IP-COM

User Guide

Ceiling AP Series

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

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! This user guide helps you configure, manage and maintain APs.

Applicable product

This user guide applies to IP-COM ceiling AP products (W63AP, Pro-6-Mini, Pro-6-LR and Pro-6-Lite). All the screenshots herein, unless otherwise specified, are taken from Pro-6-Mini.

Conventions

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

The product figures and screenshots in this guide are for examples only. They may be different from the actual products you purchased, but do not affect the normal use.

In this guide, unless otherwise specified:

- The "AP" and "product" mentioned in this guide refer to IP-COM ceiling AP.
- The firmware version uses V1.0.0.2(2762) of Pro-6-MiniV1.0 as an example.
- The screenshots use the AP mode as an example. For other working modes, the actual web UI prevails.

APs of this series support central management by IP-COM ProFi, IP-COM Access Point Controller (AC) or IP-COM routers that support the AP management function. For detailed information, refer to user guides of IP-COM ProFi, target ACs or routers.

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

Item	Presentation	Example
Cascading menus	>	Navigate to **System** > **Live Users**.
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
UI control	Bold	On the **Policy** page, click the **OK** button.

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

Symbol	Meaning
	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 the device.
	This format is used to highlight a procedure that will save time or resources.

For more documents

Go to our website at www.ip-com.com.cn and search for the latest documents for this product.

Technical support

Contact us if you need more help. We will be glad to assist you as soon as possible.

Email address: info@ip-com.com.cn

Website: 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 user guide was released.

Version	Date	Description
V1.2	2024-11-18	- Added the description of Mesh network. - Optimized the description of view system status, Internet settings, RF settings and RF optimization. - Optimized sentence expression.
V1.1	2024-09-25	- Added the description of remote web management function. - Optimized the description about login, security mode, RF settings, RF optimization, advanced settings, QVLAN settings, cloud maintenance, reset, account and factory default settings. - Optimized sentence expression.
V1.0	2024-03-28	Original publication.

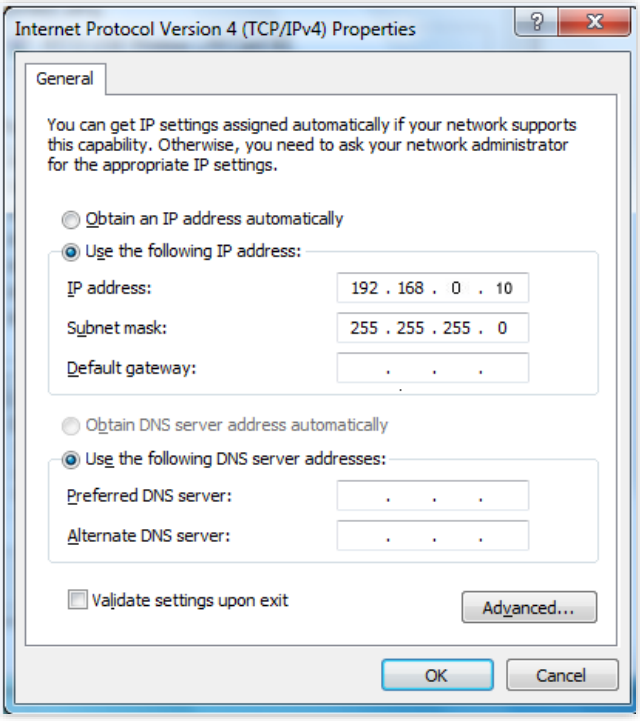
Contents

1 Login and logout

1.1 Login

1. Use an Ethernet cable to connect the management computer to the AP or the switch connected to the AP.
2. Configure the IP address of the computer to one in a same network segment as the AP.

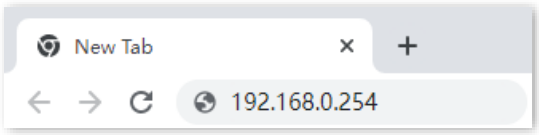
   For example, if IP address of the AP is **192.168.0.254**, then the IP address of the computer can be configured to **192.168.0.*X*** (*X* ranges from 2 to 253 and is unused) and subnet mask is **255.255.255.0**.



3. Start a web browser (such as Chrome) on your computer, and visit the IP address (**192.168.0.254** by default) of the AP.

Tip

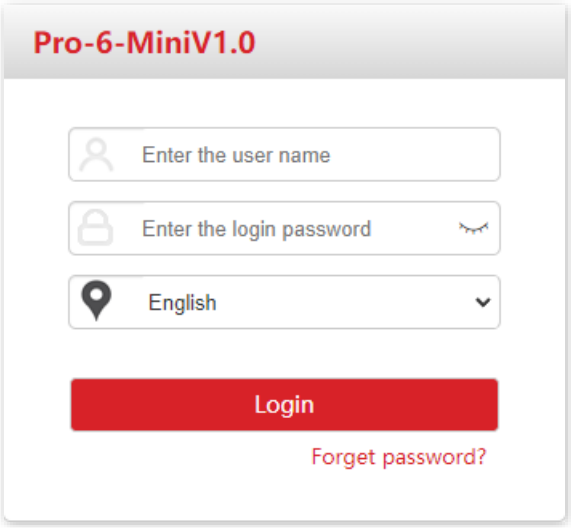
Some APs can log in to the web UI using domain name **ipcwifi.com**. The actual product prevails.



4. Enter the login user name and password, and click **Login**.

Tip

When logging in to the web UI of the AP for the first time, you need to set your user name and password. If the user name and password cannot be customized for the first login, it is possible that you have not upgraded the AP firmware to the latest version. In this case, it is recommended to upgrade the firmware.



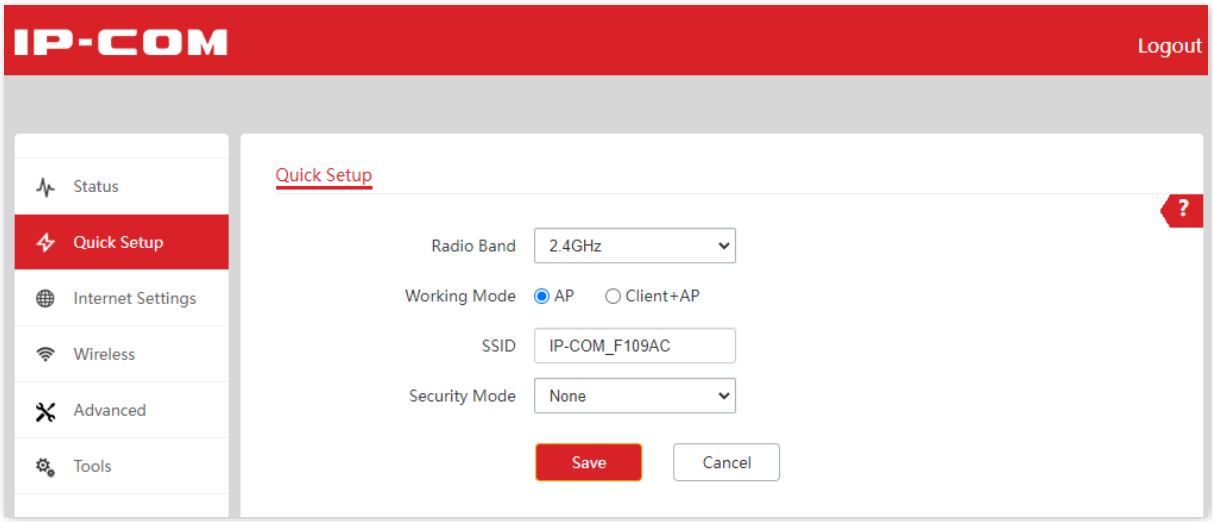
---End

Tip

If the above page does not appear, try the following solutions:

- Ensure that the Ethernet cable is properly connected and not loose.
- If multiple APs are deployed in the network without the DHCP server, IP address conflicts may occur, causing web UI login errors. Connect the APs to the network one by one and modify the IP addresses of the APs.
- If the LAN where the AP is deployed with DHCP server (including IP-COM AC, and IP-COM router that supports AP management), AP may automatically obtain the new IP address from the DHCP server. In this case, you can first check the IP address obtained by the AP in the client list of the DHCP server, and then log in to the web UI of the AP using the new IP address. The computer can be set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Reset the AP and try logging in again.

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



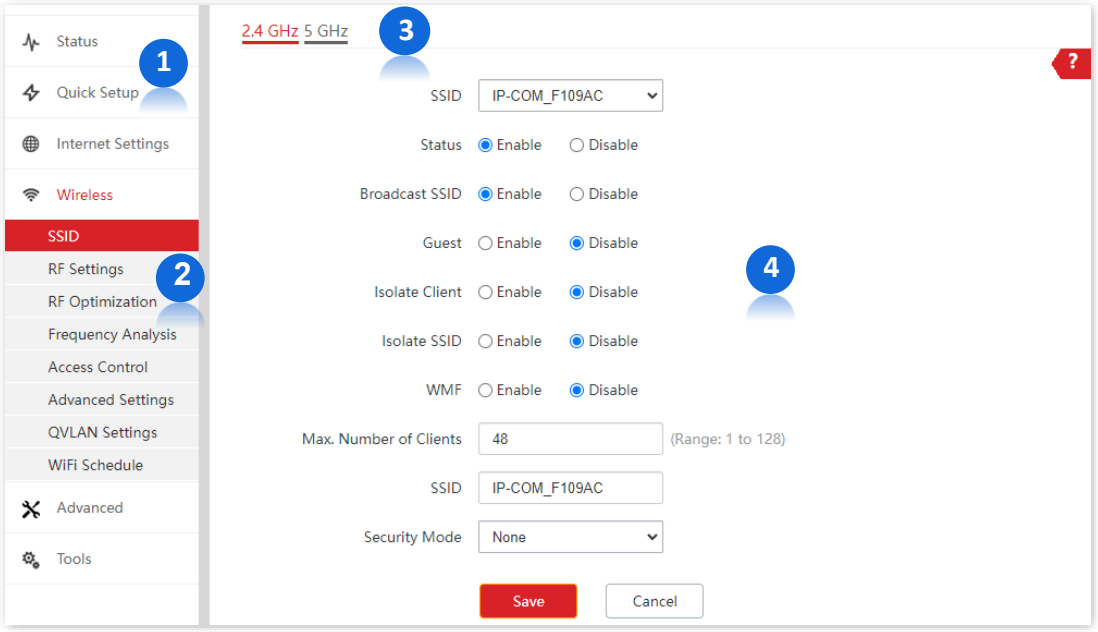
1.2 Logout

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

2 Web UI

2.1 Layout

The web UI is composed of four parts: level-1 navigation bar, level-2 navigation bar, tab page area, and the configuration area. See the following figure.



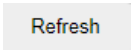
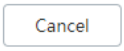
Tip

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

No.	Name	Description
1	Level-1 navigation bar	Used to display the function menu of the AP. Users can select functions in the navigation bars and the configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Tab page area	
4	Configuration area	Area where you perform or check configurations.

2.2 Common buttons

Buttons commonly used on the web UI are illustrated as below.

Common button	Description
	Used to refresh the current page.
	Used to save configurations on the current page and make the configurations take effect.
	Used to cancel the unsaved configurations on the current page and restore to previous configurations.
	Used to check the help information of the current page.

3 Quick setup

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

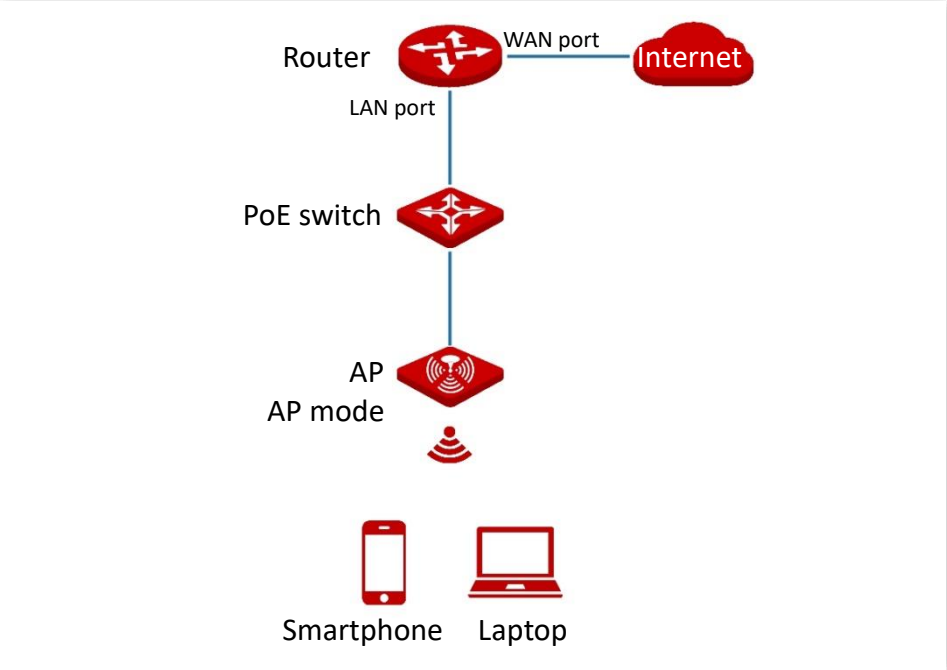
To access the page, log in to the web UI of the AP, and navigate to **Quick Setup**.

On this page, you can set up the AP in a quick way to enable internet access for your WiFi-enabled devices (such as smartphones and laptops).

3.1 AP mode

3.1.1 Overview

In this mode, AP connects to the internet using Ethernet cables and transforms wired signals to wireless signals for wireless coverage. AP works under this mode by default. See the following topology.

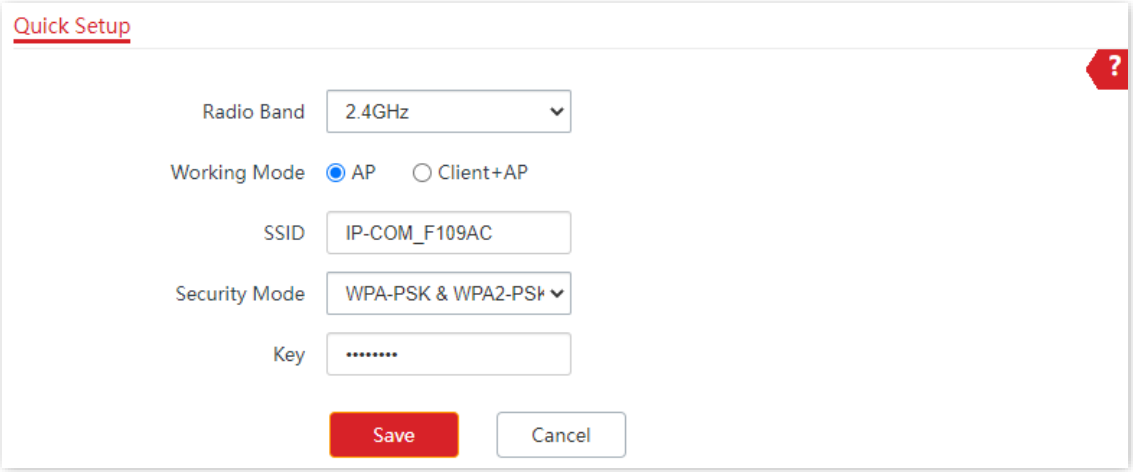


3.1.2 Configure AP mode

Tip

Ensure that the upstream router has been connected to the internet before configuration.

1. Log in to the web UI of the AP, and navigate to **Quick Setup**.
2. Select the **Radio Band** to configure, which is **2.4GHz** in this example.
3. Set **Working Mode** to **AP**.
4. Set an **SSID** (the first SSID).
5. Select a **Security Mode** and configure the incurred parameters.
6. Click **Save**.



7. If you need to configure the other radio band, repeat steps **2** - **6**.

---End

Search and connect your WiFi-enabled devices (such as smartphones) to the **SSID** you set. Enter the wireless password (the **Key** you set) and you can access the internet.

Parameter description

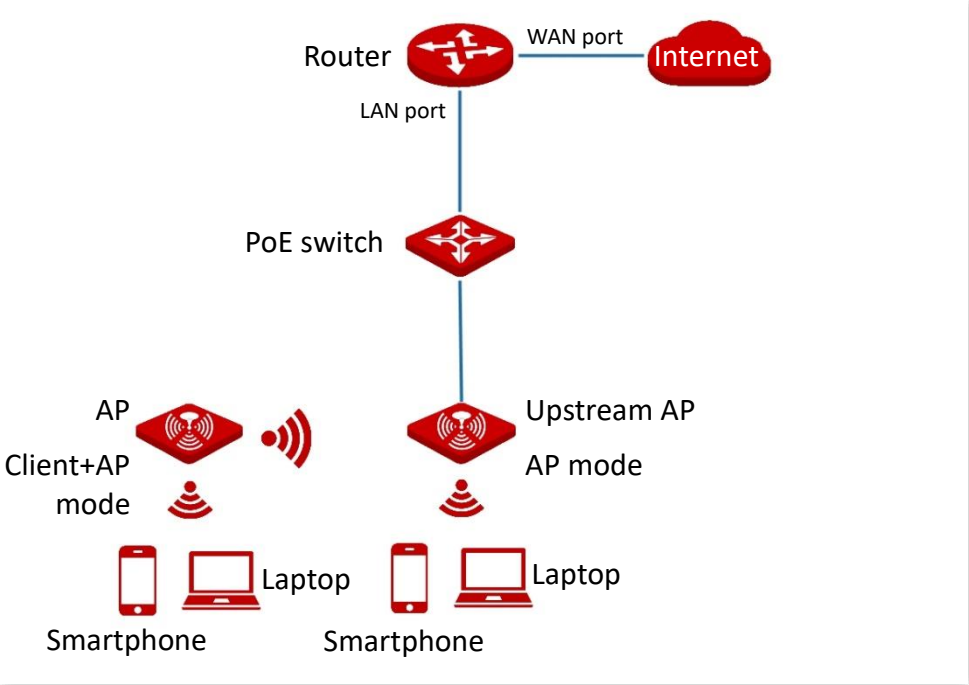
Parameter	Description
Radio Band	Used to select the radio band to configure.
Working Mode	Specifies the working mode of the AP. Select the AP mode to transform the wired network to wireless network.
SSID	Click to modify the wireless name of the first network under the selected radio band.

Parameter	Description
Security Mode	Used to select the security modes for target wireless networks. The security modes for different radio bands may differ. Supported security modes are as follows: None, WEP, WPA-PSK, WPA2-PSK, WPA-PSK&WPA2-PSK, WPA, WPA2, WPA3-SAE and WPA2-PSK&WPA3-SAE. Tip The security modes may differ with different models of APs. The actual product prevails.

3.2 Client+AP mode

3.2.1 Overview

In this mode, the AP is wirelessly bridged to an upstream device (such as a wireless router or AP) to extend the wireless network coverage of the upstream device. See the following figure.

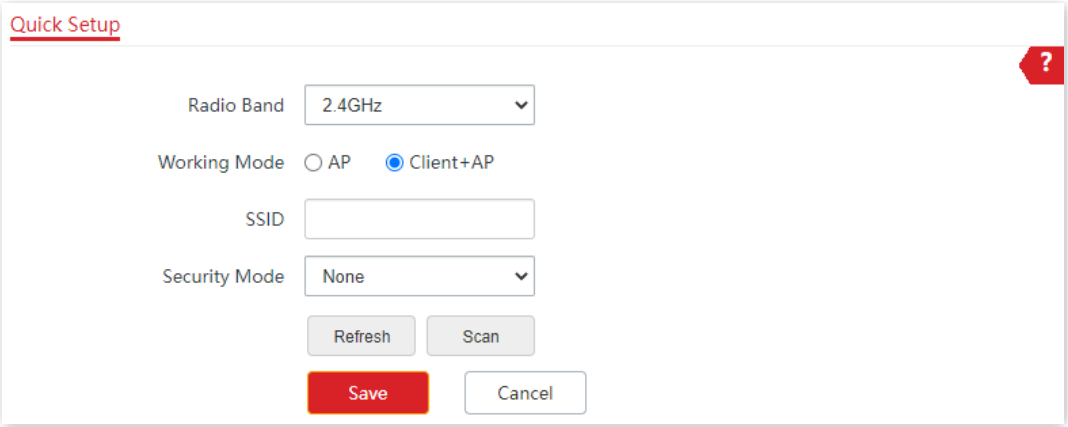


3.2.2 Configure client+AP mode

Tip

Ensure that the upstream AP has been connected to the internet before configuration.

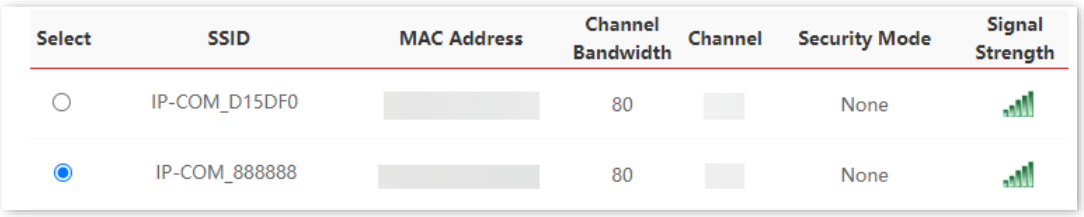
1. Log in to the web UI of the AP, and navigate to **Quick Setup**.
2. Select the **Radio Band** to configure, which is **2.4GHz** in this example.
3. Set **Working Mode** to **Client+AP**.
4. Click **Scan**.



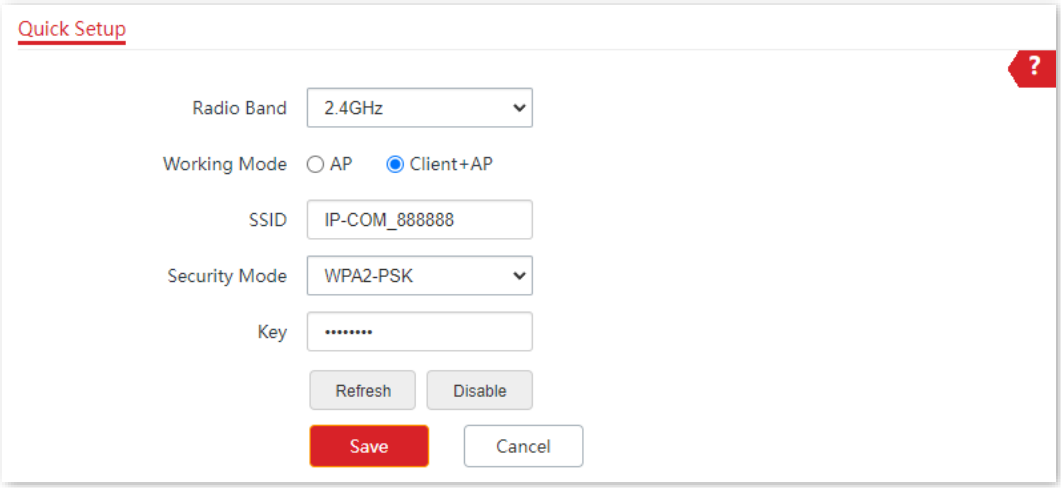
5. Select the wireless network to be extended from the wireless network list that appears.

Tip

- If no wireless network is found, navigate to **Wireless** > **RF Settings**, ensure that **Wireless Network** for the corresponding frequency band is enabled, and try again.
- After a wireless network to be extended is selected, the SSID, security mode, and channel of the wireless network are populated automatically.



6. If the wireless network of the upstream device is encrypted, enter the wireless password of the upstream device in the **Key** box.
7. Click **Save**. The following figure is for reference only.



---End

After the configuration is completed, you can select the SSID on your WiFi-enabled devices (such as smartphones) and enter your wireless password (the **Key** you set) to connect to the wireless network of the AP and access the internet through the AP.

Tip

Navigate to **Wireless** > **SSID** to enter the page, you can view the SSID and key of the AP.

Parameter description

Parameter	Description
Radio Band	Specifies the radio band of the wireless network to be configured.
Working Mode	Specifies the working mode of the AP. Select the Client+AP mode to bridge the upstream wireless network.
SSID	Specifies the wireless name (SSID) of the wireless network to be bridged. After you select the upstream wireless network from the scanned wireless network list, this parameter will be populated automatically.

Parameter	Description
Security Mode	Specifies the security mode of which the upstream wireless network adopted. After you select the upstream wireless network from the scanned wireless network list, this parameter will be populated automatically. The security modes for different radio bands may differ. The AP can support wireless network encrypted with None, WEP WPA-PSK, WPA2-PSK, WPA-PSK&WPA2-PSK, WPA, WPA2, WPA3-SAE and WPA2-PSK&WPA3-SAE. Note - If the wireless network to be bridged adopts the **WEP** security mode, **Authentication Type**, **Default Key**, and **Key *X*** (*X* ranges from 1 to 4) need to be entered manually. - If the wireless network to be bridged adopts the WPA-PSK, WPA2-PSK, WPA-PSK&WPA2-PSK, WPA3-SAE or WPA2-PSK&WPA3-SAE security mode, you need to enter the **Key**.
Refresh	Used to refresh the scan results.
Scan Disable	Scan : Used to scan for available wireless networks nearby. The scan results are displayed at the bottom of the page. Disable : Used to stop scanning and collapse the scan results. This button only appears after you click **Scan**.

4 Status

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

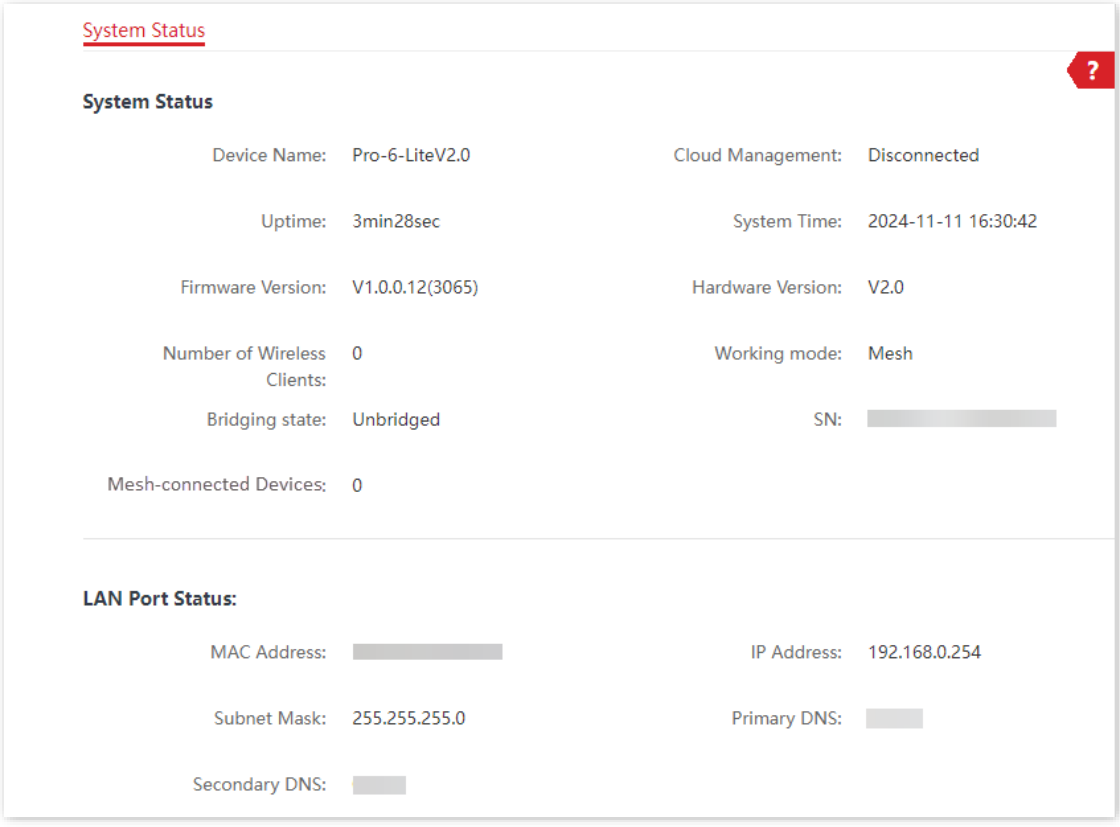
4.1 View system status

Tip

Pro-6-LiteV2.0 is used for illustration here.

To access the page, log in to the web UI of the AP, and navigate to **Status** > **System Status**.

On this page, you can view the system and LAN port status of the AP.



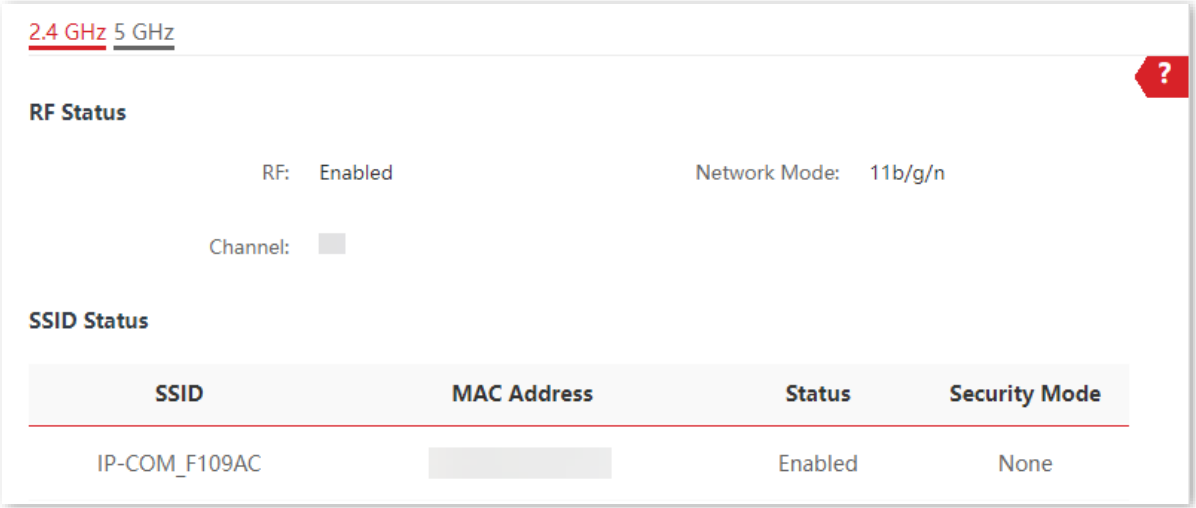
Parameter description

Parameter		Description
System Status	Device Name	Specifies the name of the AP. You can change the AP name on the Internet Settings module.
	Cloud Management	Specifies the connection status between the AP and the ProFi cloud platform.
	Uptime	Specifies the time that has elapsed since the AP was started last time.
	System Time	Specifies the system time of the AP.
	Firmware Version	Specifies the firmware version of the AP.
	Hardware Version	Specifies the hardware version of the AP.
	Number of Wireless Clients	Specifies the number of wireless clients connected to the AP.
	Working mode	Specifies the working mode of the AP.
	Bridging state	Specifies the bridging status of the AP.
	SN	Specifies the of series number of the AP.
	Mesh-connected Devices	Specifies the number of devices connected to the Mesh network with the AP. Tip It is available only when the Mesh network function is enabled.
LAN Port Status	MAC Address	Specifies the physical address of the LAN port of the AP.
	IP Address	Specifies the IP address of the AP and it is also the management IP address of the AP. The web UI of the AP is accessible by visiting this IP address. You can change the IP address on the Internet Settings module.
	Subnet Mask	Specifies the subnet mask of the AP.
	Primary DNS	Specifies the IP address of the primary DNS server of the AP.
	Secondary DNS	Specifies the IP address of the secondary DNS server of the AP.

4.2 View wireless status

To access the page, log in to the web UI of the AP, and navigate to **Status** > **Wireless Status**.

On this page, you can view the RF status and SSID status of the AP. By default, the page displays the information of 2.4 GHz wireless status. To view the wireless status of 5 GHz, click **5 GHz.**



Parameter description

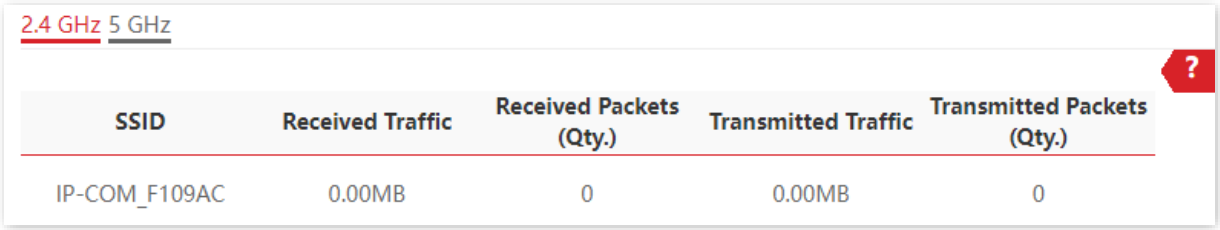
Parameter		Description
RF Status	RF	Specifies the status of the wireless function of the AP.
	Network Mode	Specifies the wireless network mode of the AP.
	Channel	Specifies the working channel of the AP.
SSID Status	SSID	Specifies the names of the wireless networks of the AP.
	MAC Address	Specifies the physical addresses corresponding to the SSIDs of the AP.
	Status	Specifies the status of the wireless networks corresponding to the SSIDs of the AP.
	Security Mode	Specifies the security modes of the wireless networks corresponding to the SSIDs of the AP.

4.3 View traffic statistics

To access the page, log in to the web UI of the AP, and navigate to **Status** > **Traffic Statistics**.

On this page, you can view the packet statistics for the wireless network of the AP.

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



Parameter description

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

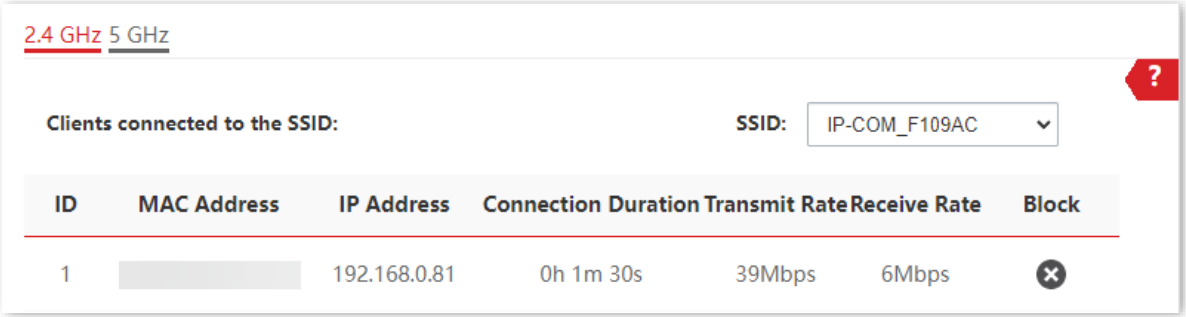
Note

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

4.4 View client list

To access the page, log in to the web UI of the AP, and navigate to **Status** > **Client List**.

On this page, you can view the information about the wireless clients connected to the wireless networks corresponding to the SSIDs of the AP. You can also disconnect certain connected clients.



By default, the page displays information about the wireless clients connected to the 2.4 GHz wireless network corresponding to the first SSID of the AP. You can select the SSID from the drop-down list box on the upper-right corner. To view information about the wireless clients connected to the 5 GHz wireless network corresponding to the SSID, click the **5 GHz** tab.

Parameter description

Parameter	Description
SSID	Used to select a wireless name from the drop-down menu to view wireless clients connected to the wireless network.
MAC Address	Specifies the MAC address of the wireless client.
IP Address	Specifies the IP address of the wireless client.
Connection Duration	Specifies the online duration of the wireless client.
Transmit Rate	Specifies the transmit rate of the wireless client.
Receive Rate	Specifies the receive rate of the wireless client.
Block	Click to disconnect the corresponding wireless client, and the client is added to the blocklist of the Access Control. The client cannot connect to the AP again by reconnecting to the wireless network. To unblock a client, navigate to Access Control.

5 Internet settings

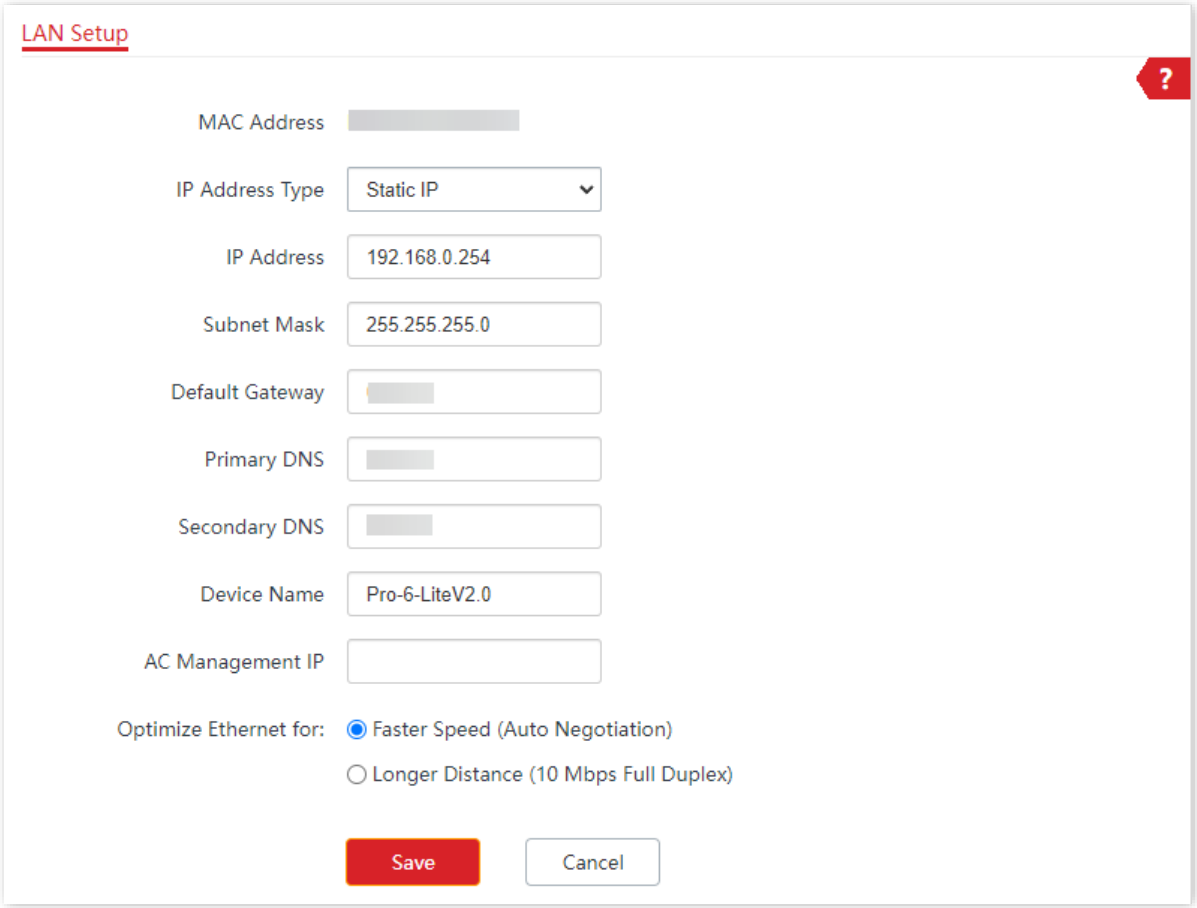
This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

Tip

Pro-6-LiteV2.0 is used for illustration here.

To access the page, log in to the web UI of the AP, and navigate to **Internet Settings**.

On this page, you can view the MAC address of the LAN port of the AP and set the IP address, device name, and other related parameters of the AP.



Parameter description

Parameter	Description
MAC Address	Specifies the MAC address of the LAN port of the AP.
IP Address Type	Specifies the IP address obtaining mode of the AP. – **Static IP**: It indicates that the IP address, subnet mask, gateway, and DNS server of the AP is set manually. It is proper for the scenarios where only one or several APs are required in the network. – **DHCP (Dynamic IP Address)**: It indicates that the IP address, subnet mask, gateway, and DNS server of the AP is obtained from a DHCP server on your LAN. It is proper for the scenarios where a large group of APs are required in the network.  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	Specifies the IP address of the AP. The web UI of the AP is accessible at this IP address. The default IP address is **192.168.0.254**.
Subnet Mask	Specifies the subnet mask of the IP address of the AP. The default subnet mask is **255.255.255.0**.
Default Gateway	Specifies the gateway IP address of the AP. Generally, set the gateway IP address to the LAN IP address of your LAN router connected to the internet, so that the AP can access the internet.
Primary DNS	Specifies the primary DNS server of the AP. If your LAN router connected to the internet provides the DNS proxy function, this IP address can be the LAN IP address of the router. Otherwise, enter a correct DNS server IP address.
Secondary DNS	Specifies the IP address of the secondary DNS server of the AP. This parameter is optional. If a DNS server IP address in addition to the IP address of the primary DNS server is available, enter the additional IP address in this field.
Device Name	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.

Parameter	Description
AC Management IP	The AP that is configured with this option will be used as a lighthouse AP. The AP will discover the AC based on the AC address filled in. At the same time, it will guide other APs in the local area network to discover AC. If the current AP is offline, other APs that have been managed by AC in the same local area network will replace it and guide other APs in the LAN to add AC. There is only one lighthouse AP in a local area network.  This function is available on some APs. The actual product prevails.
Optimize Ethernet for	Specifies the Ethernet mode of the PoE power-supply port of this AP. – **Fast Speed (Auto Negotiation)**: This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. – **Longer Distance (10 Mbps Full Duplex)**: This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps). The **Longer Distance (10 Mbps Full Duplex)** mode is recommended only if the Ethernet cable that connects the PoE power-supply port of the AP to a peer device exceeds 100 meters. In this case, the connected LAN port of the peer device must work in auto-negotiation mode. Otherwise, the PoE power-supply port of the AP may not be able to properly transmit or receive data.  This function is available on some APs. The actual product prevails.

6 Wireless settings

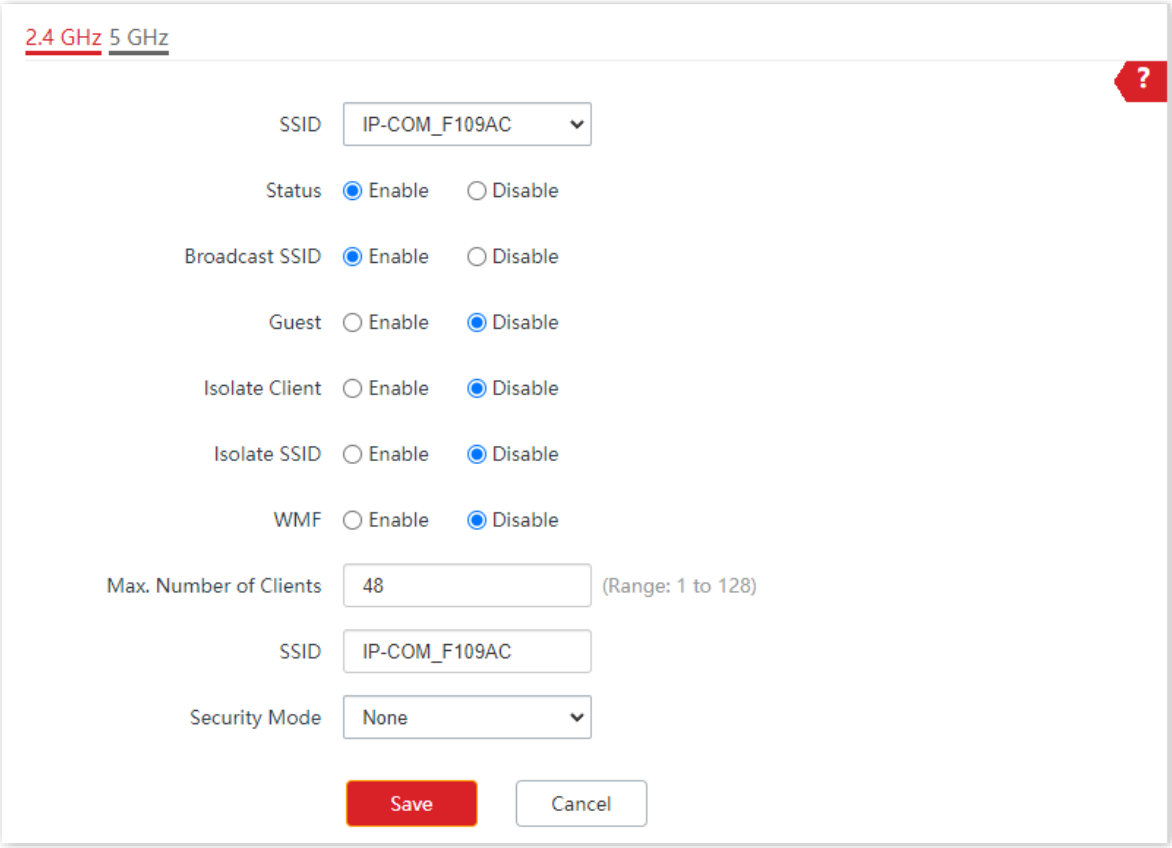
This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

6.1 SSID settings

6.1.1 Overview

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **SSID**.

On this page, you can set SSID-related parameters of the AP.



Parameter description

Parameter	Description
2.4 GHz 5 GHz	Used to select the radio band of the AP to be configured.
SSID	Specifies the SSID to be configured. The first SSID displayed on the page under the radio band tab is the primary SSID of the radio band by default.
Status	Specifies the status of the selected SSID. The first SSID is enabled by default while other SSIDs are disabled by default. You can enable them as required.
Broadcast SSID	Specifies whether to enable the broadcast SSID function. After this function is disabled, the AP does not broadcast the SSID and nearby wireless clients cannot detect the SSID. In this case, you need to enter the SSID manually on your wireless client if you want to connect to the wireless network corresponding to the SSID. It enhances the security of the wireless network.
Guest	Specifies whether to enable the guest function. After this function is enabled, wireless clients connected to the wireless network can only access the internet and cannot access LAN resources (including the web UI of the AP).
Isolate Client	Specifies whether to enable the isolate client function. After this function is enabled, 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.  It is available only when the Guest function is disabled.
Isolate SSID	Specifies whether to enable the isolate SSID function. After this function is enabled, WiFi-enabled devices connected to different SSIDs of the AP cannot communicate with each other, enhancing the security of the wireless network.  It is available only when the Guest function is disabled.

Parameter	Description
WMF	Specifies whether to enable the WMF function. 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	Specifies the maximum number of clients that can be concurrently connected to the wireless network corresponding to an SSID. After this upper limit is reached, new clients cannot connect to the SSID unless some clients cut off their connections.
SSID	Used to change the selected SSID.
Security Mode	Specifies the security mode of the selected SSID. The options include: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, WPA2, WPA3-SAE and WPA2-PSK&WPA3-SAE. Tip The security modes may differ with different models of APs. The actual product prevails.

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.

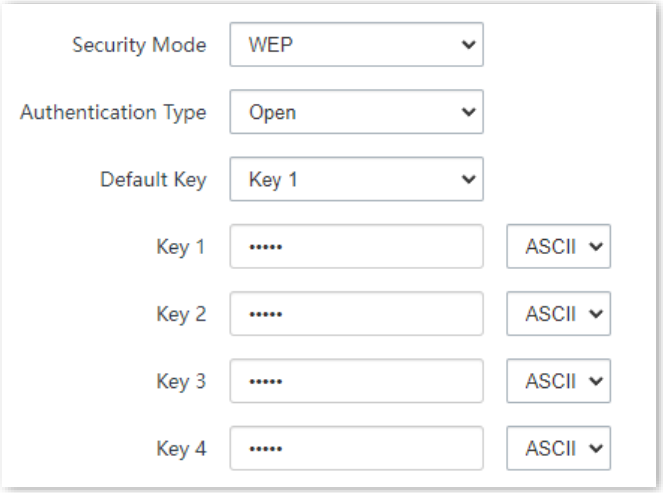
The AP supports various security modes for network encryption, including None, WEP, WPA-PSK, WPA2-PSK, WPA-PSK&WPA2-PSK (Mixed WPA/WPA2-PSK), WPA, WPA2, WPA3-SAE and WPA2-PSK&WPA3-SAE.

- **None**

  It indicates that any wireless client can connect to the wireless network. This option is not recommended because it affects network security.

- **WEP**

  It uses a static key to encrypt all exchanged data, and ensures that a wireless LAN has the same level of security as a wired LAN. Data encrypted based on WEP can be easily cracked. In addition, WEP supports a maximum wireless network throughput of only 54 Mbps. Therefore, this security mode is not recommended.



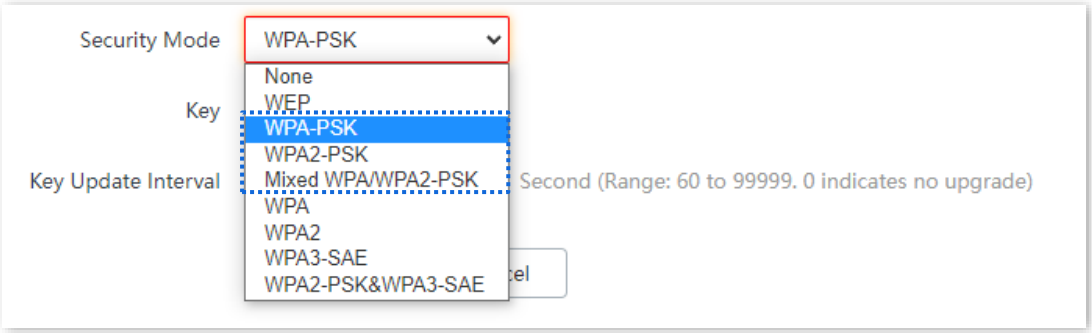
Parameter description

Parameter	Description
Authentication Type	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	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	Specifies 4 WEP keys which 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 WPA-PSK&WPA2-PSK (Mixed WPA/WPA2-PSK)**

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

WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK (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 wireless networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all clients 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.

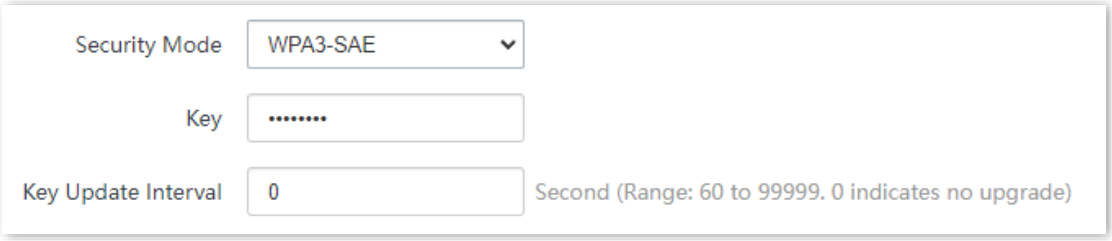


- **WPA3-SAE**

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 wireless experience is unsatisfying, you are recommended to set the security mode to WPA2-PSK.



- **WPA2-PSK&WPA3-SAE**

It indicates that the wireless network adopts the mixed encryption mode of WPA2-PSK/AES and WPA3-SAE/AES to ensure safety.

Parameter description

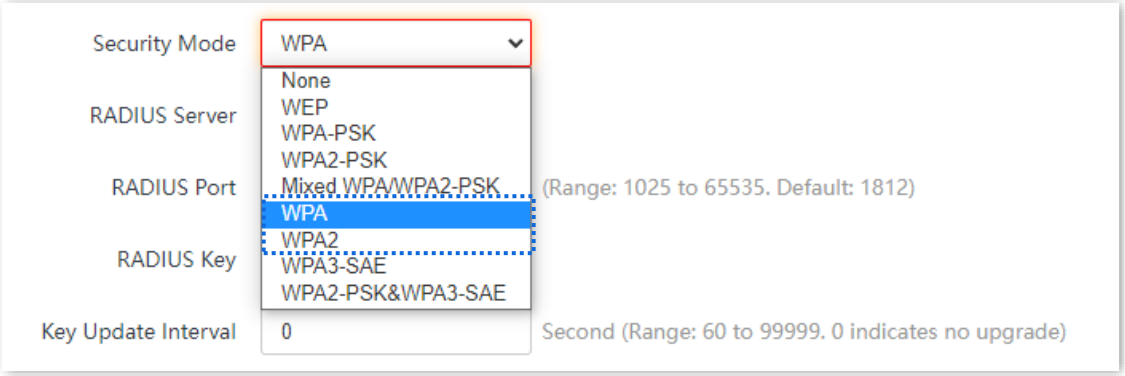
Parameter	Description
Security Mode	Specifies the personal or pre-shared key security mode, including **WPA-PSK**, **WPA2-PSK**, **WPA-PSK&WPA2-PSK (Mixed WPA/WPA2-PSK)**, **WPA3-SAE** and **WPA2-PSK&WPA3-SAE**. – **WPA-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA-PSK. – **WPA2-PSK**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA2-PSK. – **WPA-PSK&WPA2-PSK (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. – **WPA3-SAE**: It indicates that the wireless network corresponding to the selected SSID is encrypted with WPA3-SAE. – **WPA2-PSK&WPA3-SAE**: The wireless network adopts the mixed encryption mode of WPA2-PSK/AES and WPA3-SAE/AES to ensure safety.
Key	Specifies a pre-shared WPA key, that is, the password clients use to connect to the wireless network.
Key Update Interval	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 Wi-Fi Alliance puts forward WPA and WPA2, which use 802.1x to authenticate clients and generate data encryption–oriented root keys. WPA and WPA2 use the root keys to replace the pre-shared keys that set manually, but adopt the same encryption process as WPA-PSK and WPA2-PSK.

WPA and WPA2 uses 802.1x to authenticate clients and the login information of a client is managed by the client. This effectively reduces the probability of information leakage. In addition, each time a client 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 client. This makes it difficult for attackers to obtain the key. These features of WPA and WPA2 help significantly

increase network security, making WPA and WPA2 the preferred security modes of wireless networks that require high security.



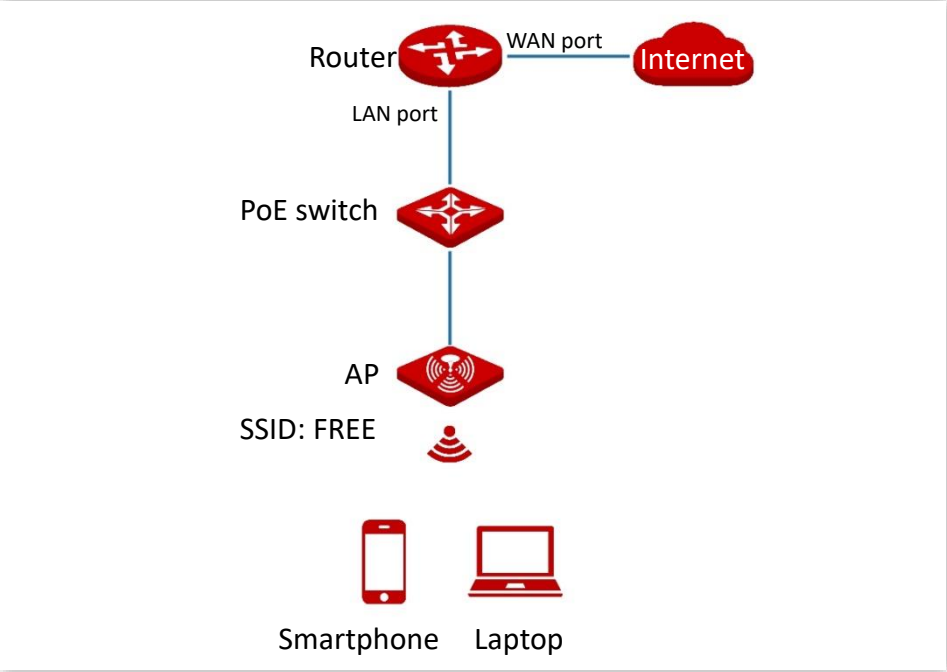
Parameter description

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	Specifies the IP address of the RADIUS server for client authentication.
RADIUS Port	Specifies the port number of the RADIUS server for client authentication.
RADIUS Key	Specifies the shared key of the RADIUS server.
Key Update Interval	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.

6.1.2 Example of setting up an open wireless network

Networking requirements

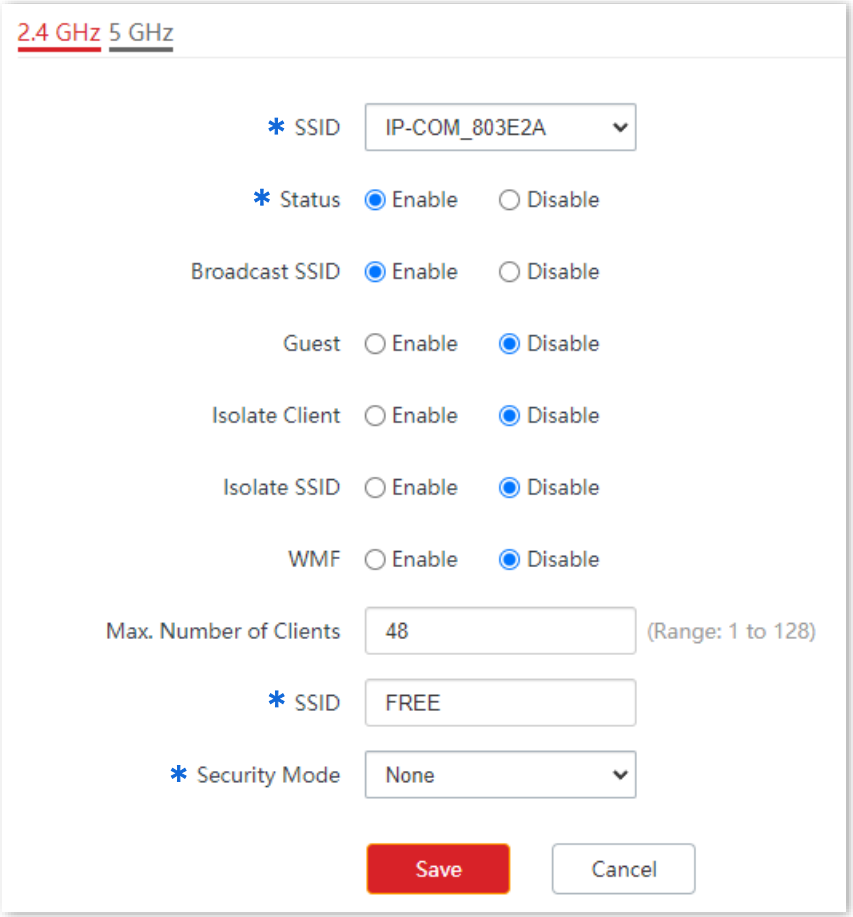
In a hotel lounge, guests can connect to the wireless network without a password and access the internet through the wireless network.



Configuration procedure

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

1. Log in to the web UI of the AP, and navigate to **Wireless** > **SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Set **SSID** to **FREE**.
5. Set **Security Mode** to **None**.
6. Click **Save**.



---End

Verification

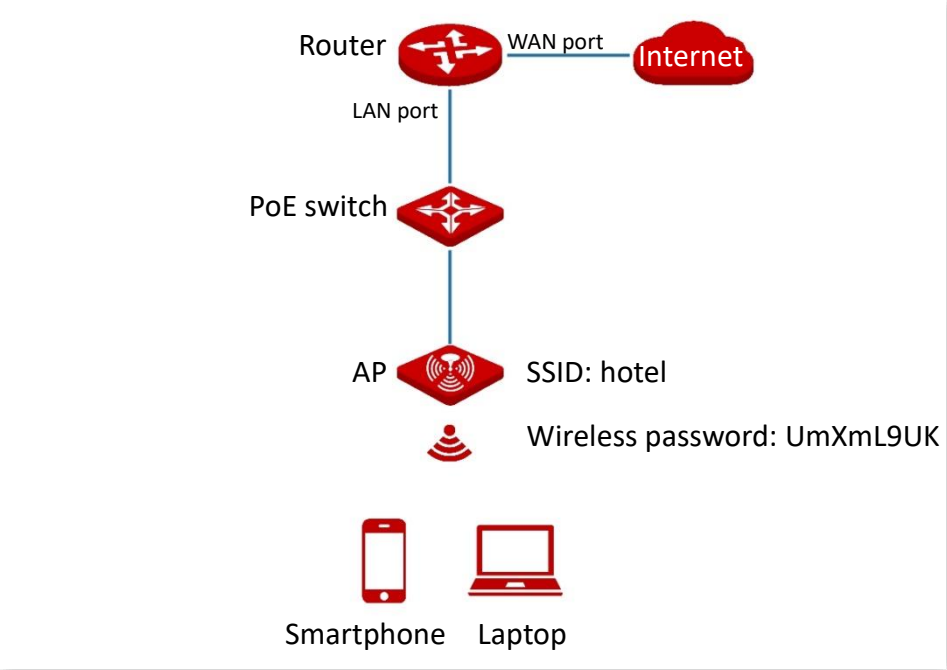
Verify that WiFi-enabled devices can connect to the **FREE** wireless network without a password.

6.1.3 Example of setting up a wireless network encrypted with PSK

Networking requirements

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

Assume that the SSID is **hotel** and the wireless password is **UmXmL9UK**. See the following figure.

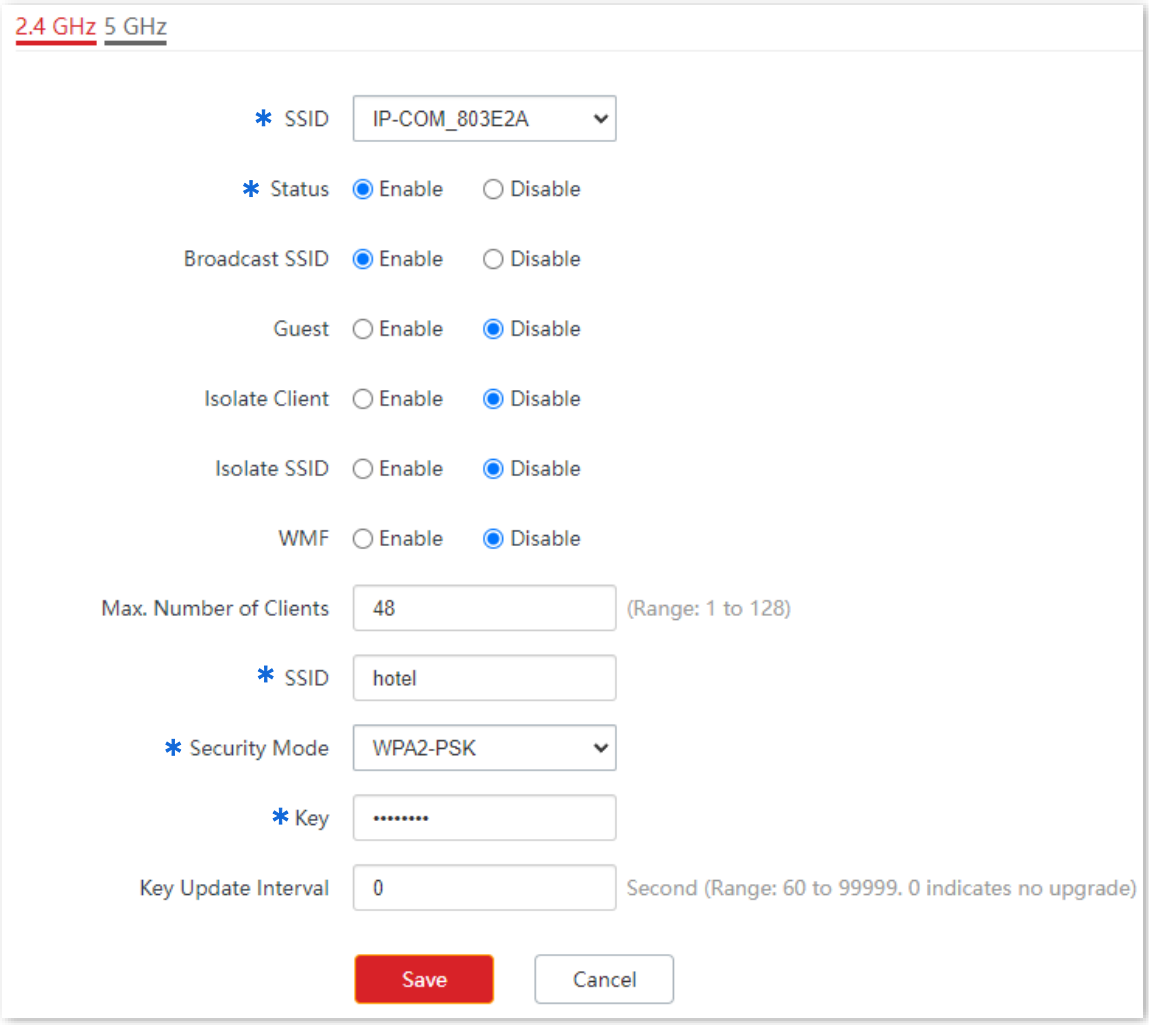


Configuration procedure

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

1. Log in to the web UI of the AP, and navigate to **Wireless** > **SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Set **SSID** to **hotel**.
5. Set **Security Mode**, which is **WPA2-PSK** in this example.
6. Set **Key** to **UmXmL9UK**.

7. Click **Save**.



---End

Verification

Verify that WiFi-enabled devices can connect to the wireless network named **hotel** with the password **UmXmL9UK**.

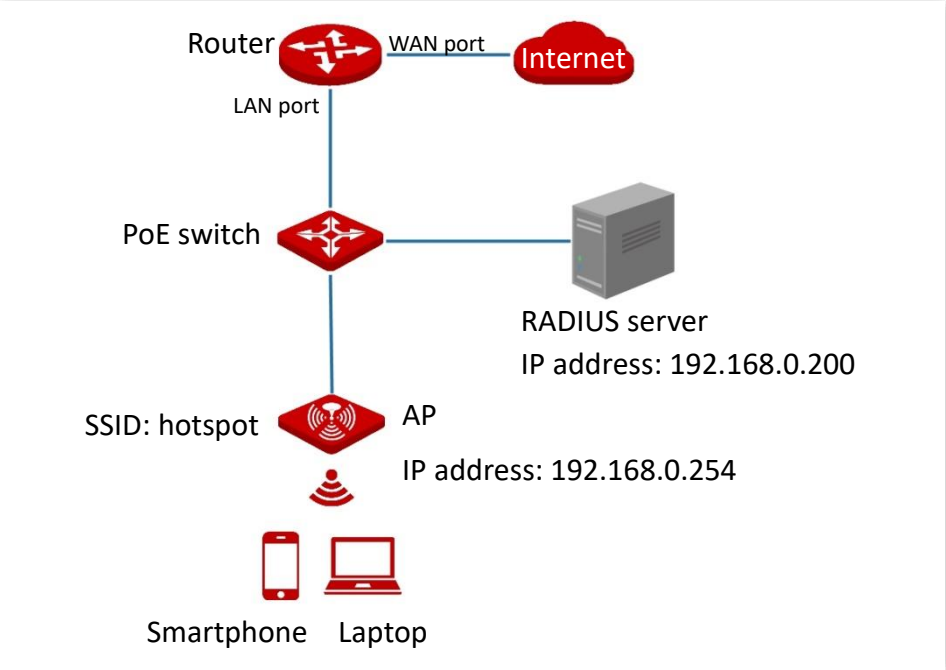
6.1.4 Example of setting up a wireless network encrypted with WPA or WPA2

Networking requirements

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.

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

- SSID: **hotspot**
- IP address of the RADIUS server: **192.168.0.200**
- RADIUS port: **1812**
- RADIUS key: **UmXmL9UK**



Configuration procedure

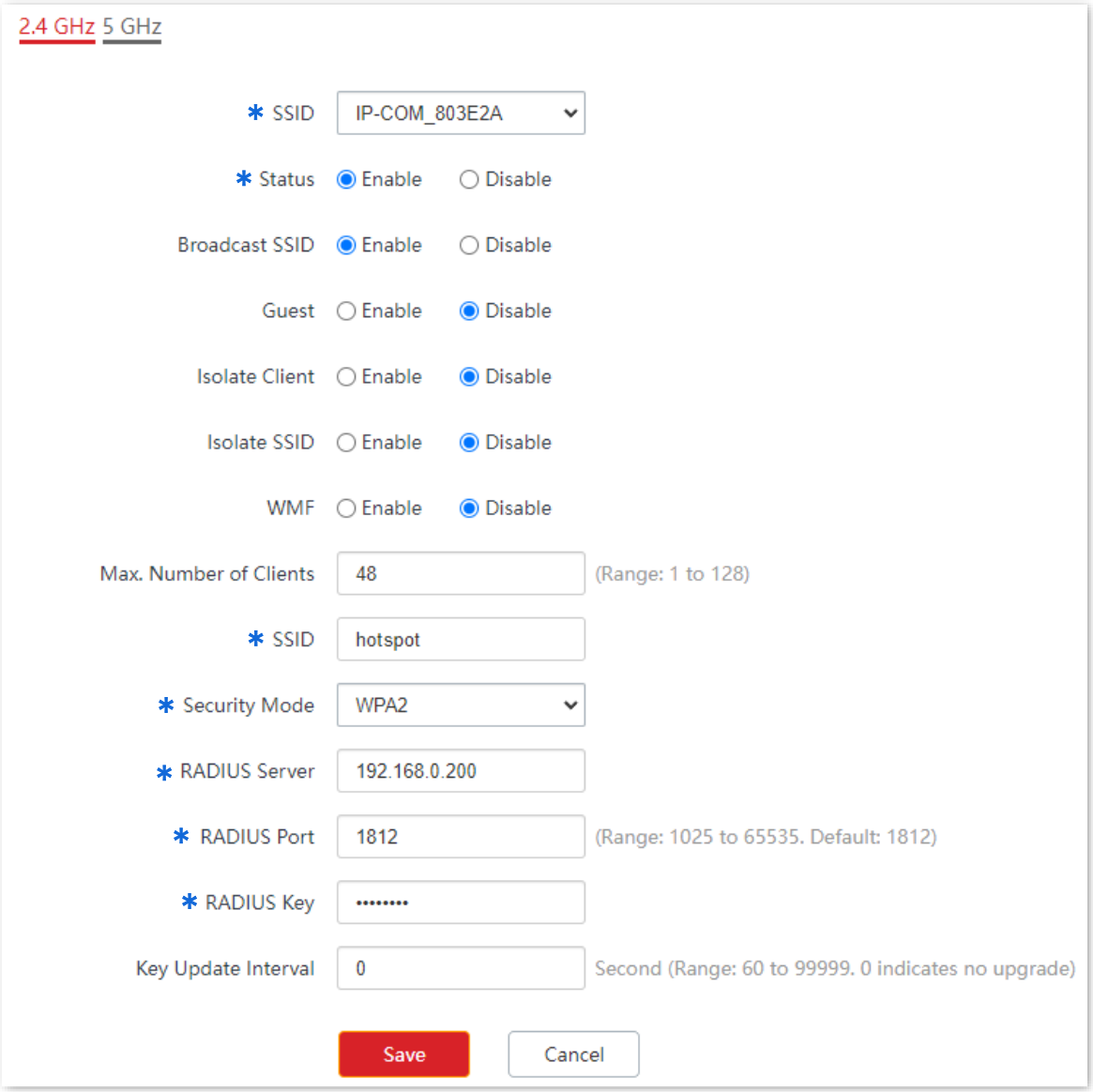
I. Configure the AP

1. Log in to the web UI of the AP, and navigate to **Wireless** > **SSID**.
2. Select the second SSID from the **SSID** drop-down list box.
3. Set **Status** to **Enable**.
4. Set **SSID** to **hotspot**.

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

6. Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Key** to **192.168.0.200**, **1812**, and **UmXmL9UK** respectively.

7. Click **Save**.



---End

II. Configure the RADIUS server

Windows 2016 is used as an example to describe how to configure the RADIUS server.

1. Install **Active Directory Certificate Services** and **Network Policy and Access Services**, and deploy the certificate.

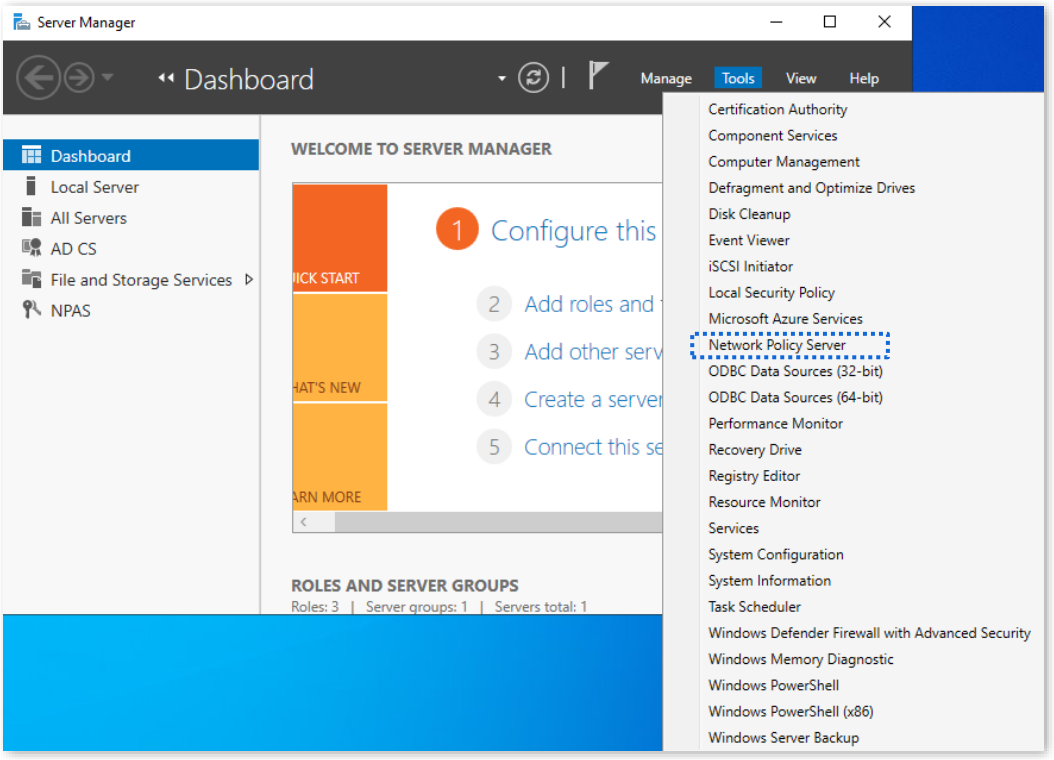
   On the **Start** > **Server Manager** > **Dashboard** page, navigate to **Add roles and features** > **Server Selection** > **Server Roles**, and tick the **Active Directory Certificate Services**. According

to the operation wizard, install the **Certification Authority** of **Active Directory Certificate Services** and **Network Policy and Access Services**.

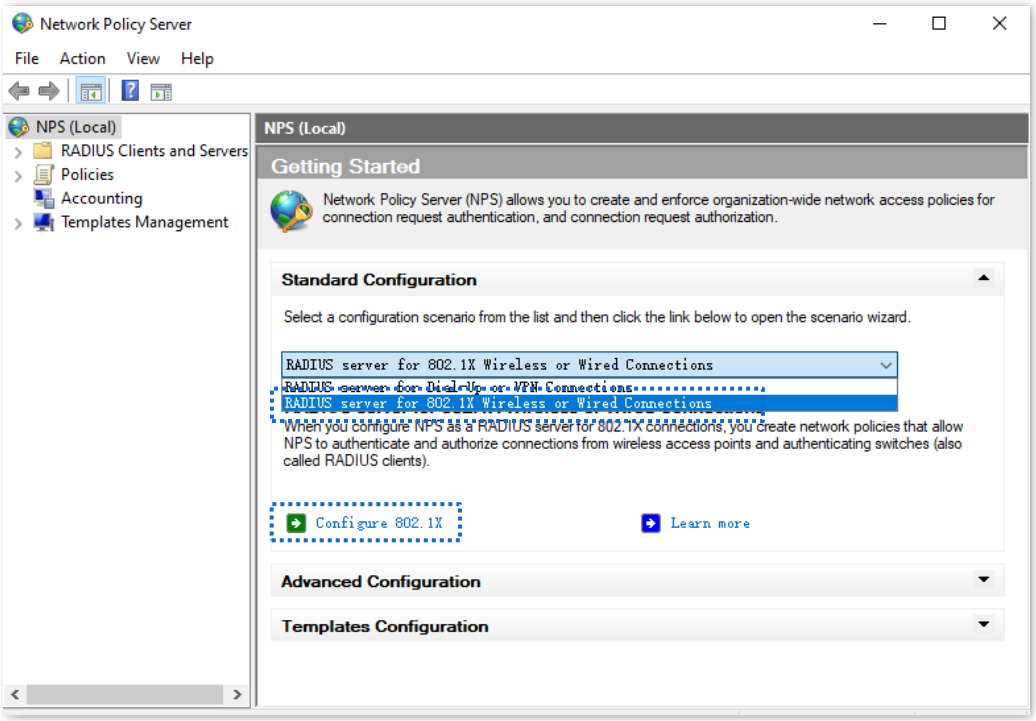
After the service installation is completed, click  in the upper right corner and follow the prompts to deploy the certificate.

2. Configure 802.1X.

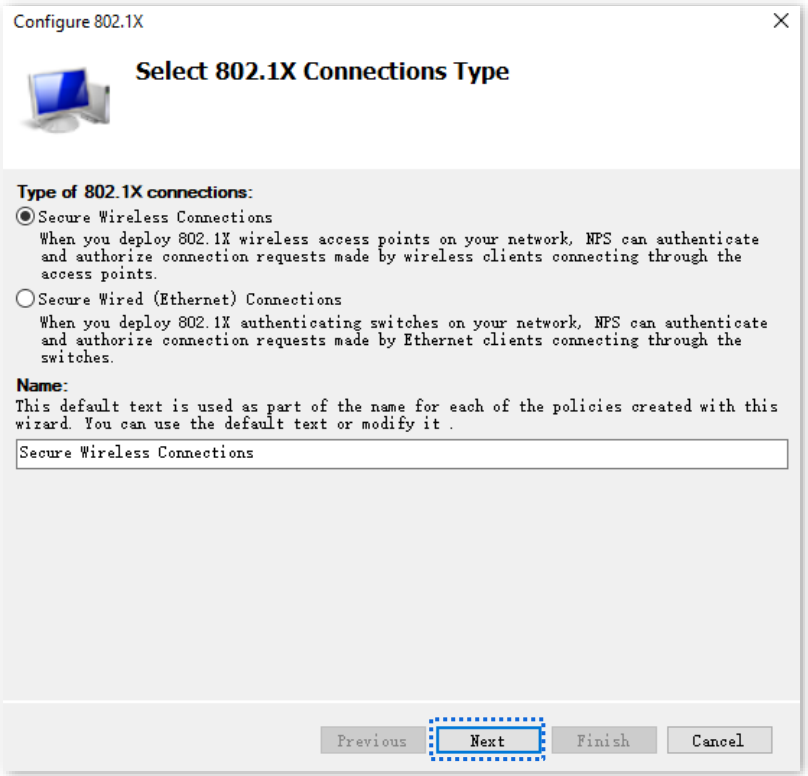
1) Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, and click **Network Policy Server**.



2) Select **RADIUS server for 802.1X Wireless or Wired Connection** from **Standard Configuration** and click **Configure 802.1X**.

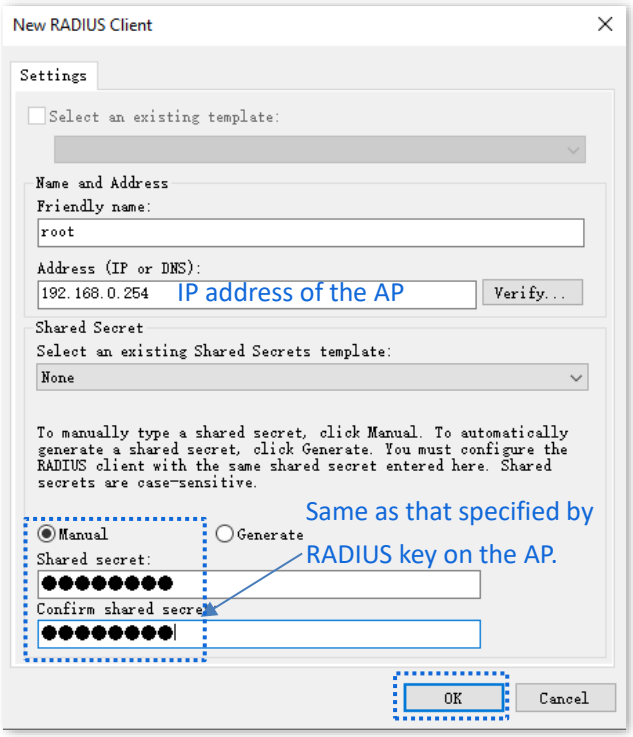


3) Select **Secure Wireless Connections** for **Type of 802.1X connections**. Modify the name as required, which is **Secure Wireless Connections** in this example, and click **Next**.

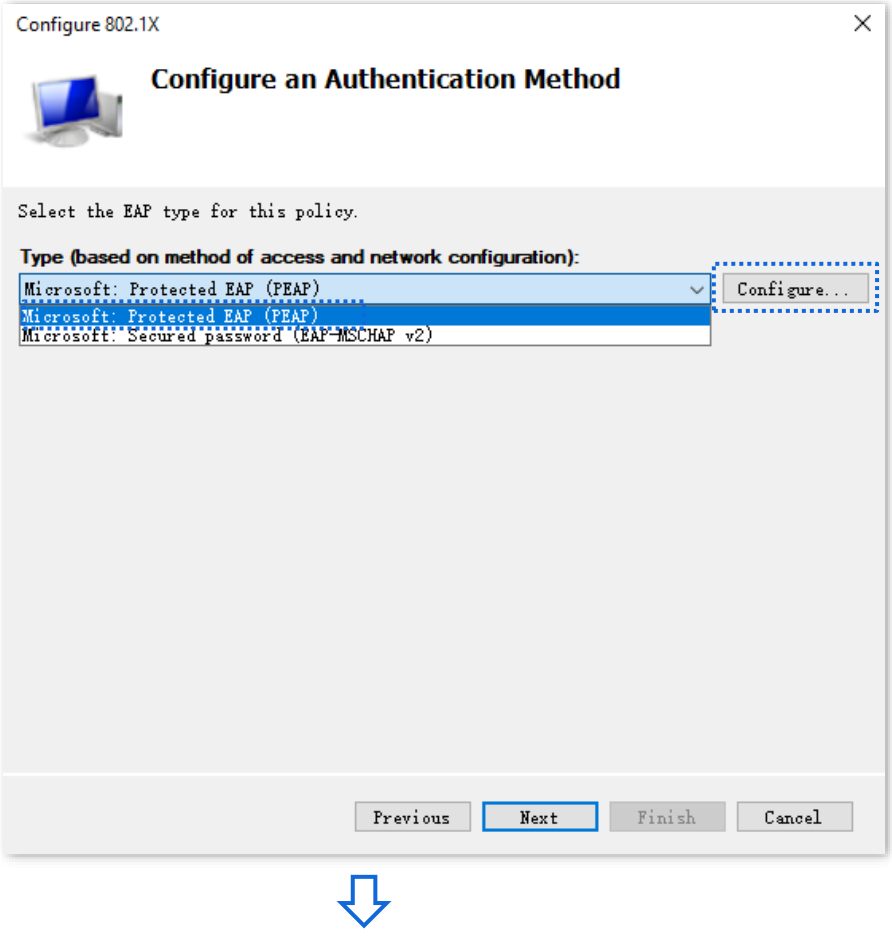


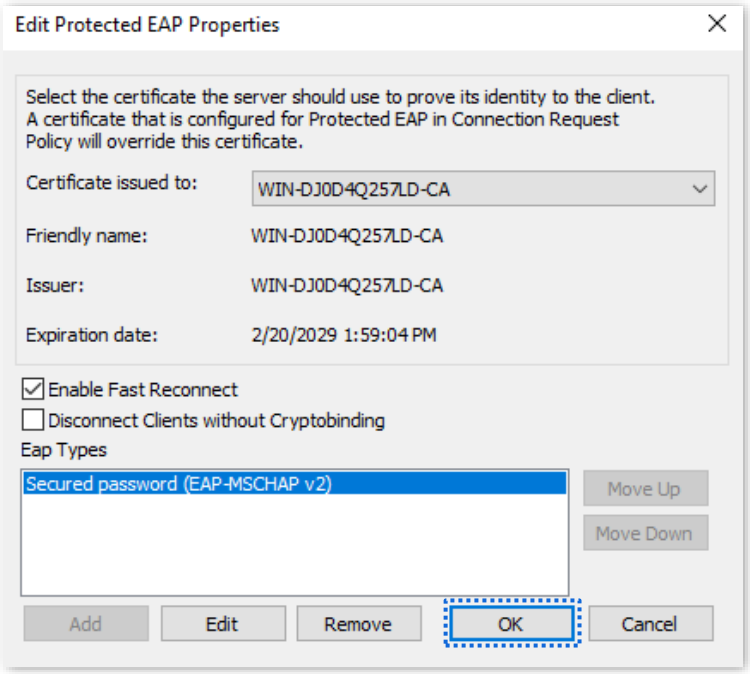
4) On the **Specify 802.1X Switches** page, click **Add**.

5) Set a RADIUS client name (which can be the name of the AP) and the IP address of the AP. Enter **UmXmL9UK** in the **Shared secret** and **Confirm shared secret** text boxes, and click **OK**.

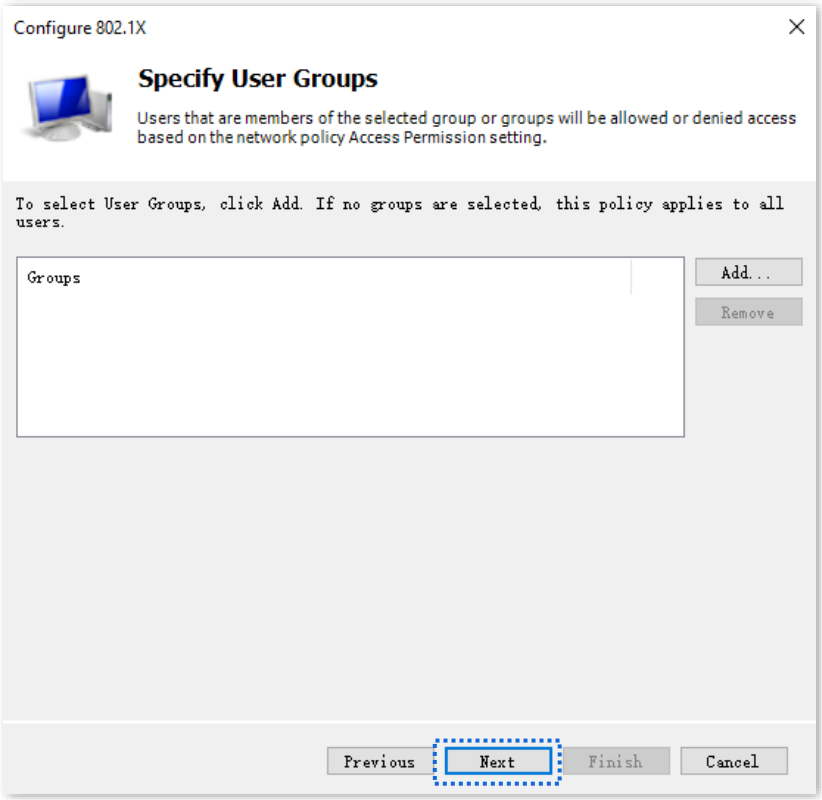


6) Select **Microsoft: Protected EAP (PEAP)** from **Type**, and click **Configure**. Select the certificate deployed in the certificate authority in the previous step, click **OK**, and click **Next** after the configuration is completed.

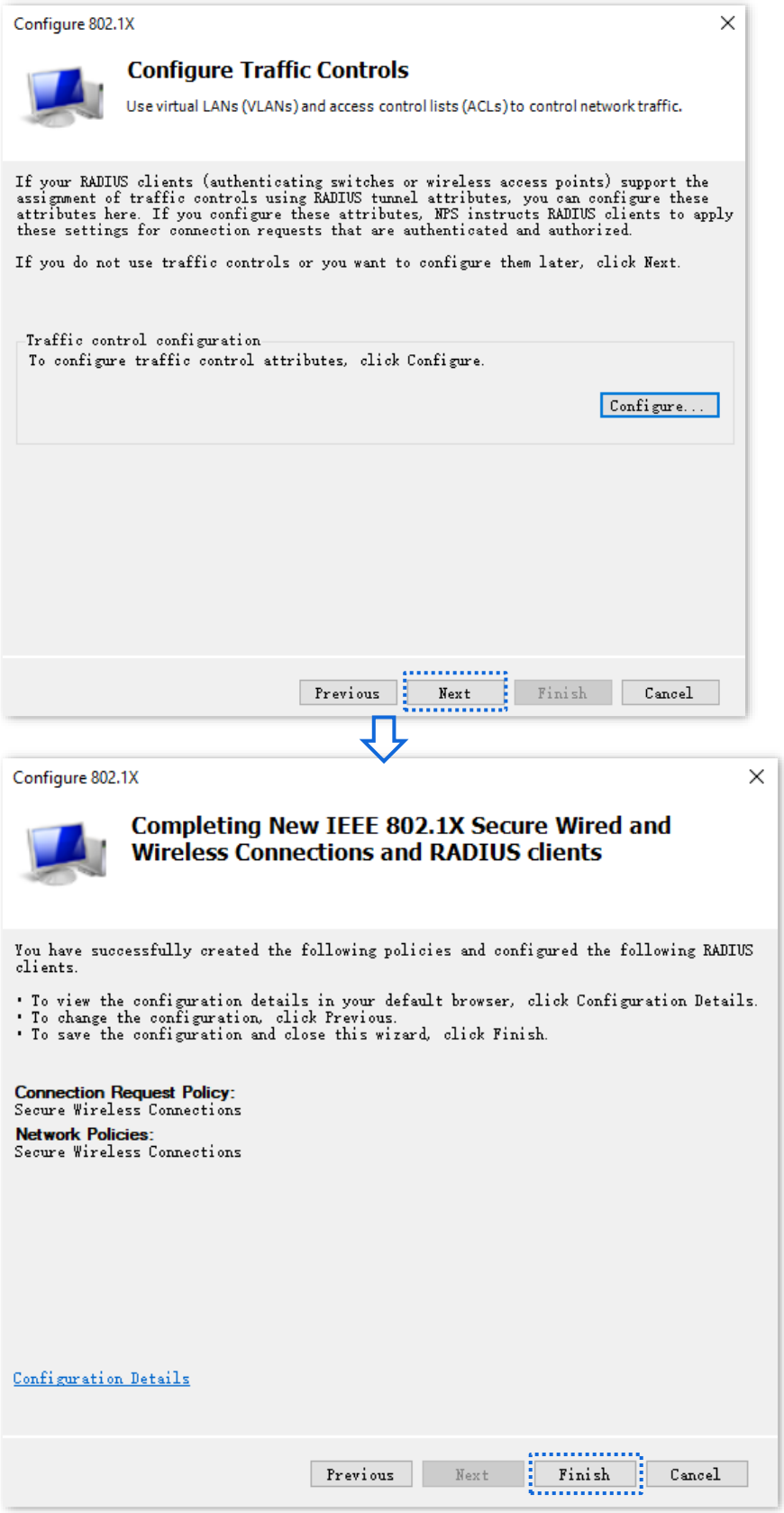




7) Click **Next** on the **Specify User Groups** page.



8) On the **Configure Traffic Controls** page, configure the parameters as required, click **Next**, and click **Finish**.

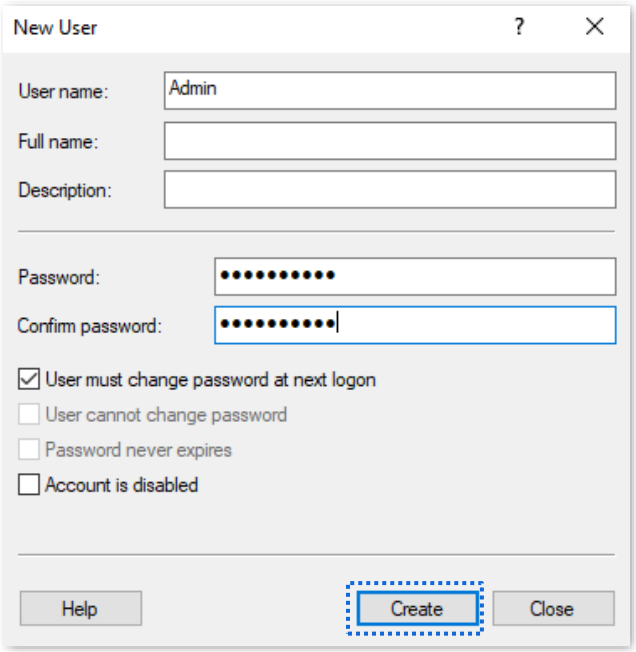


3. Configure the user and user group.

   1) Create a user.

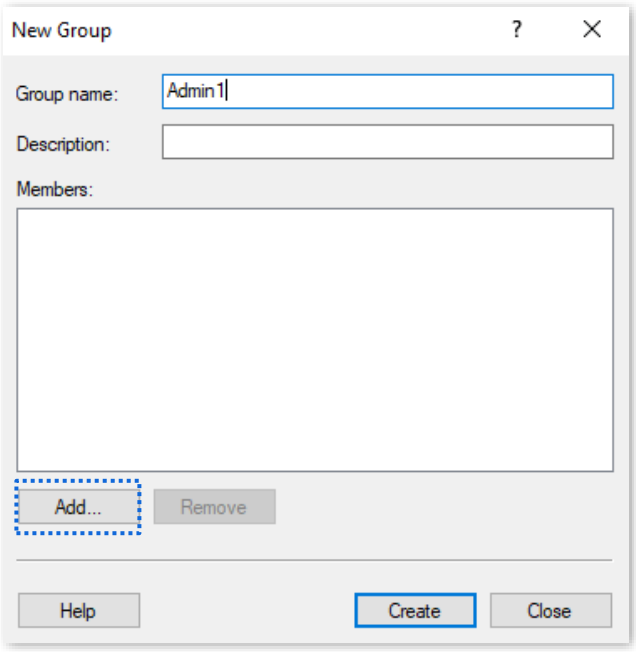
Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, click **Computer Management**, and double-click **Local Users and Groups**.

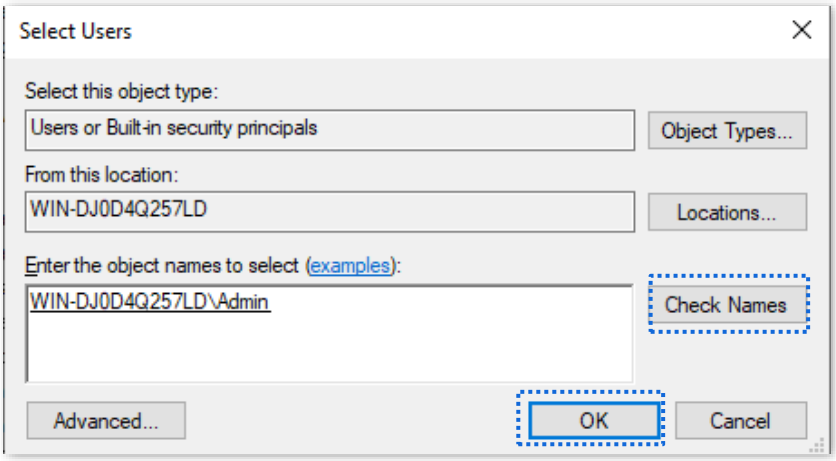
Right-click **Users**, and select **New User**. Enter the user name and password, which are **Admin** (user name) and **JohnDoe123** (password) in this example. And click **Create**.



2) Create a user group.

Right-click **Groups**, and select **New Group**. Set **Group name**, which is **Admin1** in this example, and click **Add**. In the **Enter the object names to select** column, enter the created user name, click **Check Names**, and click **OK**. In the **New Group** window, click **Create**.

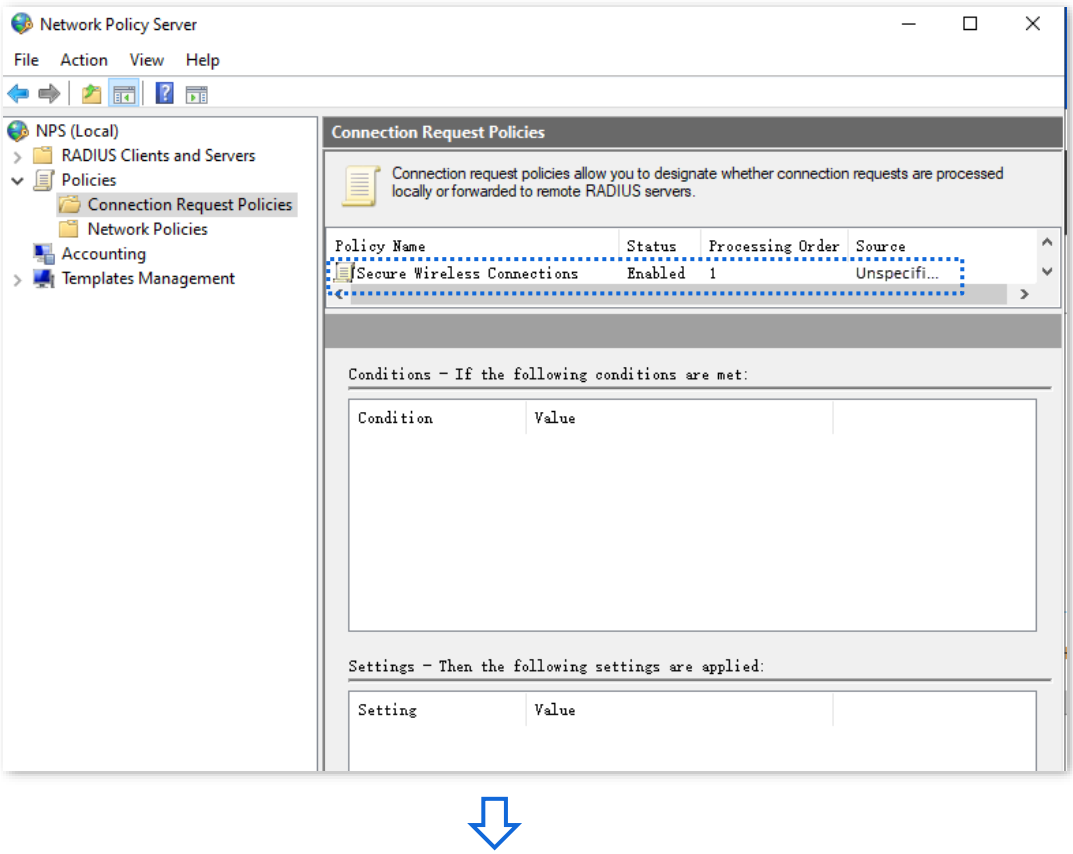


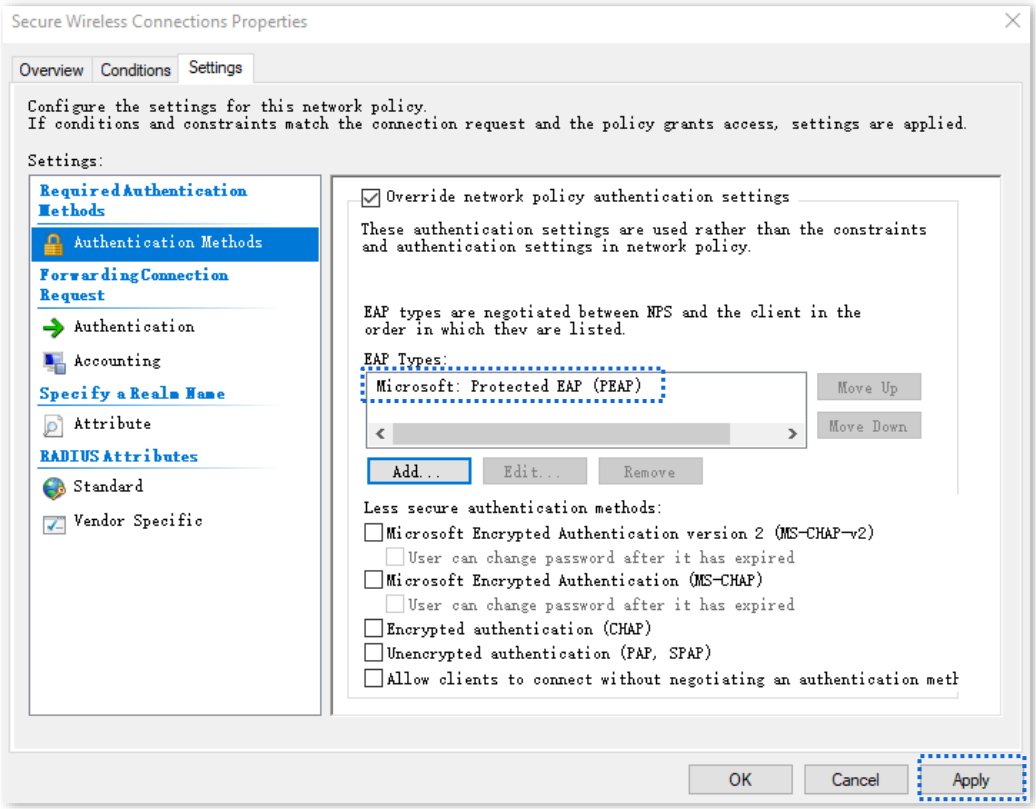


4. Configure the policies.

1) Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, click **Network Policy Server**, and double-click **Policies**.

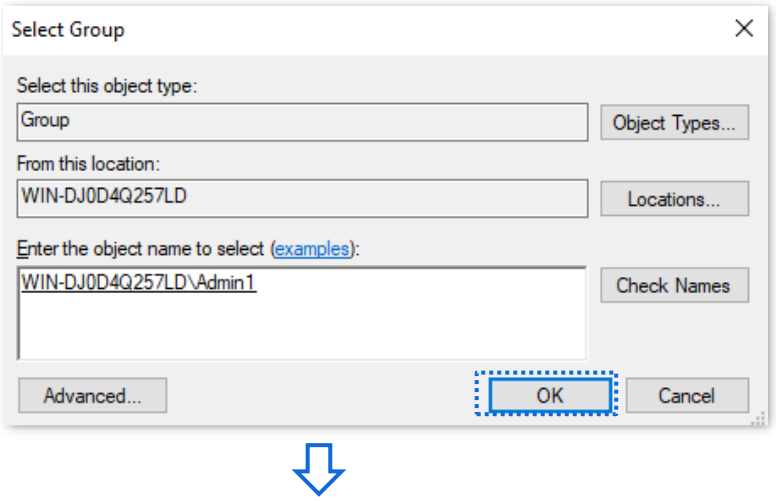
2) Click **Connection Request Policies** and double-click **Secure Wireless Connections**. On the **Secure Wireless Connections Properties** window, click **Settings** and tick **Override network policy authentication settings**. Click **Add**, add **Microsoft: Protected EAP (PEAP)** as **EAP Types**, and click **Apply**.

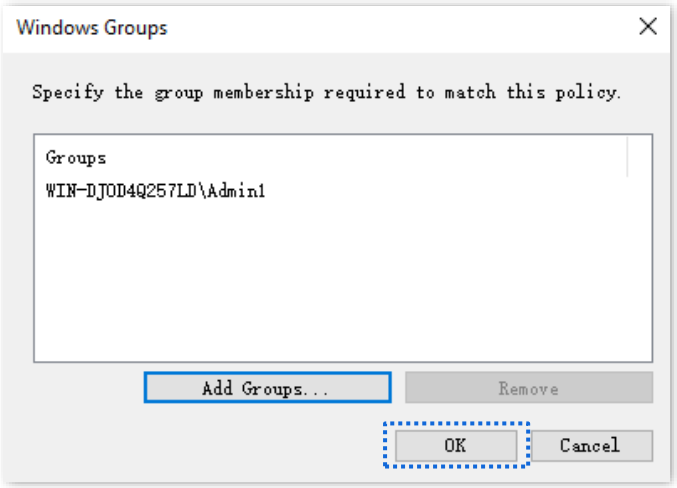




3) Click **Network Policies** and double-click **Secure Wireless Connections**. On the **Secure Wireless Connections Properties** window, click **Conditions**, and click **Add**.

Add the **Windows Groups**, enter the created user group, click **Check Names**, click **OK**, then click **OK**, and click **Apply**.





---End

III. Configure the WiFi-enabled device

Smartphone (iOS system) is used as an example.

1. Tap the (Settings) on the smartphone, tap **WLAN**, and connect the smartphone to the AP's wireless network, which is **hotspot** in this example.
2. Enter the username and password, and tap **Join**.

Tip

If a pop-up window appears asking whether to trust the certificate, tap **Trust**.

---End

Verification

The WiFi-enabled device can connect to the wireless network named **hotspot**.

Tip

If the connection fails, please:

- Ensure that the radius server and AP can communicate normally (Ping each other).
- Try to modify the firewall settings of the radius server: add inbound and outbound rules to allow TCP and UDP specific local port "1812, 1813, 1645, 1646" to connect.

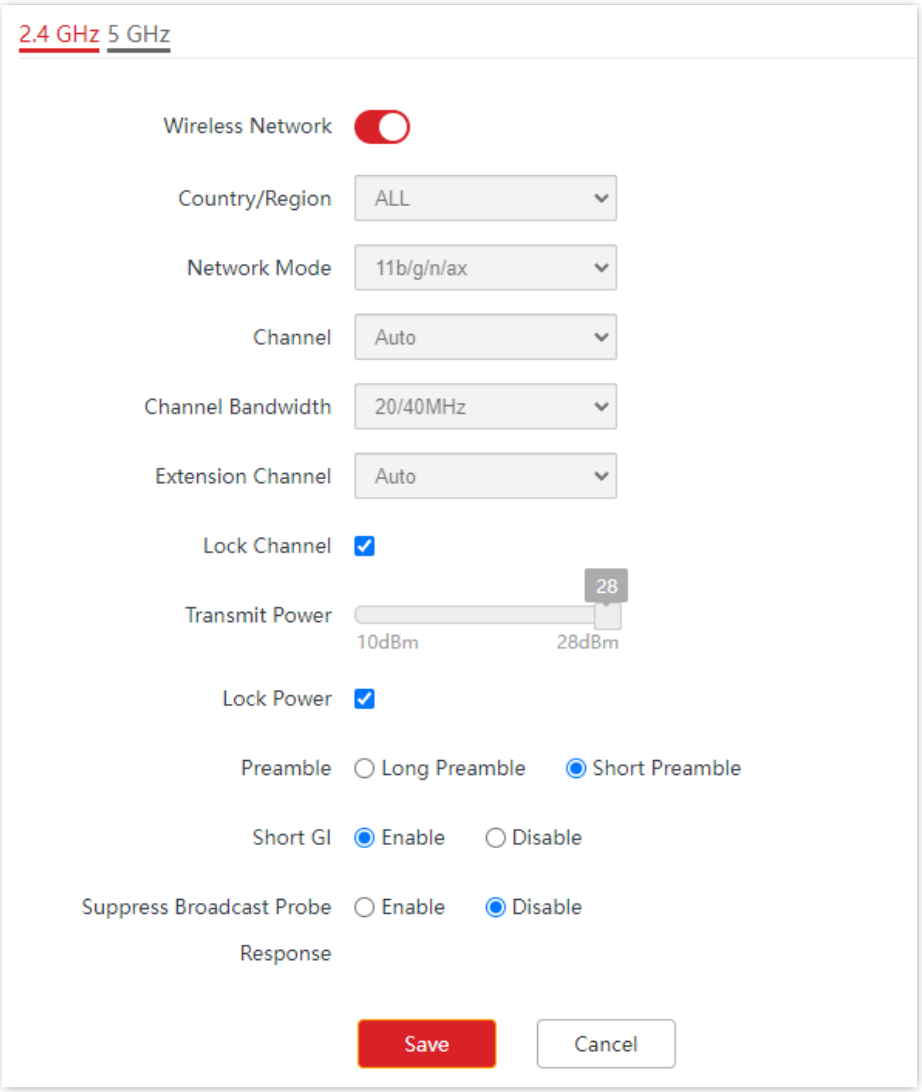
6.2 RF settings

Tip

Pro-6-LiteV2.0 is used for illustration here.

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **RF Settings**.

On this page, you can modify the basic radio parameters.



Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	

Parameter	Description
Wireless Network	Specifies whether to enable the wireless network function of the AP.
Country/Region	Specifies the country or region where the AP is used. This parameter helps comply with channel regulations of the country or region. This parameter can be set if Lock Channel is not selected.
Network Mode	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 WiFi-enabled 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 WiFi-enabled 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 WiFi-enabled 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. WiFi-enabled devices compliant with 802.11b or 802.11g and WiFi-enabled 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 WiFi-enabled 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 WiFi-enabled 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 WiFi-enabled 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. Tip The wireless network modes of the AP may differ with different models of APs. The actual product prevails.

Parameter	Description
Channel	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	Specifies the wireless channel bandwidth of the AP. This parameter can be set if the AP works in 802.11 b/g/n, 802.11 b/g/n/ax, 802.11ac, 802.11a/n, 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. – **160 MHz**: 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. Tip The wireless channel bandwidths of the AP may differ with different models of APs. The actual product prevails.
Extension Channel	Used to determine the operating frequency band of this device when it uses the 40 MHz channel bandwidth in 11n mode. This parameter can be set if Lock Channel is not selected.
Lock Channel	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 **Extension Channel** cannot be changed.
Transmit Power	Specifies the transmit power of the AP. This parameter can be set if Lock Power is not selected. 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	Specifies whether the current transmit power settings of the AP can be changed. If it is selected, the settings cannot be changed.

Parameter	Description
Preamble	Specifies 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** 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**.
Short GI	Specifies whether to enable the short guard interval function. 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	Specifies whether to enable the suppress broadcast probe response function. By default, WiFi-enabled devices keep sending Probe Request packets that include the SSID field to scan their nearby wireless networks. After receiving such packets, the AP determines whether the WiFi-enabled 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

Tip

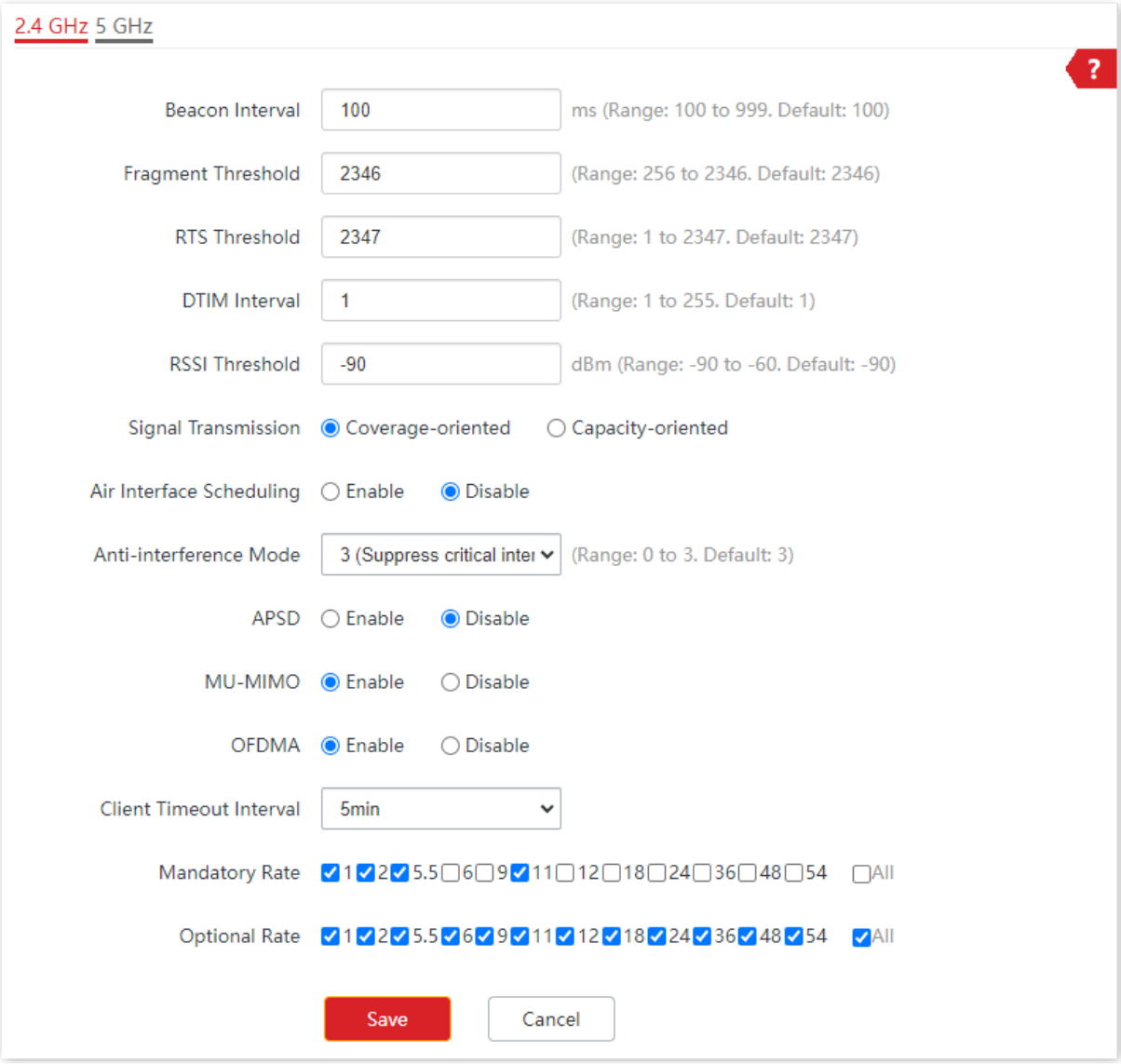
Pro-6-LiteV2.0 is used for illustration here.

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **RF Optimization**.

On this page, you can modify the radio parameters to optimize performance.

Note

You are recommended to retain the default settings if without the professional guidance.



Parameter description

Parameter	Description
2.4 GHz 5 GHz	Used to select the radio band of the AP to be configured.
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.
Fragment Threshold	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	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	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.

Parameter	Description
RSSI Threshold	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 WiFi-enabled devices to connect to the AP with stronger signal in case of multiple APs exist.
Signal Transmission	Select the option based on your actual situation. – **Coverage-oriented**: This mode broadens wireless 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 and airports.
Air Interface Scheduling	Specifies whether to enable the air interface scheduling function of the AP. This enables the users experiencing high download rates to download more data, so that this device can achieve higher system throughput and connect to a greater number of clients.
Anti-interference Mode	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	Specifies whether to enable the automatic power save delivery function. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, it is disabled.
MU-MIMO	Multi-User Multiple-Input Multiple-Output. If this function is enabled, AP can communicate with multiple users concurrently, avoiding wireless 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.

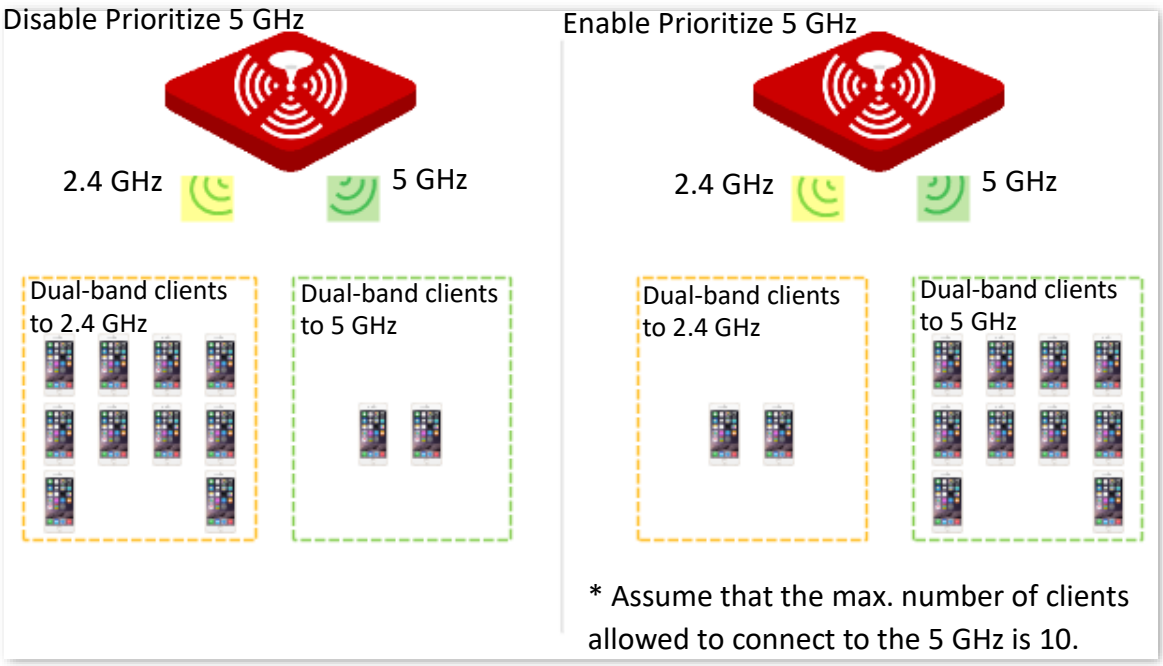
Parameter	Description
Client Timeout Interval	Used to set the wireless client disconnection interval of this device. The device disconnects from a wireless client if no traffic is transmitted or received by the wireless client within the interval.
Mandatory Rate	Specifies rates that wireless clients must support in order to connect to the wireless networks of this device.
Optional Rate	Specifies the additional rates that the AP supports, which are optional to wireless clients. The clients meeting the mandatory rate can connect to the AP with higher rate.
Prioritize 5 GHz	Specifies whether to enable the prioritize 5 GHz function. If this function is enabled, dual band WiFi-enabled devices prefer the 5 GHz wireless network of the AP to connect when the 5 GHz signal strength transmitted by devices is greater than or equal to the **Prioritize 5 GHz Threshold**.
Prioritize 5 GHz Threshold	With this function enabled, if the strength of the signals transmitted by a WiFi-enabled device is greater than or equal to this threshold, the WiFi-enabled device connects to the 5 GHz wireless network. Otherwise, it connects to the 2.4 GHz wireless network.

- **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 First-in First-out (FIFO) 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

6.4.1 Overview

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Frequency Analysis**.

On this page, you can analyze frequency and scan channels.

- **Frequency analysis**

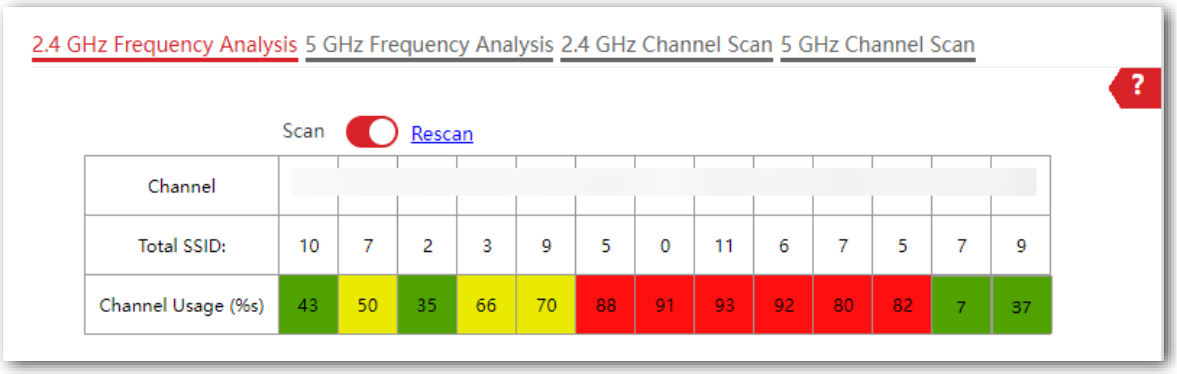
  From the intuitive result, you can check how many wireless networks (total SSIDs) use the same channel and choose a channel with low usage as the operating channel of the device for better wireless transmission efficiency.

- **Channel scan**

  The scan result list presents you with information about nearby wireless network, including SSID, MAC address, channel, channel bandwidth and signal strength.

6.4.2 View frequency analysis

1. Log in to the web UI of the AP, and navigate to **Wireless** > **Frequency Analysis**.
2. Click **2.4 GHz Frequency Analysis** or **5 GHz Frequency Analysis** tab to select the wireless network radio band for frequency analysis, which is **2.4 GHz Frequency Analysis** in this example.
3. Enable **Scan**.



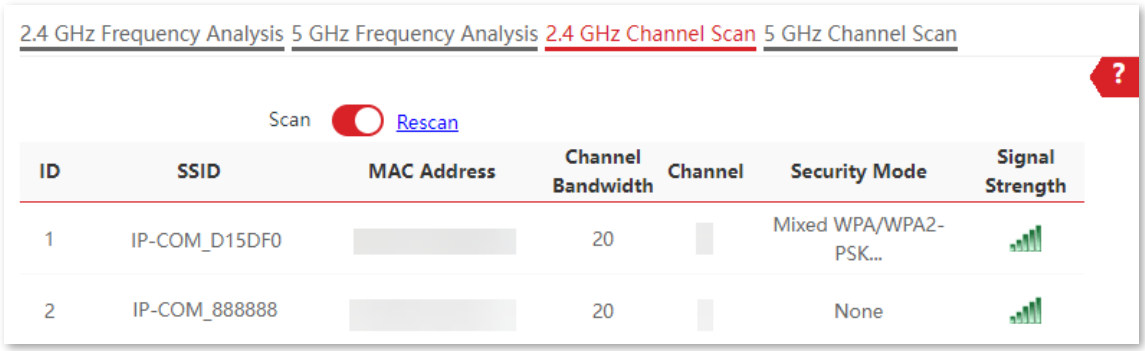
---End

After scanning, you can select a channel with low usage as the AP operating channel.

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

6.4.3 Execute channel scan

1. Log in to the web UI of the AP, and navigate to **Wireless** > **Frequency Analysis**.
2. Click **2.4 GHz Channel Scan** or **5 GHz Channel Scan** tab to select the wireless network radio band for channel scan, which is **2.4 GHz Channel Scan** in this example.
3. Enable **Scan**.



---End

6.5 WMM settings

Tip

W63APV3.0 is used for illustration here.

6.5.1 Overview

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

WMM is a wireless QoS protocol used to ensure that packets with high priorities are transmitted first. This ensures better 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.

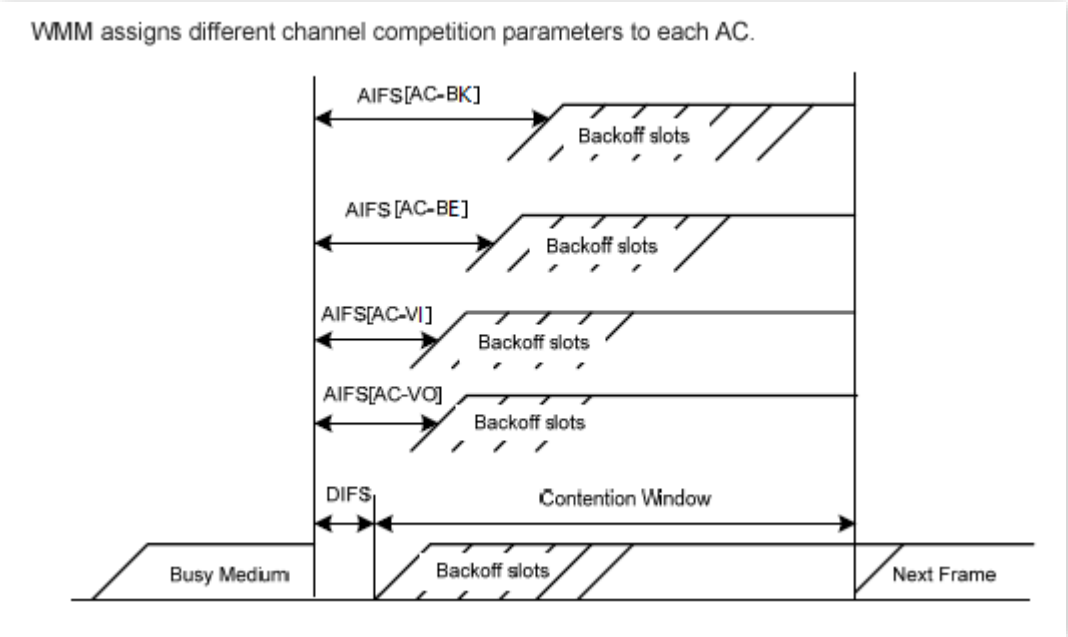
According to the 802.11 protocol family, all devices listen on a channel before using the channel to send data. If the channel stays idle for or longer than a specified period, the devices wait a random backoff period within the contention window. The device whose backoff period expires first can use 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. The ACs help achieve different service levels.

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

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



- **ACK policies**

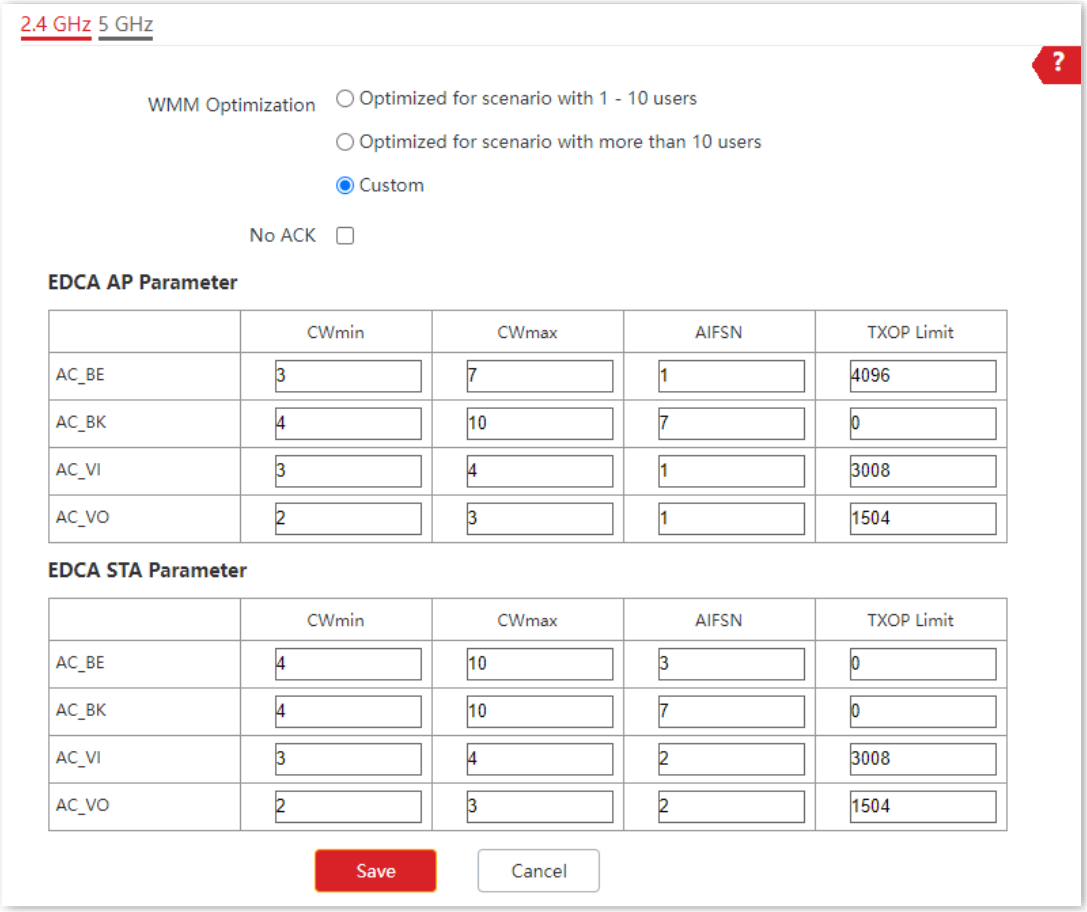
WMM specifies the Normal ACK and No ACK policies.

- According to the No Acknowledgment (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.

6.5.2 Configure WMM

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **WMM**.

On this page, you can configure related WMM parameters.



Parameter description

Parameter	Description
2.4 GHz 5 GHz	Used to select the radio band of the AP to be configured.
WMM Optimization	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.

Parameter	Description
No ACK	Available only when **WMM Optimization** is set to **Custom**. No Acknowledgement (No ACK): When this policy is used, the recipient will not acknowledge received packets during wireless packet exchange. It is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy improves transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. – 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 AP Parameter EDCA STA Parameter	For details, refer to the overview of the WMM settings.

6.6 Access control

6.6.1 Overview

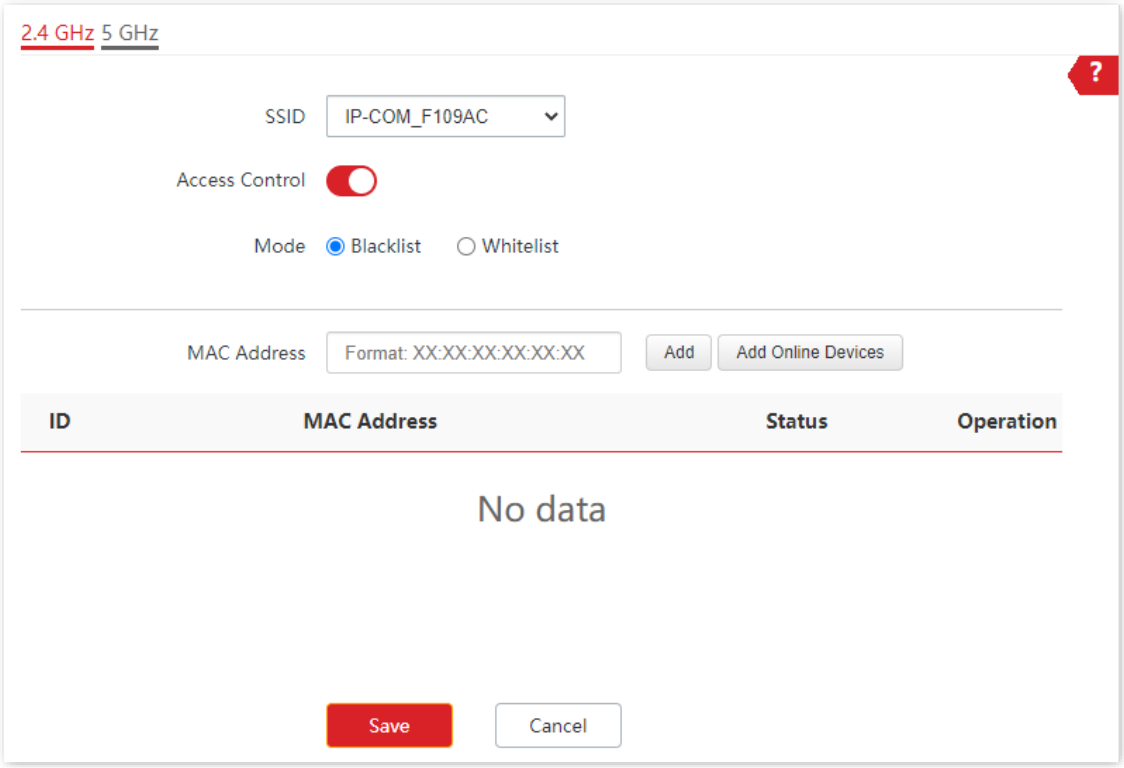
To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Access Control**.

On this page, you can configure the access control function to allow or disallow the devices to access the wireless network of the AP based on their MAC addresses.

The AP supports the following 2 filter modes:

- **Whitelist**: It indicates that only the WiFi-enabled devices with the specified MAC addresses can access the wireless networks of the AP.
- **Blacklist**: It indicates that only the WiFi-enabled devices with the specified MAC addresses cannot access the wireless networks of the AP.

The access control function is disabled by default. The following figure displays the page when access control is enabled.



Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	

Parameter	Description
SSID	Specifies the wireless network to which the policy applies.
Access Control	Specifies whether to enable the access control function.
Mode	Specifies the mode of the access control. – **Blacklist**: Wireless clients with MAC addresses on the access control list cannot access the wireless network of AP. – **Whitelist**: Wireless clients with MAC addresses on the access control list can access the wireless network of AP.
MAC Address	Specifies the MAC address of a client.
Add	Used to manually add the device with the MAC address you specified to the access control list.
Add Online Devices	Used to add the online wireless clients to the access control list conveniently.
Status	Specifies the status of the policy. You can enable or disable it as required.
Operation	Click to delete the policy.

6.6.2 Configure access control

1. Log in to the web UI of the AP, and navigate to **Wireless** > **Access Control**.
2. Select a wireless network radio band on which access control must be implemented.
3. Select the SSID to which the access control is applied from the **SSID** drop-down list.
4. Enable the **Access Control** function.
5. Set **Mode** to **Blacklist** or **Whitelist** as required.
6. Enter the MAC addresses of the WiFi-enabled devices to which the policy applies, and 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.

7. Click **Save**.

---End

6.6.3 Example of configuring access control

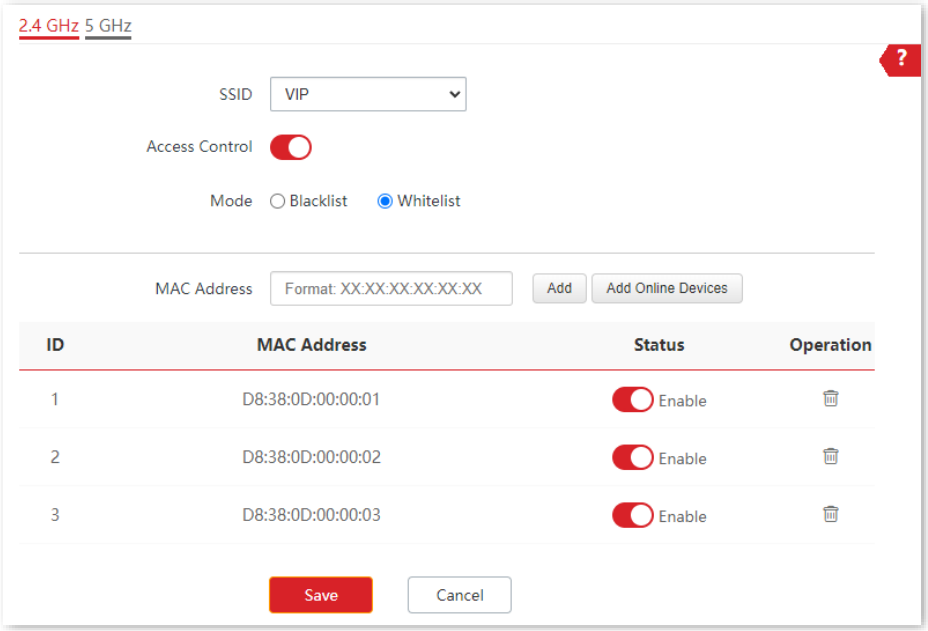
Networking requirements

A wireless network whose SSID is **VIP** under the 5 GHz radio band has been set up in an Enterprise. 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 WiFi-enabled devices whose MAC addresses are **D8:38:0D:00:00:01**, **D8:38:0D:00:00:02**, **D8:38:0D:00:00:03**.

Configuration procedure

1. Log in to the web UI of the AP, and navigate to **Wireless** > **Access Control** > **5 GHz**.
2. Select **VIP** from the **SSID** drop-down list.
3. Enable the **Access Control** function, and set **Mode** to **Whitelist**.
4. Enter **D8:38:0D:00:00:01** in the **MAC Address** text box and click **Add**. Repeat this step to add **D8:38:0D:00:00:02** and **D8:38:0D:00:00:03**.
5. Click **Save**.



---End

Verification

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

6.7 Advanced settings

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Advanced Settings**.

On this page, you can set the client type identification, broadcast packet filter and fast roaming of the AP.

- **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, Windows Phone, Windows, Mac OS.

- **Broadcast packet filter**

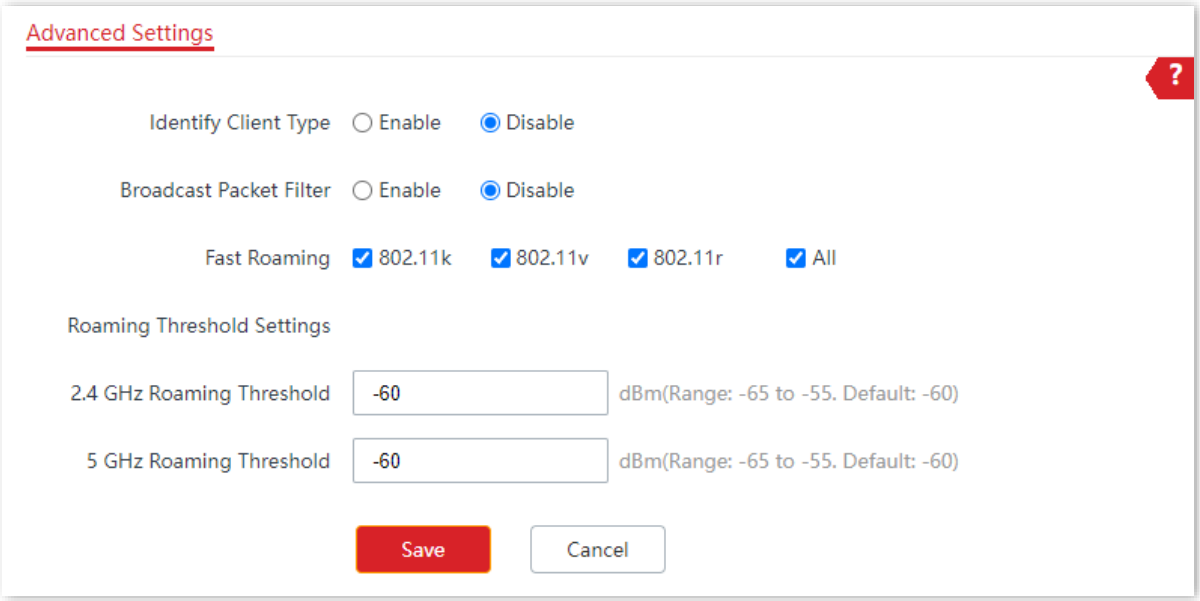
  By default, this device forwards lots of invalid broadcast packets from wired networks, which may affect business data transfer. The broadcast packet filter function allows you to filter broadcast packets by types so that invalid packets are not forwarded. This reduces air interface resources usage and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

- **Fast roaming**

  Wireless roaming means that a client automatically connects to the AP with better signal and disconnects from the original AP when it moves to a critical area covered by two or more APs. The premise is that the SSID, security mode and key of these APs are the same.

  The 802.11k/v/r fast roaming protocol can effectively solve the following problems.

  - The packet loss is serious in the traditional roaming process.
  - The roaming trigger is not timely.
  - The roaming target is not the most suitable AP.



Parameter description

Parameter	Description
Identify Client Type	Specifies whether to enable the identify client type function. With the function enabled and the client accesses the http URL, the operating system type of WiFi-enabled devices connected to the AP's wireless network can be viewed by navigating to **Status** > **Client List**.
Broadcast Packet Filter	Specifies whether to enable the broadcast packet filter function. With the function enabled, the AP can reduce air interface resources usage and ensure the bandwidth for business data transfer.
Fast Roaming	Specifies whether to enable the fast roaming function. – **802.11k:** Wireless spectrum resource measurement protocol. With the protocol enabled, the client will be assisted in scanning roamable target APs, solving the problem of whether you should roam and when you need to roam. – **802.11v:** Wireless network management protocol. With the protocol enabled, the client will be assisted in selecting roamable target APs, solving the problem of which AP to roam to. – **802.11r:** Specifies the fast BSS conversion protocol. With the protocol enabled, it will reduce roaming time without the handshake metric during wireless reconnection, solving the problem of how to roam quickly.
2.4 GHz Roaming Threshold 5 GHz Roaming Threshold	Used to set 2.4 GHz or 5 GHz roaming threshold, which means setting the sensitivity of the client to roaming. When the signal strength received by the client from the AP is lower than the roaming threshold, the roaming is triggered and the AP with better link quality is switched over. Tip The larger the roaming threshold, the higher the roaming sensitivity. The smaller the roaming threshold, the lower the roaming sensitivity.

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.

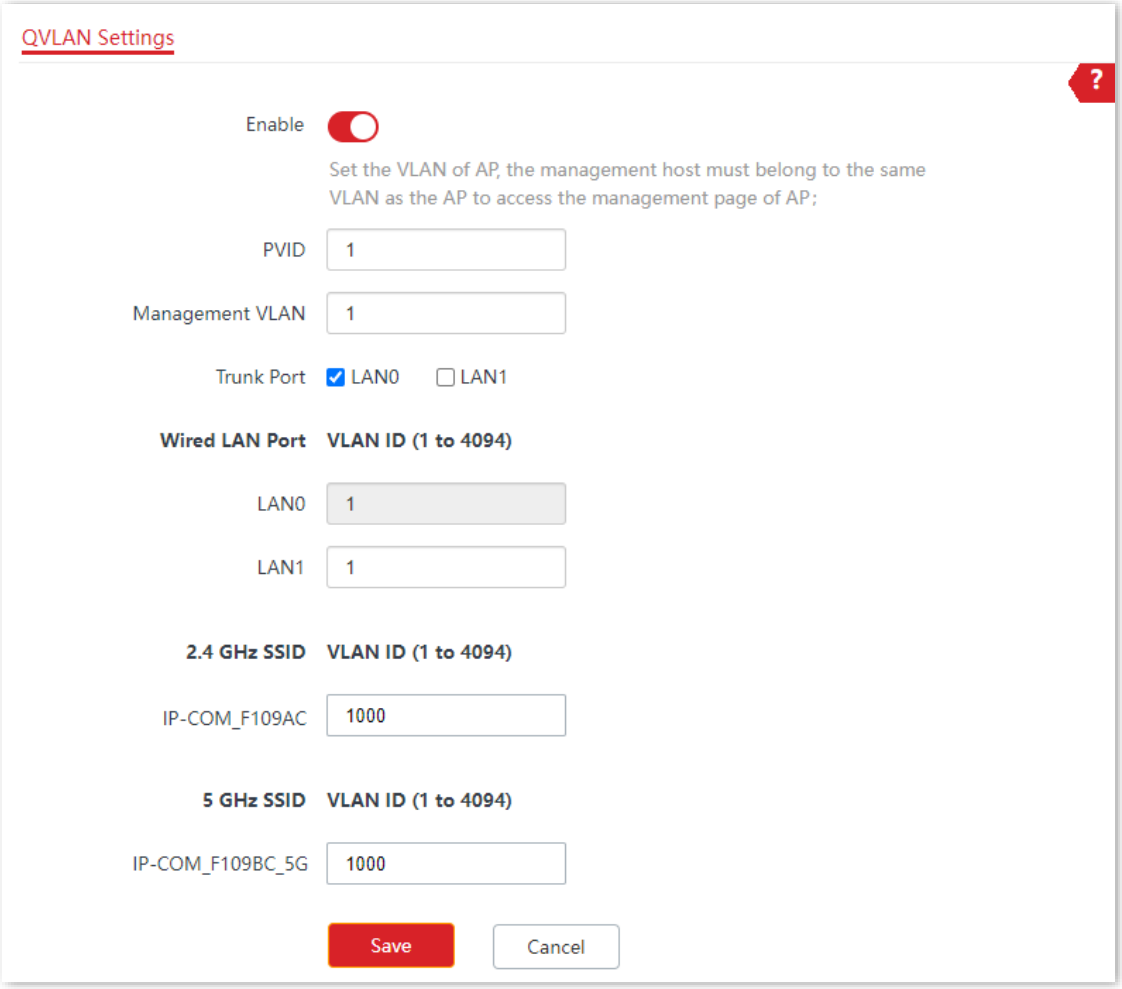
Port	Method to process received data		Method to process transmitted data
	Tagged data	Untagged data	
Access	Forward the data to other ports of the VLAN corresponding to the VID in the data.	Forward the data to the other ports of the VLAN corresponding to the PVID of the port that receives the data.	Transmit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

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **QVLAN Settings**.

On this page, you can set VLAN IDs of all wireless networks.

Tip

Pro-6-LRV2.0 is used for illustration here.



Parameter description

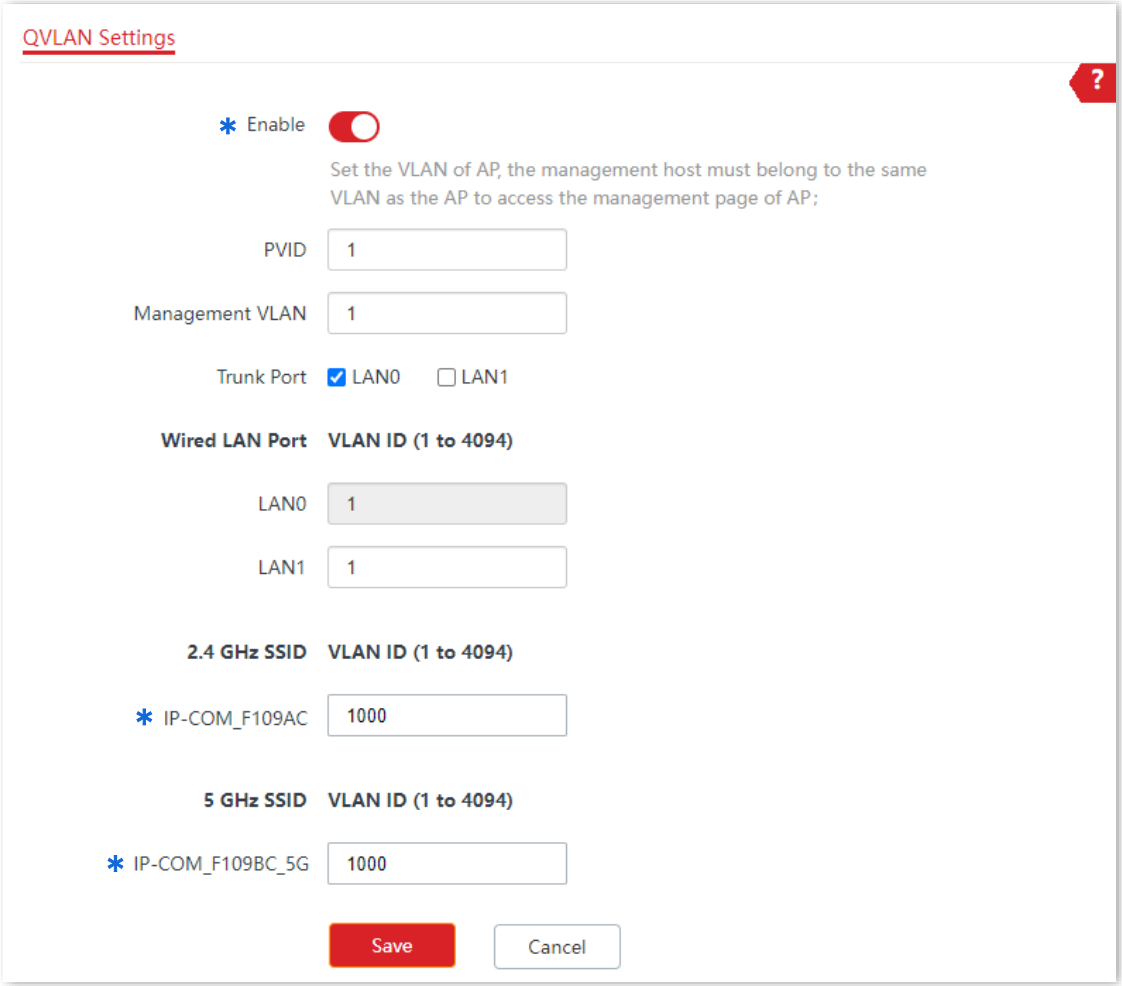
Parameter	Description
Enable	Specifies whether to enable the 802.1Q VLAN function of the AP. By default, it is disabled.
PVID	Specifies the ID of the default native VLAN of the trunk port of the AP. The default value is **1**.
Management VLAN	Specifies the ID of the AP management VLAN. The default value 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.

Parameter	Description
Trunk Port	Used to 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. Tip 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.
Wired LAN Port	Specifies the Ethernet port of the AP and the ID of the VLAN to which a LAN port belongs. – **LAN0**: The PoE power and data transmission multi-functional port of the AP. – **LAN1**: The data transmission port of the AP. Tip Ethernet port not set as the trunk port is seen as the access port and you can set its VLAN ID.
2.4 GHz SSID 5 GHz SSID	Specify the currently enabled SSIDs of the AP at 2.4 GHz or 5 GHz band, and VLAN IDs corresponding to SSIDs. Tip
VLAN ID	After the QVLAN function is enabled, the wireless ports corresponding to SSIDs functions as access ports. The PVID and VLAN ID of an access port are the same.

6.8.2 Configure the QVLAN function

1. Log in to the web UI of the AP, and navigate to **Wireless** > **QVLAN Settings**.
2. Enable **QVLAN** function.
3. Modify the parameters as required.

   Generally, you only need to modify the **2.4 GHz SSID VLAN ID** and **5 GHz SSID VLAN ID** settings.
4. Click **Save**. Pro-6-LRV2.0 is used for illustration here.



---End

6.8.3 Example of configuring QVLAN settings

Networking requirements

A hotel has the following wireless network coverage requirements:

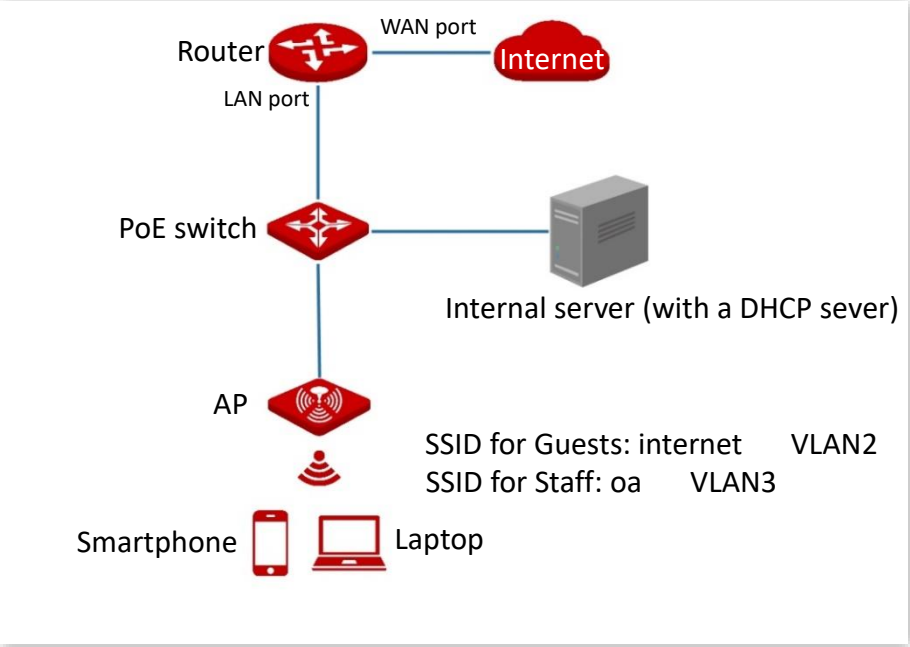
- Guests are connected to VLAN 2 and can access only the internet.
- Staff are connected to VLAN 3 and can access only the intranet.

Solution

- Set the SSID to **internet** for guests and **oa** for staff on the 2.4 GHz network.
- Configure VLANs for the above SSIDs on the AP.
- Configure VLAN forwarding policies on the switch.

Tip

The internal server must be deployed with a DHCP server in the LAN to assign IP addresses to downlink devices.

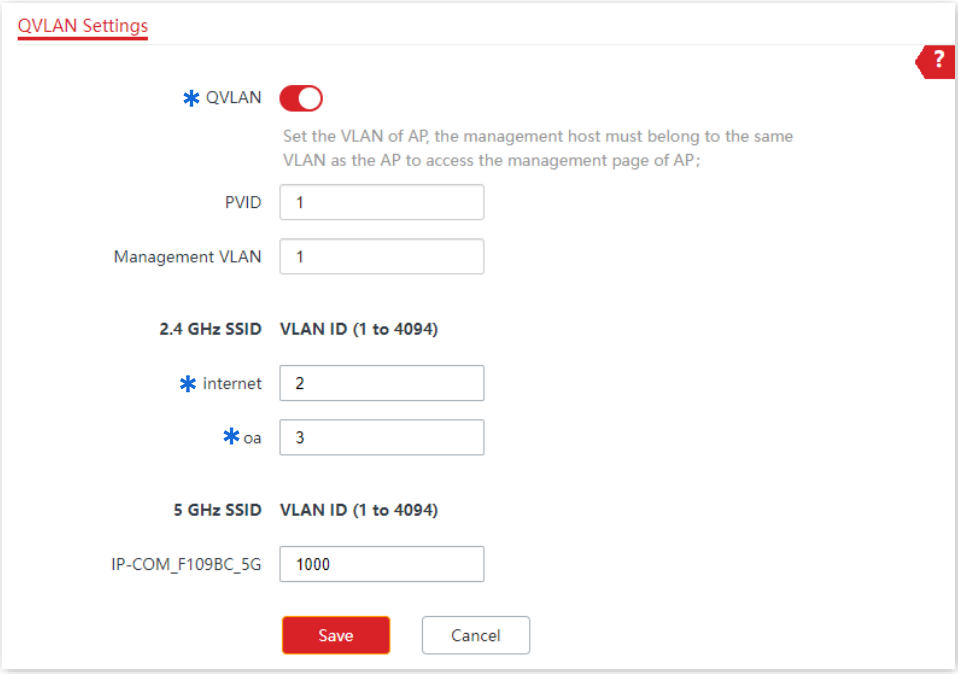


Configuration procedure

I. Configure the AP (Example: Pro-6-MiniV1.0)

1. Log in to the web UI of the AP, and navigate to **Wireless** > **QVLAN Settings**.

2. Enable the **QVLAN** function.
3. Modify the VLAN ID of the SSIDs at 2.4 GHz band. Set the VLAN of **internet** to **2** and **oa** to **3** respectively.
4. Click **Save**.



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	Trunk	1
Internal server	3	Access	3
Router	2	Access	2

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

---End

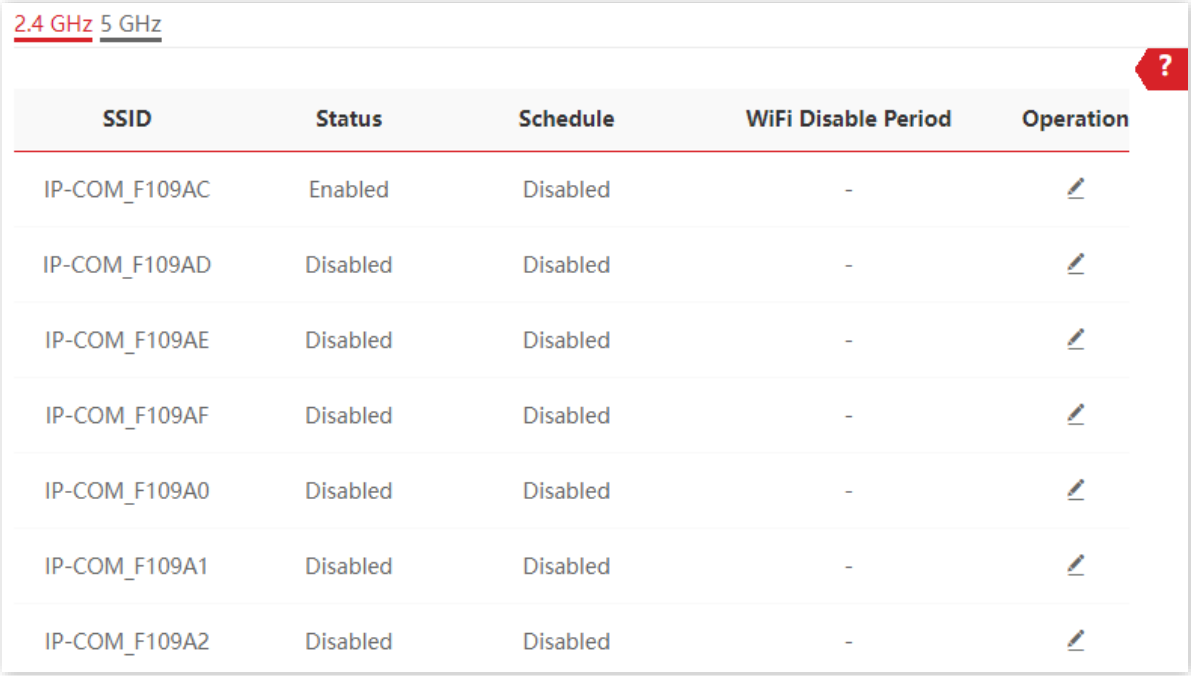
Verification

Wireless clients connected to the **internet** wireless network can only access the internet, and wireless clients connected to the **oa** wireless network can only access the intranet.

6.9 WiFi schedule

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **WiFi Schedule**.

On this page, you can disable the wireless network of the AP during a specified period. During the scheduled disable period, WiFi-enabled devices such as smartphones cannot search for the wireless networks.



Parameter description

Parameter	Description
2.4 GHz 5 GHz	Used to select the radio band of the AP to be configured.
SSID	Specifies the name of the wireless network.
Status	Specifies the status of the wireless network, including **Enabled** or **Disabled**.
Schedule	Specifies the status of the WiFi schedule of the wireless network.
WiFi Disable Period	Specifies the period when the wireless network automatically disables.
Operation	Click to set the WiFi schedule function of the wireless network, including enabling or disabling the WiFi schedule function and setting the period for the wireless network to automatically disable.

6.10 Mesh network

6.10.1 Overview

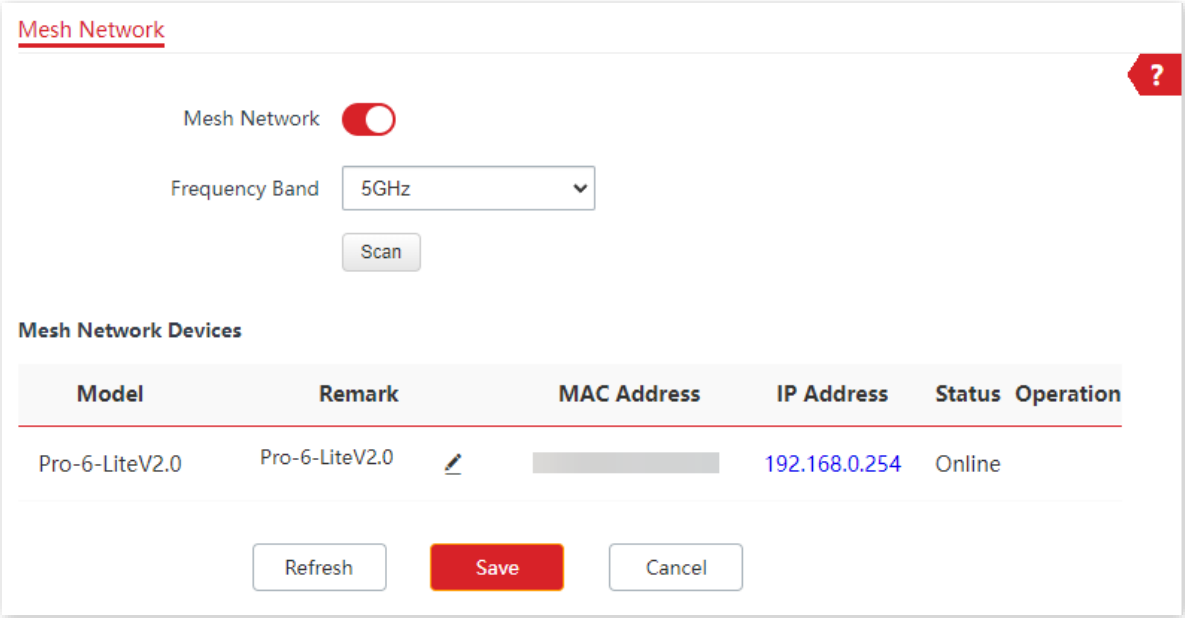
Tip

Currently, some APs can be used as the primary node to network with IP-COM APs that can use the Mesh network function. Pro-6-LiteV2.0 is used for illustration here.

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Mesh Network**.

On this page, you can add other APs to the network of this AP through the configuration of the web UI of the AP.

With the function enabled, APs that support Mesh network function will be paired and networked, and wireless configurations will be automatically synchronized, which can greatly reduce the cost and complexity of network deployment.



Parameter description

Parameter	Description
Mesh Network	Specifies whether to enable the Mesh network function of the AP. By default, it is disabled.
Frequency Band	Used to select 2.4GHz or 5GHz for Mesh networks. It is recommended to select 5GHz.

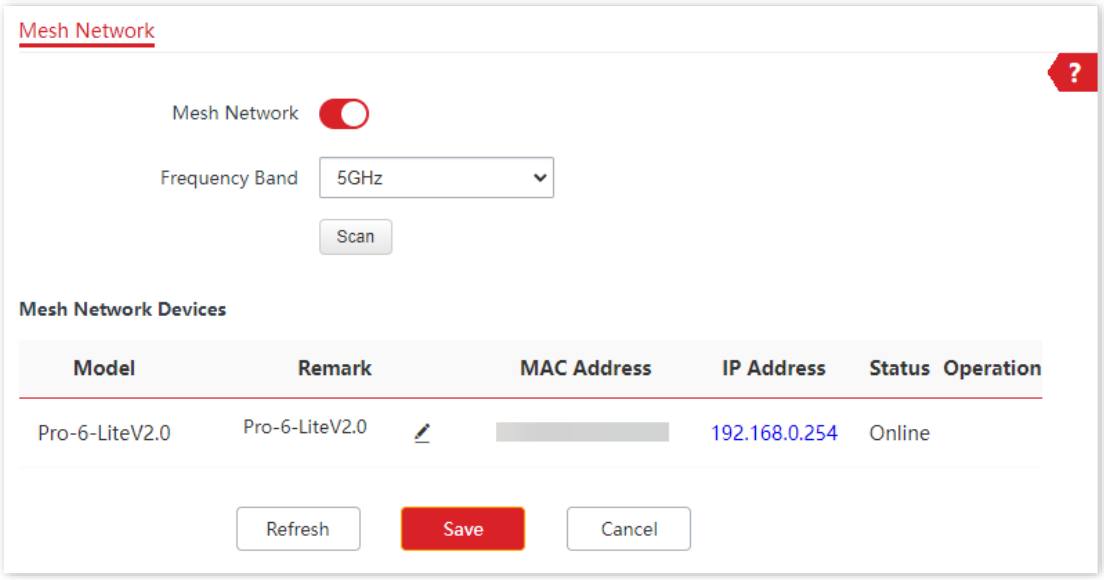
Parameter	Description
Model	
Remark	
MAC Address	Displays the device information in the Mesh network. A Mesh network can have a maximum number of 4 devices.
IP Address	
Status	
Operation	Used to delete, reboot and view the secondary node. : Used to remove the secondary node from the Mesh network. : Used to reboot the secondary node. : Used to view details of the secondary node.

6.10.2 Configure Mesh networking

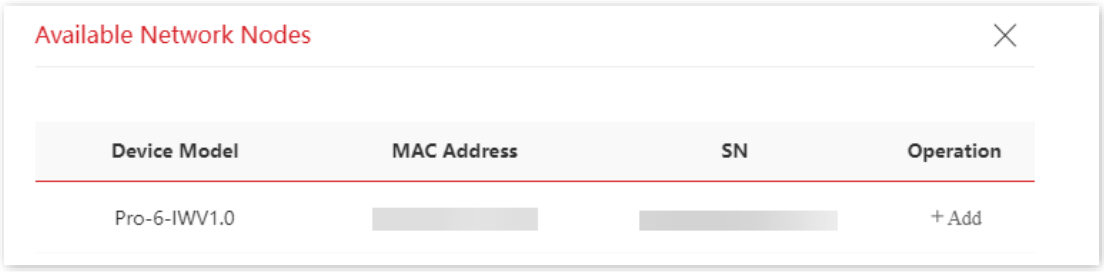
Tip

- Place the new AP (secondary node) near the existing AP (primary node) within 3 meters.
- If there are more than two secondary nodes, place the primary node in the key area and ensure that no more than one node is between the primary node and the secondary node.
- Before networking, ensure that the secondary node is restored to the factory settings and is not managed by other devices.
- The AP can be networked with IP-COM APs that can use the Mesh network function. If the AP fails to be added to an existing network, contact IP-COM customer service for help. The following uses Pro-6-Lite (primary mode) and Pro-6-IW (secondary node) as an example.

1. Log in to the web UI of the AP, and navigate to **Wireless** > **Mesh Network**.
2. Enable the **Mesh Network** function.
3. Select **Frequency Band**, which is **5GHz** in this example.
4. Click **Scan**.

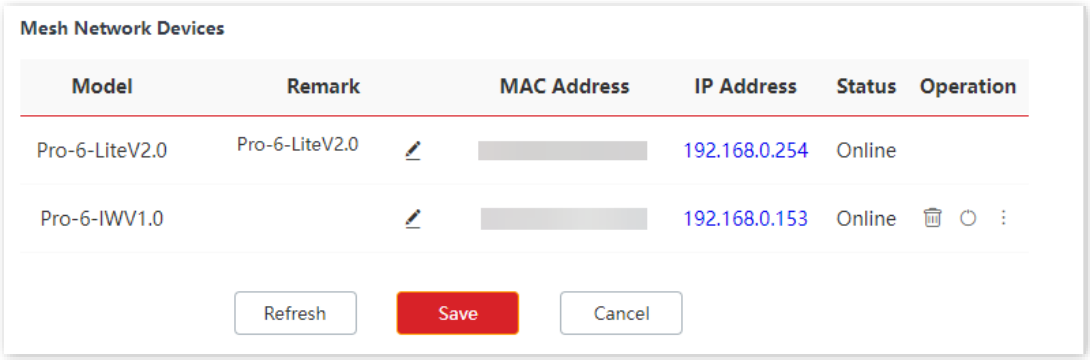


5. The system discovers new nodes, ensure that the SN is the same as the SN on the label of the new AP, select a node, and click **Add**. The following figure is for reference only.



---End

Wait until the networking is completed, the secondary node will be displayed on the **Mesh Network Devices** module.



7 Advanced settings

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

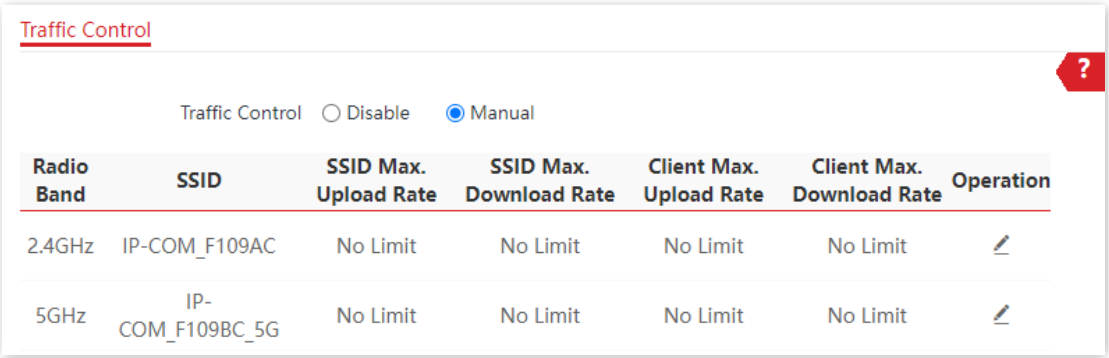
7.1 Traffic control

7.1.1 Overview

The traffic control function allows you to set limits on the internet speed of clients to guarantee a proper allocation of limited broadband resources.

To access the page, log in to the web UI of the AP, and navigate to **Advanced** > **Traffic Control**.

By default, the traffic control function is disabled. The following figure displays the page when traffic control is enabled.

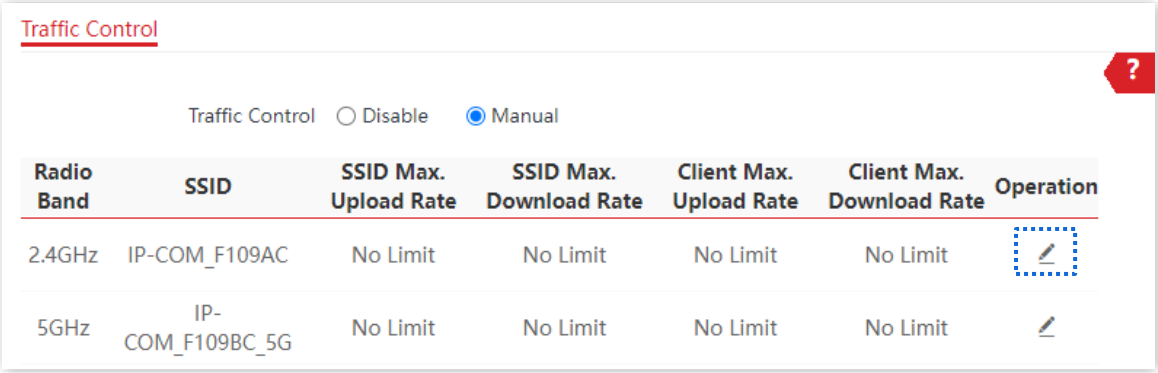


Parameter description

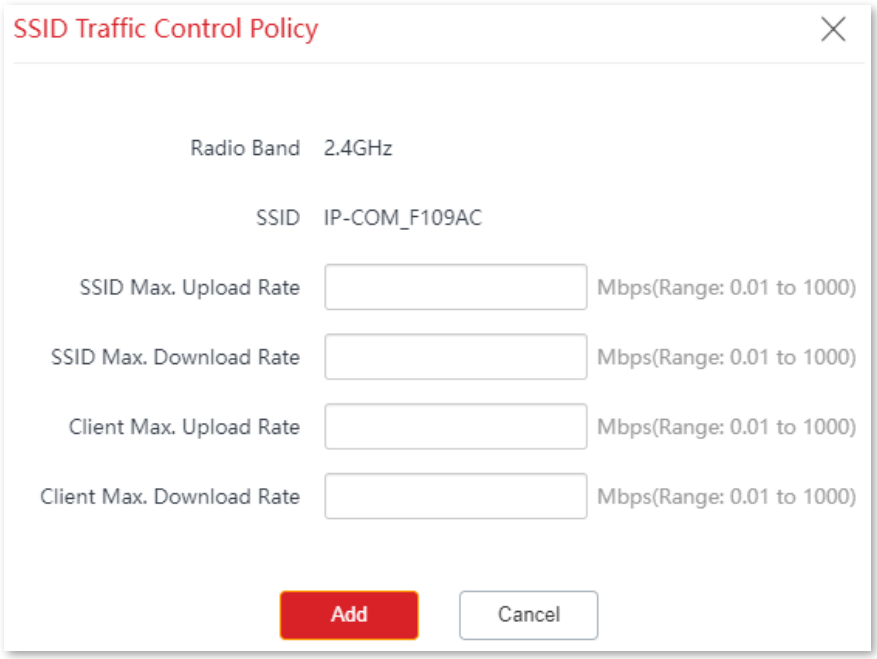
Parameter	Description
Traffic Control	Specifies whether to enable the traffic control function. – **Disable**: The traffic control function is disabled. – **Manual**: The traffic control function is enabled. The network administrator manually sets the maximum upload or download rate of SSIDs and user 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	Specifies the radio band of the wireless network on which you manually set a traffic control rule.
SSID	Specifies the name of the wireless network on which you manually set a traffic control rule.
SSID Max. Upload Rate	Specify the maximum upload or download rate allowed for a wireless network. If you leave it blank, the maximum upload or download rate of the target wireless network are not limited. It is available only when you manually set a traffic control rule.
SSID Max. Download Rate	
Client Max. Upload Rate	Specify the maximum upload or download rate allowed for every user device connected to the target wireless network. If you leave it blank, the maximum upload or download rate of every user device connected to the target wireless network are not limited. It is available only when you manually set a traffic control rule.
Client Max. Download Rate	
Operation	Click  to set the maximum upload or download rate allowed for the target wireless network and the maximum upload or download rate allowed for every user device connected to the target wireless network. It is available only when you manually set a traffic control rule.

7.1.2 Configure traffic control

1. Log in to the web UI of the AP, and navigate to **Advanced** > **Traffic Control**.
2. Set **Traffic Control** to **Manual**.
3. Click ✎ on the row where the wireless network to be controlled resides.



4. Set the maximum upload or download rate allowed for the wireless network and the maximum upload or download rate allowed for every user device connected to the wireless network.
5. Click **Add**.



---End

7.2 Cloud maintenance

7.2.1 Overview

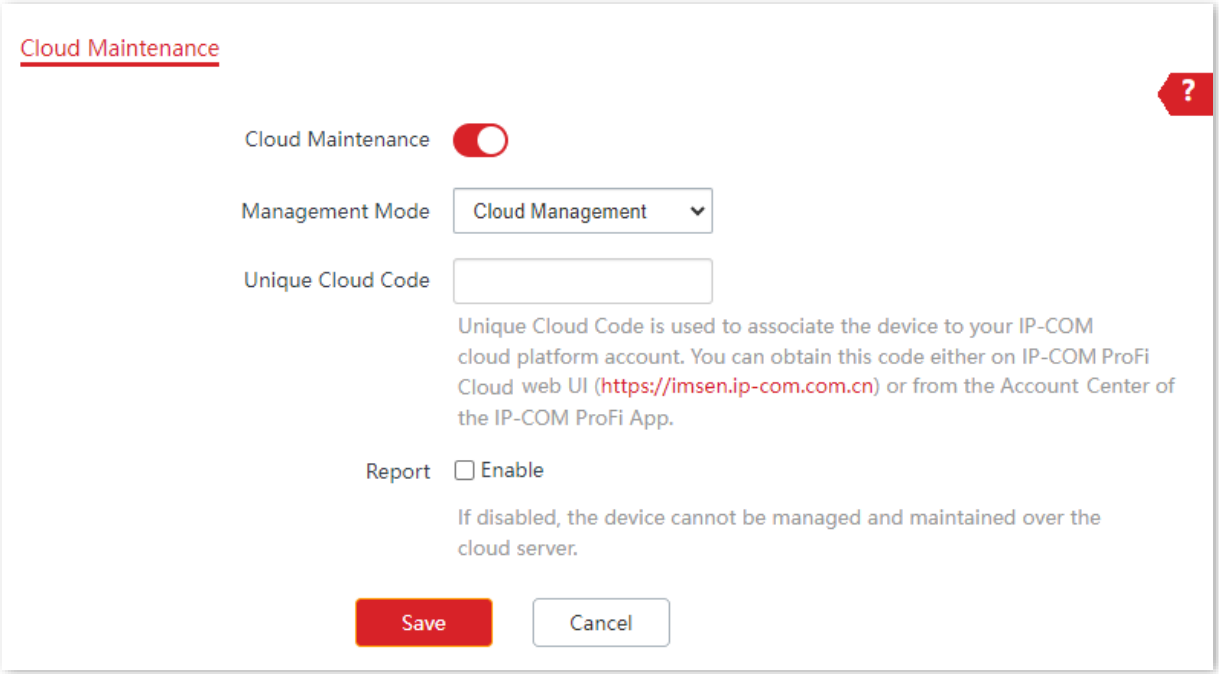
ProFi is a cloud platform provided by IP-COM, which can centrally manage IP-COM devices that support IP-COM ProFi cloud management.

After an AP is added to the IP-COM ProFi cloud platform, you can view and configure the relevant parameters of the AP on the IP-COM ProFi cloud platform, or locally log in to the web UI of the AP to view and configure parameters.

To access the page, log in to the web UI of the AP, and navigate to **Advanced** > **Cloud Maintenance**.

On this page, you can add the AP to the IP-COM ProFi cloud platform.

The cloud maintenance function is disabled by default. The following figure displays the page when cloud maintenance is enabled.



Parameter description

Parameter	Description
Cloud Maintenance	Specifies whether to enable the cloud maintenance function of the AP.

Parameter	Description
Management Mode	Specifies the modes under which your AP is managed. – **Cloud Management**: Applicable to scenarios that require unified configuration and maintenance through the IP-COM ProFi cloud platform. In this mode, all configuration of the device is delivered by the IP-COM ProFi cloud platform. – **Local Management**: Applicable to scenarios that require unified status monitoring through the IP-COM ProFi cloud platform. In this mode, all configurations of the device are completed on its own web UI, and the information is reported to the IP-COM ProFi cloud platform.
Unique Cloud Code	Specifies the ProFi cloud platform account associated with the device. You can obtain it from the IP-COM ProFi cloud web UI (https://imsen.ip-com.com.cn) or the IP-COM ProFi App.
Report	Specifies whether to enable the report function. This function is disabled by default. If this function is enabled, parameter information of your APs is reported to the IP-COM ProFi cloud platform and you can manage and maintain your APs on the platform.

7.2.2 Example of configuring cloud maintenance

Manage AP through the ProFi App

Networking requirements

The AP can be managed through the ProFi App, and all its configuration is delivered by the IP-COM ProFi cloud platform.

Configuration procedure

Tip

Before configuring the cloud maintenance function of the AP, ensure that the internet where the AP is deployed is connected.

I. Log in to ProFi App and obtain unique cloud code.

You can download the ProFi App on your mobile device by scanning the QR code or searching for it in the **Google Play** or **App Store**.

Tip

If the ProFi App has been installed on the smartphone, ensure that the software version of the App is the latest version.

Scan to download the ProFi App

ProFi App

II. Create the project and add the AP to the project.

Log in to the ProFi App. On the **Project** page of the App, add the **Traditional WLAN** project and add the AP to the project. For details, see help document in **Help Center** of ProFi App.

---End

Verification

After the configuration is completed, the AP can be managed through the ProFi App, and all its configuration is delivered by the ProFi cloud platform.

The cloud maintenance function on the AP's web UI has been enabled simultaneously, and the unique cloud code of ProFi App account is automatically filled in.

Tip

After the AP is added to the ProFi App, it will be simultaneously added to the ProFi cloud platform (https://imsen.ip-com.com.cn). At this time, you can also remotely manage the AP by logging in to the ProFi cloud platform.

Manage AP through the ProFi cloud platform

Networking requirements

The AP can be managed through the IP-COM ProFi cloud platform, and all its configuration is delivered by the IP-COM ProFi cloud platform.

Configuration procedure

Tip

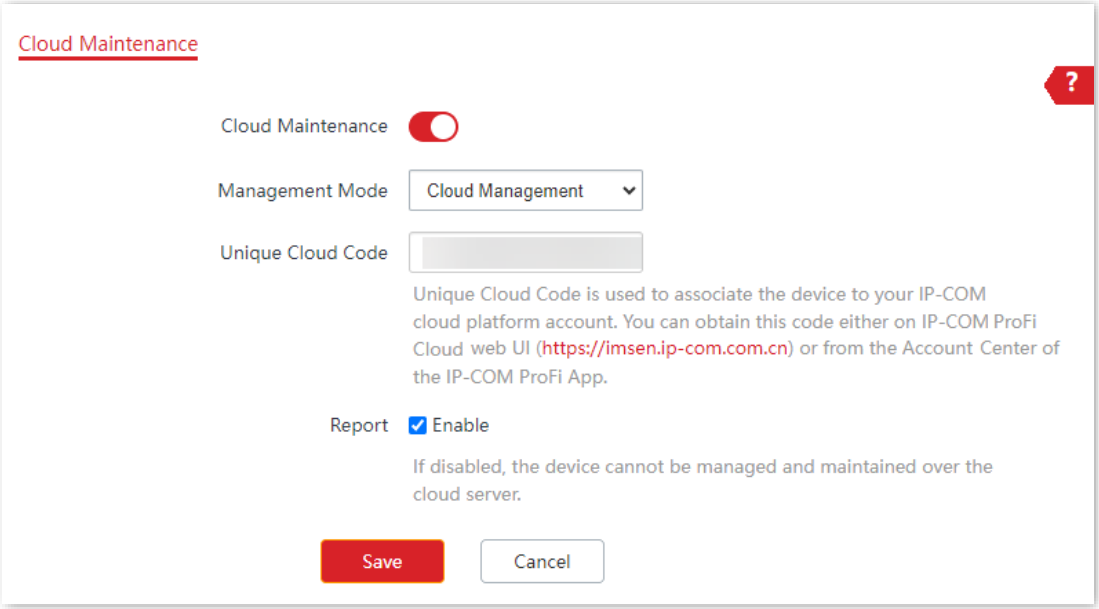
Before configuring the cloud maintenance function of the AP, ensure that the internet where the AP is deployed is connected.

I. Log in to IP-COM ProFi cloud platform and obtain unique cloud code.

On a computer that has connected to the internet, start a web browser, visit https://imsen.ip-com.com.cn, and log in to IP-COM ProFi cloud platform to obtain the unique cloud code.

II. Enable and configure the cloud maintenance function of the AP.

1. Log in to the web UI of the AP, and navigate to **Advanced** > **Cloud Maintenance**.
2. Enable the **Cloud Maintenance** function.
3. Set the parameters of the cloud maintenance function.
   1) Set **Management Mode**, which is **Cloud Management** in this example.
   2) Paste the **Unique Cloud Code** in the input box.
   3) Enable the **Report** function.
4. Click **Save**.



III. Log in to IP-COM ProFi cloud platform and add the AP to the project.

On a computer that has connected to the internet, start a web browser, and visit https://imsen.ip-com.com.cn. Log in to IP-COM ProFi cloud platform, and add the AP to the project. For details, see help document in **Help Center** of ProFi cloud platform (https://imsen.ip-com.com.cn).

Verification

After the configuration is completed, the AP can be managed through the web UI of the IP-COM ProFi cloud platform, and all its configuration is delivered by the IP-COM ProFi cloud platform.

Tip

After the AP is added to the ProFi cloud platform web UI, it will be simultaneously added to the ProFi App. At this time, you can also remotely manage the AP on the ProFi App.

7.3 Remote web management

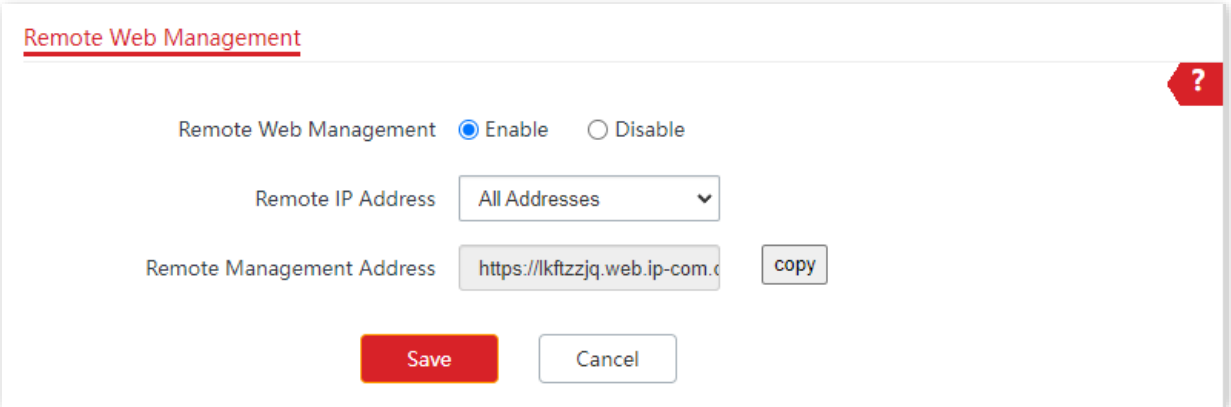
7.3.1 Overview

Generally, you can log in to the web UI of the AP only when you connect to the LAN port or the wireless network of the AP. However, the remote web management function enables access to the web UI remotely through the domain name in special cases (like when you need remote technical support).

To access the page, log in to the web UI of the AP, and navigate to **Advanced** > **Remote Management**.

On this page, you can enable or disable the remote web management and restrict the hosts that can remotely log in to the local AP.

The remote web management function is disabled by default. The following figure displays the page when remote web management is enabled.



Parameter description

Parameter	Description
Remote Web Management	Specifies whether to enable the remote web management function of the AP.
Remote IP Address	Specifies the IP address of the device that can access the web UI of the AP remotely. – **All Addresses**: Devices with any IP address on the internet can access the web UI of the AP. For network security, this option is not recommended. – **Specified Address**: Only devices with specified IP addresses can access the web UI of the AP. If the device is in the local area network, the IP address (public IP address) of the gateway of the device should be filled in.
Remote Management Address	Specifies the domain name used for remote access. The internet users can access the web UI of the AP using the domain name when the remote web management function is enabled.

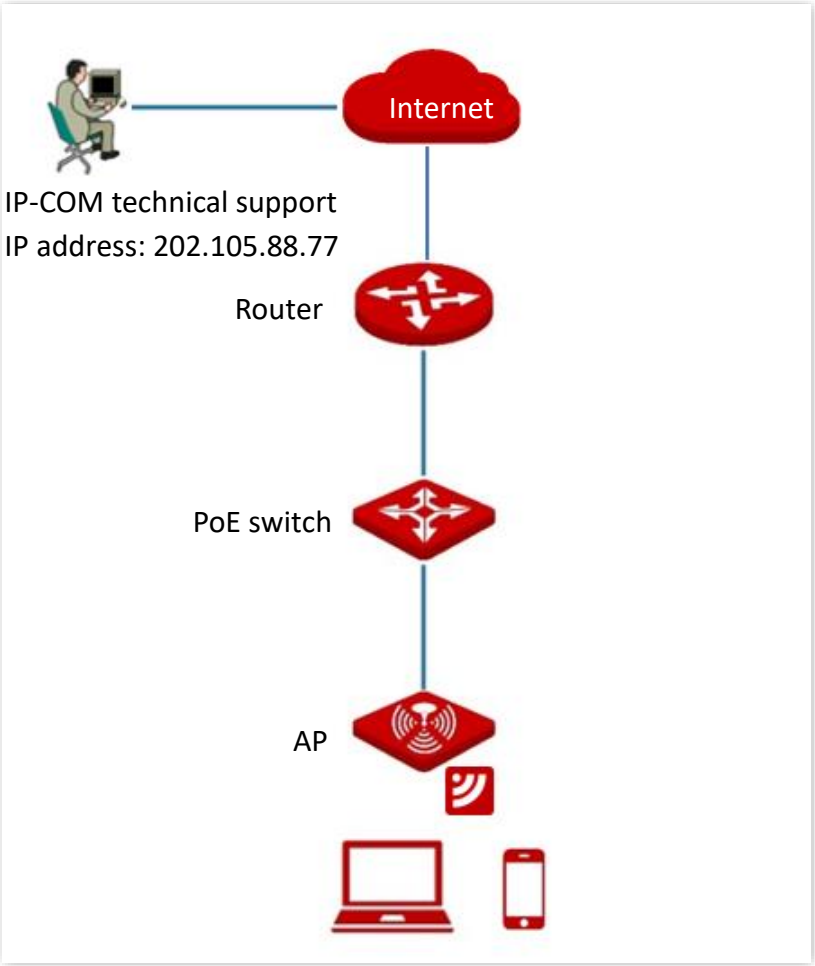
7.3.2 Example of configuring remote management

Networking requirements

An enterprise uses the AP to set up a network and has connected to the internet. The network administrator encountered a problem during configurations and needs the IP-COM technical support to remotely log in to the web UI of the AP to perform analysis and troubleshooting.

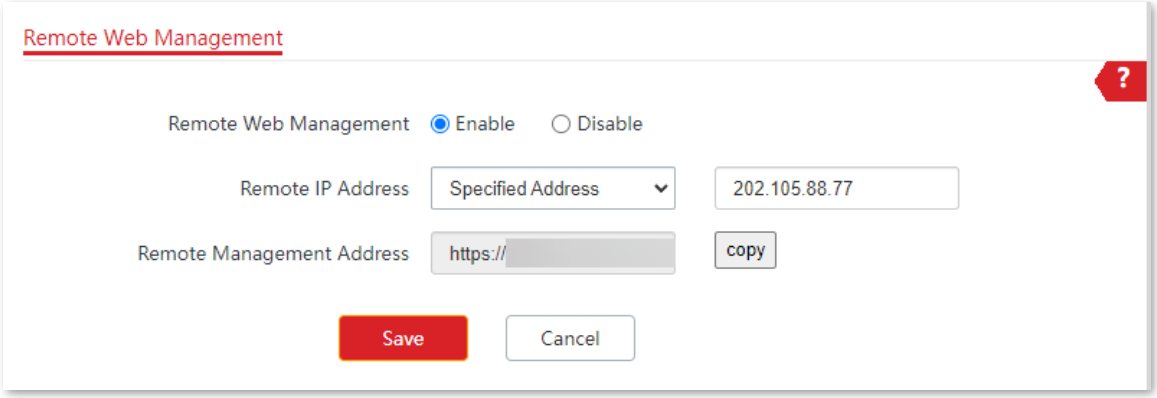
Solution

You can use the remote web management function to meet the requirements.



Configuration procedure

1. Log in to the web UI of the AP.
2. Navigate to **Advanced** > **Remote Management**.
3. Enable the **Remote Web Management** function.
4. Set **Remote IP Address** to **Specified Address.** And enter the IP address of the computer supported by IP-COM technology, which is **202.105.88.77** in this example**.**
5. Click **Save**.



Verification

The IP-COM technical support can log in to the web UI of the AP by visiting the remote management address on the computer (the IP address of the computer is 202.105.88.77).

8 Tools

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

8.1 Date & Time

To access the page, log in to the web UI of the AP, and navigate to **Tools** > **Date & Time**.

On this page, you can set the system time and login timeout interval of the AP.

8.1.1 System time

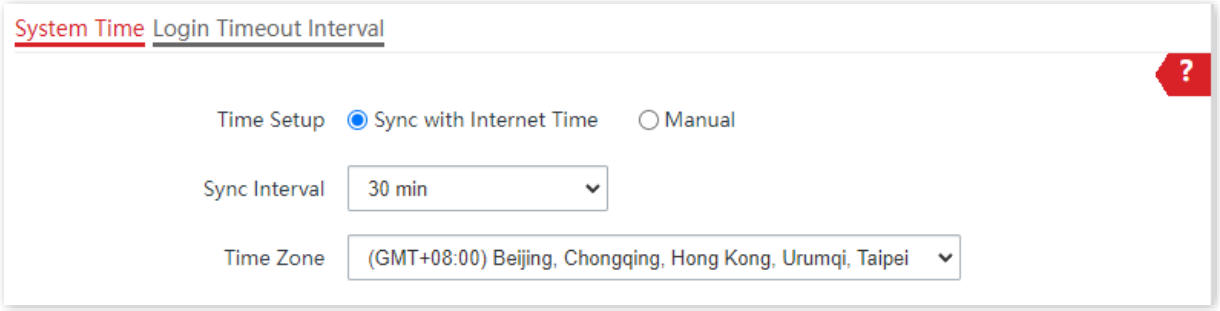
To access the page, log in to the web UI of the AP, and navigate to **Tools** > **Date & Time** > **System Time**.

Ensure that the system time of the AP is correct, so that time-based functions can take effect properly. The AP allows you to set the system time by synchronizing the time with the internet or manually setting the time.

Synchronize 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 Internet settings.



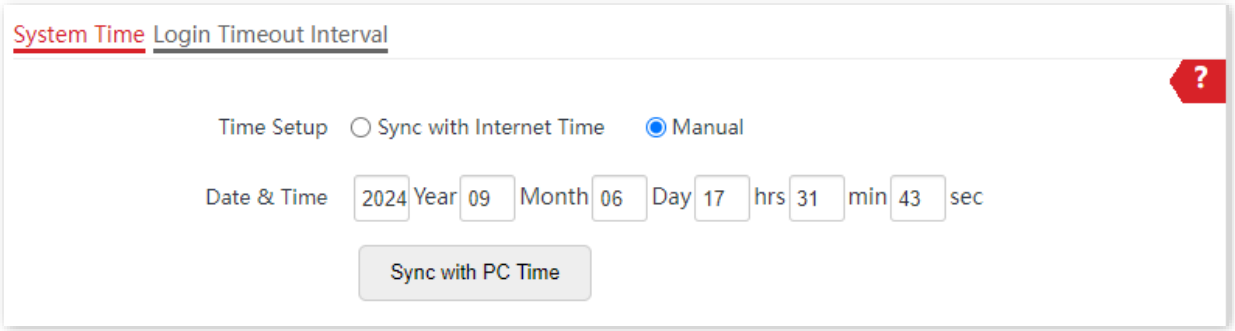
Parameter description

Parameter	Description
Time Setup	Specifies the modes to set the system time.
Sync Interval	Specifies the interval at which the AP will automatically synchronize with a time server of the internet. Tip It is available only when **Sync with Internet Time** is selected.
Time Zone	Specifies the standard time zone of the region in which the AP locates. Tip It is available only when **Sync with Internet Time** is selected.

Manually set the time

You can manually set the system time of the AP. If you select 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.

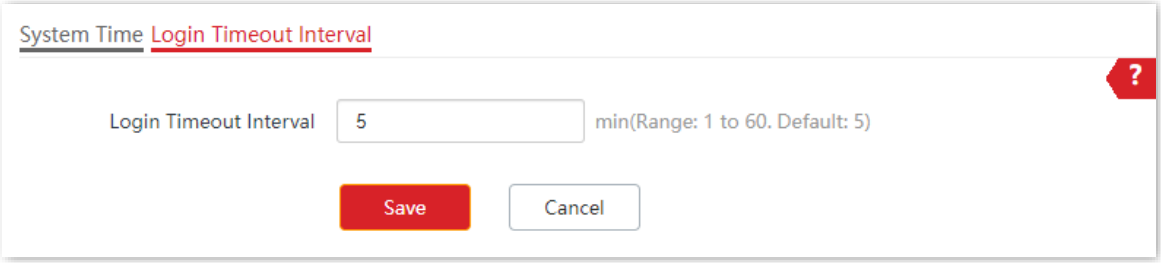


8.1.2 Login timeout interval

To access the page, log in to the web UI of the AP, and navigate to **Tools** > **Date & Time** > **Login Timeout Interval**.

On this page, you can set the 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.



8.2 Maintenance

Log in to the web UI of the AP, and navigate to **Tools** > **Maintenance**, you can reboot and reset AP, upgrade firmware, back up or restore settings, and control LED indicator.

8.2.1 Reboot

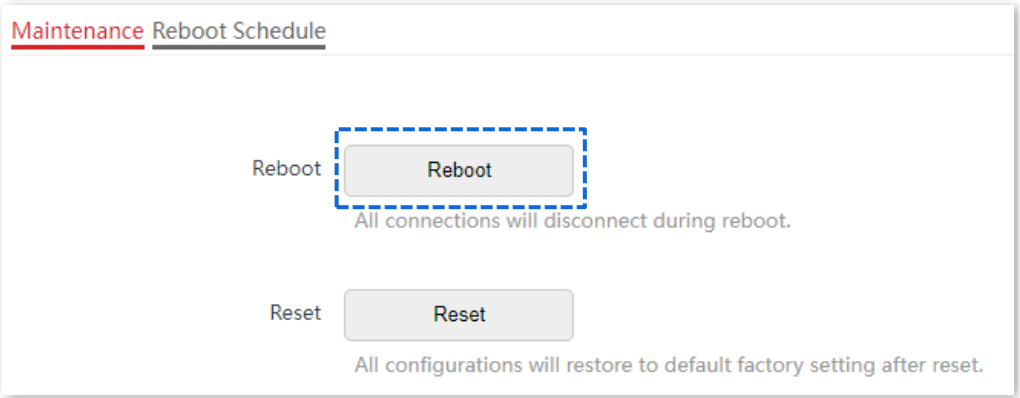
Tip

Rebooting the AP will disconnect all connections. You are recommended to reboot the AP at an idle hour.

Manual reboot

If a setting does not take effect or the AP works improperly, you can try rebooting the AP manually to resolve the problem.

Log in to the web UI of the AP, navigate to **Tools** > **Maintenance** > **Maintenance** and click **Reboot**.



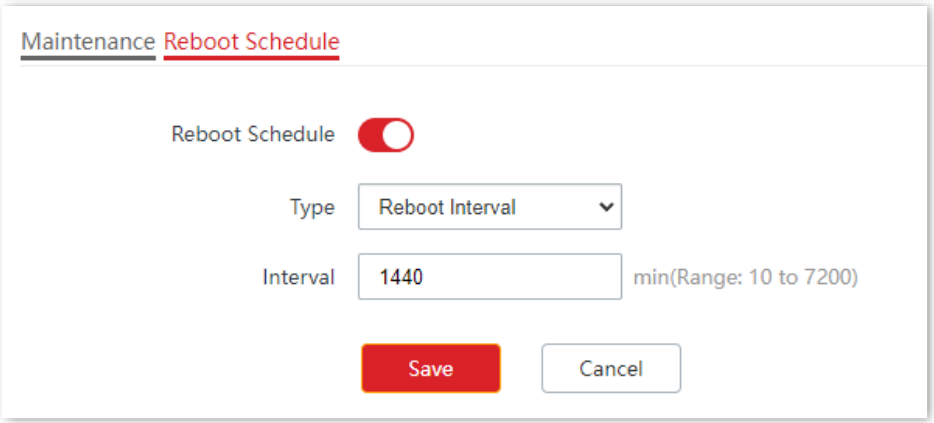
Reboot schedule

This function enables 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 can reboot:

- Reboot interval: The AP reboots at the interval that you specify.
- Reboot schedule: The AP automatically reboots at the specified date and time.

Configure the AP to reboot at an interval

1. Log in to the web UI of the AP, and navigate to **Tools** > **Maintenance** > **Reboot Schedule**.
2. Enable the **Reboot Schedule** function.
3. Set **Type** to **Reboot Interval**.
4. Set **Interval** to a value in minutes, which is **1440** in this example.
5. Click **Save**.



---End

After the configuration is completed, the AP will automatically reboot in a day.

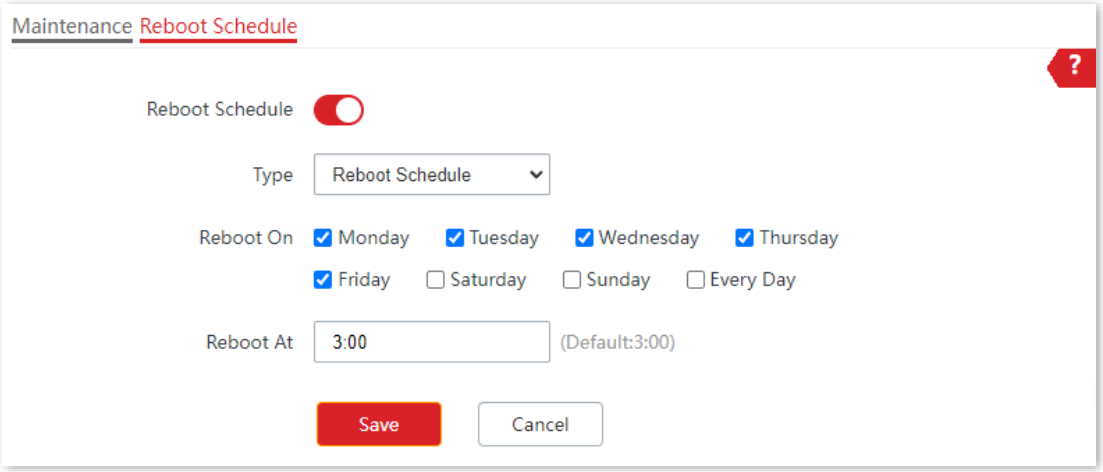
Configure the AP to reboot at specified time

Tip

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

1. Log in to the web UI of the AP, and navigate to **Tools** > **Maintenance** > **Reboot Schedule**.
2. Enable the **Reboot Schedule** function.

3. Set **Type** to **Reboot Schedule**.
4. Select the date when the AP reboots, which is **Monday** to **Friday** in this example.
5. Set the time when the AP reboots, which is **3:00** in this example.
6. Click **Save**.



---End

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

8.2.2 Reset

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

Note

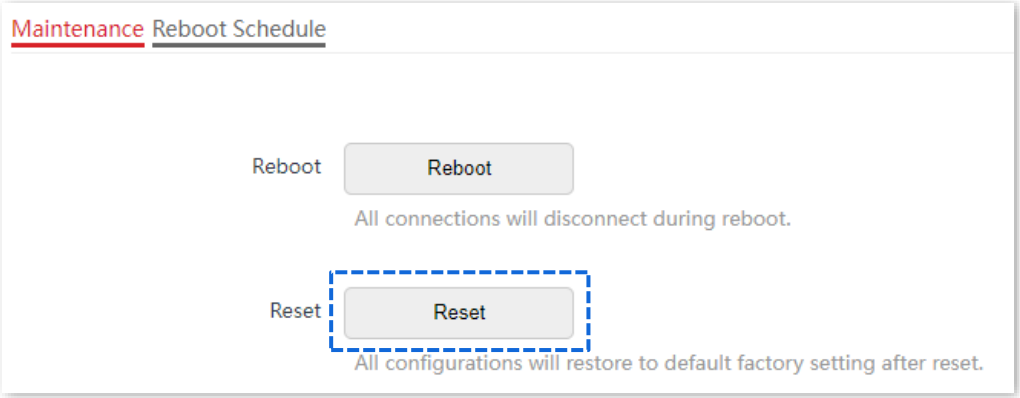
- When the factory settings are restored, your configuration will be cleared. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.
- After the factory settings are restored, the login IP address of the AP is changed to **192.168.0.254** by default.

Method 1

When the AP is idle, hold down the reset button (**RST**, **RESET**) with a needle-like object for about 8 seconds, and wait until the AP is reset successfully for about 1 minute.

Method 2

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



8.2.3 Firmware upgrade

This function upgrades the firmware of the AP for more functions and higher stability.

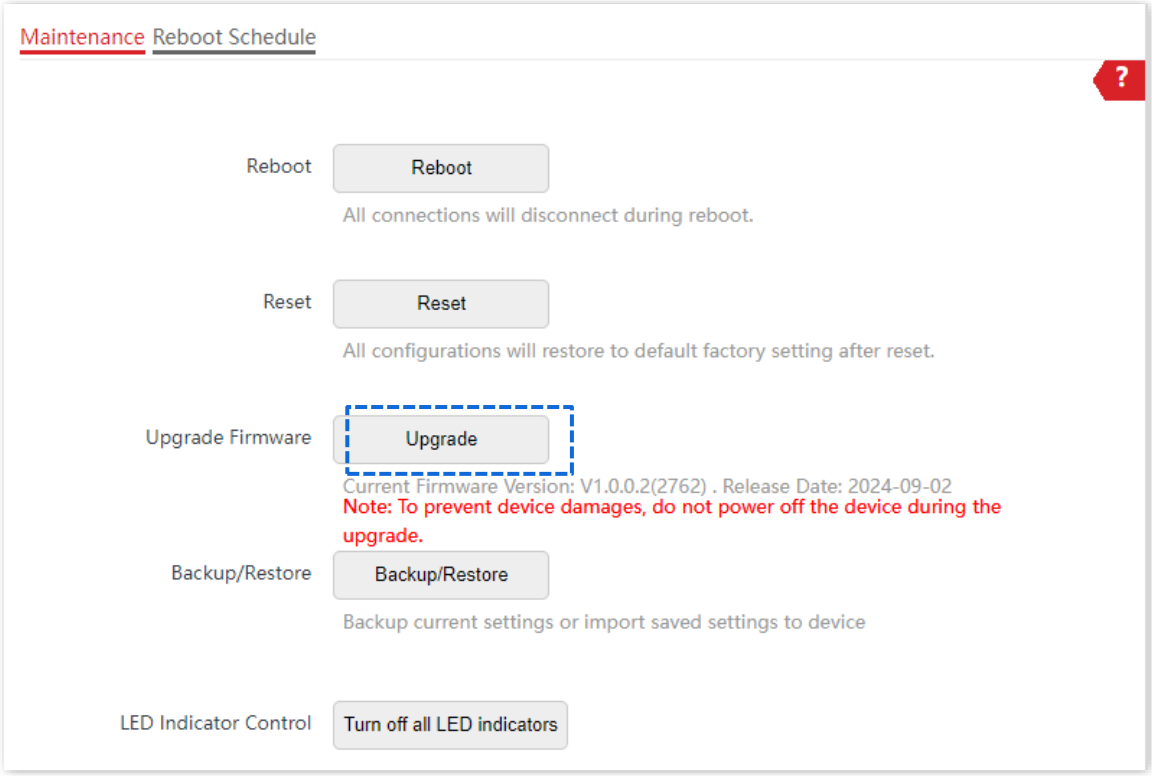
Note

To ensure a correct upgrade and avoid damage:

- Ensure that the new firmware is applicable to the AP. Generally, the format of the decompressed file is suffixed with **.bin**.
- 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 navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Upgrade**.



4. Select the upgrade file in the pop-up window.

---End

Wait until the progress bar is complete. Log in to the web UI of the AP again, navigate to **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.

8.2.4 Backup/Restore

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

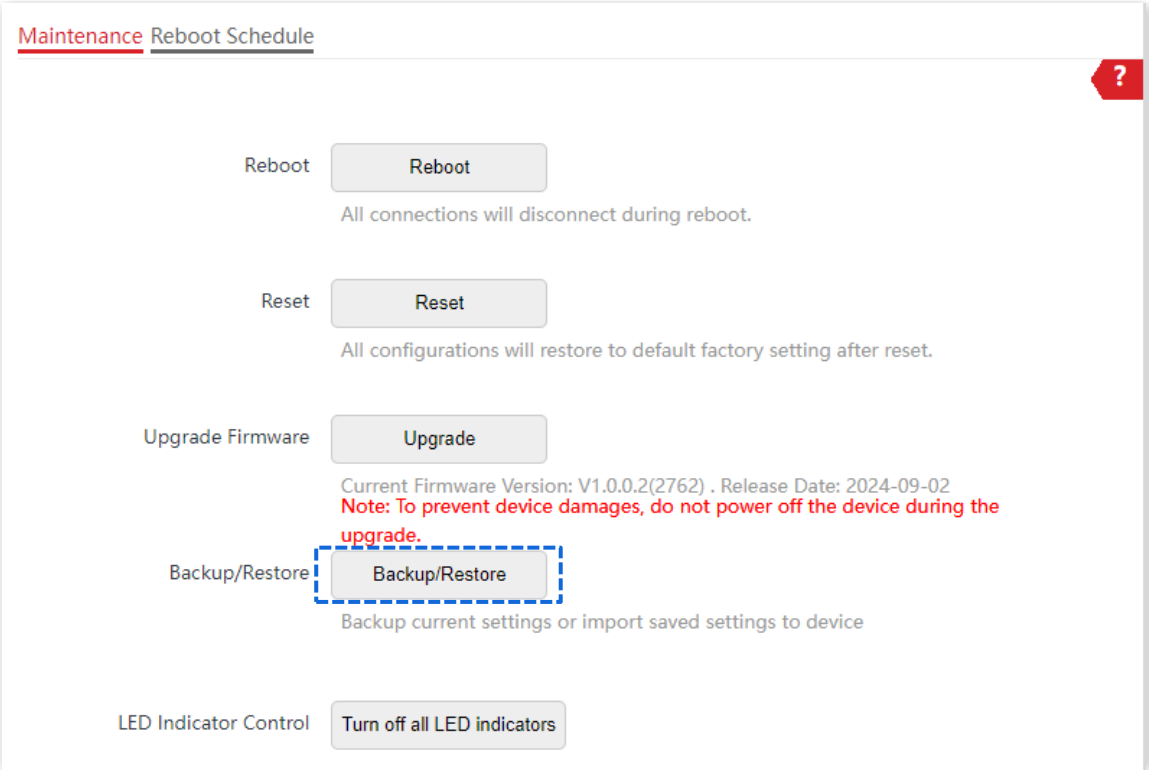
If the AP enters the optimum condition after you greatly change the configuration of the AP, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the AP.

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. Log in to the web UI of the AP, and navigate to **Tools** > **Maintenance** > **Maintenance**.
2. Click **Backup/Restore**.



3. Click **Backup**.

---End

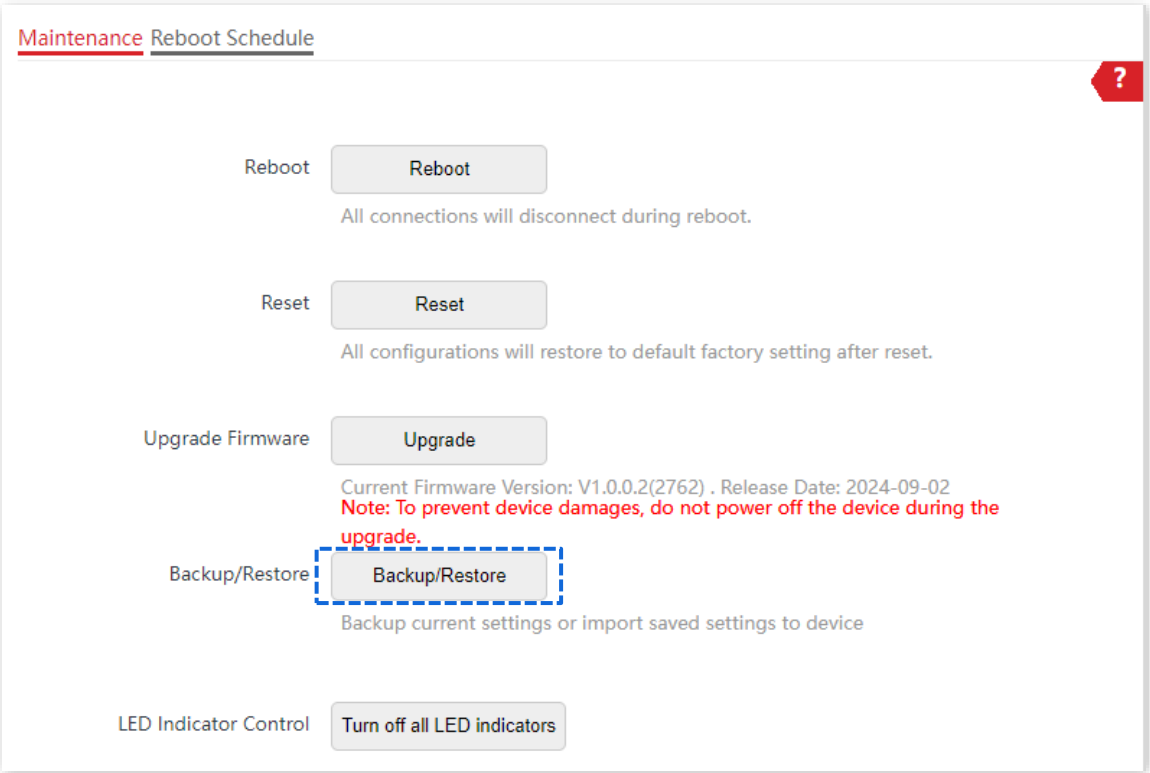
A configuration file named **APCfm.cfg** is downloaded.

Tip

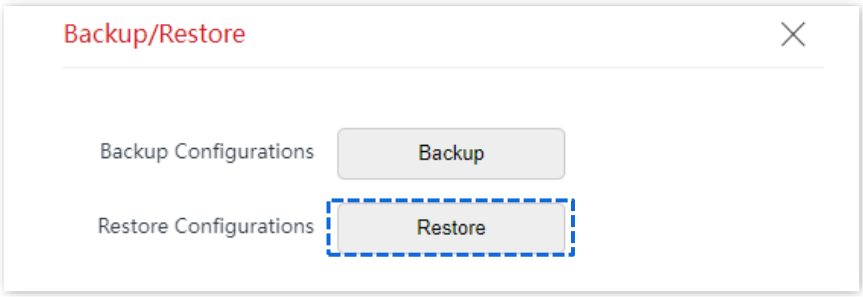
If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click “Keep”.

Restore a configuration

1. Log in to the web UI of the AP, and navigate to **Tools** > **Maintenance** > **Maintenance**.
2. Click **Backup/Restore**.



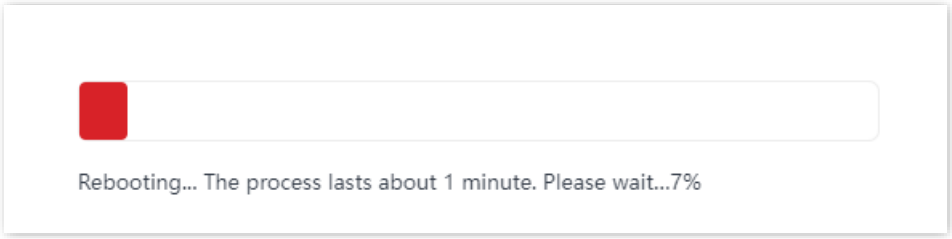
3. Click **Restore**.



4. Select the file of the configuration to be restored.

---End

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

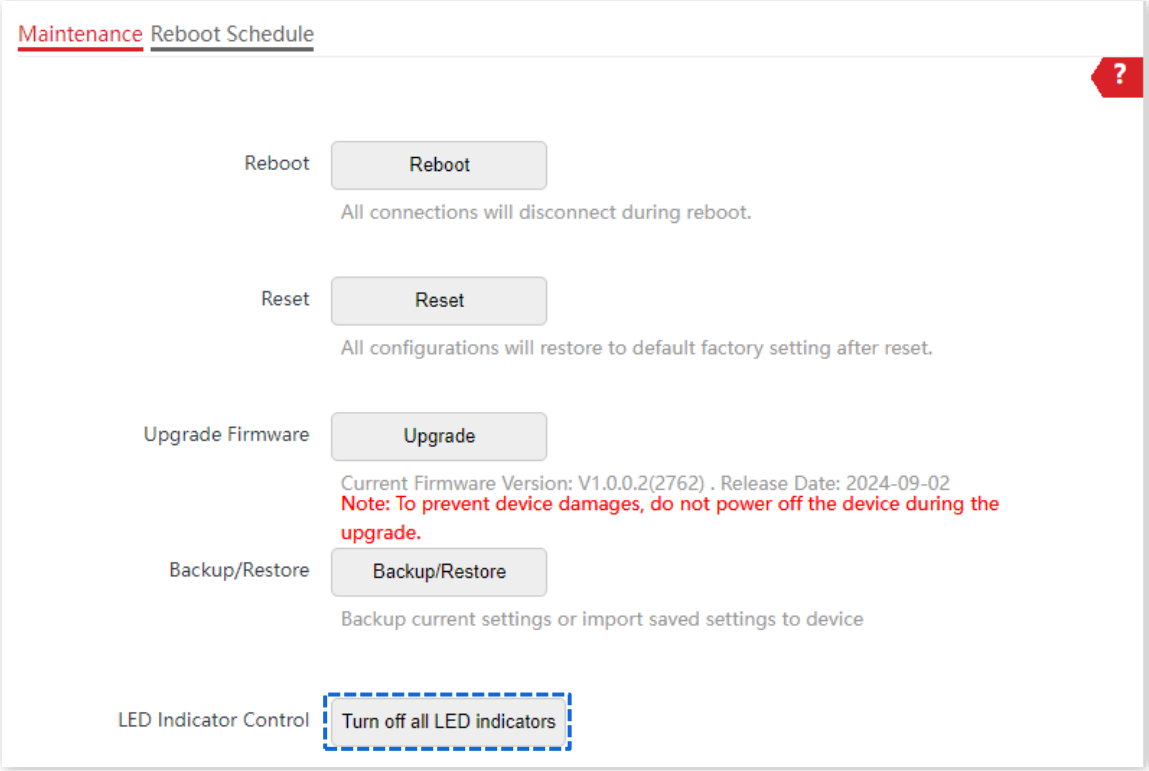


8.2.5 LED indicator control

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

Turn off the LED indicator

1. Log in to the web UI of the AP, and navigate to **Tools** > **Maintenance** > **Maintenance**.
2. Click **Turn off all LED indicators**.

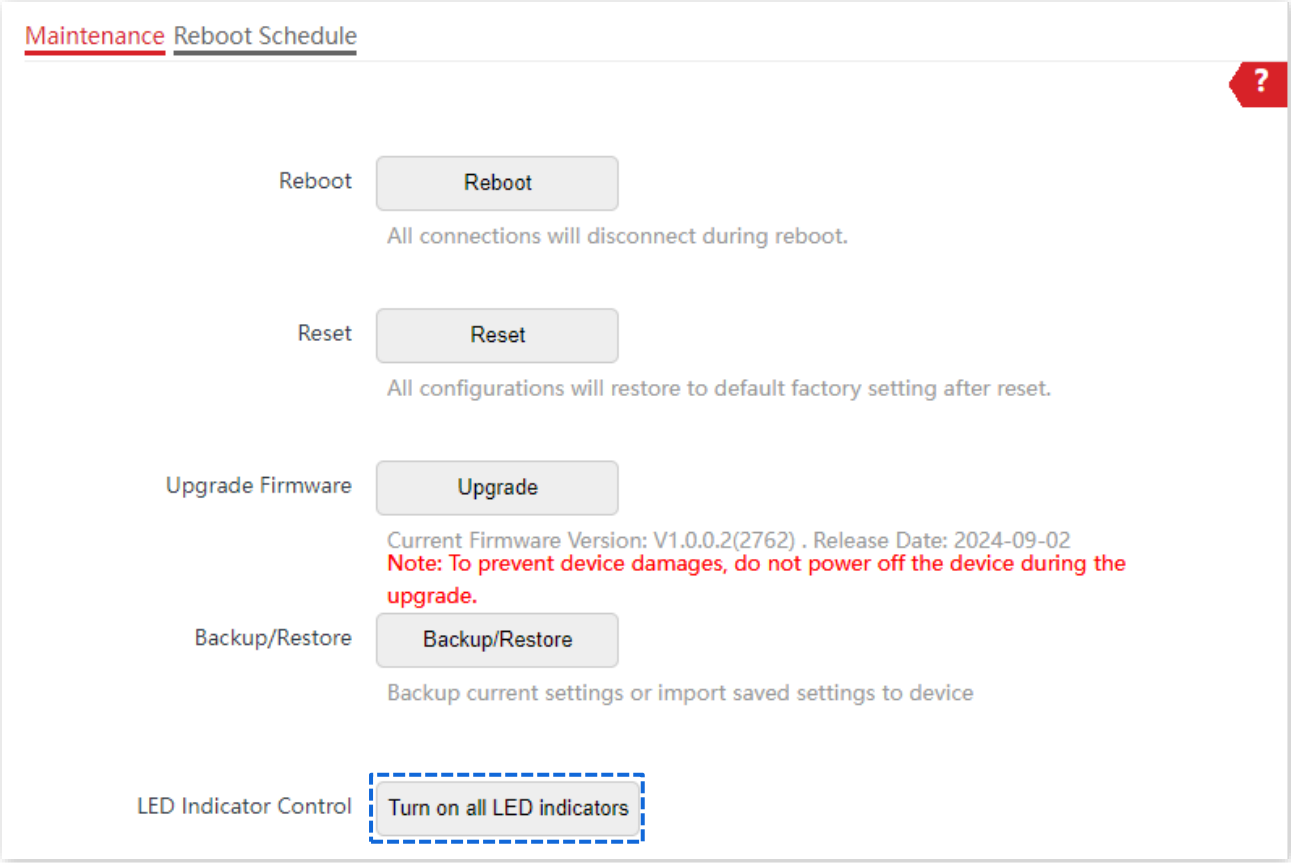


---End

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

Turn on the LED indicator

1. Log in to the web UI of the AP, and navigate to **Tools** > **Maintenance** > **Maintenance**.
2. Click **Turn on all LED indicators**.



---End

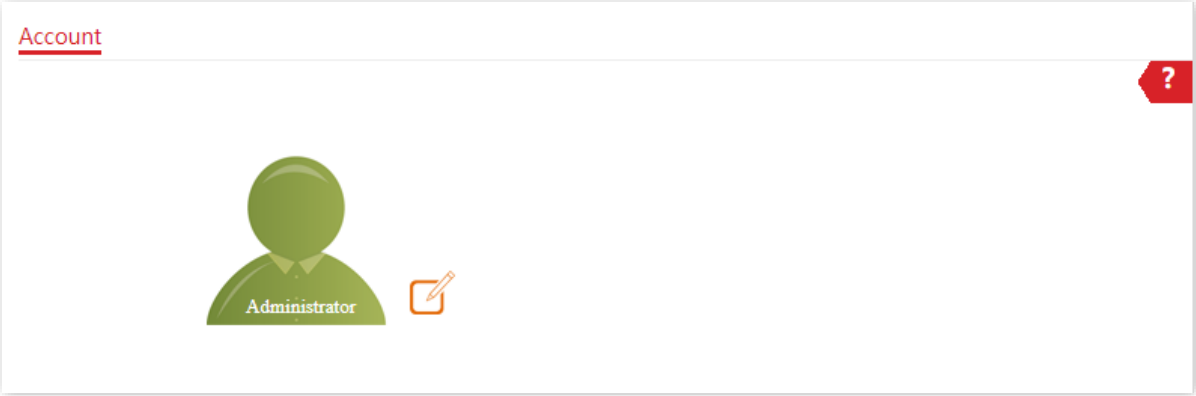
After the configuration is completed, the LED indicator lights up again and you can judge the working status of the AP.

8.3 Account

8.3.1 Overview

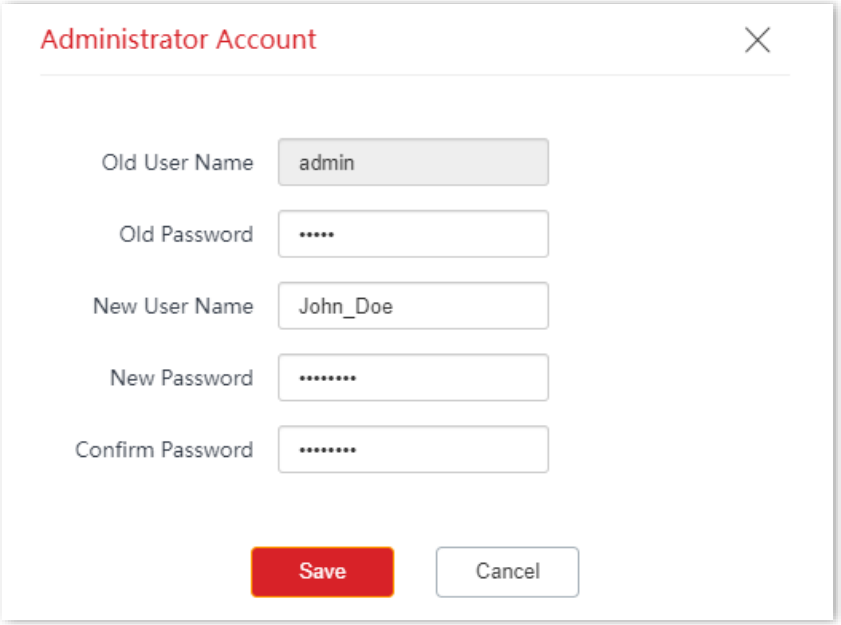
To access the page, log in to the web UI of the AP, and navigate to **Tools** > **Account**.

On this page, you can modify the information of the account to keep unauthorized users from entering the web UI and modifying configurations, thus protecting the wireless network.



8.3.2 Change the password and user name of login account

1. Log in to the web UI of the AP, and navigate to **Tools** > **Account**.
2. Click beside the account to be modified.
3. Enter the current password in **Old Password**.
4. Enter the new user name in **New User Name**, which is **John_Doe** in this example.
5. Enter the new password in **New Password**.
6. Enter again the new password in **Confirm Password**.
7. Click **Save**.



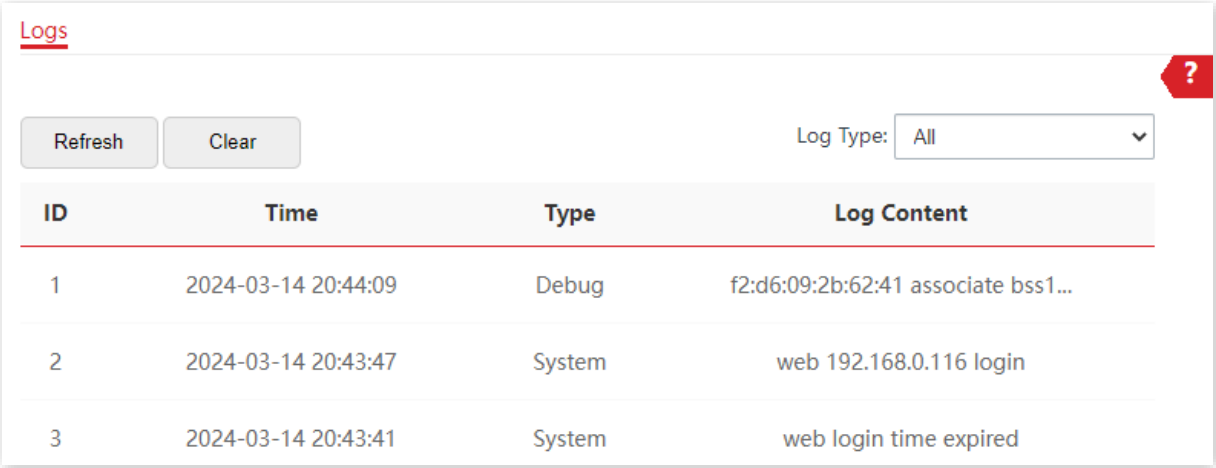
---End

Then you will be redirected to the login page. Enter the new user name and password, and click **Login** to log in to the web UI of the AP.

8.4 System log

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

To access the page, log in to the web UI of the AP, and navigate to **Tools** > **System Log**.



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

By default, the latest 300 logs are saved. To view the latest logs of the AP, click **Refresh**. To clear the existing logs of the AP, click **Clear**. Select only **Debug** or **System** log type from the **Log Type** drop-down list box.

Note

When the AP reboots, the previous logs will be cleared. 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 backed up or restored, or the factory settings are restored.

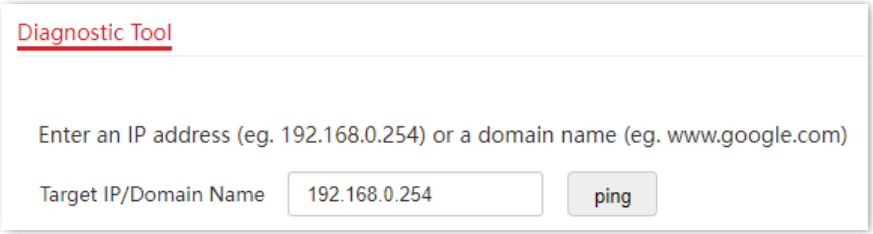
8.5 Diagnostic tool

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

Configuration procedure

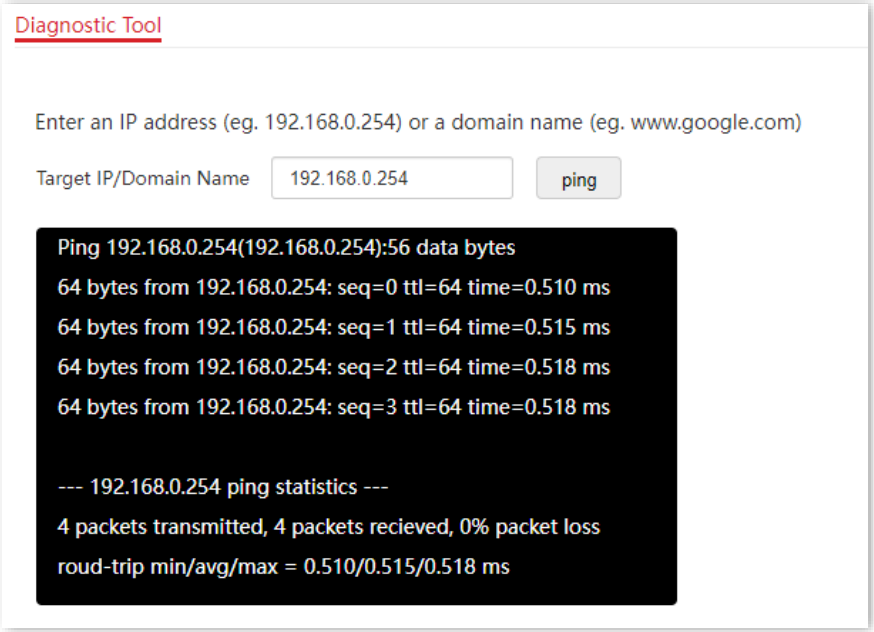
The link to **192.168.0.254** is used as an example.

1. Log in to the web UI of the AP, and navigate to **Tools** > **Diagnostic Tool**.
2. Enter the IP address or domain name to be pinged in the **Target IP/Domain Name** text box, which is **192.168.0.254** in this example.
3. Click **ping**.



---End

The diagnosis result will be displayed in a few seconds in the black text box below the **Target IP/Domain Name** text box. See the following figure.



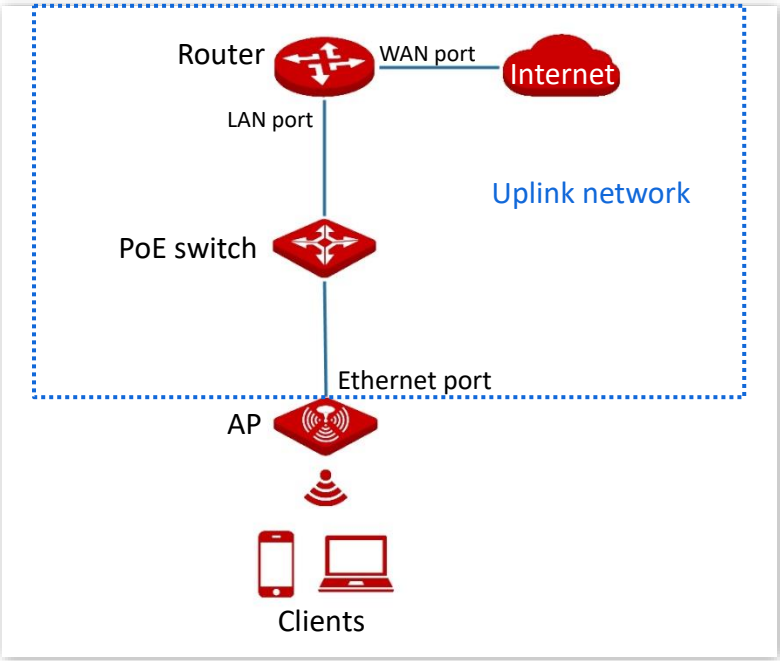
8.6 Uplink detection

8.6.1 Overview

In AP mode, the AP connects to its upstream network using the Ethernet port (LAN port). If a critical node between the Ethernet port and the upstream network fails, the AP as well as the wireless clients connected to the AP cannot access the upstream network. If uplink detection is enabled, the AP regularly pings specified hosts through the Ethernet port. If all the hosts are not reachable, the AP stops its wireless service and wireless clients cannot find the SSIDs of the AP. The client can reconnect to the AP only after the connection between the AP and the upstream networks is recovered.

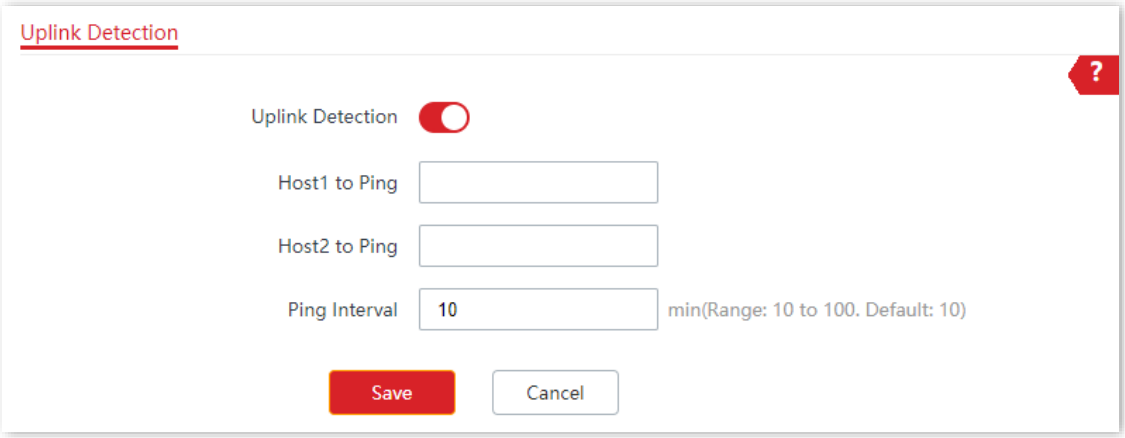
If the uplink of the AP with uplink detection enabled is faulty, wireless clients can connect to the upstream network through another nearby AP that works properly.

See the following figure (The Ethernet port serves as the uplink port).



8.6.2 Configure uplink detection

1. Log in to the web UI of the AP, and navigate to **Tools** > **Uplink Detection**.
2. Enable the **Uplink Detection** function.
3. Set **Host1 to Ping** or **Host2 to Ping** to the IP address of the host to be pinged through the LAN port of the AP, such as the IP address of the switch or router directly connected to the AP.
4. Set **Ping Interval** to the interval at which the AP checks its uplink.
5. Click **Save**.



---End

Parameter description

Parameter	Description
Uplink Detection	Specifies whether to enable the uplink detection function of the AP.
Host1 to Ping	Specify the IP address of the host to be pinged through the LAN port of the AP. It is available only when the uplink detection function is enabled.
Host2 to Ping	
Ping Interval	Specifies the interval at which the AP detects the uplink. It is available only when the uplink detection function is enabled. The default value is **10**.

Appendixes

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
Quick Setup	Working Mode		AP Mode
Internet Settings	IP Address		192.168.0.254 Tip With the DHCP server in the LAN, the AP may obtain an IP address from a DHCP server and you can check the new IP address from the client list of the DHCP server. It is available only when the AP is in factory settings.
	Subnet Mask		255.255.255.0
SSID Settings	SSID	2.4 GHz	The AP allows *X* SSIDs. X may vary with APs of different models. For details, you can log in to the web UI of the AP and view the related parameters on the **Wireless** > **SSID** page. The SSID displayed is IP-COM_*XXXXXX*. Where *XXXXXX* indicates the range from the last 6 characters to the last 6 characters + *X*-1 of the MAC address of the LAN ports of the AP. By default, the first SSID is enabled, and the other SSIDs are disabled.
		5 GHz	The AP allows *Y* SSIDs. Y may vary with APs of different models. For details, you can log in to the web UI of the AP and view the related parameters on the **Wireless** > **SSID** page. The SSID displayed is IP-COM_*XXXXXX*_5G. Where *XXXXXX* indicates the range from the last 6 characters + *X* to the last 6 characters + *X* + *Y*-1 of the MAC address of the LAN ports of the AP. By default, the first SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network		Enable

A.2 Acronyms & Abbreviations

Acronym or Abbreviation	Full Spelling
AC	Access Category
AC	Access Point Controller
ACK	Acknowledge Character
AES	Advanced Encryption Standard
AIFSN	Arbitration Inter Frame Spacing Number
AP	Access Point
APSD	Automatic Power Save Delivery
ASCII	American Standard Code for Information Interchange
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
GI	Guard Interval
ID	Identity Document
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MU-MIMO	Multi-User Multiple-Input Multiple-Output
OFDMA	Orthogonal Frequency Division Multiple Access
PoE	Power over Ethernet

Acronym or Abbreviation	Full Spelling
PSK	Pre-shared Key
PVID	Port-base VLAN ID
RTS	Request To Send
SAE	Simultaneous Authentication of Equals
Short GI	Short Guard Interval
SSID	Service Set Identifier
TXOP	Transmission Opportunity
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WMM	Wi-Fi multi-media
WPA	Wi-Fi Protected Access