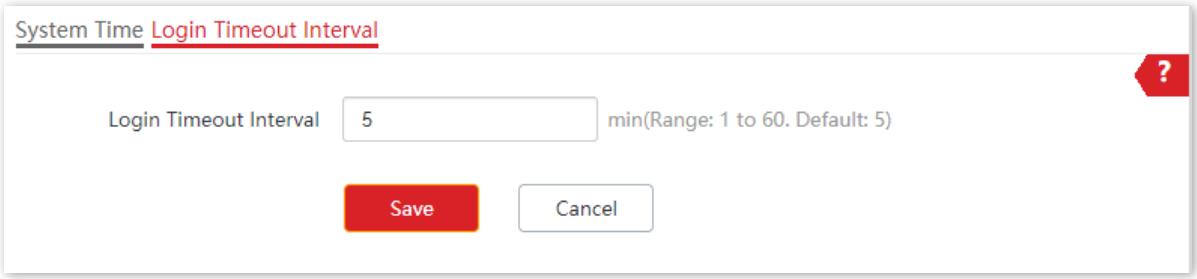


8.1.2 Login Timeout Interval

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 for network security. The default login timeout interval is **5** minutes.

The Login Timeout Interval page allows you to modify the login timeout interval.

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



8.2 Maintenance

8.2.1 Maintenance

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

To access the page, choose **Tools** > **Maintenance** > **Maintenance**.

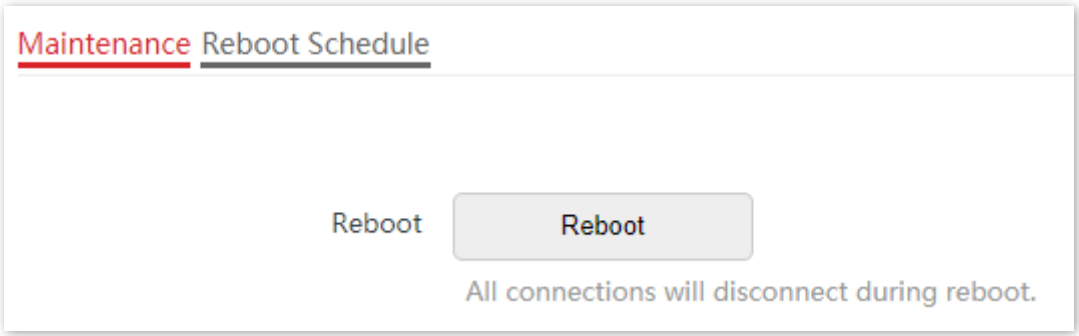
Reboot

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

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

Tip

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



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:

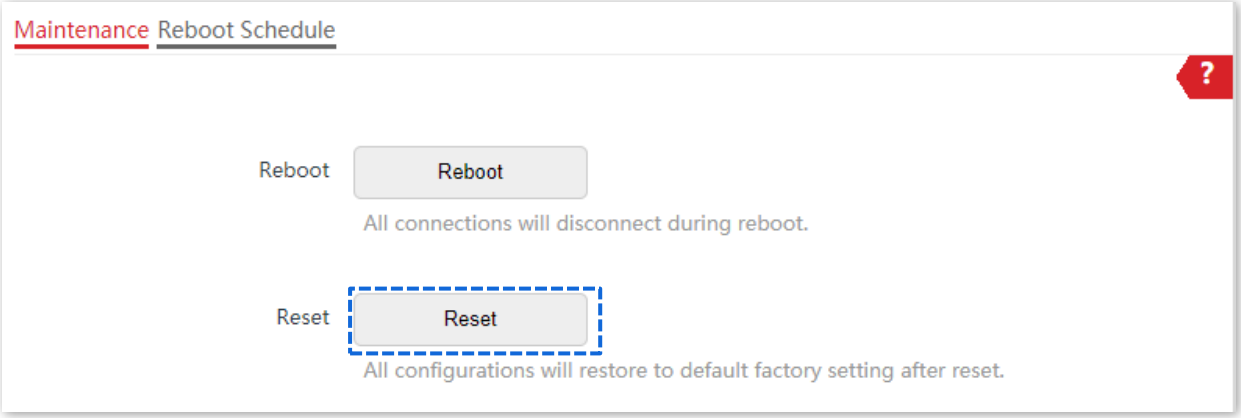
This method allows you to restore the factory settings without logging in to the web UI of the AP.

Procedure:

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**.



Upgrade Firmware

This function allows you to upgrade the firmware of the AP for more functions and higher stability.

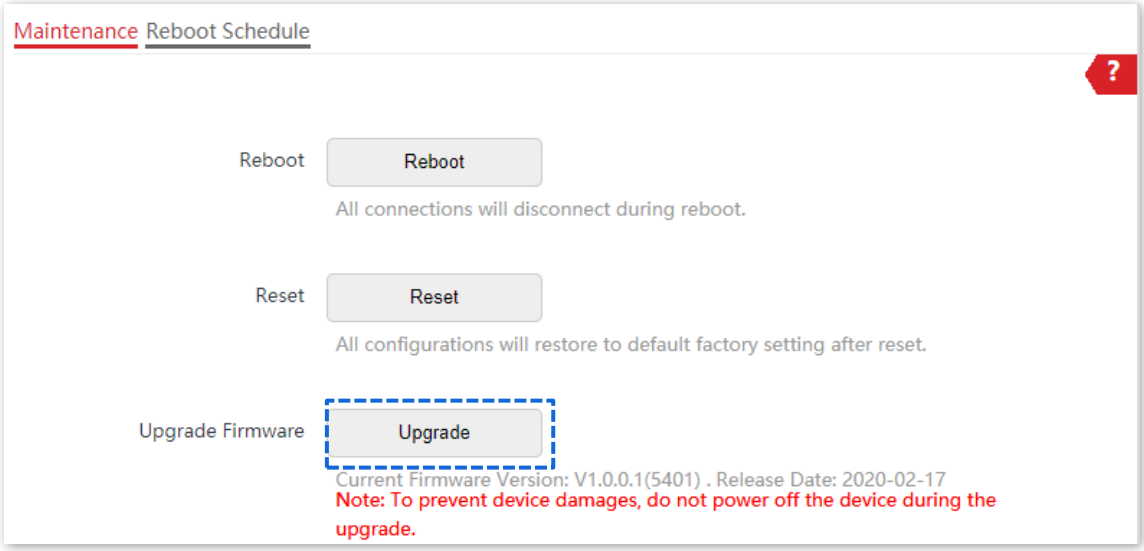
Note

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:

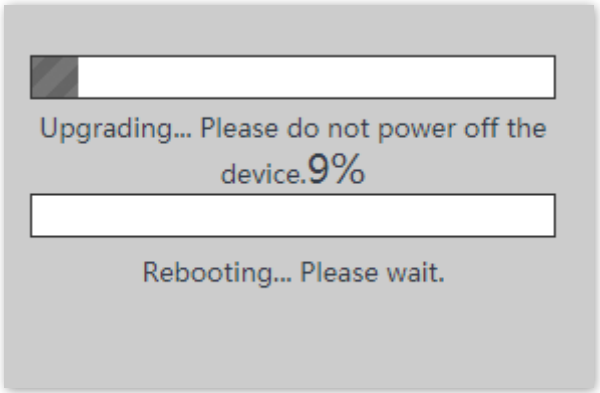
1. Download the package of a later firmware version for the AP from www.ip-com.com.cn to your local computer, and decompress the package. Generally, the package is in the format of .bin.
2. Log in to the web UI of the AP and choose **Tools** > **Maintenance** > **Maintenance**.
3. Click **Upgrade**.



4. Choose the upgrade file in the popped window.

---End

Wait until the progress bar is complete. Log in to the web UI of the AP again. Choose **Status** > **System Status** and check whether the upgrade is successful based on **Firmware Version**.



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.

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

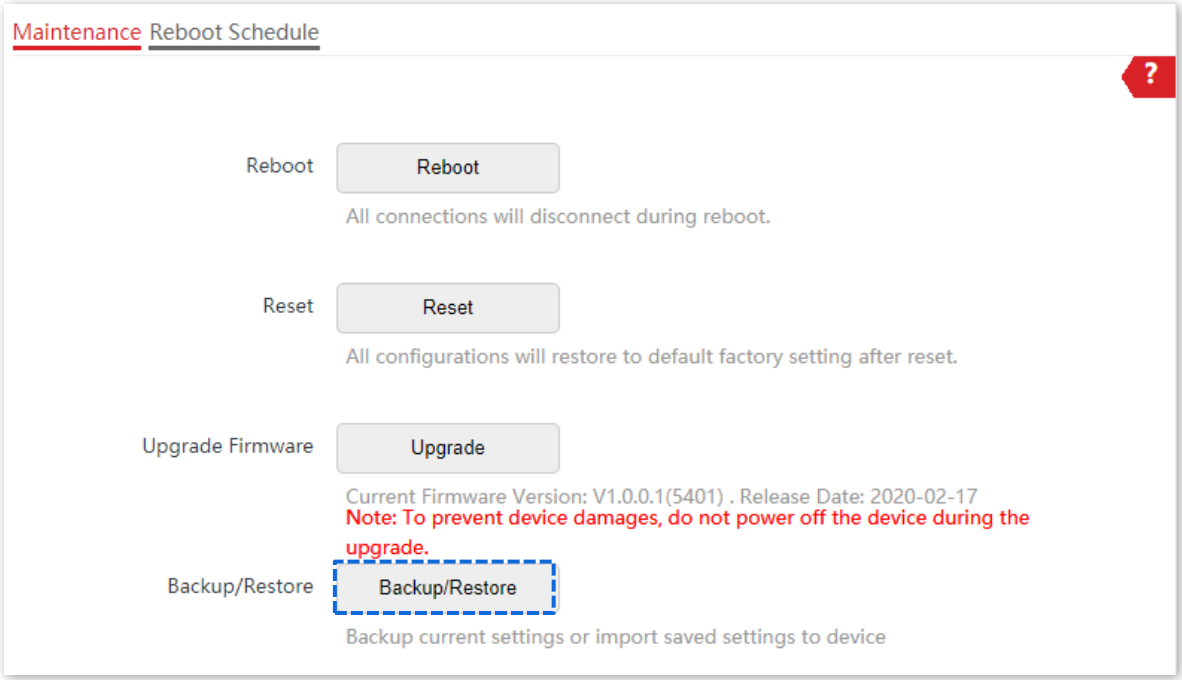
upgrading or resetting the AP.

Tip

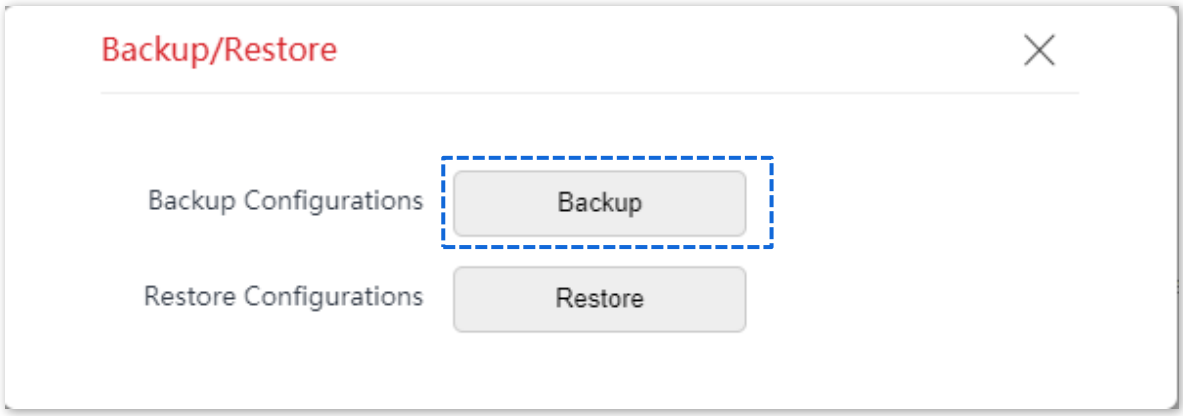
If you need to apply same or similar configurations to many APs, you can configure one of the APs, back up the configuration of the AP, and use the backup to restore the configuration on the other APs. This improves configuration efficiency.

Back Up the Current Configuration

1. Choose **Tools** > **Maintenance** > **Maintenance**.
2. Click **Backup/Restore**.



3. Click **Backup**.



---End

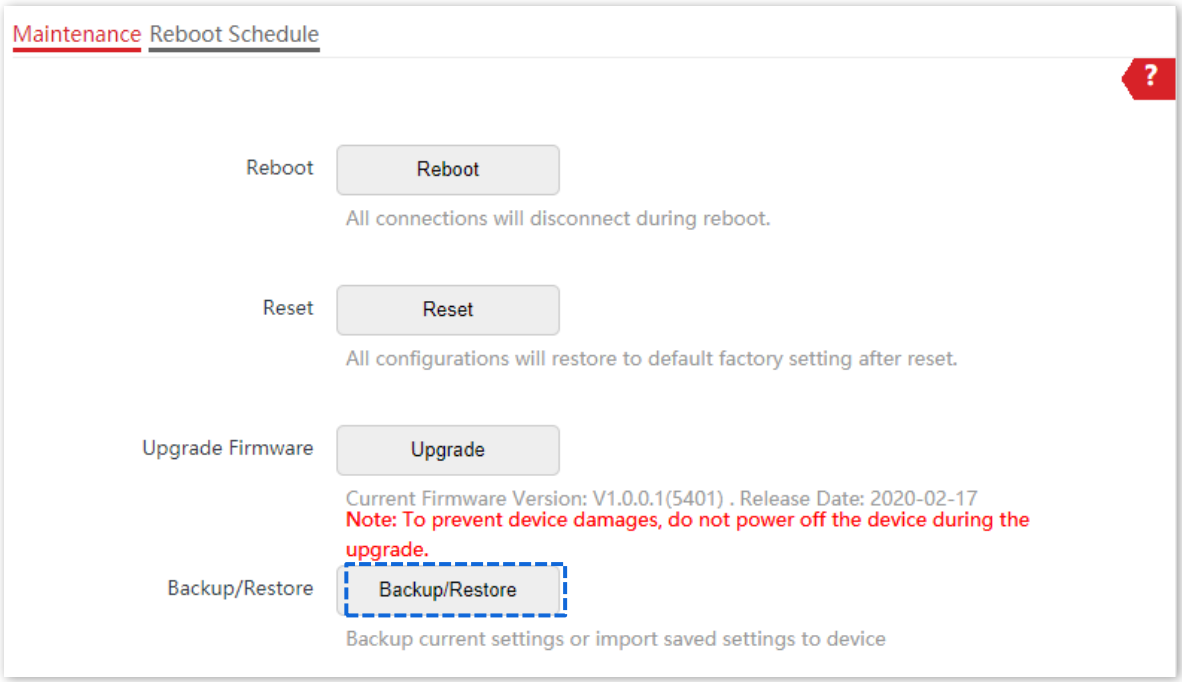
A configuration file named **APCfm.cfg** is downloaded.

Tip

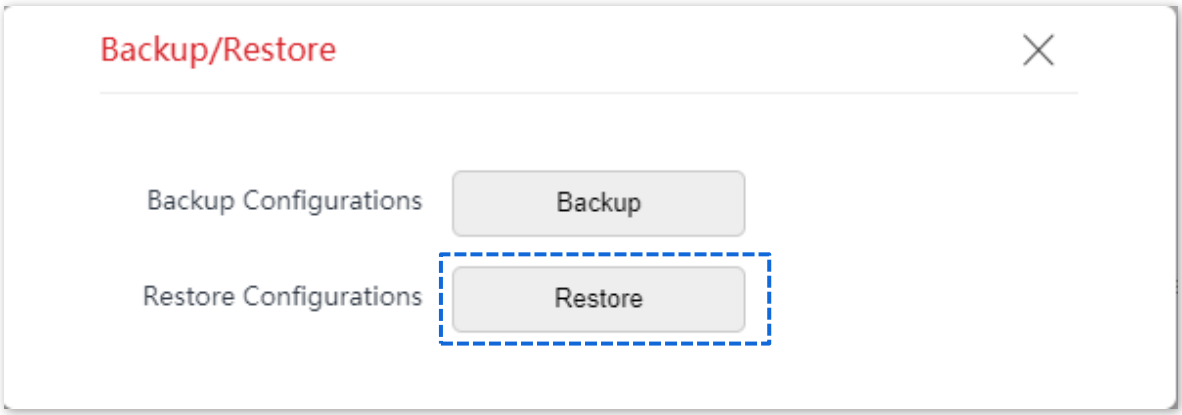
If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click “Keep”.

Restore a Configuration

1. Choose **Tools** > **Maintenance** > **Maintenance**.
2. Click **Backup/Restore**.



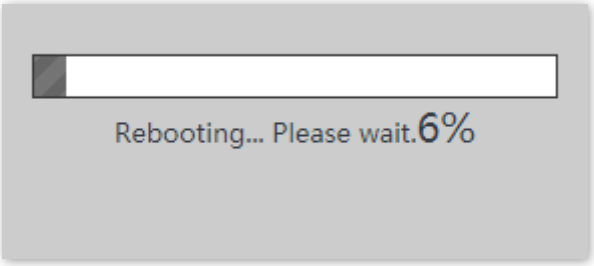
3. Click **Restore**.



4. Choose the configuration file you backed up.

---End

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

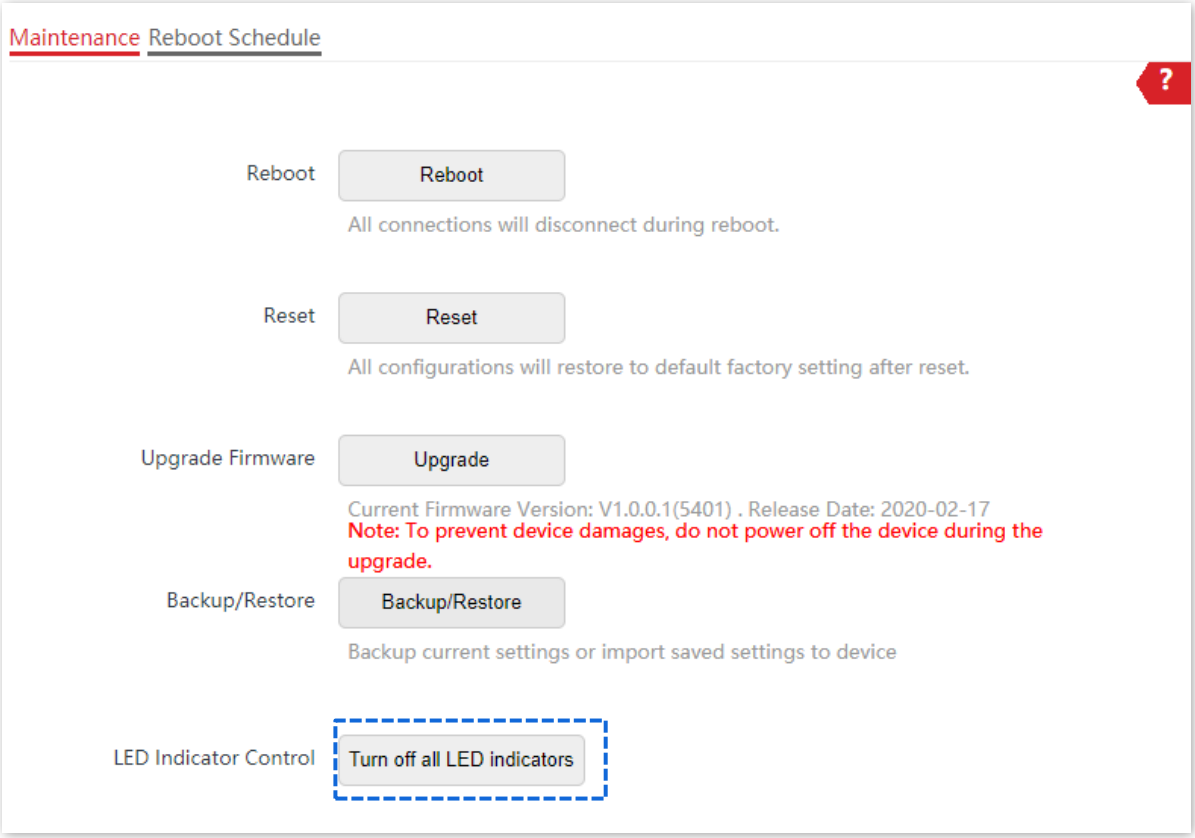


LED Indicator Control

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

Turn Off the LED Indicator

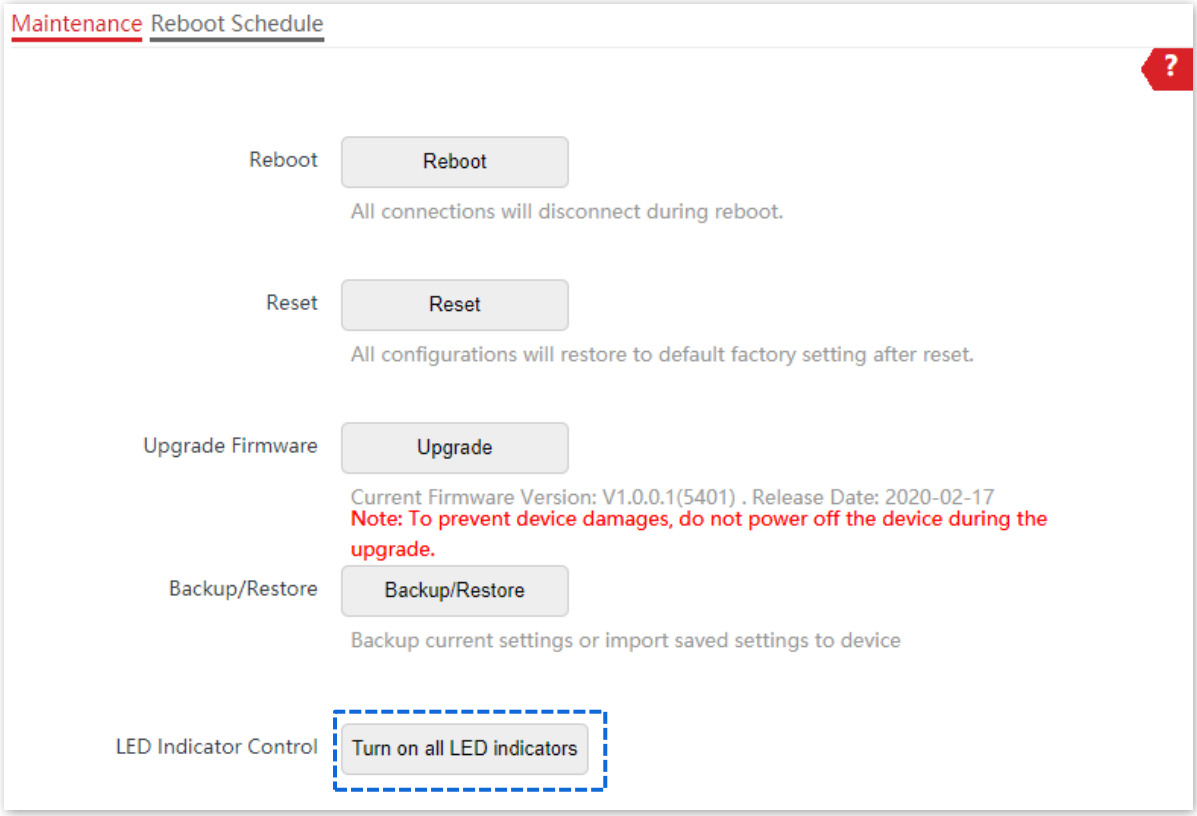
On the **Tools** > **Maintenance** > **Maintenance** page, click **Turn off all LED indicators**.



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.

8.2.2 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**: In this type, the AP reboots at the interval that you specify.
- **Reboot Schedule**: In this type, the AP reboots weekly at the time that you specify.

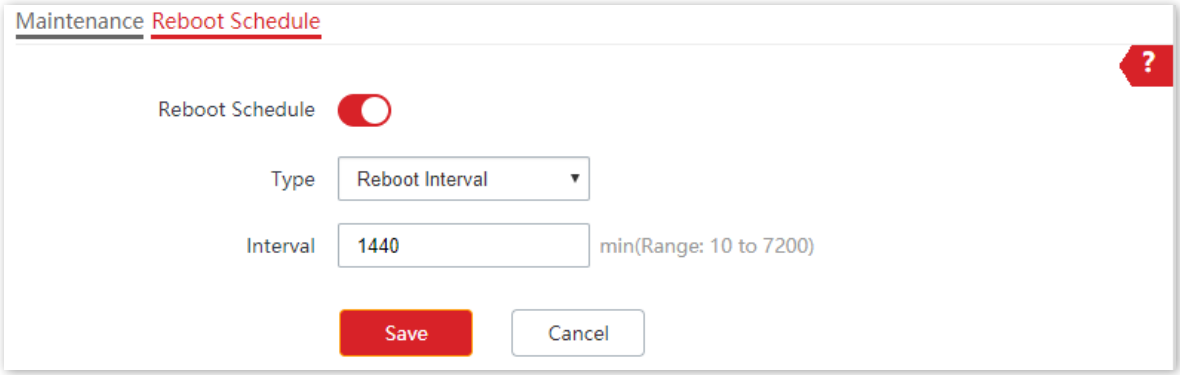
Configure the AP to Reboot Interval

Tip

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

1. Choose **Tools** > **Maintenance** > **Reboot Schedule**.
2. Enable **Reboot Schedule** function.
3. Set **Type** to **Reboot Interval**.

4. Set **Interval** to a value in minutes, such as **1440**.
5. Click **Save**.

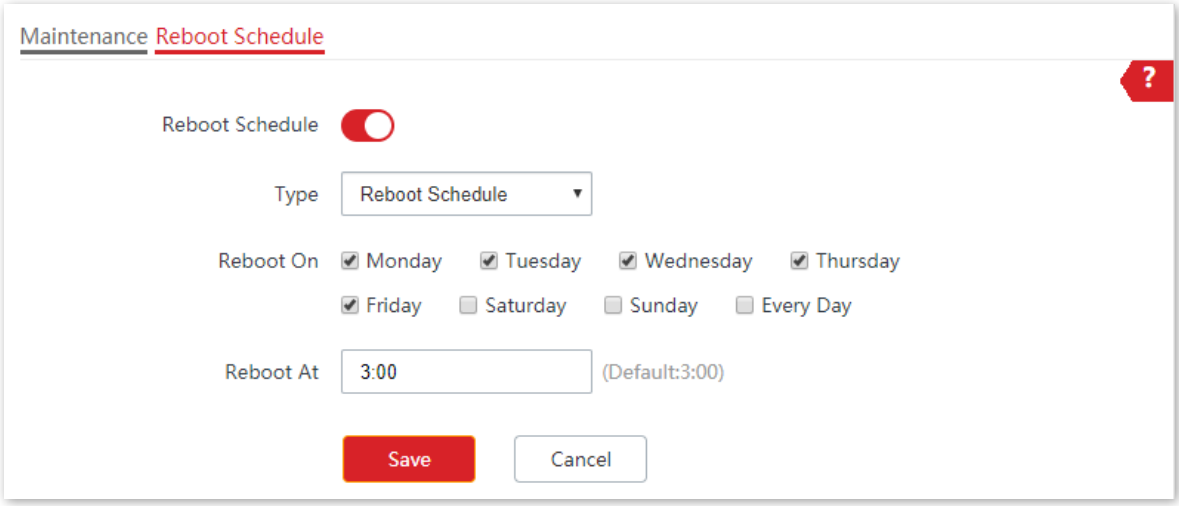


---End

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

Configure the AP to Reboot Schedule

1. Choose **Tools** > **Maintenance** > **Reboot Schedule**.
2. Enable **Reboot Schedule** function.
3. Set **Type** to **Reboot Schedule**.
4. Select the day or days when the AP reboots, such as **Monday** to **Friday**.
5. Set the time when the AP reboots, such as **3:00**.
6. Click **Save**.



---End

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

8.3 Account

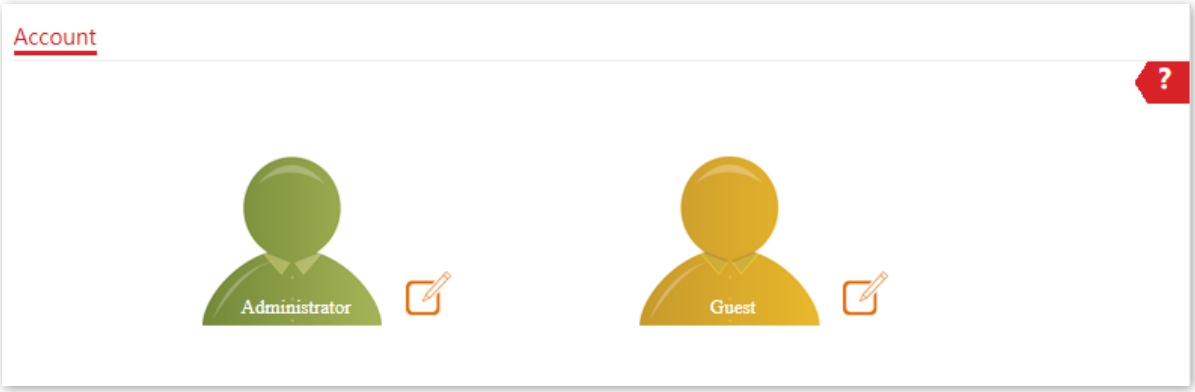
8.3.1 Overview

AP supports two account types: **Administrator** and **Guest**. The difference between them lies in their permissions.

- **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.

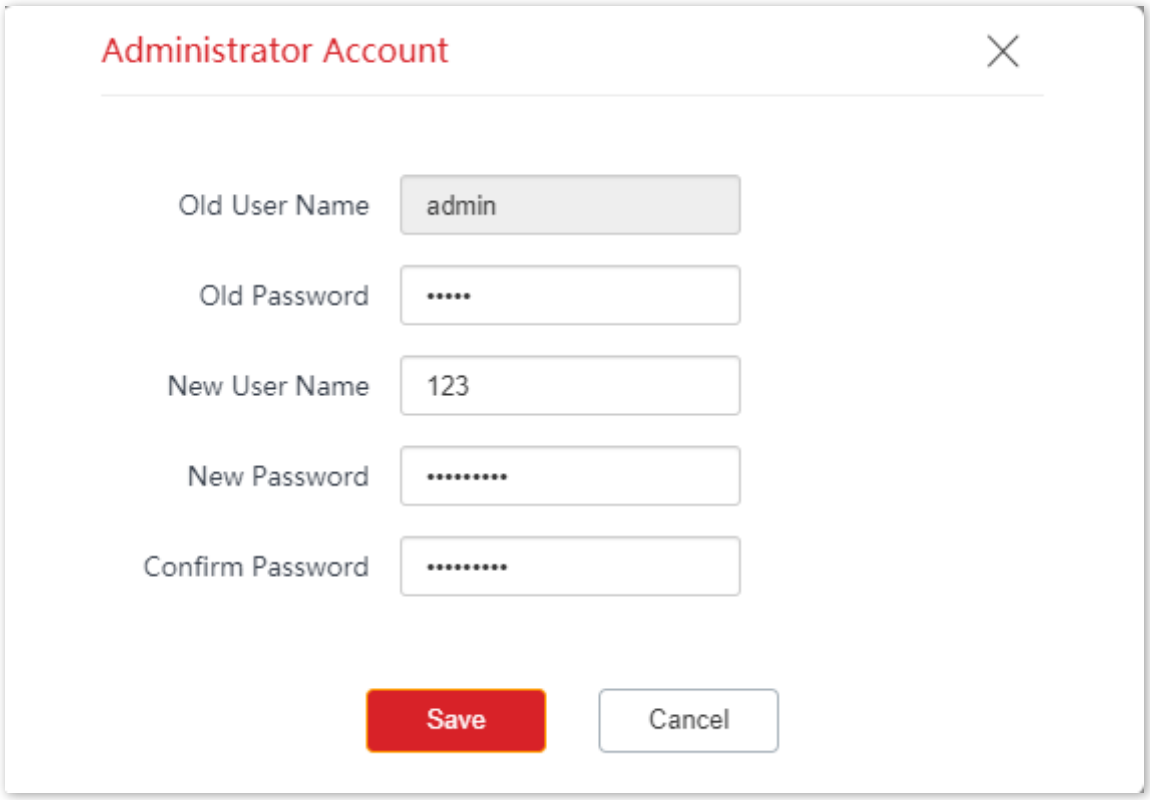
The Account page allows you to modify the information of the login account to keep unauthorized users from entering the web UI and modifying configurations, thus protecting the wireless network.

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



8.3.2 Modify the Password and User Name of Login Account

1. Choose **Tools** > **Account**.
2. Click beside the account to be modified.
3. If the account to be modified is a Guest, enable the **Guest Account** first. Otherwise, go to the next step.
4. Enter the current password in **Old Password**.
5. Enter the new account name, for example, **123**, in **New User Name**.
6. Enter the new password in **New Password**.
7. Enter again the new password in **Confirm Password**.
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.

8.4 System Log

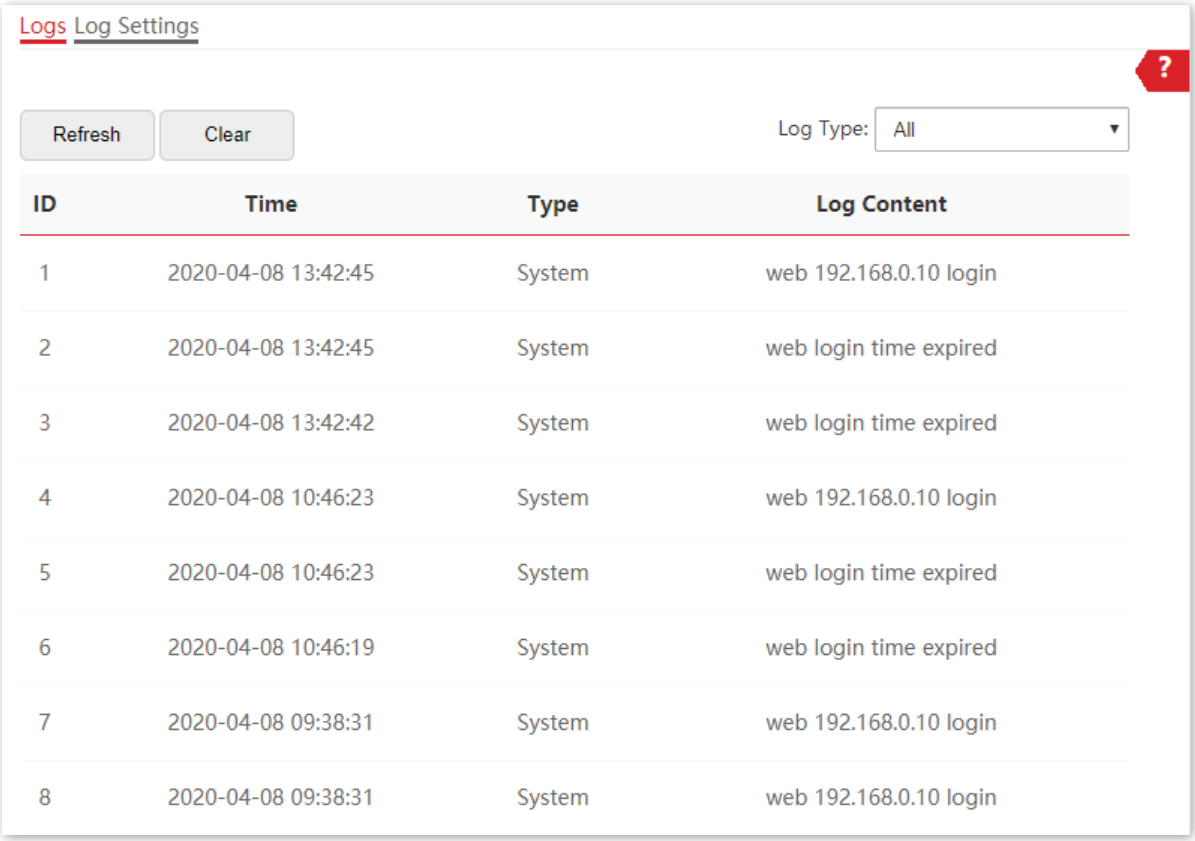
This section allows you to view system logs, configure log servers, and set the number of logs to be displayed on the page.

8.4.1 Logs

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 *X* logs. The value of *X* depends on Number of Logs. To view the latest logs of the AP, click **Refresh**. To clear the existing logs of the AP, click **Clear**.

Note

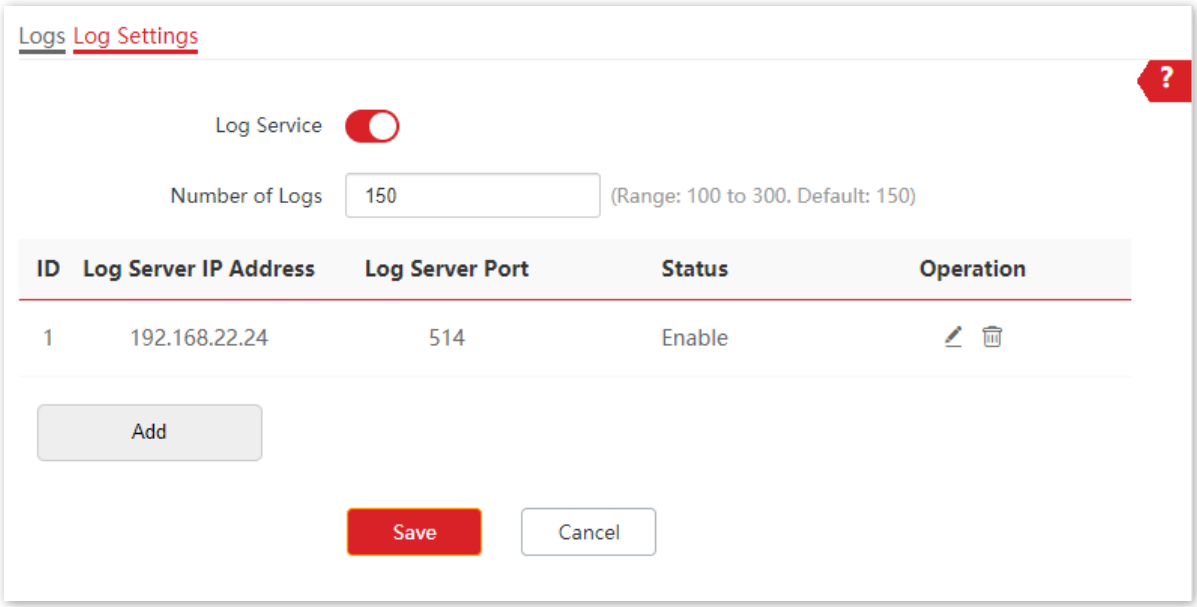
- When the AP reboots, the previous logs are lost.
- The AP reboots when the AP is powered on after a power failure, the QVLAN function is configured, the firmware is upgraded, an AP configuration is restored, or the factory settings are restored.

8.4.2 Log Settings

After you configure a log server, AP automatically synchronizes system logs to the log server you configured. You can view all the logs on the log server.

The Log Settings page allows you to set the number of logs to be displayed and configure log servers.

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



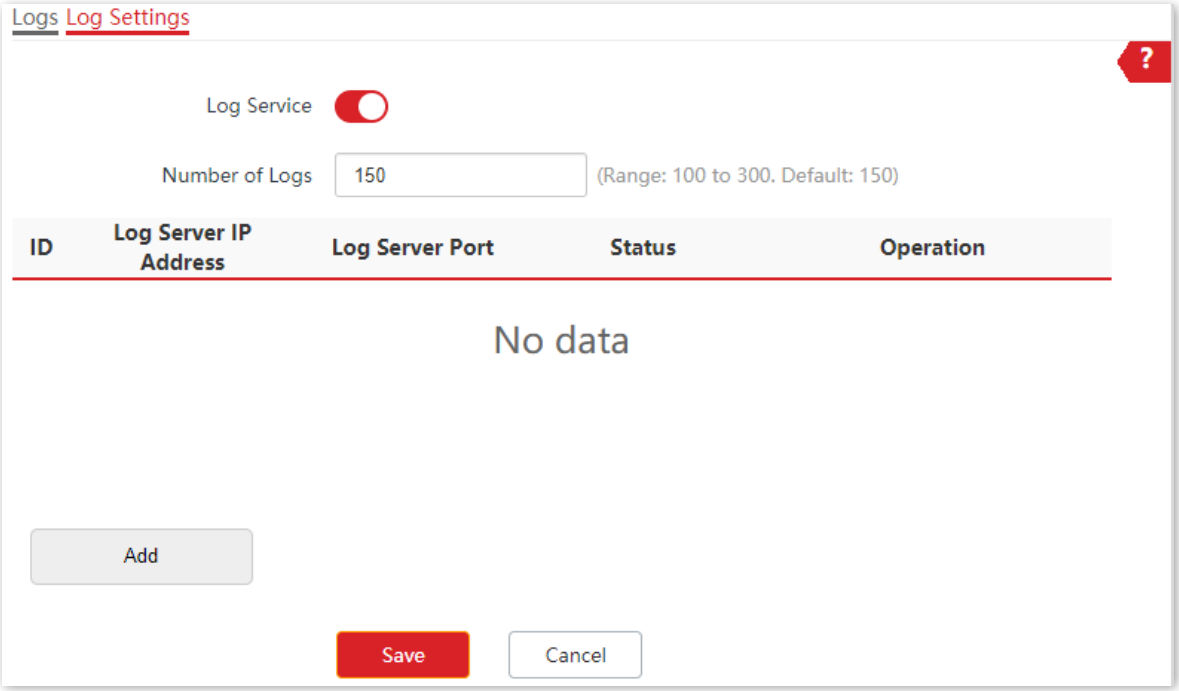
Parameter description

Parameter	Description
Log Service	It specifies whether to enable the log service function. This function is disabled by default. You can modify the number of logs to be displayed and configure log server only if the Log Service function is enabled.
Number of Logs	It specifies the largest number of logs that can be displayed on the web UI.
Log Server IP Address	It specifies the IP address of the log server. To ensure that system logs can be sent to the log server, set the **IP Address**, **Subnet Mask** and **Default Gateway** of the AP on the **Internet Settings** > **LAN Setup** page to enable the AP to access the log server.

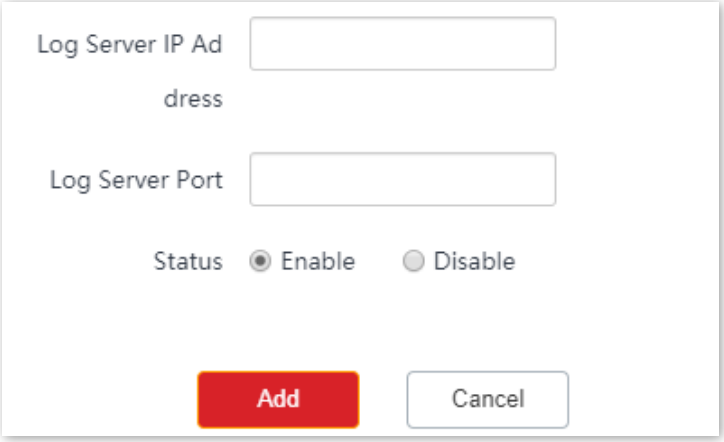
Parameter	Description
Log Server Port	It specifies the port (514 by default) used by the log service. It should be the same port with the port configured by the log server.
Status	It specifies the status of the log server rule.
Operation	It specifies the operations you can perform on the log server: – Click to modify the IP address, port, or status of the log server. – Click to delete the target log server.
Add	Click it to add a log server.

Add a Log Server

1. Choose **Tools** > **System Log** > **Log Settings**.
2. Enable **Log Service** function.
3. Click **Add**.



4. Perform the following procedures:
   (1) Set **Log Server IP Address** to the IP address of the log server.
   (2) Set **Log Server Port** to the UDP port number used to send and receive system logs. The default port number **514** is recommended.
   (3) Set **Status** to **Enable**.
   (4) Click **Add**.



5. Click **Save**.

---End

8.5 Diagnostic Tool

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

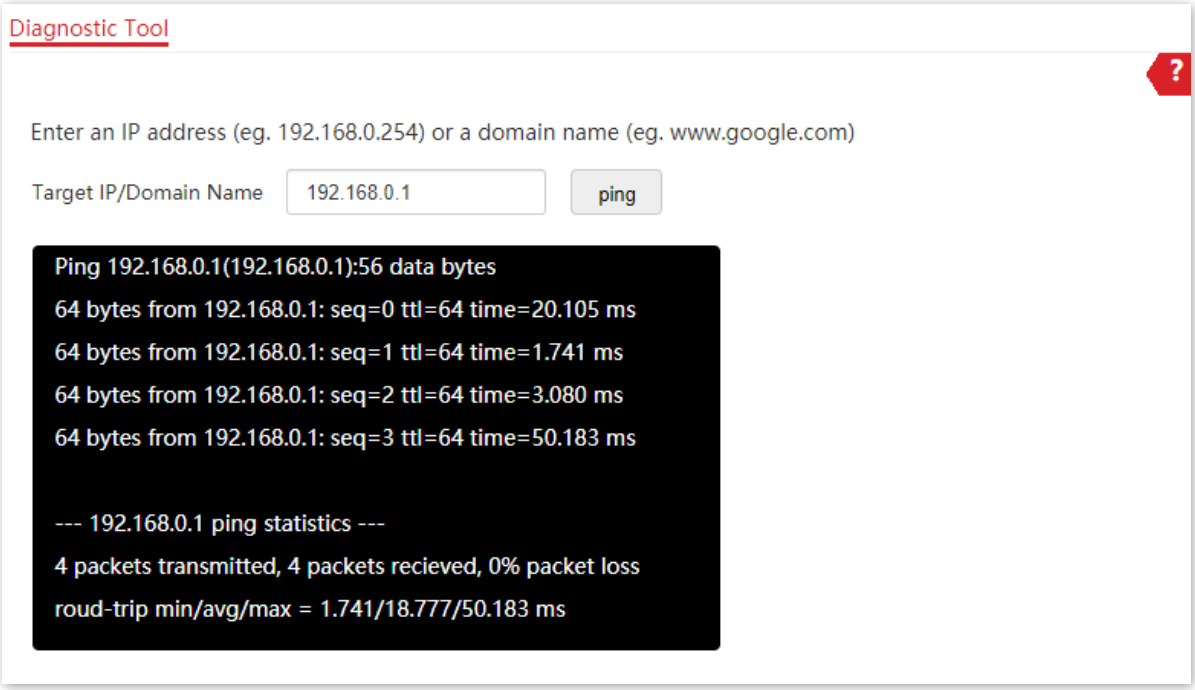
Procedure:

The target address 192.168.0.1 is used as an example.

1. Choose **Tools** > **Diagnostic Tool**.
2. Enter the IP address or domain name to be pinged in the **Target IP/Domain Name** text box. In this example, enter **192.168.0.1**.
3. Click **ping**.

---End

The diagnosis result will be displayed in a few seconds in the black text box below. See the following figure.


Diagnostic Tool
Enter an IP address (eg. 192.168.0.254) or a domain name (eg. www.google.com)
Target IP/Domain Name
192.168.0.1
ping
Ping 192.168.0.1(192.168.0.1):56 data bytes
64 bytes from 192.168.0.1: seq=0 ttl=64 time=20.105 ms
64 bytes from 192.168.0.1: seq=1 ttl=64 time=1.741 ms
64 bytes from 192.168.0.1: seq=2 ttl=64 time=3.080 ms
64 bytes from 192.168.0.1: seq=3 ttl=64 time=50.183 ms
--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 packets recieved, 0% packet loss
roud-trip min/avg/max = 1.741/18.777/50.183 ms

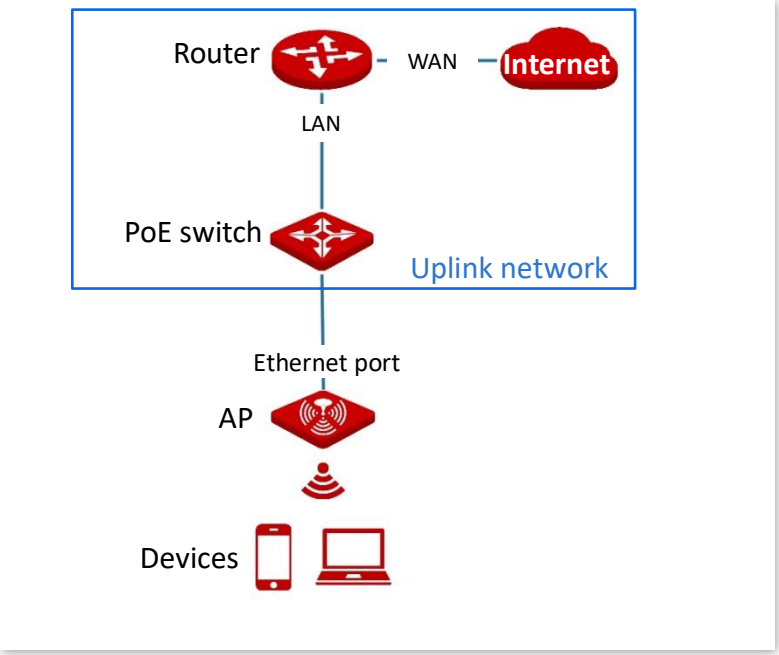
8.6 Uplink Detection

8.6.1 Overview

In AP mode, the AP connects to its upstream network using the 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 stops its wireless service and 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.

If the uplink of the AP with uplink detection enabled is faulty, wireless devices can connect to the upstream network through another nearby AP that works properly.

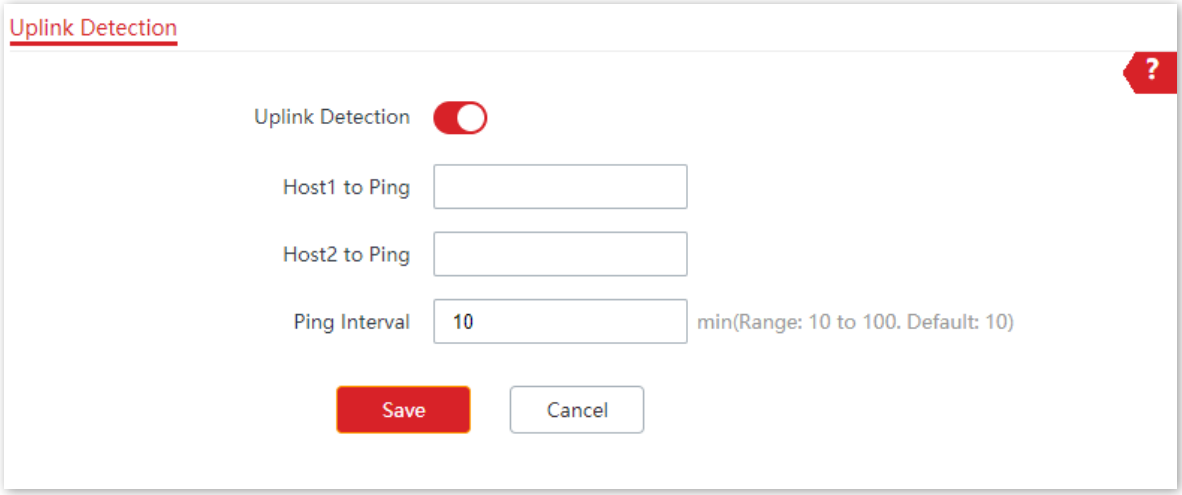
See the following typical network topology (The LAN port serves as the uplink port).



8.6.2 Configure Uplink Detection

1. Choose **Tools** > **Uplink Detection**.
2. Enable **Uplink Detection** function.
3. (Supported by some model) Select an operation you want the AP to perform if an uplink disconnection occurs.

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. If there is only one host IP address, enter this IP address in both **Host1 to Ping** and **Host2 to Ping**.
5. Set **Ping Interval** to the interval at which the AP detects its uplink. The default value is **10** minutes.
6. Click **Save**.



---End

Appendix

A.1 Factory default settings

The following table lists the default values of major parameters of the AP.

Parameter			Default Value
Login	Management IP address		192.168.0.254
	User Name/Password	Administrator	admin|admin
		Guest	user|user
Quick Setup	Working Mode		AP
LAN Setup	IP Address Type		DHCP
DHCP Server			Disable
SSID	SSID	2.4 GHz	Generally, the AP allows 8 SSIDs; however, some models allow only 7 SSIDs. The web UI of the target model prevails. The displayed SSID is IP-COM_XXXXXX, where XXXXXX indicates the range from the last 6 characters to the last 6 characters + 6 / 7 of the MAC address of the LAN ports of the AP. By default, the primary SSID is enabled, and the other SSIDs are disabled.
		5 GHz	The AP allows 4 SSIDs. The displayed SSID is IP-COM_XXXXXX_5G, where XXXXXX indicates the range from the last 6 characters + 7 / 8 to the last 6 characters + 10 / 11 of the MAC address of the LAN ports of the AP. By default, the primary SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network		Enable

A.2 Acronyms & Abbreviations

Acronyms & Abbreviations	Full Name
AC	Access Category
AC	Access Point Controller
AES	Advanced Encryption Standard
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DTIM	Delivery Traffic Indication Map
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
FIFO	First-in First-out
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NMS	Network Management System
PoE	Power over Ethernet
PSK	Pre-shared Key
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTS	Request to Send
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMF	Wireless Multicast Forwarding
WMM	WiFi Multimedia

Acronyms & Abbreviations	Full Name
WPA	Wi-Fi Protected Access