IP-COM

User Guide

Indoor/Outdoor Wi-Fi Access Point

iUAP-AC-M/Pro-6-M

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

www.ip-com.com.cn

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 a warranty of any kind, express or implied.

Preface

This guide describes how to configure each feature of the following IP-COM indoor/outdoor APs.

- iUAP-AC-M
- Pro-6-M

Note

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

In this guide, unless otherwise specified, all screenshots are taken from Pro-6-M V1.0.

Conventions

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

Item	Presentation	Example
Cascading Menus	>	Navigate to **Status** > **Device Status**
Parameter and value	Bold	Set **User Name** to **Tom**.
UI control	Bold	On the **Policy** page, click the **OK** button.
Variable	Italic	Format: *XX:XX:XX:XX:XX:XX*
Message	“ ”	The “Success” message appears.

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

Symbol	Meaning
Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
Tip	This format is used to highlight a procedure that will save time or resources.

More information and support

Visit www.ip-com.com.cn and search for the product model to get your questions answered and get the latest documents.

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 this guide was first published.

Version	Date	Description
V1.1	2025.06.25	– Added the description of quick setup wizard, WiFi schedule, and roaming settings. – Optimized the description of login, status, internet settings, SSID settings, RF settings, RF optimization, load balancing, advanced settings, cloud maintenance, system software upgrade, system account, and system log. – Optimized sentence expression.
V1.0	2022-10-18	Original publication.

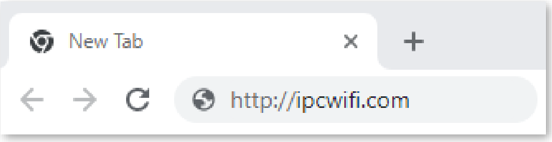
Contents

1 Quick setup wizard

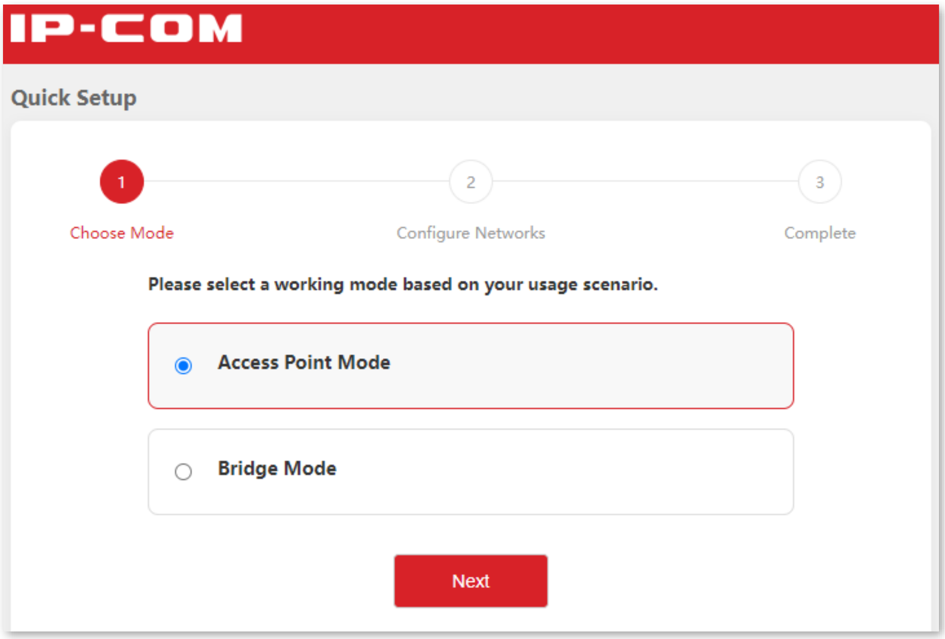
Tip

- Ensure that the internet where the AP is deployed is connected.
- If the AP is not managed by a controller (such as IP-COM ProFi Software Controller, IP-COM ProFi App or IP-COM ProFi Cloud, an AP controller (AC), or a router with AP management function), the wireless network only has a default Wi-Fi name (SSID) **IP-COM_*XXXXXX*** (***XXXXXX*** is the last six digits of the MAC address on the AP label after removing the front cover).
- If the AP is managed by the controller, log in to the web UI of the controller to view the Wi-Fi name (SSID) and password of the AP.

1. Connect a Wi-Fi-enabled device (Example: Computer) to the AP's wireless network.
2. Start a browser (such as Chrome) on your computer and visit **http://ipcwifi.com** in the address bar to log in to the web UI of the AP.



3. Set the working mode of the AP, which is **Access Point Mode** in this example. And click **Next**.



Please select a working mode based on your usage scenario.

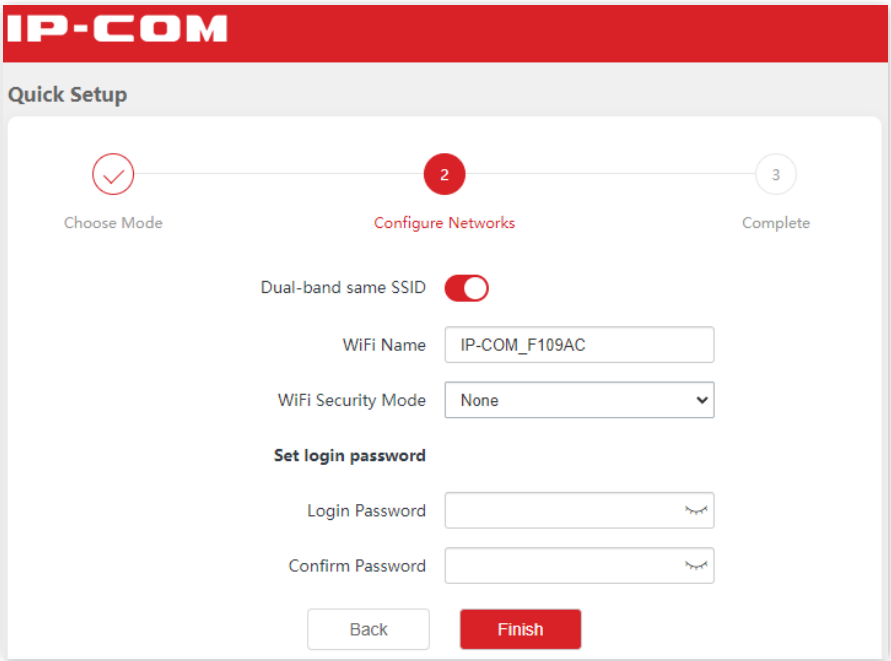
● Access Point Mode

○ Bridge Mode

4. Customize the **WiFi Name**, **WiFi Security Mode** and **Login Password**. And click **Finish**.

Note

For initial setup or after a reset, set new login and Wi-Fi passwords for privacy and security (The longer the password, the stronger the protection). The character limit and composition rules for passwords are subject to software user interface prompts.



Dual-band same SSID

WiFi Name: IP-COM_F109AC

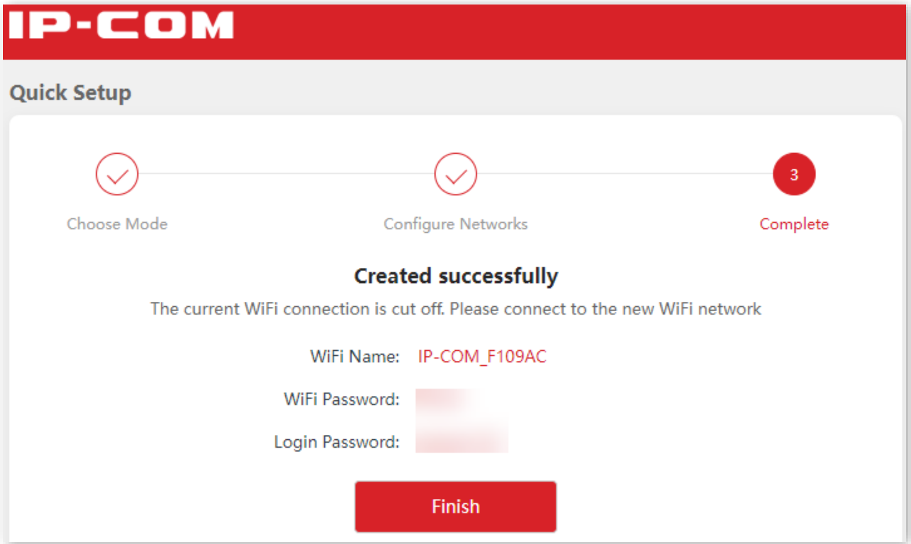
WiFi Security Mode: None

Set login password

Login Password

Confirm Password

5. If the following information is displayed, the quick setup is finished. Click **Finish**.



Created successfully

The current WiFi connection is cut off. Please connect to the new WiFi network

WiFi Name: IP-COM_F109AC

WiFi Password:

Login Password:

---End

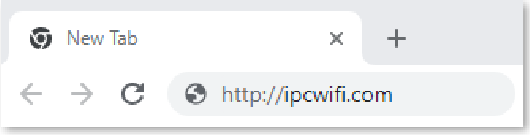
2 Login and logout

2.1 Login

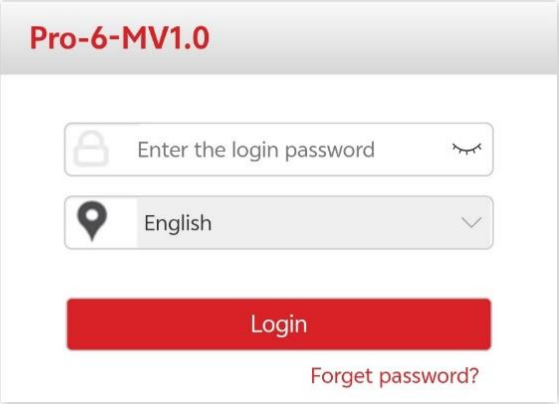
Tip

- Ensure that the internet where the AP is deployed is connected.
- If the AP is not managed by a controller (such as IP-COM ProFi Software Controller, IP-COM ProFi App or IP-COM ProFi Cloud, an AP controller (AC), or a router with AP management function), the wireless network only has a default Wi-Fi name (SSID) **IP-COM_*XXXXXX*** (***XXXXXX*** is the last six digits of the MAC address on the AP label after removing the front cover). Use the new Wi-Fi name (SSID) and password when you have customized the Wi-Fi name (SSID) and password.
- If the AP is managed by the controller, log in to the web UI of the controller to view the Wi-Fi name (SSID) and password of the AP.

1. Connect a Wi-Fi-enabled device (Example: Computer) to the AP’s wireless network.
2. Start a browser on your computer and visit **http://ipcwifi.com** to log in to the web UI of the AP.



3. Enter the login password, and click **Login**.



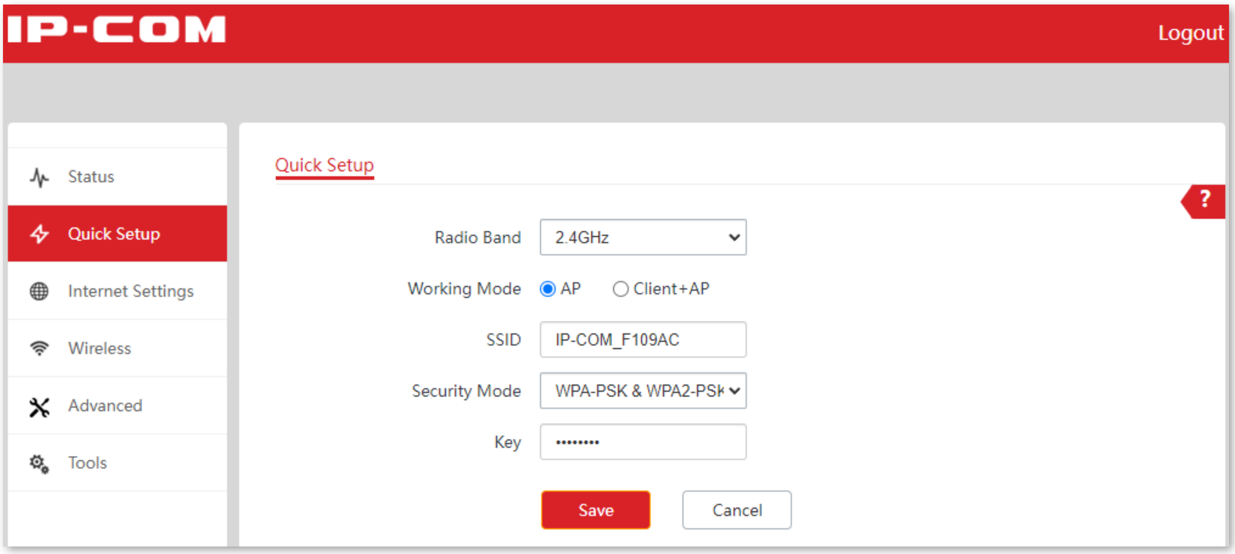
---End

Tip

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

- Ensure that the AP is working properly and the Wi-Fi-enabled device is connected to the correct wireless network.
- When logging in using your smartphone, ensure that the cellular network (mobile data) of the smartphone is disabled.
- Try to use the IP address to log in to the web UI of the AP.
  - Log in with **10.16.16.169**: Set the IP address (10.16.16.*X*, *X* ranges from 1 to 254 and is unused) of the Wi-Fi-enabled devices to the IP address within the same network segment as the AP.
  - Log in with a new IP address: If the AP obtains an IP address from the DHCP server, you can first check the new IP address from the DHCP server, and then use it to log in.
- Clear the cache of your web browser or replace the web browser, and try login again.
- Reset the AP and try again.

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



Radio Band: 2.4GHz

Working Mode: ● AP ○ Client+AP

SSID: IP-COM_F109AC

Security Mode: WPA-PSK & WPA2-PSk

Key: ••••••••

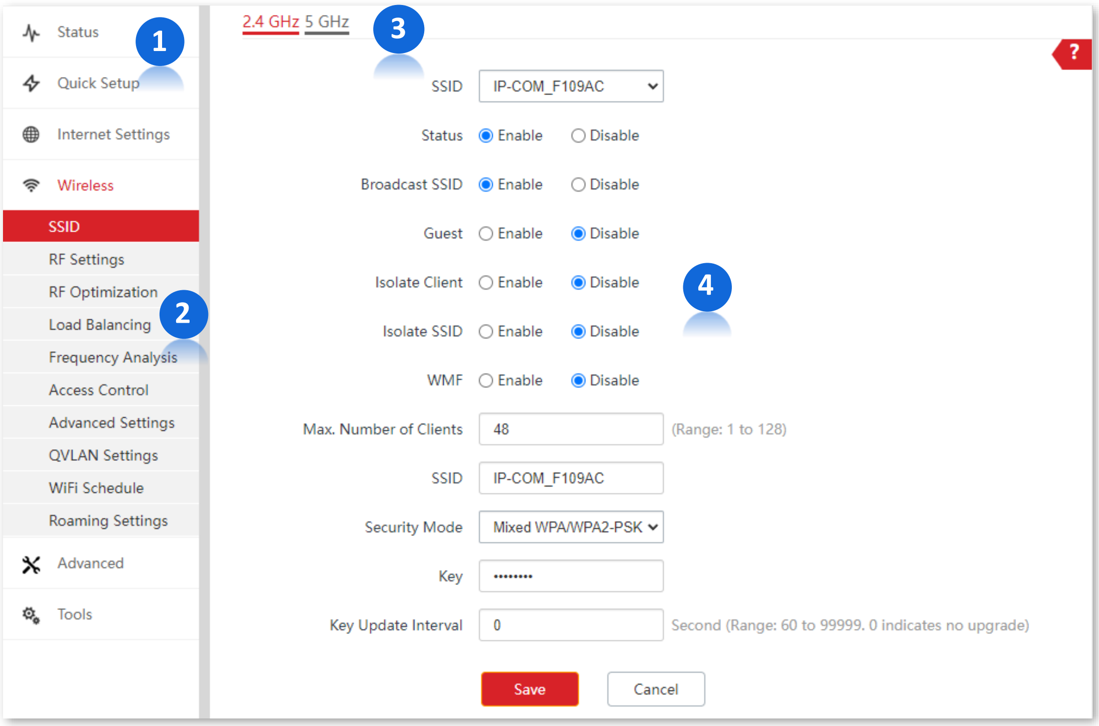
2.2 Logout

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.

3 Web UI

3.1 Layout

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



SSID: IP-COM_F109AC

Status: ● Enable ○ Disable

Broadcast SSID: ● Enable ○ Disable

Guest: ○ Enable ● Disable

Isolate Client: ○ Enable ● Disable

Isolate SSID: ○ Enable ● Disable

WMF: ○ Enable ● Disable

Max. Number of Clients: 48 (Range: 1 to 128)

SSID: IP-COM_F109AC

Security Mode: Mixed WPA/WPA2-PSK

Key: ••••••••

Key Update Interval: 0 Second (Range: 60 to 99999. 0 indicates no upgrade)

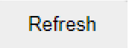
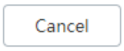
Tip

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. You 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.

3.2 Common buttons

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

Common button	Description
 Refresh	Used to refresh the current page.
Save	Used to save configurations on the current page and make the configurations take effect.
 Cancel	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.

4 Quick setup

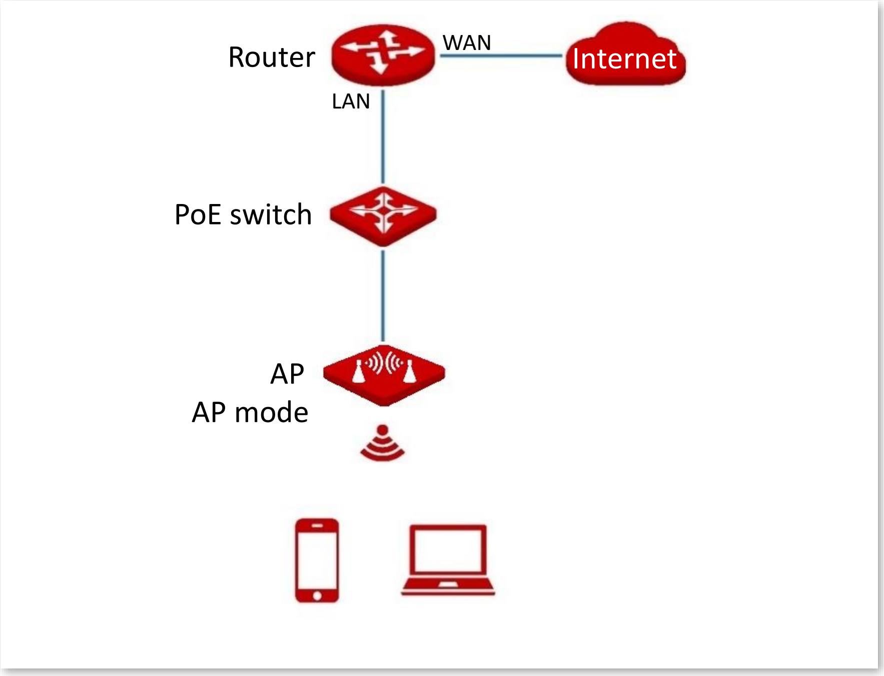
Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

To access the page, log in to the web UI of the AP, and navigate to **Quick Setup**. You can set up the AP in a quick way to enable internet access for your Wi-Fi-enabled devices (such as smartphones and laptops).

4.1 AP mode

4.1.1 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.

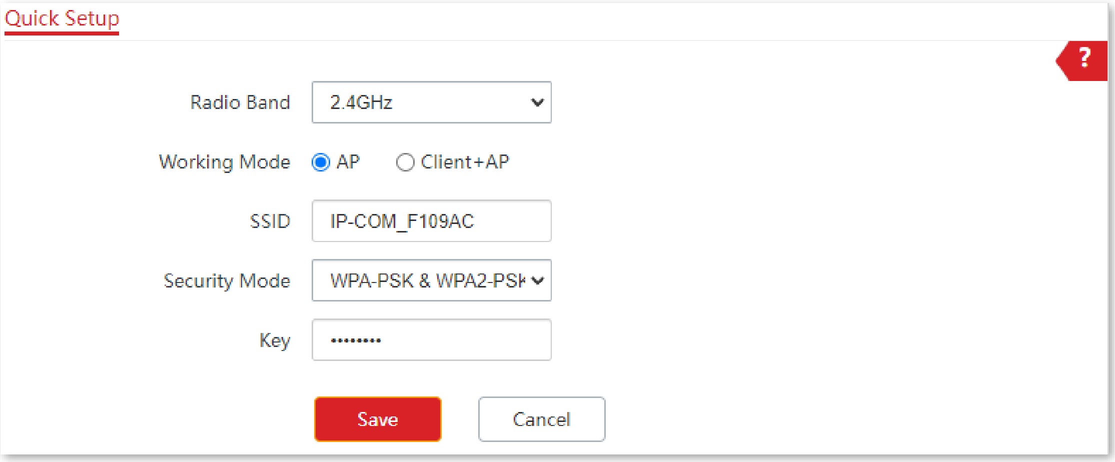


4.1.2 Configure AP mode

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 **Radio Band** to configure, which is **2.4GHz** in this example.
3. Set **Working Mode** to **AP**.
4. Set an SSID (First SSID).
5. Select a **Security Mode** and configure the incurred parameters.
6. Click **Save**.



Radio Band: 2.4GHz

Working Mode: ● AP ○ Client+AP

SSID: IP-COM_F109AC

Security Mode: WPA-PSK & WPA2-PSK

Key: ••••••••

7. If you need to configure the **5GHz** radio band as well, repeat steps 2 - 6.

---End

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

Parameter description

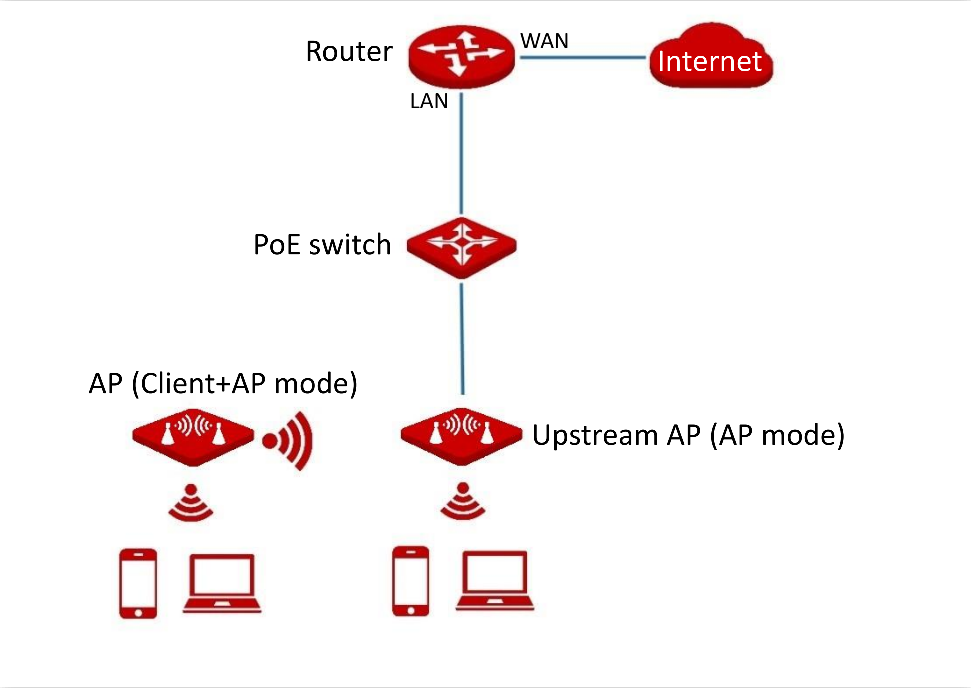
Parameter	Description
Radio Band	Used to select the radio band to configure.
Working Mode	Specifies the working mode of the AP. Select the AP mode to transform the wired network to wireless network.

Parameter	Description
SSID	Click to modify the wireless name of the first network under the selected radio band.
Security Mode	Used to select the security modes for target wireless networks. The AP can support wireless network encrypted with None, WPA-PSK, WPA2-PSK, WPA-PSK & WPA2-PSK, WPA, WPA2, WPA3-SAE and WPA2-PSK&WPA3-SAE. The security modes may differ with different models and radio bands of APs. The actual product prevails.

4.2 Client+AP mode

4.2.1 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 topology.

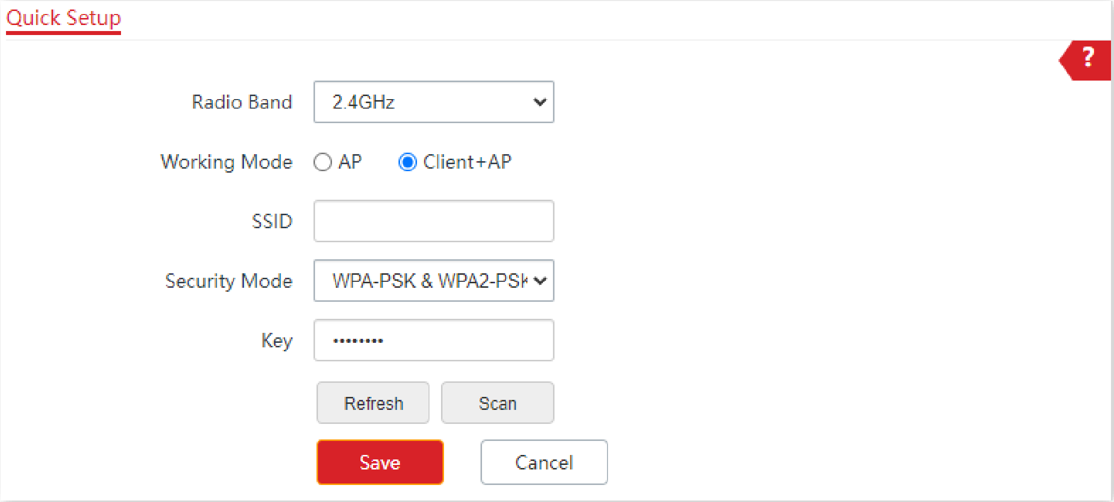


4.2.2 Configure client+AP mode

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 **Radio Band** to configure, which is **2.4GHz** in this example.
3. Set **Working Mode** to **Client+AP**.
4. Click **Scan**.



Quick Setup

Radio Band: 2.4GHz

Working Mode: ○ AP ● Client+AP

SSID:

Security Mode: WPA-PSK & WPA2-PSK

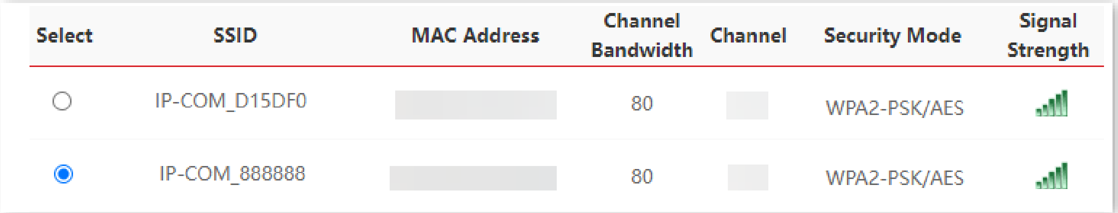
Key: ••••••••

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.

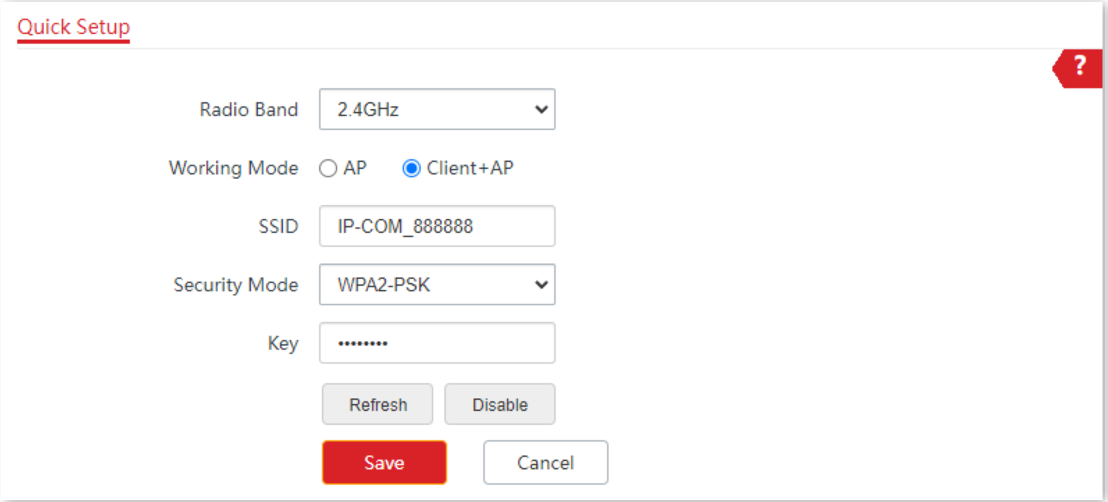
– After a wireless network to be extended is selected, the SSID, security mode and channel of the wireless network are populated automatically.



Select	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
○	IP-COM_D15DF0	[redacted]	80	[redacted]	WPA2-PSK/AES	▂▃▅▆▇
●	IP-COM_888888	[redacted]	80	[redacted]	WPA2-PSK/AES	▂▃▅▆▇

6. If the wireless network of the upstream device is encrypted, enter the Wi-Fi password of the upstream device in the **Key** box.

7. Click **Save**. The following figure is for reference only.



Quick Setup

Radio Band: 2.4GHz

Working Mode: ○ AP ● Client+AP

SSID: IP-COM_888888

Security Mode: WPA2-PSK

Key: ••••••••

---End

After the configuration is completed, you can select the SSID on your Wi-Fi-enabled devices (such as smartphones) and enter your Wi-Fi 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 Wi-Fi 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.

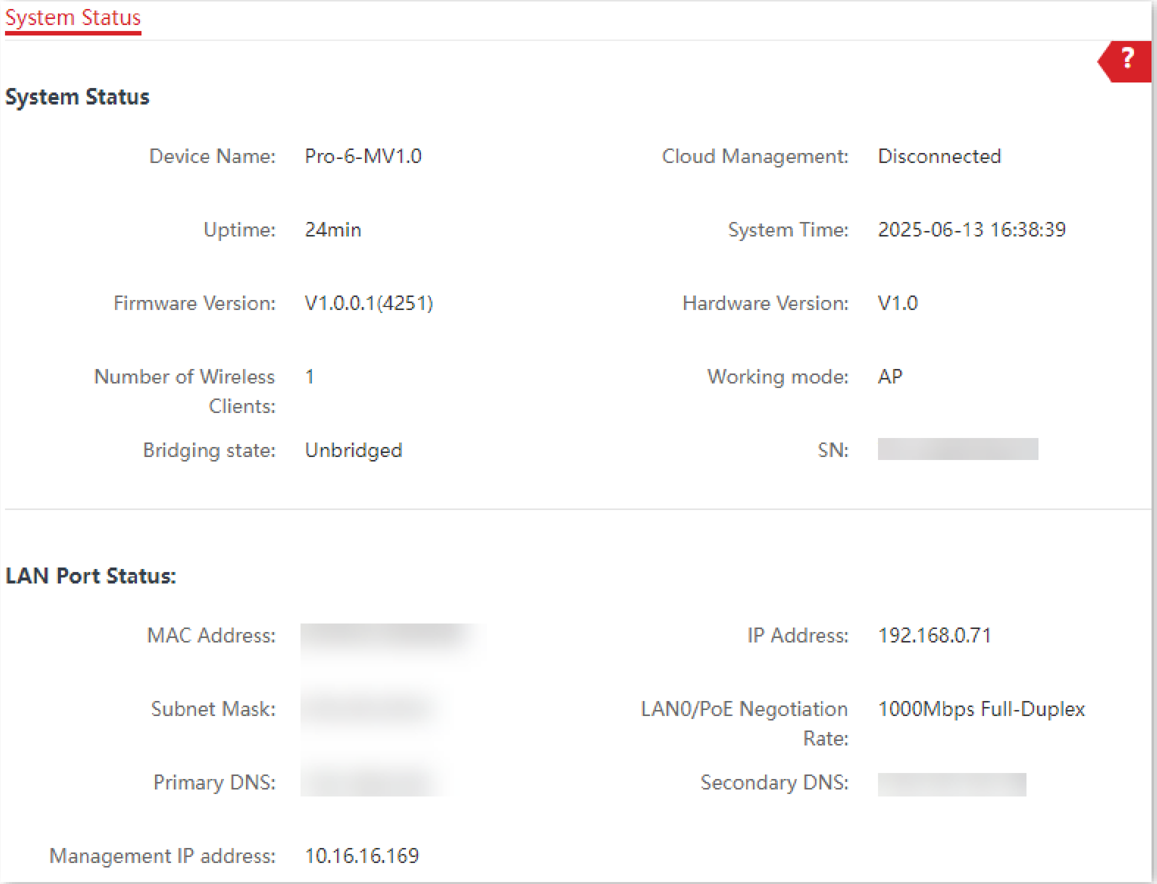
Parameter	Description
Security Mode	Specifies the security mode of which the upstream wireless network adopted. After you select the upstream wireless network from the scanned wireless network list, this parameter will be populated automatically. The AP can bridge wireless network encrypted with None, WPA-PSK, WPA2-PSK, WPA-PSK & WPA2-PSK, WPA3-SAE and WPA2-PSK&WPA3-SAE. The security modes may differ with different models and radio bands of APs. The actual product prevails. Note 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**.

5 Status

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

5.1 View system status

To access the page, log in to the web UI of the AP, and navigate to **Status** > **System Status**. You can view the system and LAN port status of the AP.



System Status

System Status

Device Name: Pro-6-MV1.0

Cloud Management: Disconnected

Uptime: 24min

System Time: 2025-06-13 16:38:39

Firmware Version: V1.0.0.1(4251)

Hardware Version: V1.0

Number of Wireless Clients: 1

Working mode: AP

Bridging state: Unbridged

SN: [redacted]

LAN Port Status:

MAC Address: [redacted]

IP Address: 192.168.0.71

Subnet Mask: [redacted]

LAN0/PoE Negotiation Rate: 1000Mbps Full-Duplex

Primary DNS: [redacted]

Secondary DNS: [redacted]

Management IP address: 10.16.16.169

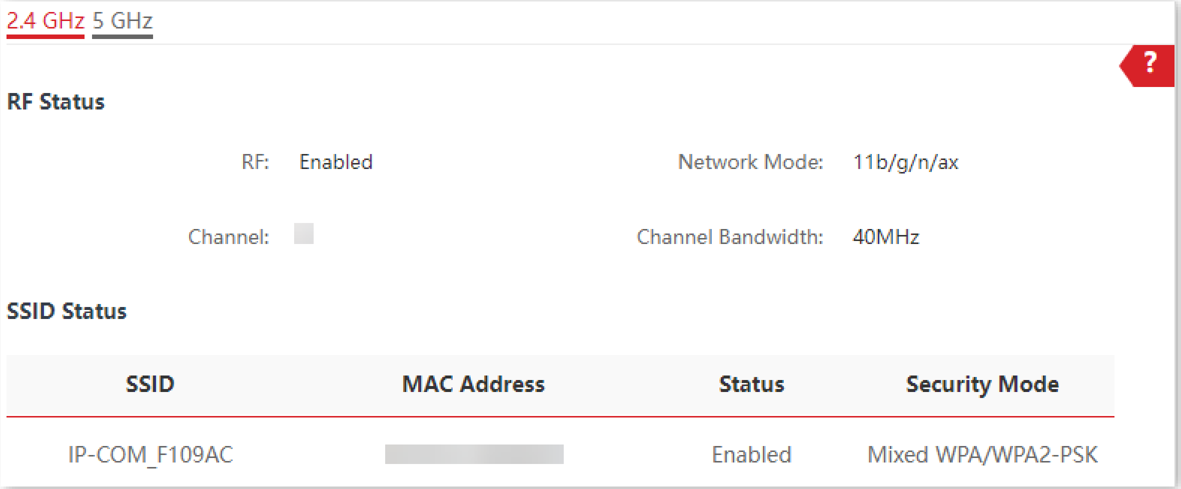
Parameter description

Parameter		Description
System Status	Device Name	Specifies the name of the AP. You can modify the AP name on the LAN setup page.
	Cloud Management	Specifies the connection status between the AP and the IP-COM ProFi cloud platform.
	Uptime	Specifies the time that has elapsed since the AP was started.
	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 serial number of the AP.
LAN Port Status	MAC Address	Specifies the physical address of the LAN port of the AP.
	IP Address	Specifies the LAN IP address of the AP. LAN devices can log in to the web UI of the AP using this IP address. By default, this IP address is obtained from the LAN's DHCP server. If there is no DHCP server in the LAN, the default IP address is 192.168.0.254. You can change the IP address on the LAN setup page. Tip – Before logging in with this IP address, ensure that the IP addresses of login devices are on the same subnet as it. – If the QVLAN function is enabled, only users connected to the AP management VLAN member ports can log in to the web UI of the AP using this IP address.
	Subnet Mask	Specifies the subnet mask corresponding to the LAN port IP address of the AP.
	LAN0/PoE Negotiation Rate	Specifies the network speed negotiated between the AP's Ethernet port and the peer device.

Parameter		Description
	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.
	Management IP address	Specifies the management IP address of the AP. LAN devices can log in to the web UI of the AP using this IP address. The default IP address is 10.16.16.169. You can change the IP address on the management IP page. Tip – Before logging in with this IP address, ensure that IP addresses of login devices are on the same subnet as it. – If the QVLAN function is enabled, only users connected to the AP management VLAN member ports can log in to the web UI of the AP using this IP address.

5.2 View wireless status

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



RF Status

RF: Enabled

Network Mode: 11b/g/n/ax

Channel: [redacted]

Channel Bandwidth: 40MHz

SSID Status

SSID	MAC Address	Status	Security Mode
IP-COM_F109AC	[redacted]	Enabled	Mixed WPA/WPA2-PSK

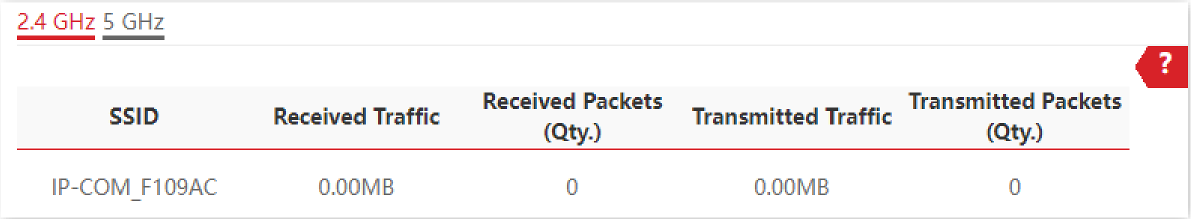
Parameter description

Parameter		Description
RF Status	RF	Specifies the status of the wireless function for the corresponding radio band of the AP.
	Network Mode	Specifies the wireless network mode for the corresponding radio band of the AP.
	Channel	Specifies the working channel for the corresponding radio band of the AP.
	Channel Bandwidth	Specifies the channel bandwidth for the corresponding radio band of the AP.
SSID Status	SSID	Specifies the names of the wireless networks for the corresponding radio band of the AP.
	MAC Address	Specifies the physical addresses corresponding to the SSIDs of the AP.
	Status	Specifies whether to enable 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.

5.3 View traffic statistics

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



SSID	Received Traffic	Received Packets (Qty.)	Transmitted Traffic	Transmitted Packets (Qty.)
IP-COM_F109AC	0.00MB	0	0.00MB	0

Parameter description

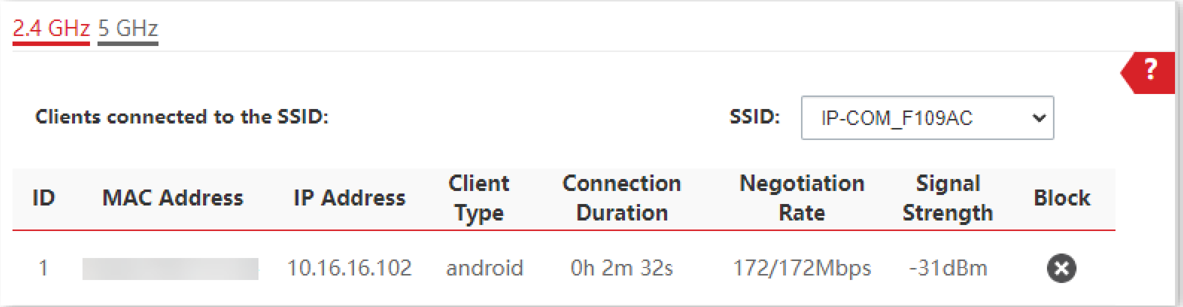
Parameter	Description
SSID	Specifies the name of the wireless network.
Received Traffic	Specifies the total number of bytes received by a wireless network.
Received Packets (Qty.)	Specifies the total number of packets received by a wireless network.
Transmitted Traffic	Specifies the total number of bytes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

Note

- All packet statistics are cleared when the AP is rebooted.
- All packet statistics for that radio band are cleared when the wireless function of the AP's corresponding radio band is disabled.
- All packet statistics of an SSID are cleared when the SSID is disabled.

5.4 View client list

To access the page, log in to the web UI of the AP, and navigate to **Status** > **Client List**. You can view the information about the wireless clients connected to the wireless networks corresponding to the SSIDs of the AP. And you can disconnect certain connected clients.



Clients connected to the SSID: SSID: IP-COM_F109AC

ID	MAC Address	IP Address	Client Type	Connection Duration	Negotiation Rate	Signal Strength	Block
1	[redacted]	10.16.16.102	android	0h 2m 32s	172/172Mbps	-31dBm	⊗

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 in 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

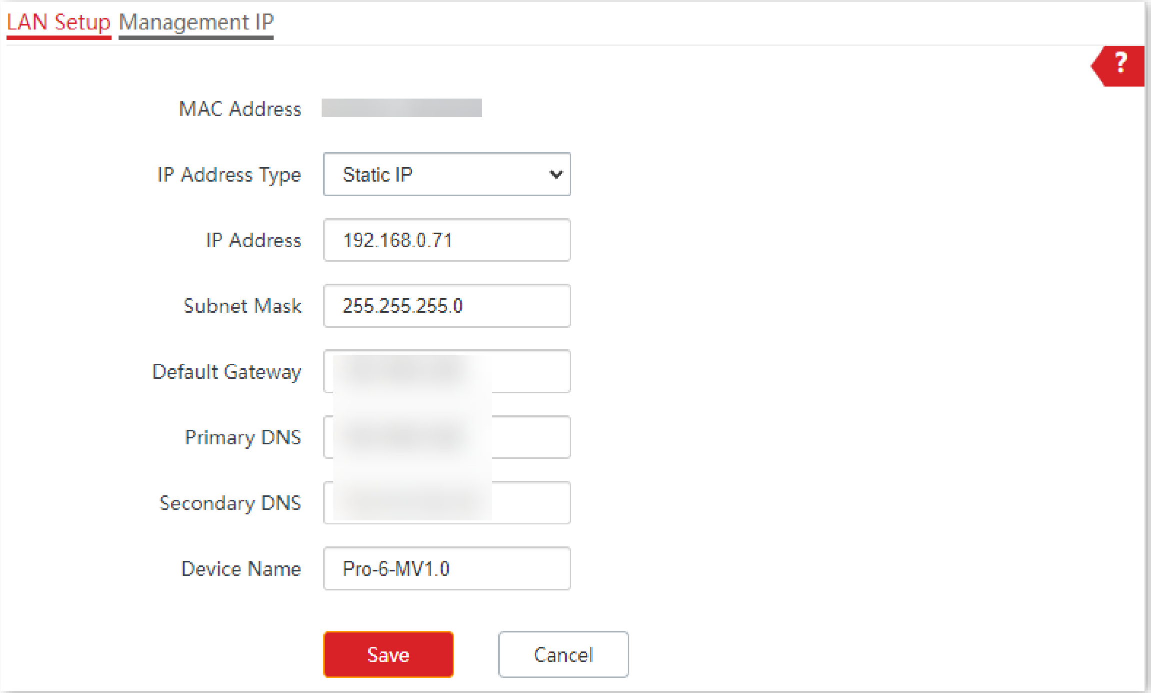
Parameter	Description
SSID	Used to select a Wi-Fi name (SSID) from the drop-down menu to view wireless clients connected to the wireless network.
MAC Address	Specifies the MAC address of the wireless client.
IP Address	Specifies the IP address of the wireless client.
Client Type	Specifies the operating system type of the wireless client. Tip It is available only when the identify client type function of the AP is enabled.
Connection Duration	Specifies the online duration of the wireless client.
Negotiation Rate	Specifies the transmit rate and receive rate of the wireless client.
Signal Strength	Specifies the Wi-Fi signal strength of the 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. To unblock a client, navigate to Access Control.

6 Internet settings

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

6.1 Configure LAN setup

To access the page, log in to the web UI of the AP, and navigate to **Internet Settings** > **LAN Setup** > **LAN Setup**. You can view the MAC address of the LAN port of the AP and set the LAN IP address, device name, and other related parameters of the AP.



MAC Address [redacted]

IP Address Type Static IP

IP Address 192.168.0.71

Subnet Mask 255.255.255.0

Default Gateway [redacted]

Primary DNS [redacted]

Secondary DNS [redacted]

Device Name Pro-6-MV1.0

Parameter description

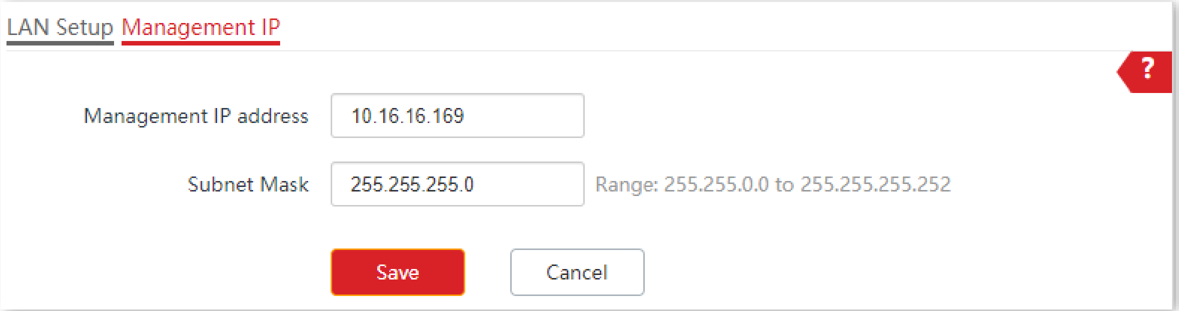
Parameter	Description
MAC Address	Specifies the MAC address of the LAN port of the AP.

Parameter	Description
IP Address Type	Specifies the LAN IP address obtaining mode of the AP. – **Static IP**: It indicates that the LAN IP address, subnet mask, gateway, and DNS server of the AP are set manually. It is proper for the scenarios where only one or several APs are deployed in the network. – **DHCP (Dynamic IP Address)**: It indicates that the LAN IP address, subnet mask, gateway, and DNS server of the AP are obtained from a DHCP server on your LAN. It is proper for the scenarios where a large group of APs are deployed in the network. Tip If **IP Address Type** is set to **DHCP (Dynamic IP Address)**, the LAN IP address of the AP may change. Before logging in to the web UI of the AP, you can first check the LAN IP address from the DHCP server, and then use it to log in.
IP Address	Specifies the LAN IP address of the AP. LAN devices can log in to the web UI of the AP using this IP address. By default, this IP address is obtained from the LAN's DHCP server. If there is no DHCP server in the LAN, the default IP address is 192.168.0.254. Tip – Before logging in with this IP address, ensure that IP addresses of login devices are on the same subnet as it. – If the QVLAN function is enabled, only users connected to the AP management VLAN member ports can log in to the web UI of the AP using this IP address.
Subnet Mask	Specifies the subnet mask of the LAN IP address of the AP. The default subnet mask is **255.255.255.0**.
Default Gateway	Specifies the default gateway corresponding to the LAN IP address of the AP. Generally, set the gateway IP address to the LAN IP address of your egress router.
Primary DNS	Specifies the primary DNS server of the AP. If your egress router provides the DNS proxy function, this IP address can be the LAN IP address of the egress router. Otherwise, enter a correct DNS server IP address.
Secondary DNS	Specifies the secondary DNS server address 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.

Parameter	Description
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 Garden-north), so that you can easily identify the AP when managing many APs.
Optimize Ethernet for	Specifies the Ethernet mode of the PoE/LAN port of this AP. – **Faster 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 when the Ethernet cable that connects the PoE/LAN 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/LAN port of the AP may not be able to properly transmit or receive data. Tip This function is available on some APs. The actual product prevails.

6.2 Configure management IP

To access the page, log in to the web UI of the AP, and navigate to **Internet Settings** > **LAN Setup** > **Management IP**. You can modify the management IP address and subnet mask.



LAN Setup Management IP

Management IP address: 10.16.16.169

Subnet Mask: 255.255.255.0 Range: 255.255.0.0 to 255.255.255.252

Parameter description

Parameter	Description
Management IP address	Specifies the management IP address of the AP. LAN devices can log in to the web UI of the AP using this IP address. The default IP address is 10.16.16.169. Tip – Before logging in with this IP address, ensure that the IP addresses of login devices are on the same subnet as it. – If the QVLAN function is enabled, only users connected to the AP management VLAN member ports can log in to the web UI of the AP using this IP address.
Subnet Mask	Specifies the subnet mask of the management IP address.

6.3 Configure intelligent DHCP service

6.3.1 Overview

In a network environment without the DHCP server, you can use the intelligent DHCP service function. With the function enabled, the AP acts as a DHCP server to automatically assign IP addresses to clients connected to the AP. The assigned IP address resides in the same subnet as the AP's management address, allowing clients to access the AP management page using the management IP address. When a DHCP server exists in the network, the intelligent DHCP service status will be automatically disabled.

Tip

If the AP has been managed by an IP-COM wireless controller (or an IP-COM router that supports AP management), you need to reset the AP to re-enable the intelligent DHCP service.

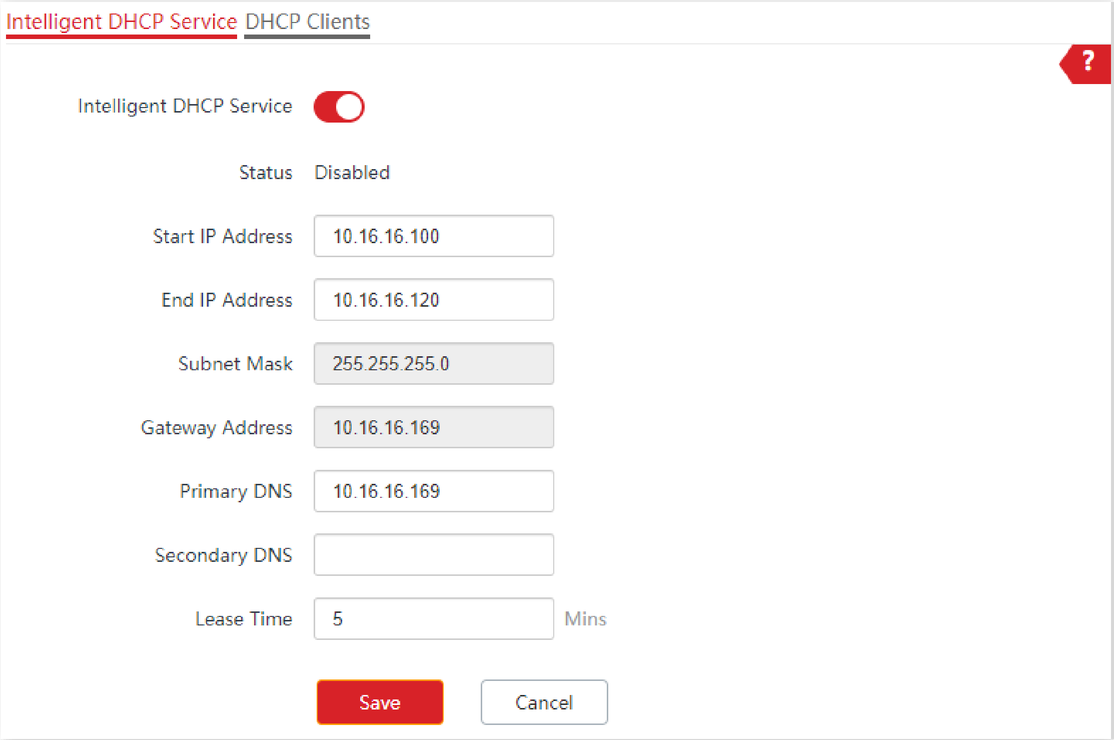
6.3.2 Set intelligent DHCP service

1. Log in to the web UI of the AP, and navigate to **Internet Settings** > **Intelligent DHCP Service** > **Intelligent DHCP Service**.

2. Enable the **Intelligent DHCP Service** function.

3. Set parameters as required.

4. Click **Save**.



Intelligent DHCP Service ●

Status Disabled

Start IP Address 10.16.16.100

End IP Address 10.16.16.120

Subnet Mask 255.255.255.0

Gateway Address 10.16.16.169

Primary DNS 10.16.16.169

Secondary DNS

Lease Time 5 Mins

---End

Parameter description

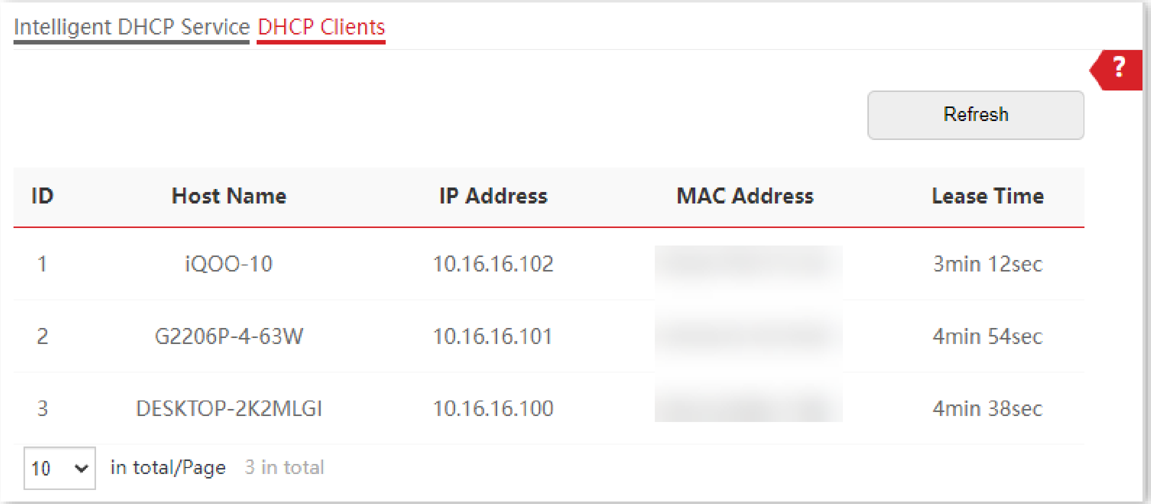
Parameter	Description
Intelligent DHCP Service	Specifies whether to enable the intelligent DHCP service function of the AP.
Status	Specifies the status of the intelligent DHCP service function of the AP.
Start IP Address	Specify the start or end IP address of the DHCP server's IP address pool.
End IP Address	
Subnet Mask	Specifies the subnet mask assigned by the DHCP server to clients. By default, it is the subnet mask corresponding to the management IP address of the AP.
Gateway Address	Specifies the gateway IP address assigned by the DHCP server to clients. By default, it is the management IP address of the AP.
Primary DNS	Specifies the IP address of the primary DNS server assigned by the DHCP server to clients.

Parameter	Description
Secondary DNS	Specifies the IP address of the secondary DNS server assigned by the DHCP server to clients. This parameter is optional, which indicates you can leave it blank if the DHCP server does not assign this parameter.
Lease Time	Specifies the validity period of an IP address assigned by the DHCP server to a client. When the lease time expires: – If the client is still connected to the AP, the client will renew the lease and continue to keep the IP address. – If the client is no longer connected to the AP, the AP will release the IP address. If another client sends a request to apply for an IP address, the AP can assign the IP address to such client.

6.3.3 View DHCP clients

After enabling the intelligent DHCP service function, log in to the web UI of the AP, and navigate to **Internet Settings** > **Intelligent DHCP Service** > **DHCP Clients**, you can view DHCP clients and the connection information.

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



ID	Host Name	IP Address	MAC Address	Lease Time
1	iQOO-10	10.16.16.102	[redacted]	3min 12sec
2	G2206P-4-63W	10.16.16.101	[redacted]	4min 54sec
3	DESKTOP-2K2MLGI	10.16.16.100	[redacted]	4min 38sec

10 in total/Page 3 in total

Parameter description

Parameter	Description
Host Name	Specifies the host name of the DHCP client.
IP Address	Specifies the IP address of the DHCP client.
MAC Address	Specifies the physical address of the DHCP client.

Parameter	Description
Lease Time	Specifies the validity period of an IP address assigned by the DHCP server to a device.
Refresh	Used to refresh the current results.

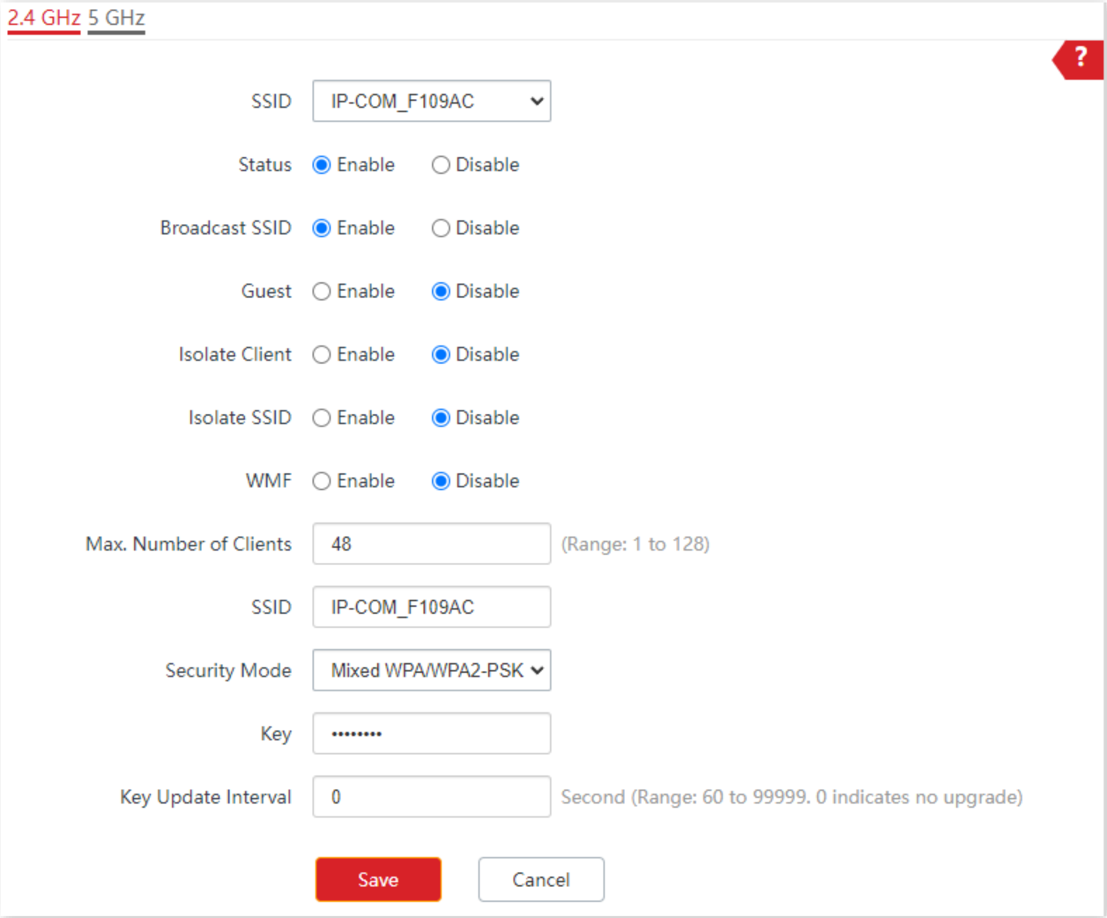
7 Wireless settings

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

7.1 SSID settings

7.1.1 Overview

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **SSID**. You can set the SSID-related parameters of the AP.



SSID: IP-COM_F109AC

Status: ● Enable ○ Disable

Broadcast SSID: ● Enable ○ Disable

Guest: ○ Enable ● Disable

Isolate Client: ○ Enable ● Disable

Isolate SSID: ○ Enable ● Disable

WMF: ○ Enable ● Disable

Max. Number of Clients: 48 (Range: 1 to 128)

SSID: IP-COM_F109AC

Security Mode: Mixed WPA/WPA2-PSK

Key: ••••••••

Key Update Interval: 0 Second (Range: 60 to 99999. 0 indicates no upgrade)

Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	
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.
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). Configuring a guest network meets guests' internet needs while protecting the security of the primary network.
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. Tip 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, Wi-Fi-enabled devices connected to different SSIDs of the AP cannot communicate with each other, enhancing the security of the wireless network. Tip 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.
Chinese SSID Encoding	Specifies the encoding format of Chinese characters in an SSID. The default value is **UTF-8**. If multiple SSIDs of the AP are enabled and contain Chinese characters, you are recommended to set this parameter to **UTF-8** for some SSIDs and to **GB2312** for others, so that any wireless clients can identify these SSIDs. Tip This function is available on some APs. The actual product prevails.
Security Mode	Specifies the security mode of the selected SSID. The options include: None, 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 and radio bands 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 (available on some APs), WPA-PSK, WPA2-PSK, WPA-PSK & WPA2-PSK (Mixed WPA/WPA2-PSK), WPA, WPA2, WPA3-SAE and WPA2-PSK&WPA3-SAE. The security modes may differ with different models and radio bands of APs. The actual product prevails.

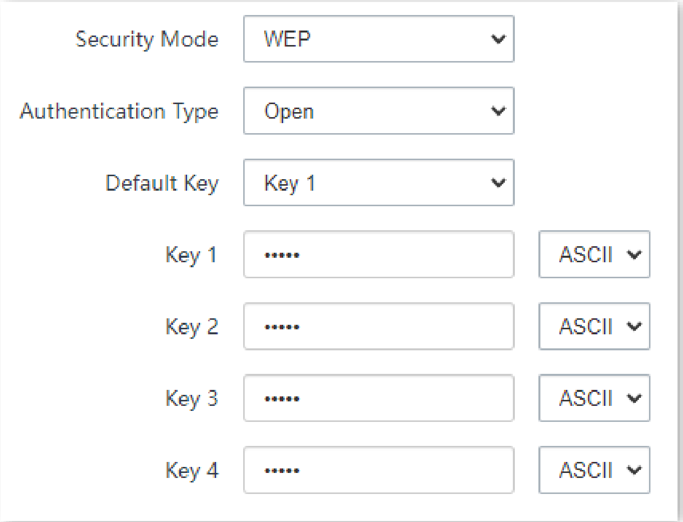
- **None**

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

- **WEP**

  This security mode is available on some APs. The actual product prevails.

  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. However, 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.



Security Mode: WEP

Authentication Type: Open

Default Key: Key 1

Key 1: ••••• ASCII

Key 2: ••••• ASCII

Key 3: ••••• ASCII

Key 4: ••••• ASCII

Parameter description

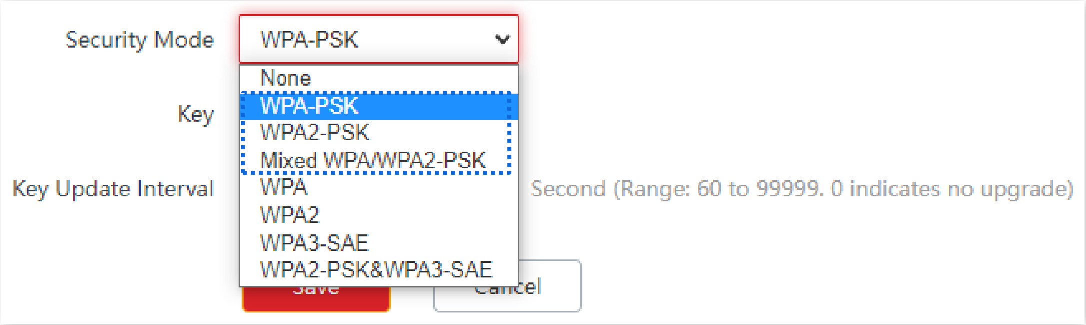
Parameter	**Description**
Authentication Type	Specifies the authentication type for the WEP security mode. The options include **Open** and **Shared**. The options share the same encryption process. – **Open**: It specifies that authentication is not required and data exchanged is encrypted with WEP. 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.

Parameter	Description
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 devices use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.



Security Mode: WPA-PSK

Key

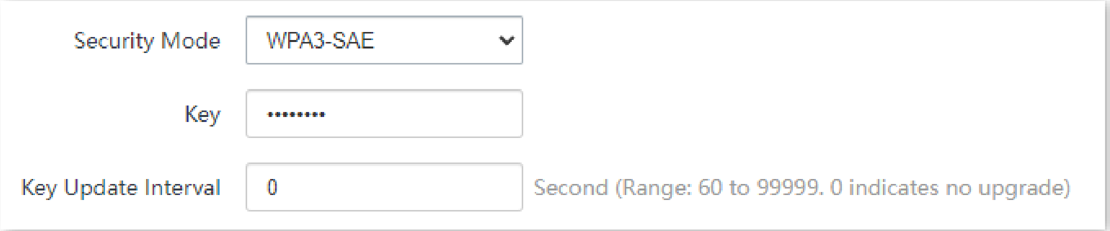
Key Update Interval — Second (Range: 60 to 99999. 0 indicates no upgrade)

- **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.



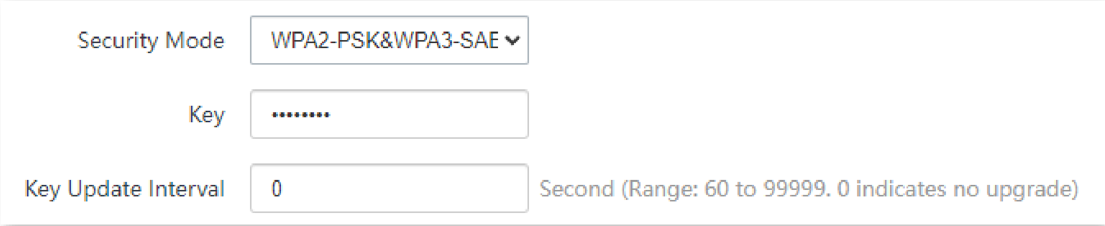
Security Mode: WPA3-SAE

Key: ••••••••

Key Update Interval: 0 Second (Range: 60 to 99999. 0 indicates no upgrade)

- **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.



Security Mode: WPA2-PSK&WPA3-SAE

Key: ••••••••

Key Update Interval: 0 Second (Range: 60 to 99999. 0 indicates no upgrade)

Parameter description

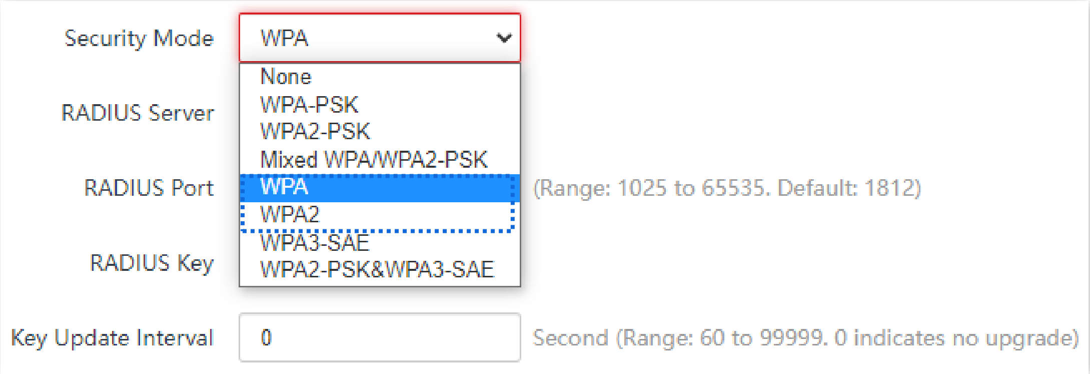
Parameter	Description
Security Mode	Specifies the personal or pre-shared key security mode, including **WPA-PSK**, **WPA2-PSK**, **WPA-PSK&WPA2-PSK (Mixed WPA/WPA2-PSK)**, **WPA3-SAE** and **WPA2-PSK&WPA3-SAE**. – **WPA-PSK**: It indicates that the wireless network corresponding to the selected SSID 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.

Parameter	Description
Encryption Algorithm	Specifies the encryption algorithm corresponding to the selected security mode. If **Security Mode** is set to **WPA-PSK**, this parameter has the **AES** and **TKIP** values. If **Security Mode** is set to **WPA2-PSK** or **WPA-PSK & WPA2-PSK (Mixed WPA/WPA2-PSK)**, this parameter has the **AES**, **TKIP**, and **TKIP&AES** values. – **AES**: It indicates the Advanced Encryption Standard. – **TKIP**: It indicates the Temporal Key Integrity Protocol. If **TKIP** is used, the maximum wireless throughput of the AP is limited to 54 Mbps. – **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. Tip This function is available on some APs. The actual product prevails.
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 WPA 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.



Security Mode: WPA

RADIUS Server

RADIUS Port (Range: 1025 to 65535. Default: 1812)

RADIUS Key

Key Update Interval: 0 Second (Range: 60 to 99999. 0 indicates no upgrade)

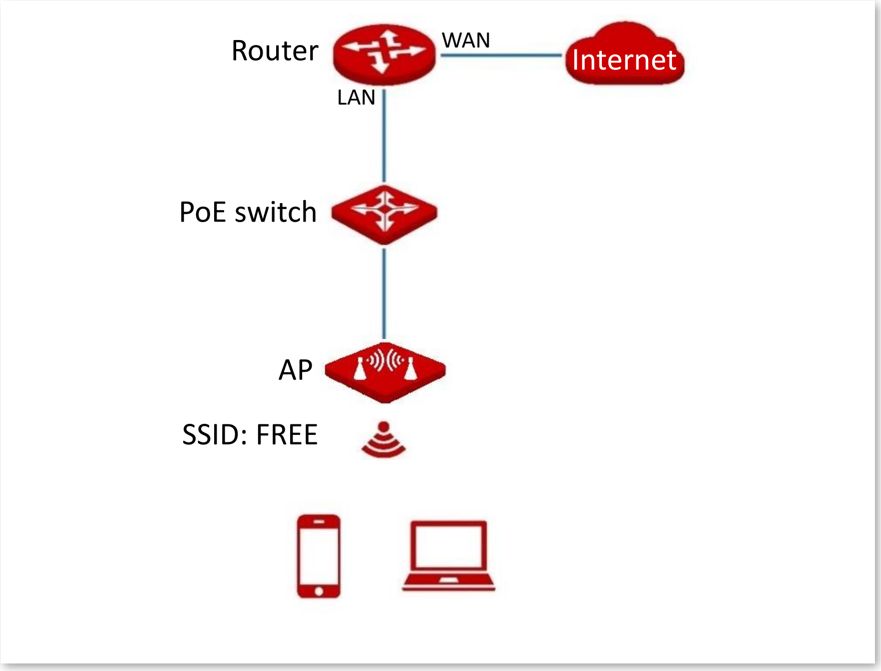
Parameter description

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 password of the RADIUS server.
Encryption Algorithm	Specifies the encryption algorithm corresponding to the selected security mode. The available options include **AES**, **TKIP**, and **TKIP&AES**. – **AES**: It indicates the Advanced Encryption Standard. – **TKIP**: It indicates the Temporal Key Integrity Protocol. If TKIP is used, the maximum wireless throughput of the AP is limited to 54 Mbps. – **TKIP&AES**: It indicates that both TKIP and AES encryption algorithms are supported. Wireless clients can connect to the wireless network corresponding to the selected SSID using TKIP or AES. Tip This function is available on some APs. The actual product prevails.
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 WPA key is not updated.

7.1.2 Example of setting up an open wireless network

Networking requirements

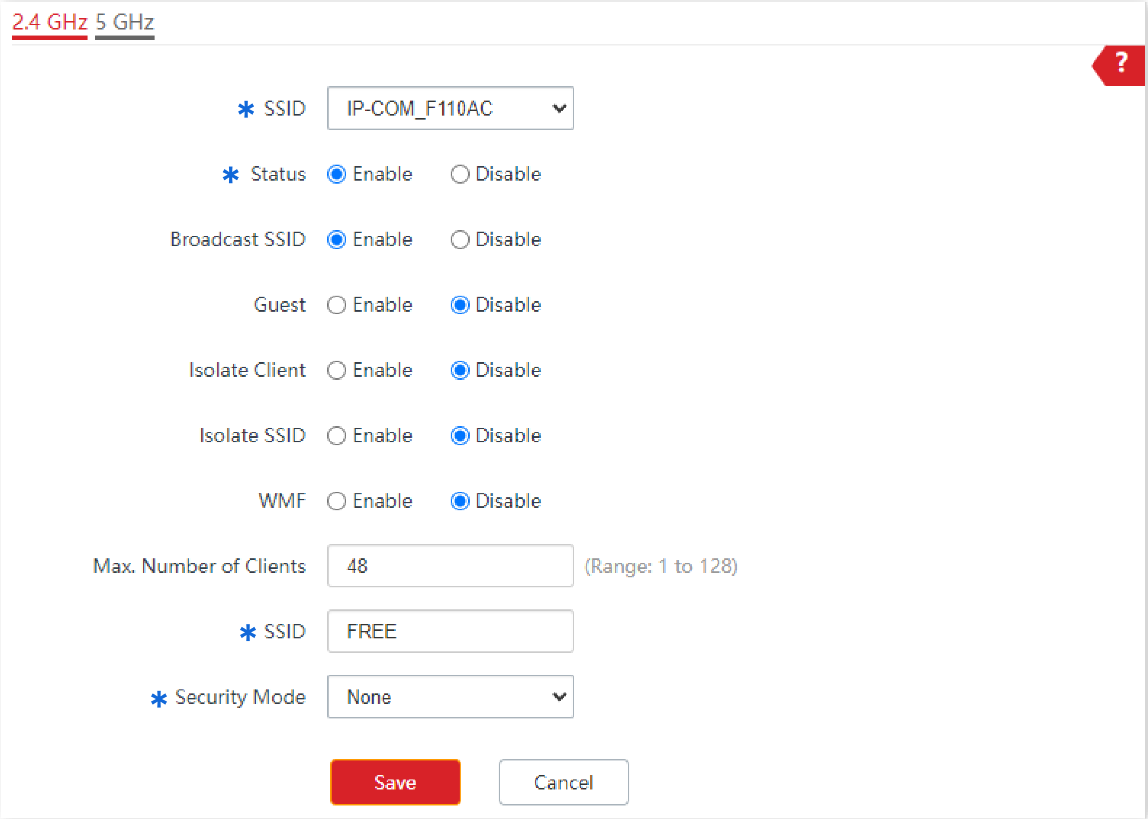
In an industrial park, guests can connect to the wireless network without a password and access the internet through the wireless network.



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**.



* SSID	IP-COM_F110AC
* Status	● Enable ○ Disable
Broadcast SSID	● Enable ○ Disable
Guest	○ Enable ● Disable
Isolate Client	○ Enable ● Disable
Isolate SSID	○ Enable ● Disable
WMF	○ Enable ● Disable
Max. Number of Clients	48 (Range: 1 to 128)
* SSID	FREE
* Security Mode	None

---End

Verification

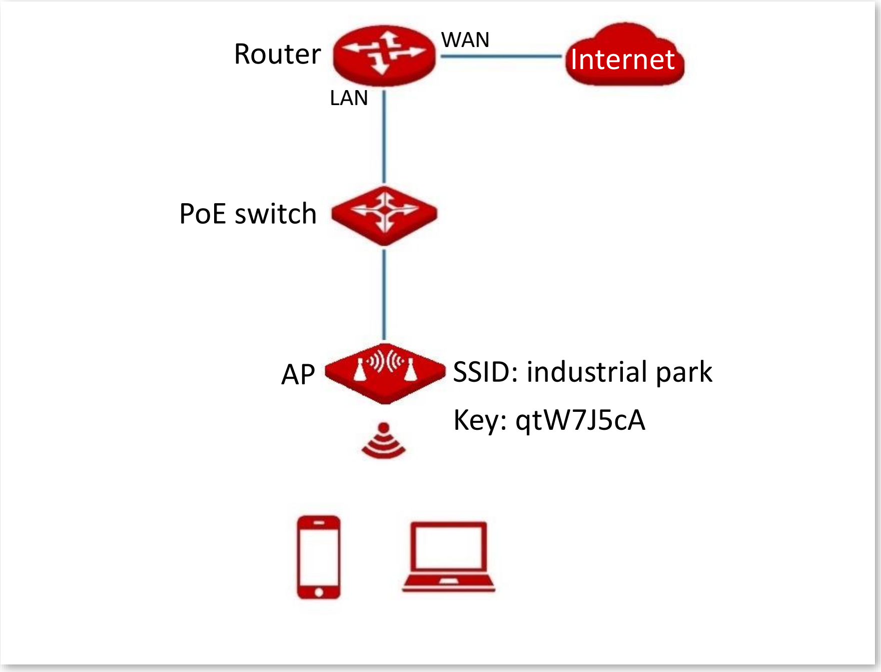
Verify that Wi-Fi-enabled devices can connect to the **FREE** wireless network without a password.

7.1.3 Example of setting up a wireless network encrypted with PSK

Networking requirements

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

Assume that the SSID is **industrial park** and the key (Wi-Fi password) is **qtW7J5cA**. See the following topology.



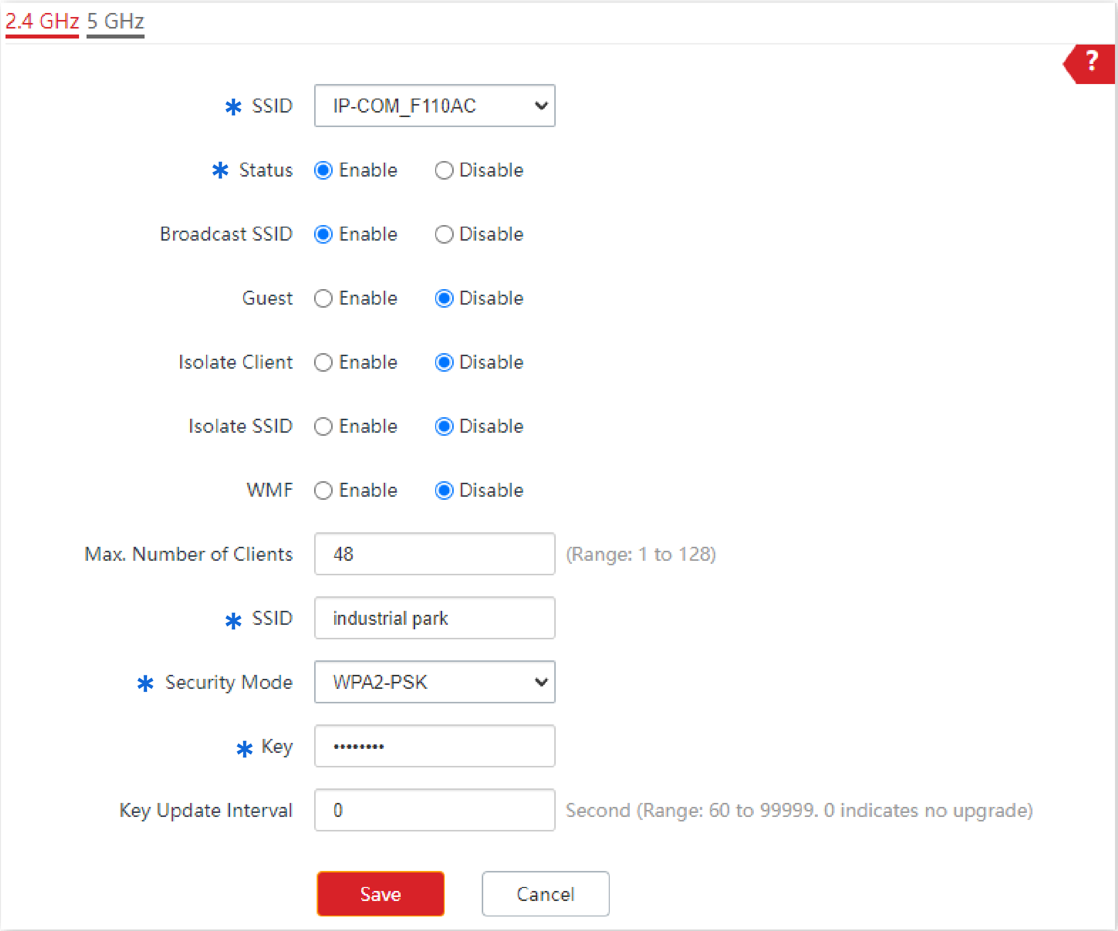
Configuration procedure

Assume that the second SSID of the 2.4 GHz radio band of the AP and the WPA2-PSK security mode are used.

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 **industrial park**.
5. Set **Security Mode**, which is **WPA2-PSK** in this example.

6. Set **Key** to **qtW7J5cA**.

7. Click **Save**.



2.4 GHz 5 GHz

* SSID	IP-COM_F110AC	
* Status	● Enable ○ Disable	
Broadcast SSID	● Enable ○ Disable	
Guest	○ Enable ● Disable	
Isolate Client	○ Enable ● Disable	
Isolate SSID	○ Enable ● Disable	
WMF	○ Enable ● Disable	
Max. Number of Clients	48	(Range: 1 to 128)
* SSID	industrial park	
* Security Mode	WPA2-PSK	
* Key	••••••••	
Key Update Interval	0	Second (Range: 60 to 99999. 0 indicates no upgrade)

---End

Verification

Verify that Wi-Fi-enabled devices can connect to the wireless network named **industrial park** with the password **qtW7J5cA**.

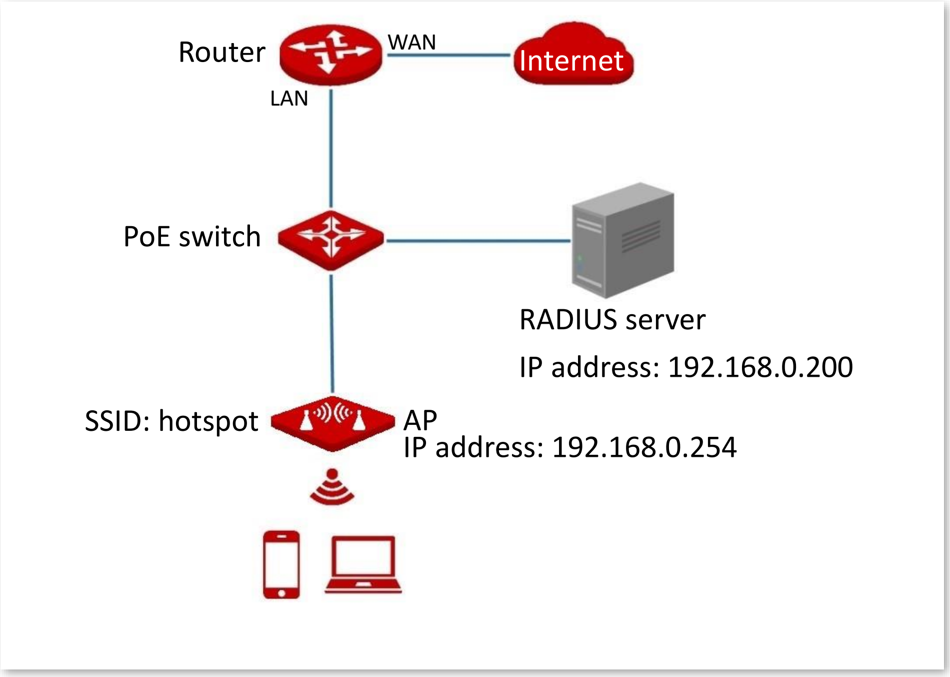
7.1.4 Example of setting up a wireless network encrypted with WPA or WPA2

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 topology.

Assume that:

- SSID: **hotspot**
- IP address of the RADIUS server: **192.168.0.200**
- RADIUS port: **1812**
- RADIUS key: **qtW7J5cA**



Configuration procedure

I. Configure the AP

Assume that the second SSID of the 2.4 GHz radio band of the AP and the WPA2 security mode are used.

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.

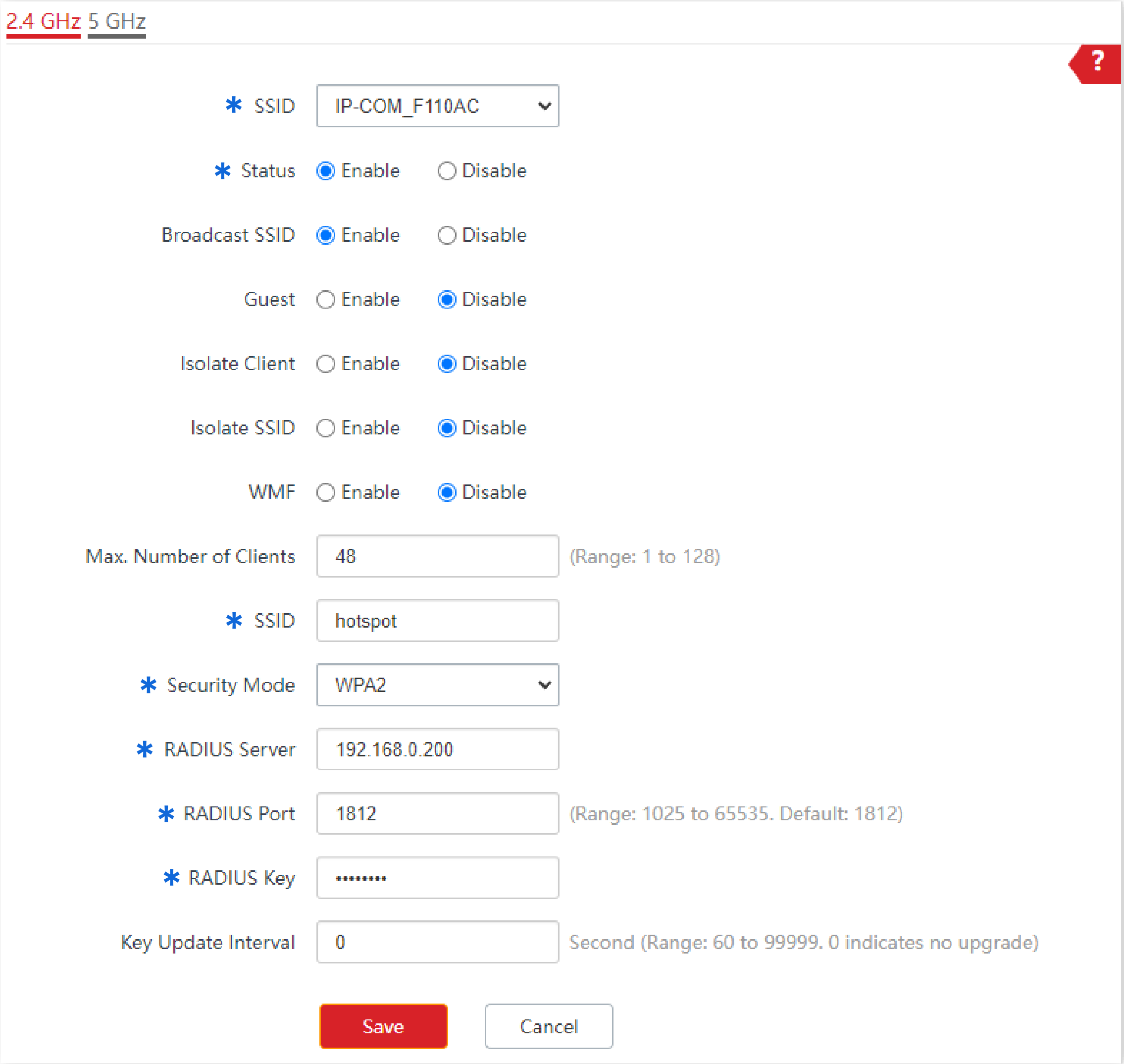
3. Set **Status** to **Enable**.

4. Set **SSID** to **hotspot**.

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

6. Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Password** to **192.168.0.200**, **1812**, and **qtW7J5cA** respectively.

7. Click **Save**.



* SSID	IP-COM_F110AC	
* Status	● Enable ○ Disable	
Broadcast SSID	● Enable ○ Disable	
Guest	○ Enable ● Disable	
Isolate Client	○ Enable ● Disable	
Isolate SSID	○ Enable ● Disable	
WMF	○ Enable ● Disable	
Max. Number of Clients	48	(Range: 1 to 128)
* SSID	hotspot	
* Security Mode	WPA2	
* RADIUS Server	192.168.0.200	
* RADIUS Port	1812	(Range: 1025 to 65535. Default: 1812)
* RADIUS Key	••••••••	
Key Update Interval	0	Second (Range: 60 to 99999. 0 indicates no upgrade)

---End

II. Configure the RADIUS server

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

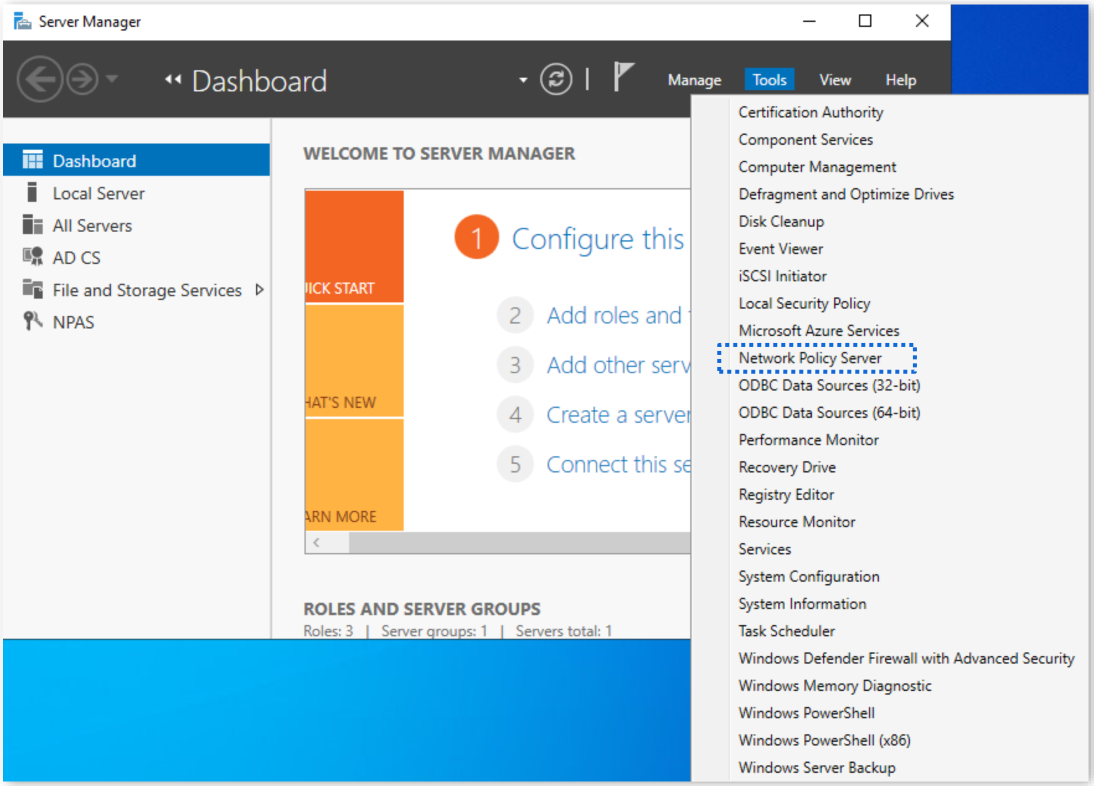
1. Install **Active Directory Certificate Services** and **Network Policy and Access Services**, and deploy the certificate.

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**.

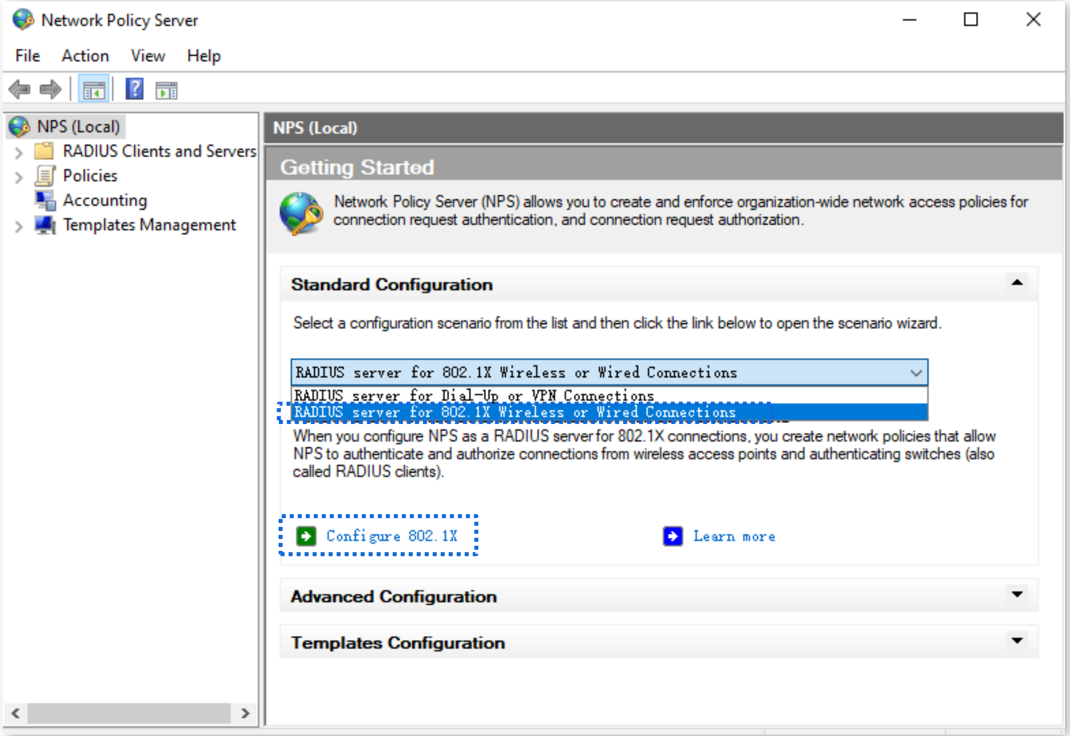
After the service installation is completed, click ⚑ in the upper right corner and follow the prompts to deploy the certificate.

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 Connections** from **Standard Configuration** and click **Configure 802.1X**.



Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

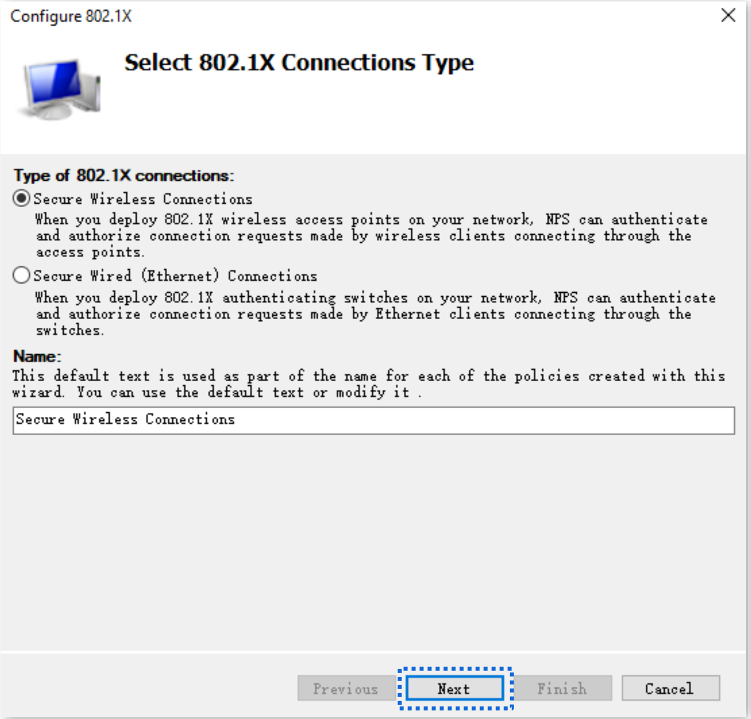
RADIUS server for 802.1X Wireless or Wired Connections

RADIUS server for Dial-Up or VPN Connections

RADIUS server for 802.1X Wireless or Wired Connections

When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).

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**.



Select 802.1X Connections Type

Type of 802.1X connections:

● Secure Wireless Connections

When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.

○ Secure Wired (Ethernet) Connections

When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

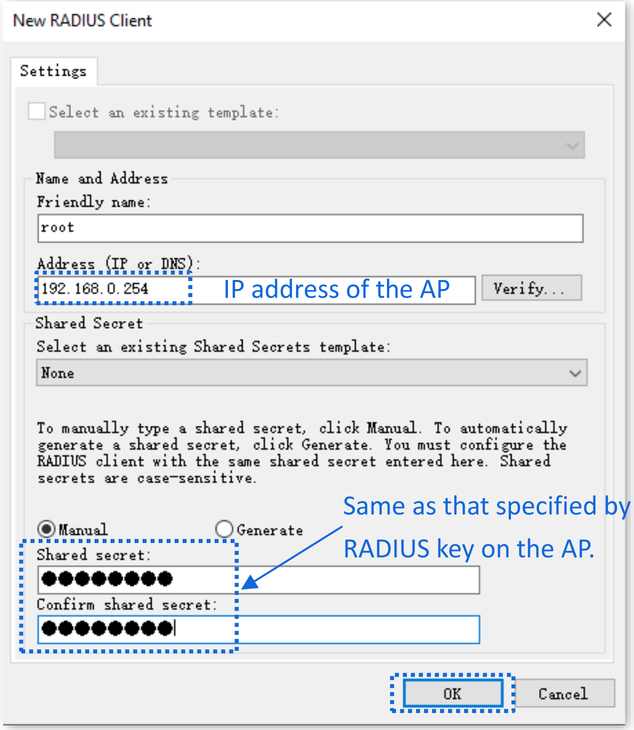
Name:

This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it .

Secure Wireless Connections

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**.



New RADIUS Client

Settings

□ Select an existing template:

Name and Address

Friendly name: root

Address (IP or DNS): 192.168.0.254

IP address of the AP

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

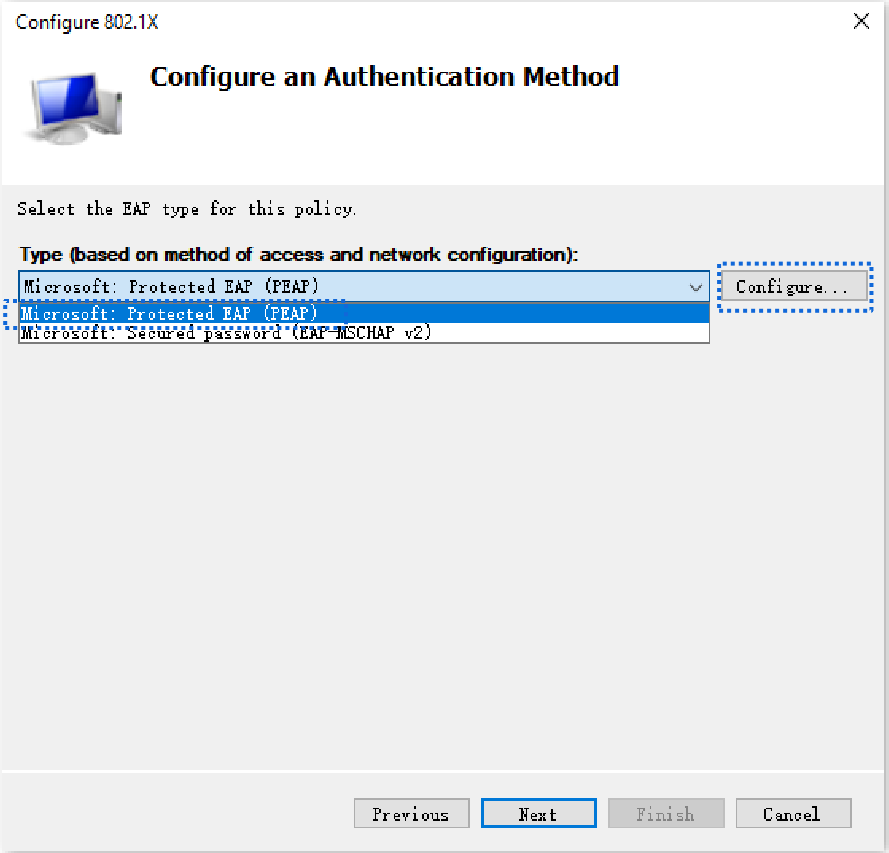
● Manual ○ Generate

Shared secret: ●●●●●●●●

Confirm shared secret: ●●●●●●●●

Same as that specified by RADIUS key on the AP.

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.



Configure 802.1X

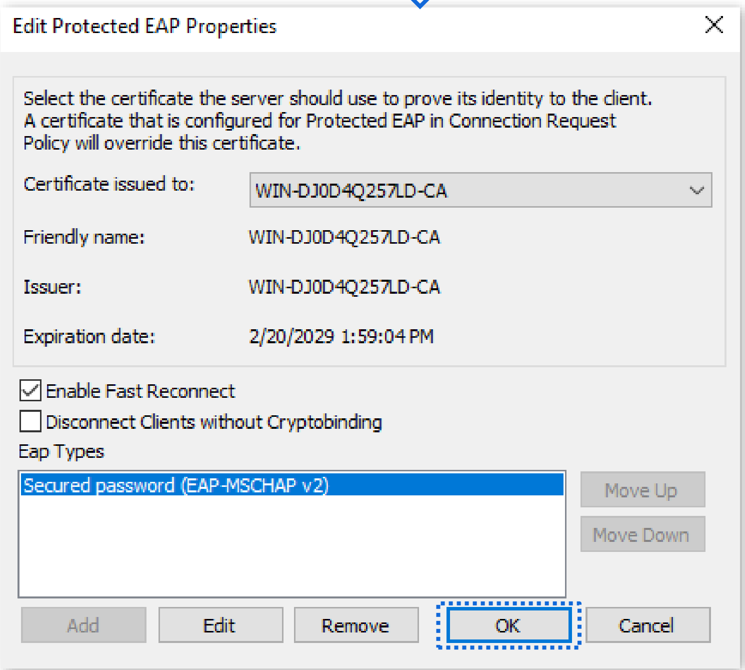
Configure an Authentication Method

Select the EAP type for this policy.

Type (based on method of access and network configuration):

Microsoft: Protected EAP (PEAP)

Microsoft: Protected EAP (PEAP)
Microsoft: Secured password (EAP-MSCHAP v2)



Edit Protected EAP Properties

Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued to: WIN-DJ0D4Q257LD-CA

Friendly name: WIN-DJ0D4Q257LD-CA

Issuer: WIN-DJ0D4Q257LD-CA

Expiration date: 2/20/2029 1:59:04 PM

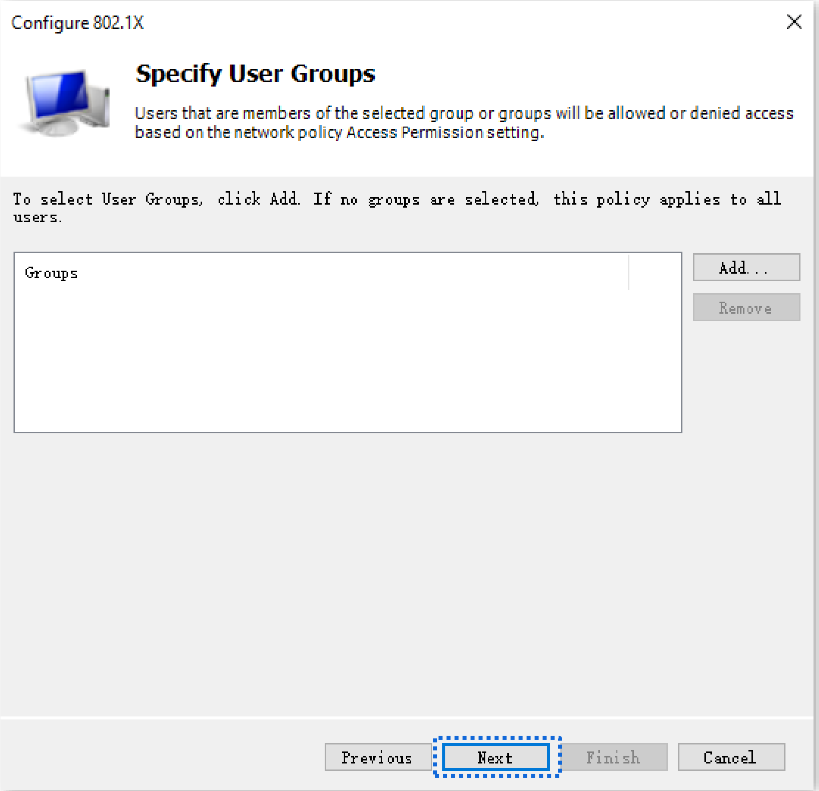
☑ Enable Fast Reconnect

□ Disconnect Clients without Cryptobinding

Eap Types

Secured password (EAP-MSCHAP v2)

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



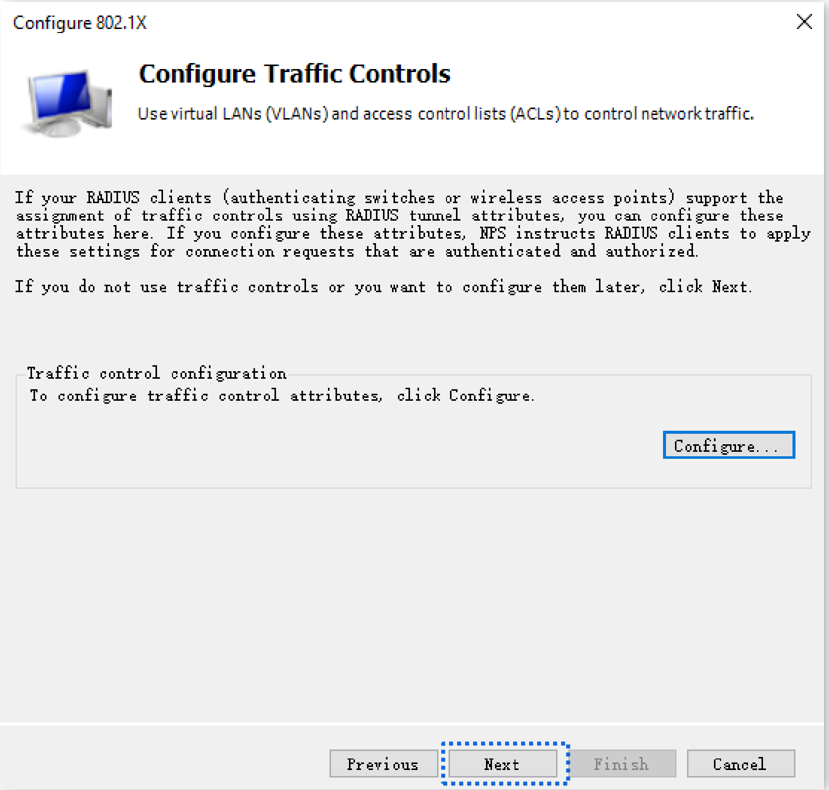
Configure 802.1X

Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

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



Configure 802.1X

Configure Traffic Controls

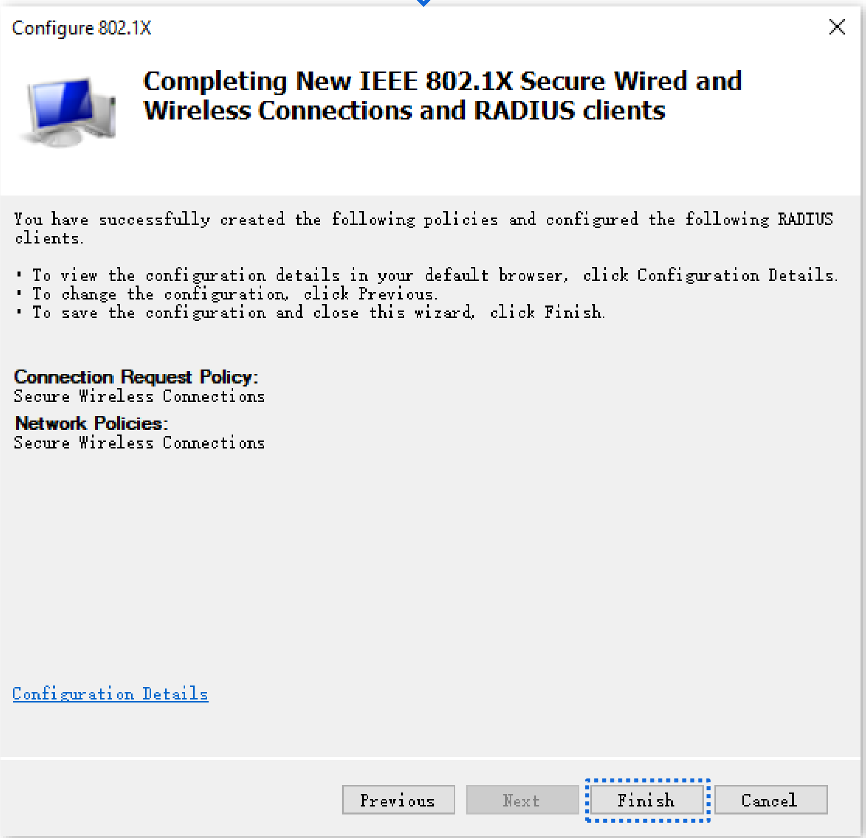
Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, NPS instructs RADIUS clients to apply these settings for connection requests that are authenticated and authorized.

If you do not use traffic controls or you want to configure them later, click Next.

Traffic control configuration

To configure traffic control attributes, click Configure.



Configure 802.1X

Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

Connection Request Policy:
Secure Wireless Connections

Network Policies:
Secure Wireless Connections

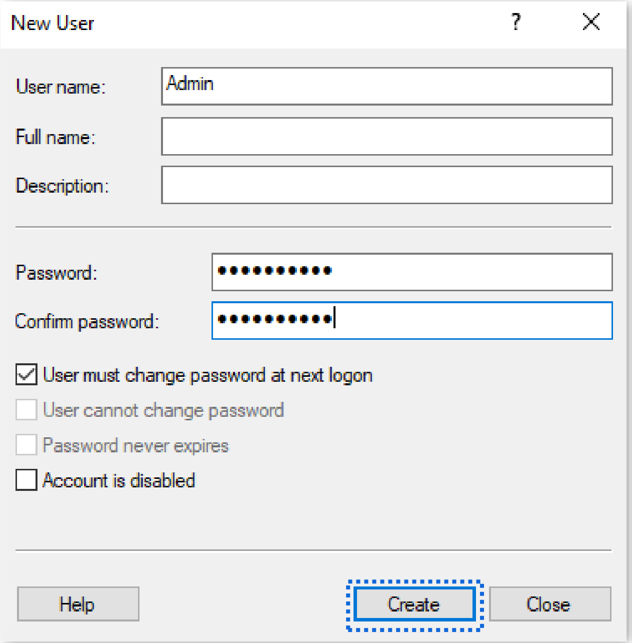
Configuration Details

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**.



User name: Admin

Full name:

Description:

Password: ••••••••••

Confirm password: ••••••••••

☑ User must change password at next logon

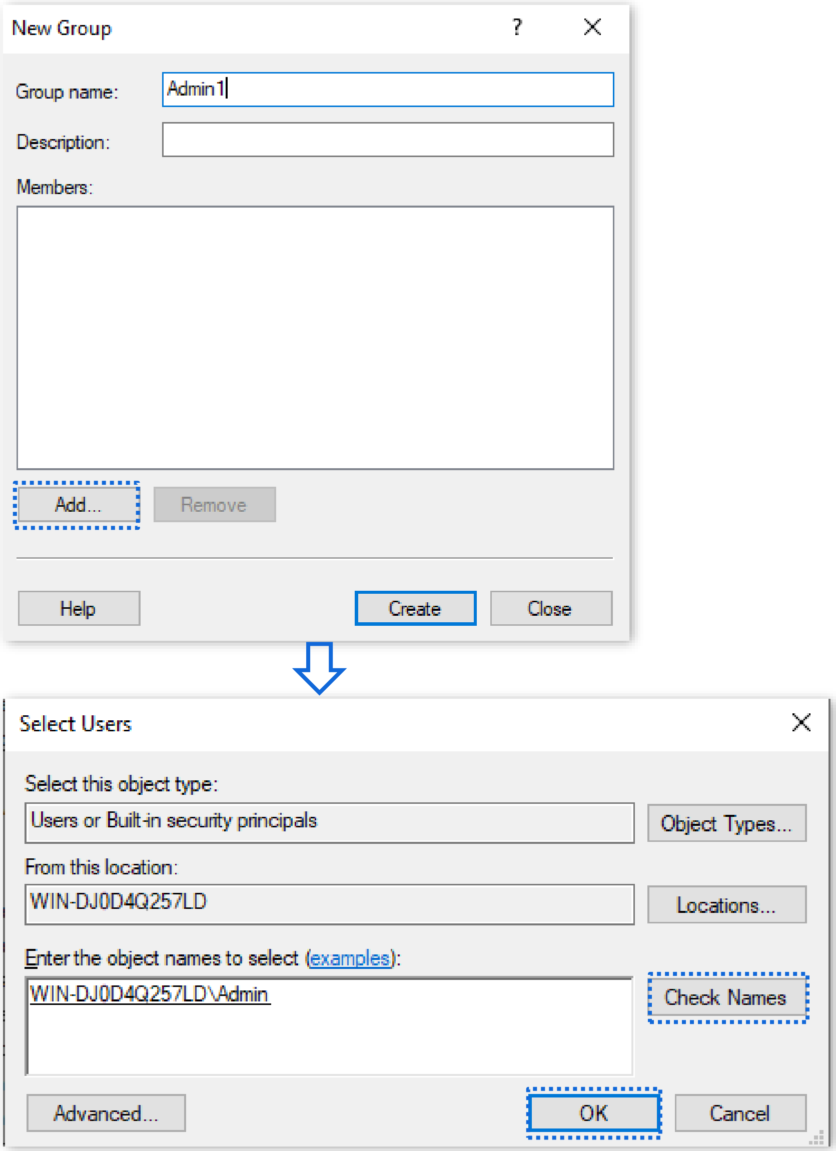
□ User cannot change password

□ Password never expires

□ Account is disabled

   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**.


New Group

Group name: Admin1

Description:

Members:

Select Users

Select this object type:
Users or Built-in security principals

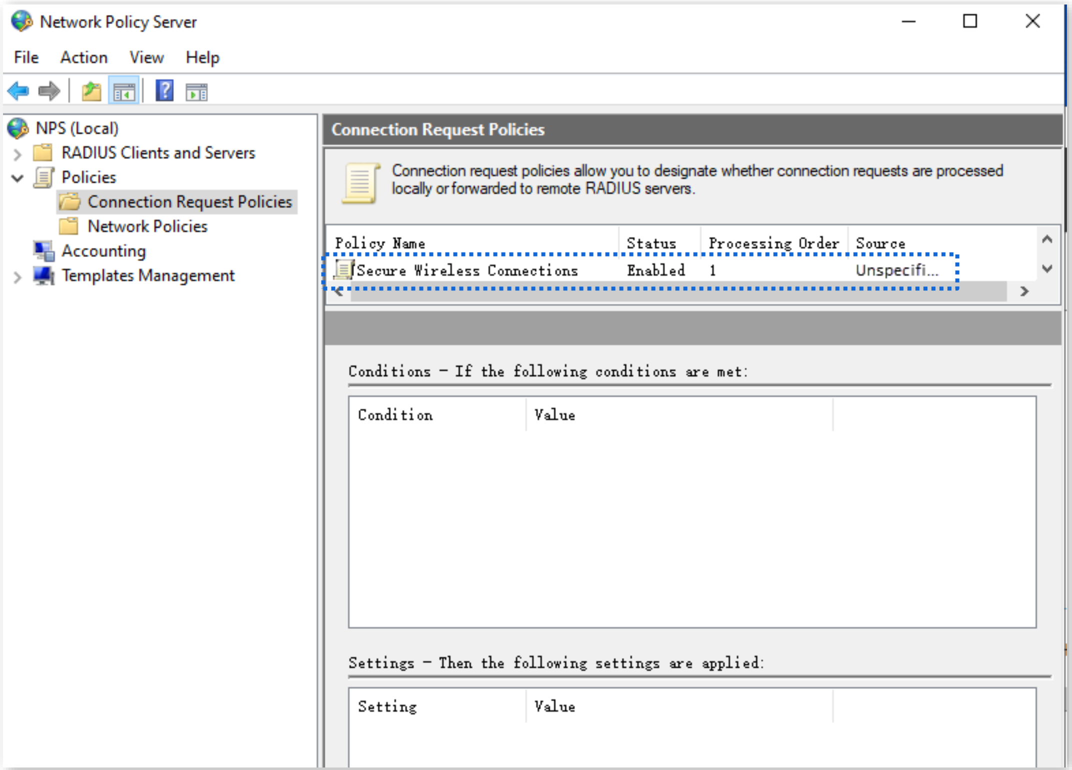
From this location:
WIN-DJ0D4Q257LD

Enter the object names to select (examples):
WIN-DJ0D4Q257LD\Admin

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**.



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

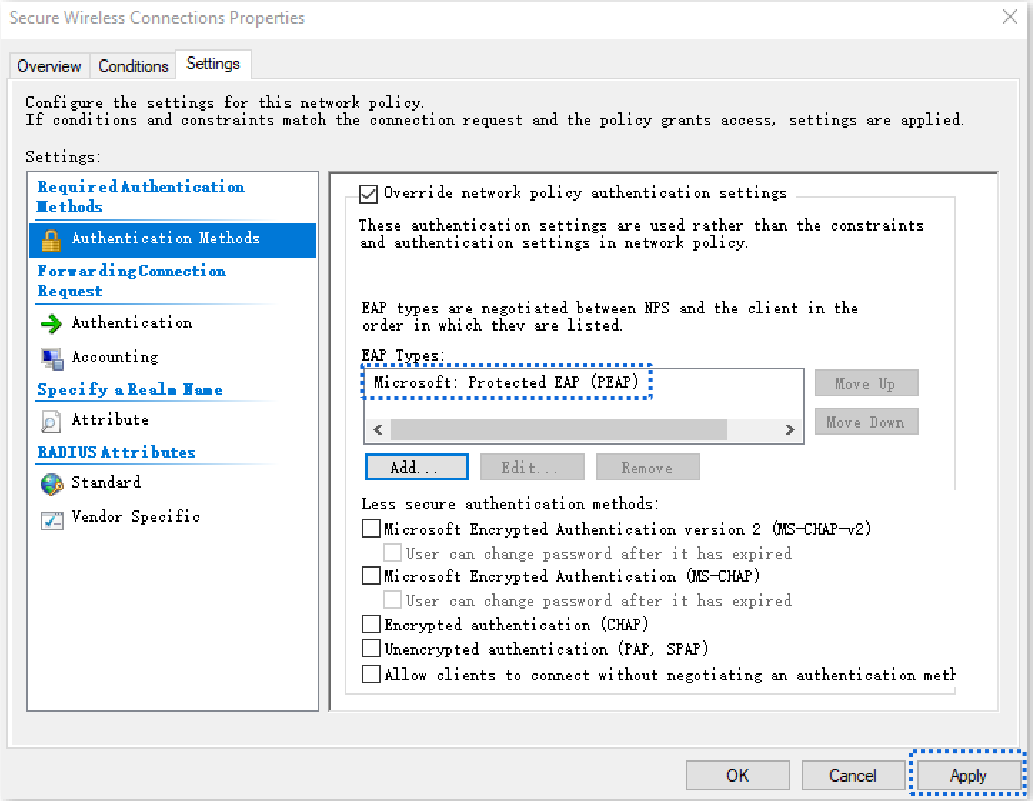
Policy Name	Status	Processing Order	Source
Secure Wireless Connections	Enabled	1	Unspecifi...

Conditions - If the following conditions are met:

Condition	Value

Settings - Then the following settings are applied:

Setting	Value



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

☑ Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy.

EAP types are negotiated between NPS and the client in the order in which they are listed.

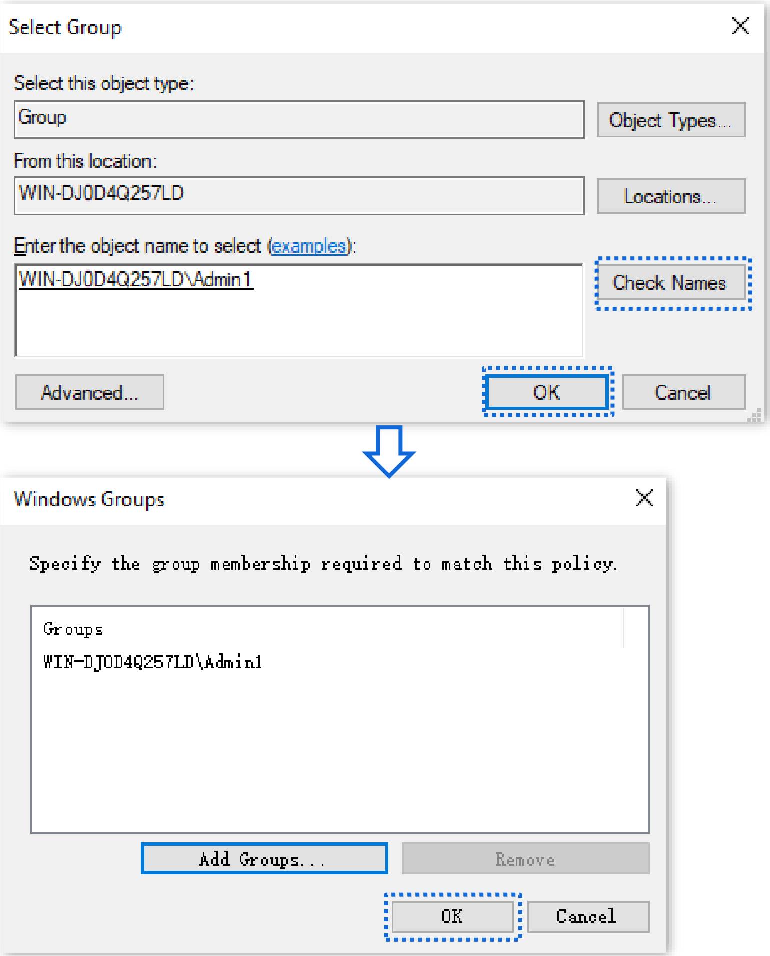
EAP Types:
Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
☐ User can change password after it has expired
☐ Microsoft Encrypted Authentication (MS-CHAP)
☐ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication meth

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**.



Select Group

Select this object type:
Group

From this location:
WIN-DJ0D4Q257LD

Enter the object name to select (examples):
WIN-DJ0D4Q257LD\Admin1

Windows Groups

Specify the group membership required to match this policy.

Groups
WIN-DJ0D4Q257LD\Admin1

----End

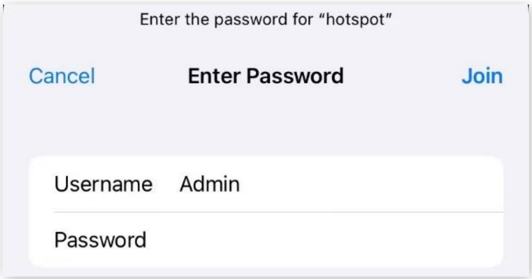
III. Configure the Wi-Fi-enabled device

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**.


Enter the password for "hotspot"

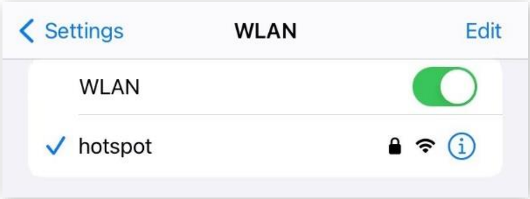
Username Admin

Password

---End

Verification

The Wi-Fi-enabled devices can connect to the wireless network named **hotspot**.



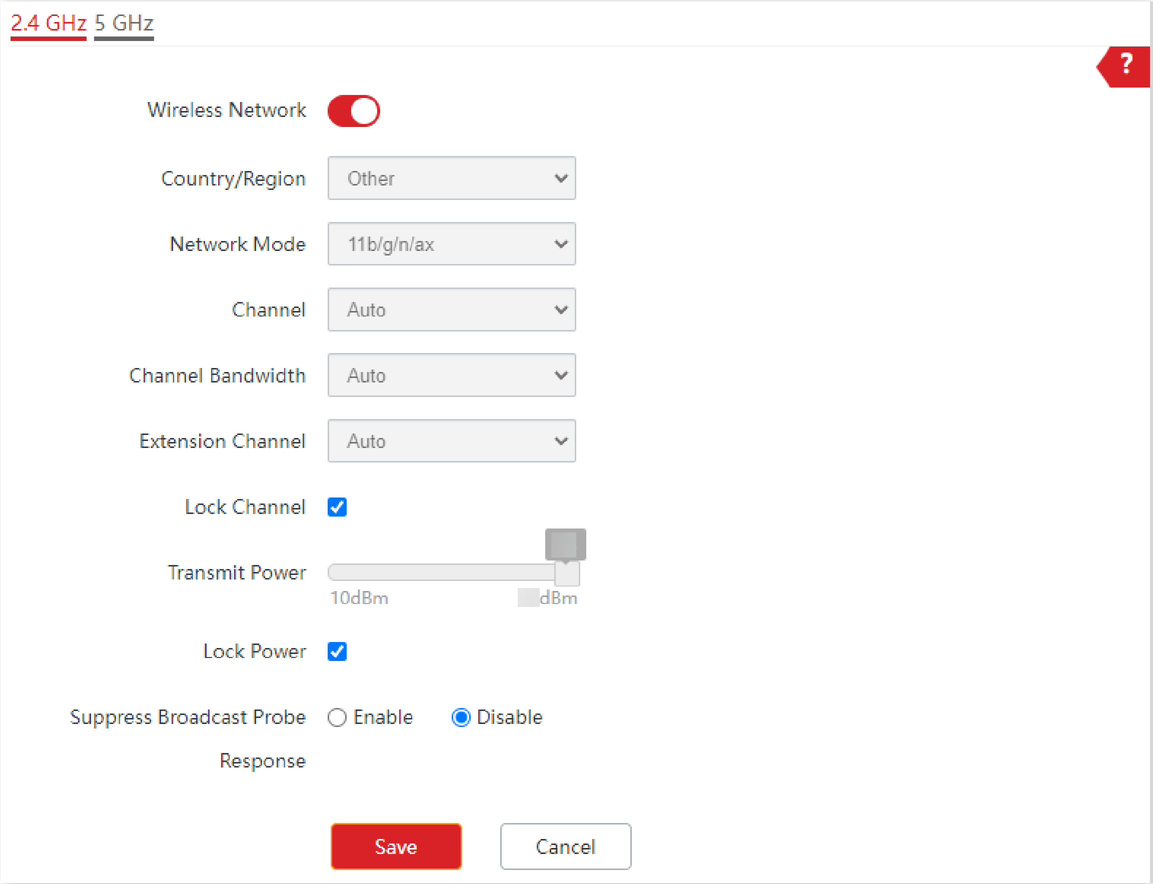
Tip

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.

7.2 RF settings

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **RF Settings**. You can modify the basic radio parameters.



2.4 GHz 5 GHz

Wireless Network: ●

Country/Region: Other

Network Mode: 11b/g/n/ax

Channel: Auto

Channel Bandwidth: Auto

Extension Channel: Auto

Lock Channel: ☑

Transmit Power: 10dBm dBm

Lock Power: ☑

Suppress Broadcast Probe Response: ○ Enable ● Disable

Parameter description

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

Parameter	Description
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**. – **11b**: The AP works in 802.11b mode and only Wi-Fi-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 Wi-Fi-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 Wi-Fi-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. Wi-Fi-enabled devices compliant with 802.11b or 802.11g and Wi-Fi-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. Wi-Fi-enabled devices compliant with 802.11b, or 802.11g and Wi-Fi-enabled devices working at 2.4 GHz and compliant with 802.11n or 802.11ax can connect to the 2.4 GHz wireless networks of the AP. Available options for 5 GHz are **11a**, **11ac**, **11a/n**, and **11a/n/ac/ax**. – **11a**: The AP works in 802.11a mode and only Wi-Fi-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 Wi-Fi-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 Wi-Fi-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. Wi-Fi-enabled devices compliant with 802.11a, or 802.11ac and Wi-Fi-enabled 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** indicates that the AP automatically adjusts its operating channel according to the ambient environment. If you frequently experience disconnections, lag, or slow speeds when connected to the AP's wireless network, try changing the AP's channel. You can use the frequency analysis function to detect channels in your vicinity that are less congested and have minimal interference.
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. – **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. 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 the AP 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 **Expansion 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.

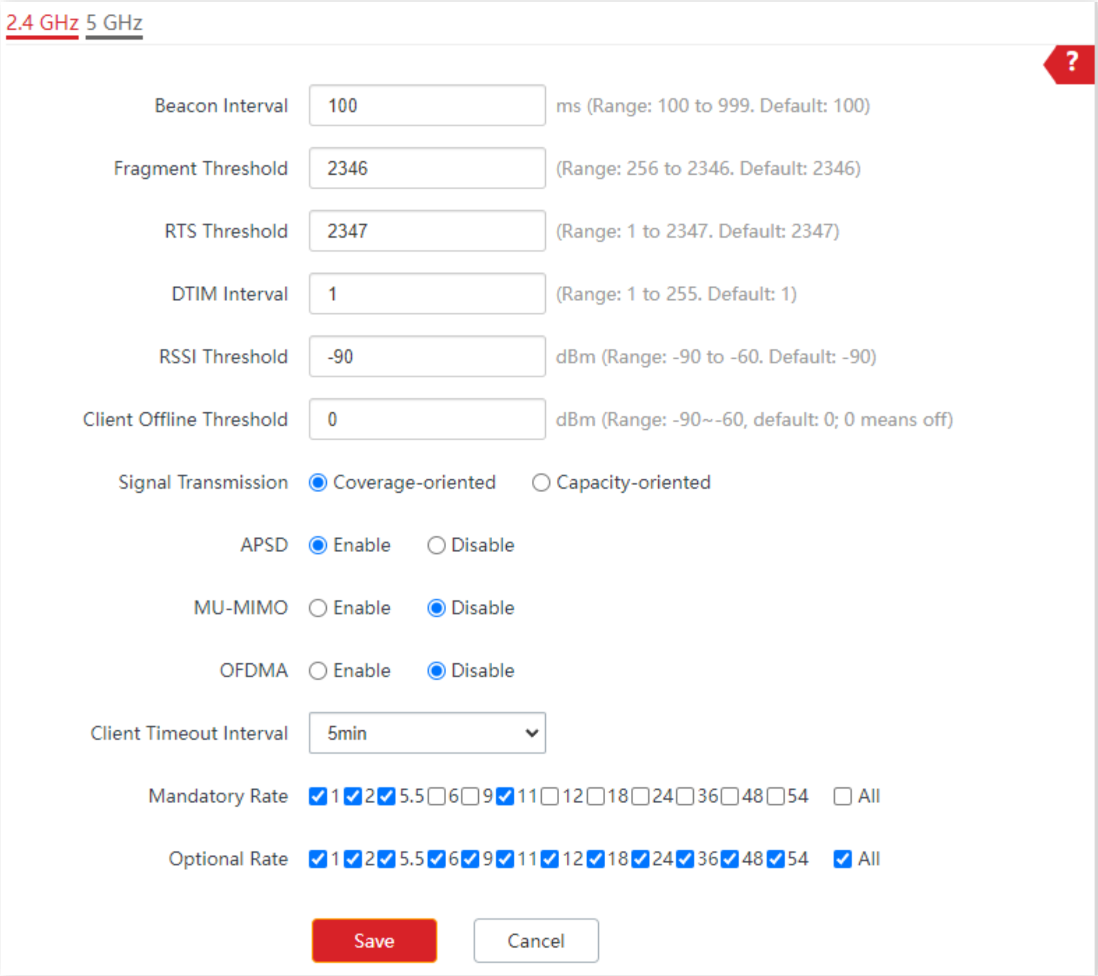
Parameter	Description
Preamble	Specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. By default, the **Long Preamble** option is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the **Short Preamble** option. Tip This function is available on some APs. The actual product prevails.
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%. Tip This function is available on some APs. The actual product prevails.
Suppress Broadcast Probe Response	Specifies whether to enable the Suppress Broadcast Probe Response function. By default, Wi-Fi-enabled devices keep sending Probe Request packets that include the SSID field to scan their nearby wireless networks. After receiving such packets, this device determines whether the Wi-Fi-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 AP does not respond to the requests without an SSID, saving wireless resources.

7.3 RF optimization

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **RF Optimization**. You can modify the radio parameters to optimize performance.

Note

Retain default settings unless professionally guided, to avoid degrading the AP’s radio performance.



Beacon Interval	100 ms (Range: 100 to 999. Default: 100)
Fragment Threshold	2346 (Range: 256 to 2346. Default: 2346)
RTS Threshold	2347 (Range: 1 to 2347. Default: 2347)
DTIM Interval	1 (Range: 1 to 255. Default: 1)
RSSI Threshold	-90 dBm (Range: -90 to -60. Default: -90)
Client Offline Threshold	0 dBm (Range: -90~-60, default: 0; 0 means off)
Signal Transmission	● Coverage-oriented ○ Capacity-oriented
APSD	● Enable ○ Disable
MU-MIMO	○ Enable ● Disable
OFDMA	○ Enable ● Disable
Client Timeout Interval	5min
Mandatory Rate	☑1 ☑2 ☑5.5 □6 □9 ☑11 □12 □18 □24 □36 □48 □54 □ All
Optional Rate	☑1 ☑2 ☑5.5 ☑6 ☑9 ☑11 ☑12 ☑18 ☑24 ☑36 ☑48 ☑54 ☑ All

Parameter description

Parameter	Description
2.4 GHz	Used to select the radio band of the AP to be configured.
5 GHz	
Beacon Interval	Used to set the interval at which this AP 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 AP sooner, while a larger interval allows the wireless network to transmit data quicker.

Parameter	Description
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 AP transmits all cached frames at one Beacon interval.
RSSI Threshold	Specifies the minimum strength of received signals acceptable to this AP. If the strength of the signals transmitted by a Wi-Fi-enabled device is weaker than this threshold, the Wi-Fi-enabled device cannot connect to this AP. A proper value facilitates Wi-Fi-enabled devices to connect to the AP with stronger signal in case of multiple APs exist.
Client Offline Threshold	Specifies the wireless client will be disconnected by the AP when the signal strength of the wireless client access is lower than the set threshold.
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.

Parameter	Description
Signal Reception	Select the option based on your actual situation. – **Default**: AP automatically adjusts the deployment mode based on the surrounding environment. – **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.
Prioritize 5 GHz	Specifies whether to enable the prioritize 5 GHz function. If this function is enabled, dual band Wi-Fi-enabled devices prefer the 5 GHz wireless network of the AP to connect when the 5 GHz signal strength transmitted by devices is stronger than the **Prioritize 5 GHz Threshold**.
Prioritize 5 GHz Threshold	With the prioritize 5 GHz function enabled, if the strength of the signals transmitted by a Wi-Fi-enabled device is stronger than this threshold, the Wi-Fi-enabled device connects to the 5 GHz wireless network. Otherwise, it connects to the 2.4 GHz wireless network.
Air Interface Scheduling	Specifies whether to enable the air interface scheduling function. 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.
MU-MIMO	Specifies whether to enable the Multi-User Multiple-Input Multiple-Output function. If this function is enabled, AP can communicate with multiple users concurrently, avoiding wireless network congestion and improving communication.

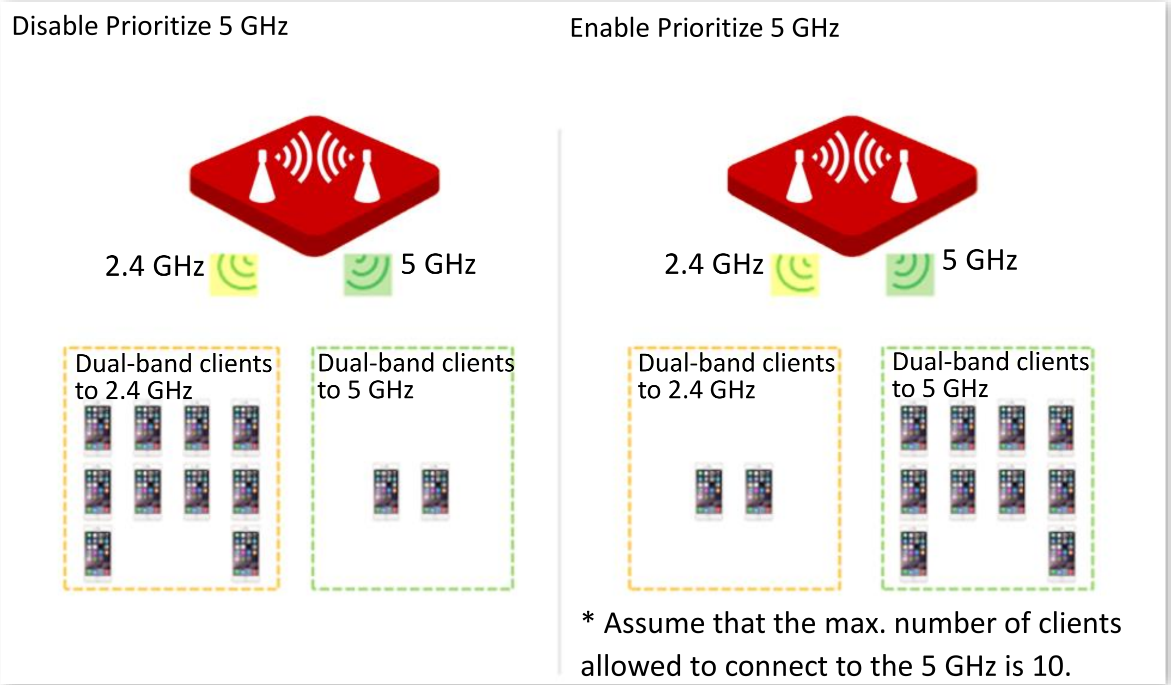
Parameter	Description
OFDMA	Orthogonal Frequency Division Multiple Access. If this function is enabled, multiple clients can transmit data at the same time, so that the transmission efficiency is improved, delay is reduced, and user experience is enhanced.
Client Timeout Interval	Used to set the wireless client disconnection interval of this AP. The AP 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 AP.
Optional Rate	Specifies the additional rates that the AP supports, which are optional to wireless clients. The clients meeting the basic requirement can connect to the AP with higher rate.

- **Prioritize 5 GHz**

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

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

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


Disable Prioritize 5 GHz
Enable Prioritize 5 GHz
2.4 GHz
5 GHz
2.4 GHz
5 GHz
Dual-band clients to 2.4 GHz
Dual-band clients to 5 GHz
Dual-band clients to 2.4 GHz
Dual-band clients to 5 GHz
* Assume that the max. number of clients allowed to connect to the 5 GHz is 10.

Note

The prioritize 5 GHz function takes effect only on the condition that 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.

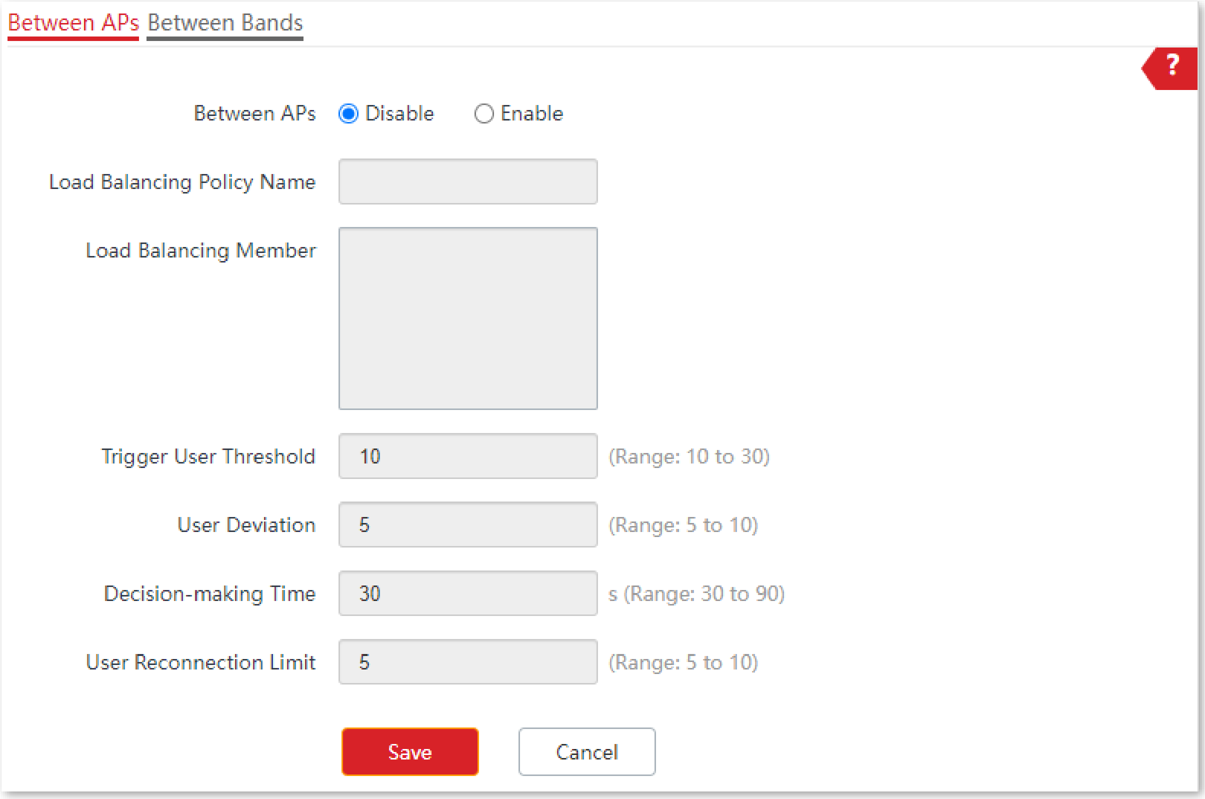
  The air interface scheduling function evenly allocates downlink transmission time to clients so that clients with high transmission rate could transmit more data, improving the throughput of each AP and number of clients allowed to be connected.

7.4 Load balancing

7.4.1 Load balancing between APs

In an actual wireless network environment, especially in high-density scenarios, it often happens that too many users connect to a certain AP. As a result, some APs are overloaded while others are idle. The load balancing between APs function can accurately balance the load among these APs. In this way, the utilization of network resources can be maximized and the utilization rate of system resources can be effectively improved.

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Load Balancing** > **Between APs**. You can view or configure the parameters of load balancing between APs.



Between APs ● Disable ○ Enable

Load Balancing Policy Name

Load Balancing Member

Trigger User Threshold 10 (Range: 10 to 30)

User Deviation 5 (Range: 5 to 10)

Decision-making Time 30 s (Range: 30 to 90)

User Reconnection Limit 5 (Range: 5 to 10)

Parameter description

Parameter	Description
Between APs	Specifies whether to enable the load balancing between APs function.

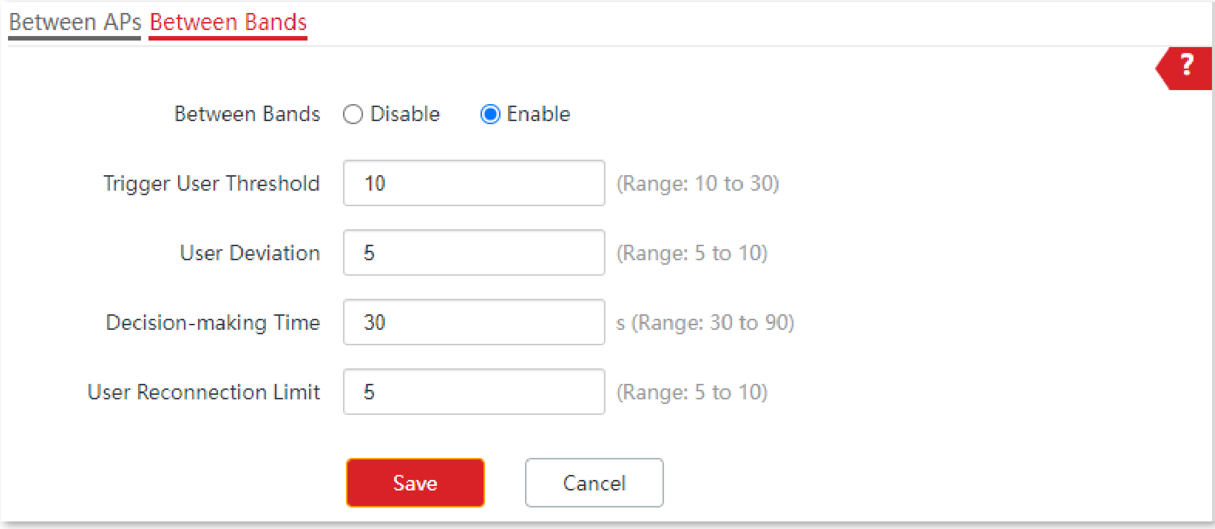
Parameter	Description
Load Balancing Policy Name	Specifies the load balancing policy between APs applied by AP. It supports load balancing based on user number. The policy can be delivered to the AP from the controller (a device with AP management and load balancing functions) or you can configure it through the AP's Web UI. Tip – The load balancing policy takes effect only when APs use the same load balancing policy name and have identical SSIDs and wireless passwords. – If there is no controller in the LAN where the AP is deployed, APs using the same load balancing policy name will automatically form a load balancing group.
Load Balancing Member	Specifies the APs added in the load balancing policy.
Trigger User Threshold	Specifies the threshold to trigger load balancing between APs. When users connected to an AP reaches the threshold, load balancing between APs is triggered.
User Deviation	Specifies the deviation between the number of users of two APs. If deviation between the user numbers of two APs applying the same load balancing policy exceeds this value, new users are directed to the AP with fewer users first.
Decision-making Time	Specifies the time period in which AP refuses user connection request. It is recommended to keep the default settings. If within this time period, the number of AP refusals has reached the **User Reconnection Limit**, AP allows access from this user. If within this time period, the number of AP refusals does not reach **User Reconnection Limit**, the number of refusals is erased.
User Reconnection Limit	Specifies the largest number of user connection attempts. If the number of AP refusals has reached this value in **Decision-making Time**, AP allows access from this user. It is recommended to keep the default settings.

7.4.2 Load balancing between bands

The AP supports wireless networks with two frequency bands, 2.4 GHz and 5 GHz. Some clients in the network only support the 2.4 GHz radio band while some support dual-band. And generally, when dual-band clients access the wireless network, the 2.4 GHz radio band is selected by default. Therefore, the 2.4 GHz radio band may be overloaded while the 5GHz radio band may be relatively idle. To prevent the above situation, it is recommended to enable the load balancing between bands function to balance the load between the radio bands of the AP and improve user's internet experience.

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Load Balancing** > **Between Bands**. You can view or configure the parameters of load balancing between bands.

This function is disabled by default. The following figure displays the page when **Between Bands** is enabled.



Between Bands ○ Disable ● Enable

Trigger User Threshold 10 (Range: 10 to 30)

User Deviation 5 (Range: 5 to 10)

Decision-making Time 30 s (Range: 30 to 90)

User Reconnection Limit 5 (Range: 5 to 10)

Parameter description

Parameter	Description
Between Bands	Specifies whether to enable the load balancing between bands function.
Trigger User Threshold	Specifies the threshold to trigger load balancing between bands. When users connected to the AP reach the threshold, load balancing between bands is triggered.
User Deviation	Specifies the deviation between the number of users connected to two bands. If the deviation exceeds this value, new users are directed to the band with fewer users first.
Decision-making Time	Specifies the time period in which AP refuses user connection request. It is recommended to keep the default settings. If within this time period, the number of AP refusals has reached the **User Reconnection Limit**, AP allows access from this user. If within this time period, the number of AP refusals does not reach **User Reconnection Limit**, the number of refusals is erased.

Parameter	Description
User Reconnection Limit	Specifies the largest number of user connection attempts. If the number of AP refusals has reached this value in **Decision-making Time**, AP allows access from this user. It is recommended to keep the default settings.

7.5 Frequency analysis

7.5.1 Overview

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Frequency Analysis**. You can analyze frequency and scan channels.

- **Frequency analysis**

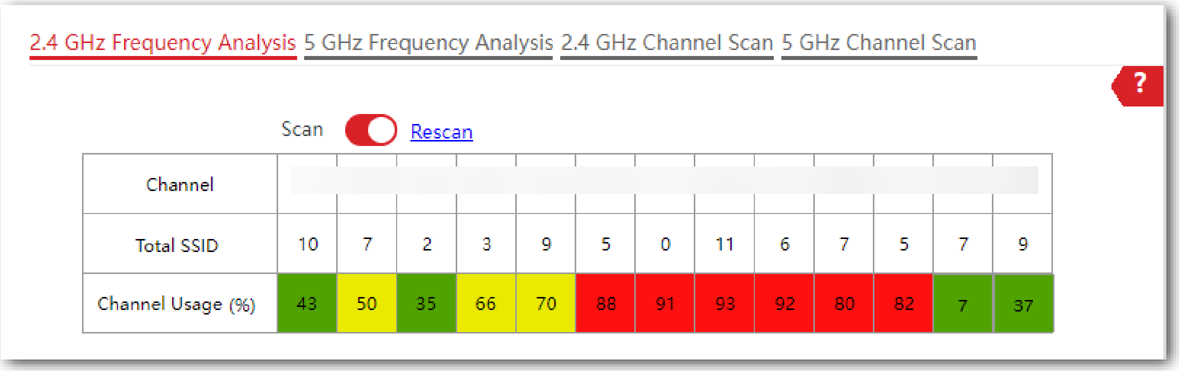
  From the intuitive result, you can check how many wireless networks (total SSIDs) use the same channel and choose a channel with low usage as the operating channel of the device for better wireless transmission efficiency.

- **Channel scan**

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

7.5.2 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**.



Channel													
Total SSID	10	7	2	3	9	5	0	11	6	7	5	7	9
Channel Usage (%)	43	50	35	66	70	88	91	93	92	80	82	7	37

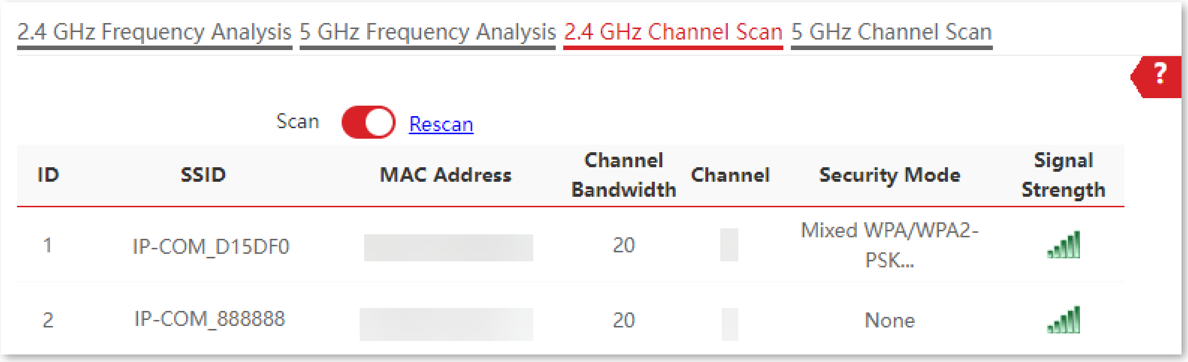
---End

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.

7.5.3 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**.



ID	SSID	MAC Address	Channel Bandwidth	Channel	Security Mode	Signal Strength
1	IP-COM_D15DF0		20		Mixed WPA/WPA2-PSK...	📶
2	IP-COM_888888		20		None	📶

---End

7.6 WMM settings

Tip

iUAP-AC-M V2.0 is used for illustration here.

7.6.1 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.

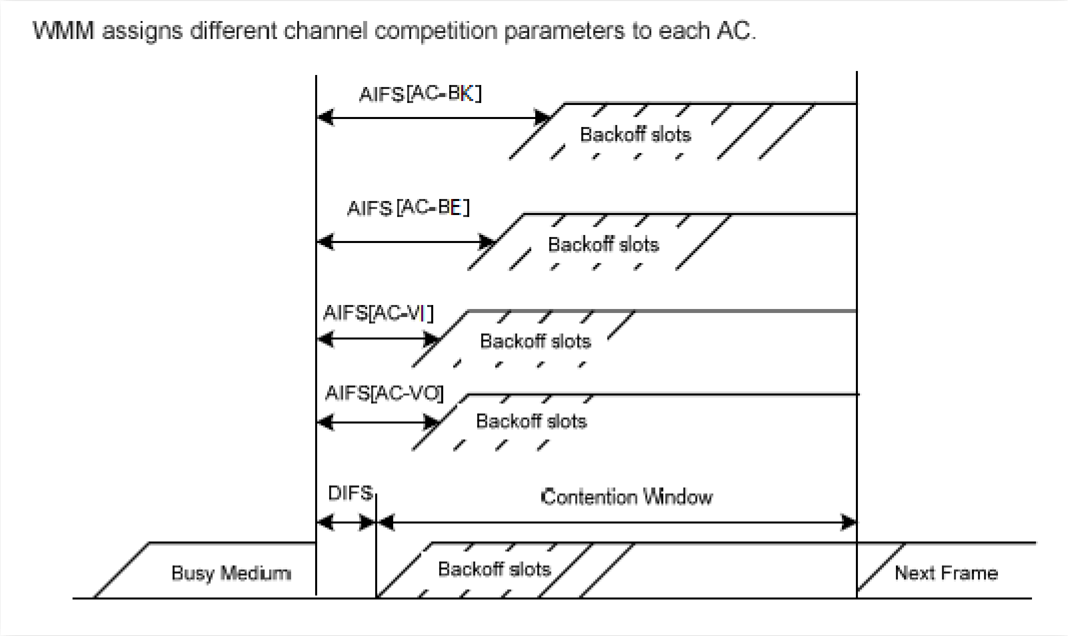
According to the 802.11 protocol family, all devices listen on a channel before using the channel to send data. If the channel stays idle for or longer than a specified period, the devices wait a random backoff period within the contention window. The device whose backoff period expires first can use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

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

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



WMM assigns different channel competition parameters to each AC.

- **ACK policies**

  WMM specifies the Normal ACK and No ACK policies.

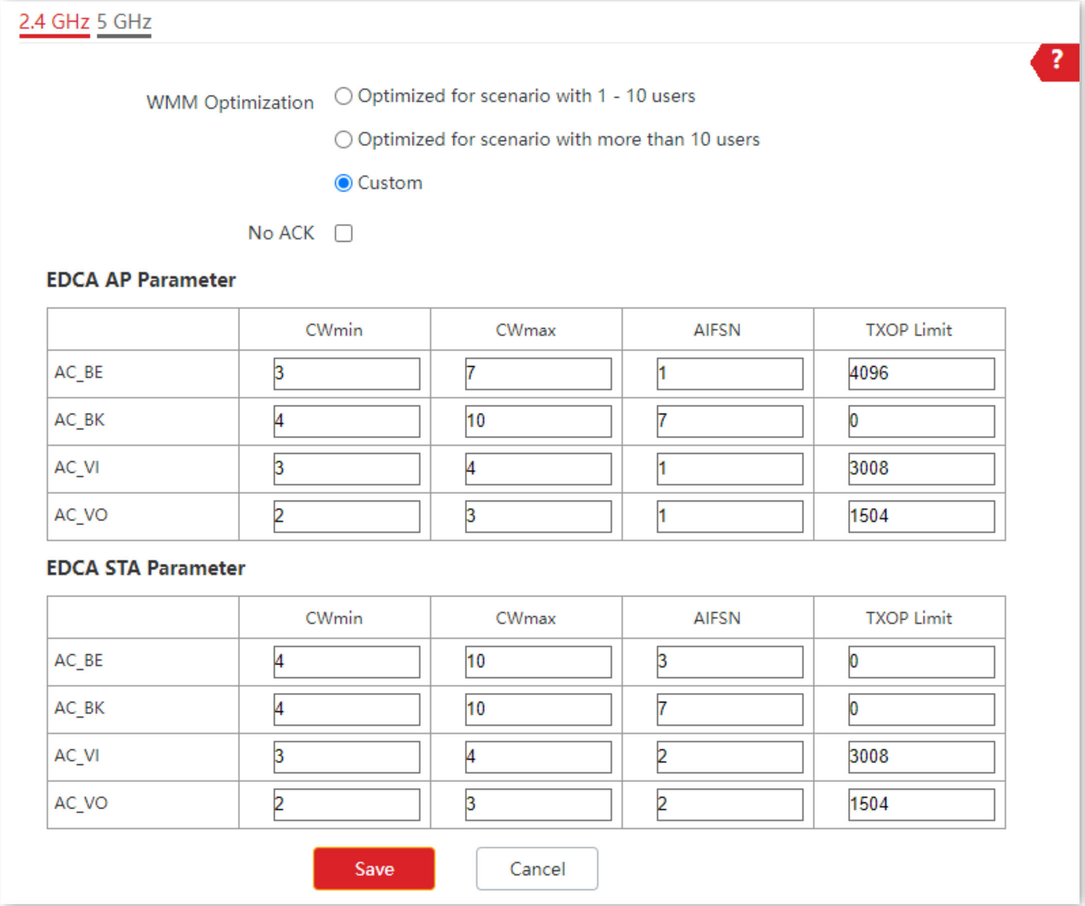
  - According to the No Acknowledgment (No ACK) policy, no ACK packet is used during wireless packet transmission to acknowledge packet reception. This policy is applicable to scenarios where interference is mild and can effectively improve transmission efficiency.

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.

7.6.2 Configure WMM

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **WMM**. You can configure related WMM parameters.



WMM Optimization ○ Optimized for scenario with 1 - 10 users
○ Optimized for scenario with more than 10 users
● Custom

No ACK □

EDCA AP Parameter

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	3	7	1	4096
AC_BK	4	10	7	0
AC_VI	3	4	1	3008
AC_VO	2	3	1	1504

EDCA STA Parameter

	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	4	10	3	0
AC_BK	4	10	7	0
AC_VI	3	4	2	3008
AC_VO	2	3	2	1504

Parameter description

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

Parameter	Description
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.
No ACK	Available 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 helps improve 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	For details, refer to EDCA parameters.
EDCA STA Parameter	

7.7 Access control

7.7.1 Overview

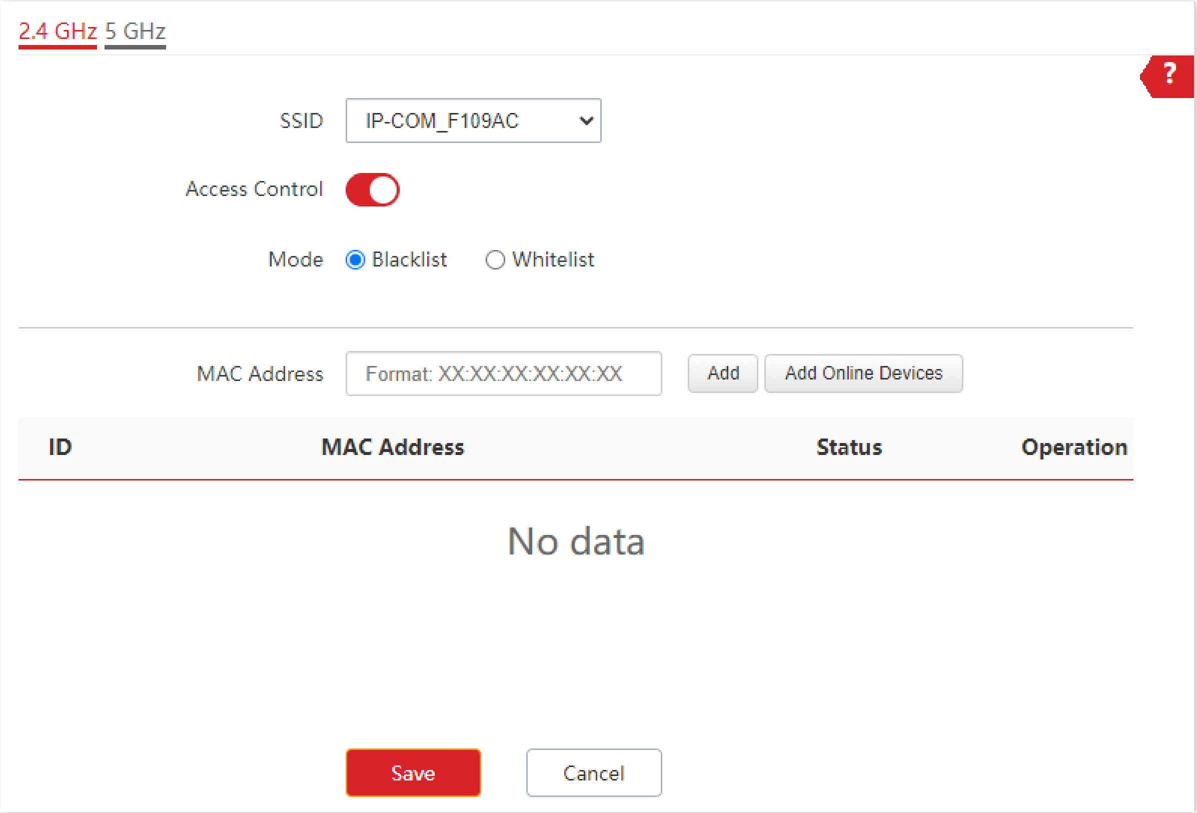
To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Access Control**. You can allow or disallow the Wi-Fi-enabled devices to access the wireless network of the AP based on their MAC addresses.

The AP supports the following 2 filter modes:

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

- **Whitelist**: It indicates that only the Wi-Fi-enabled devices with the specified MAC addresses can 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.



SSID: IP-COM_F109AC

Access Control: on

Mode: ● Blacklist ○ Whitelist

MAC Address: Format: XX:XX:XX:XX:XX:XX

ID	MAC Address	Status	Operation

No data

Parameter description

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

Parameter	Description
MAC Address	Specifies the MAC address of 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 rule. You can enable or disable it as required.

7.7.2 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 is to be implemented.
3. Select the SSID to which the access control is applied from the **SSID** drop-down list menu.
4. Enable the **Access Control** function.
5. Set **Mode** to **Blacklist** or **Whitelist** as required.
6. Enter the MAC addresses of the Wi-Fi-enabled devices to which the rule applies. Then click **Add**.

Tip

If the Wi-Fi-enabled 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

7.7.3 Example of configuring access control

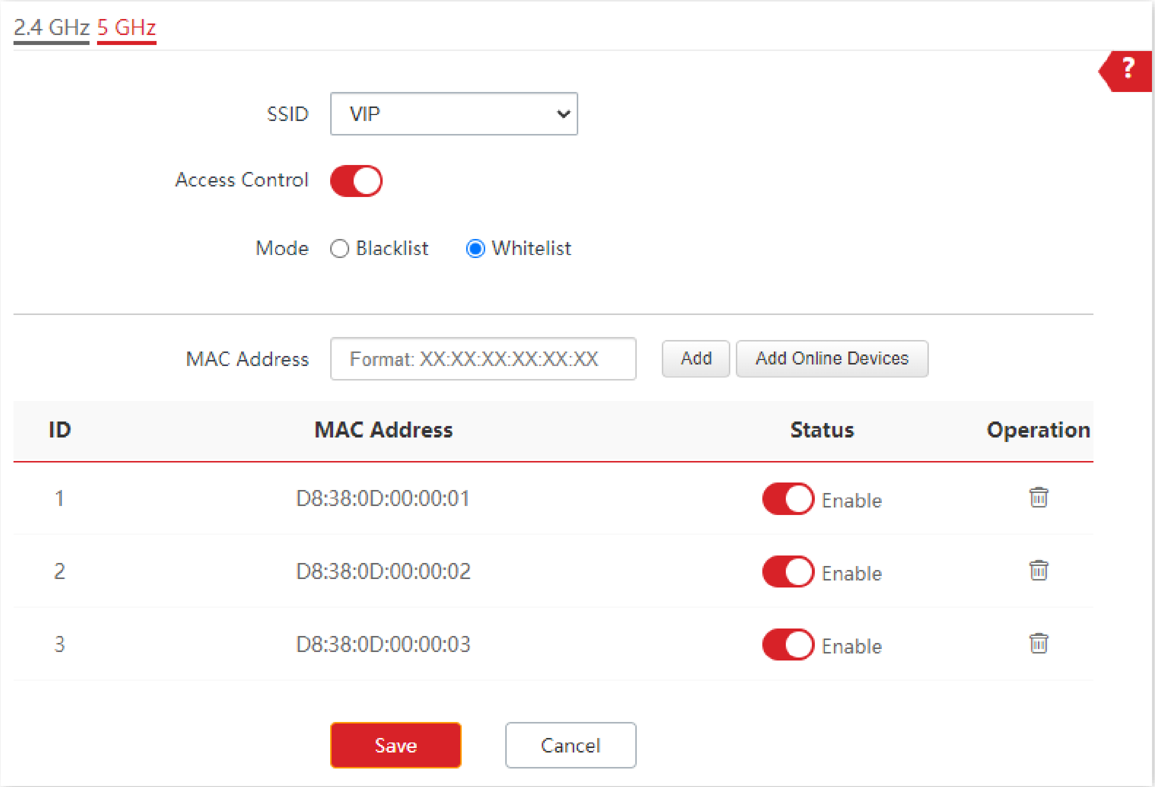
Networking requirements

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

The access control function of the AP is recommended. The members have three Wi-Fi-enabled devices whose MAC addresses are **D8:38:0D:00:00:01**, **D8:38:0D:00:00:02**, and **D8:38:0D:00:00:03**.

Configuration procedure

1. 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 **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 the step to add **D8:38:0D:00:00:02** and **D8:38:0D:00:00:03**.
5. Click **Save**.



SSID: VIP

Access Control: Enabled

Mode: ○ Blacklist ● Whitelist

MAC Address: Format: XX:XX:XX:XX:XX:XX

ID	MAC Address	Status	Operation
1	D8:38:0D:00:00:01	Enable	🗑
2	D8:38:0D:00:00:02	Enable	🗑
3	D8:38:0D:00:00:03	Enable	🗑

---End

Verification

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

7.8 Advanced settings

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Advanced Settings**. You can set the client type identification, broadcast and multicast packet control, and virtual controller of the AP.

- **Identify client type**

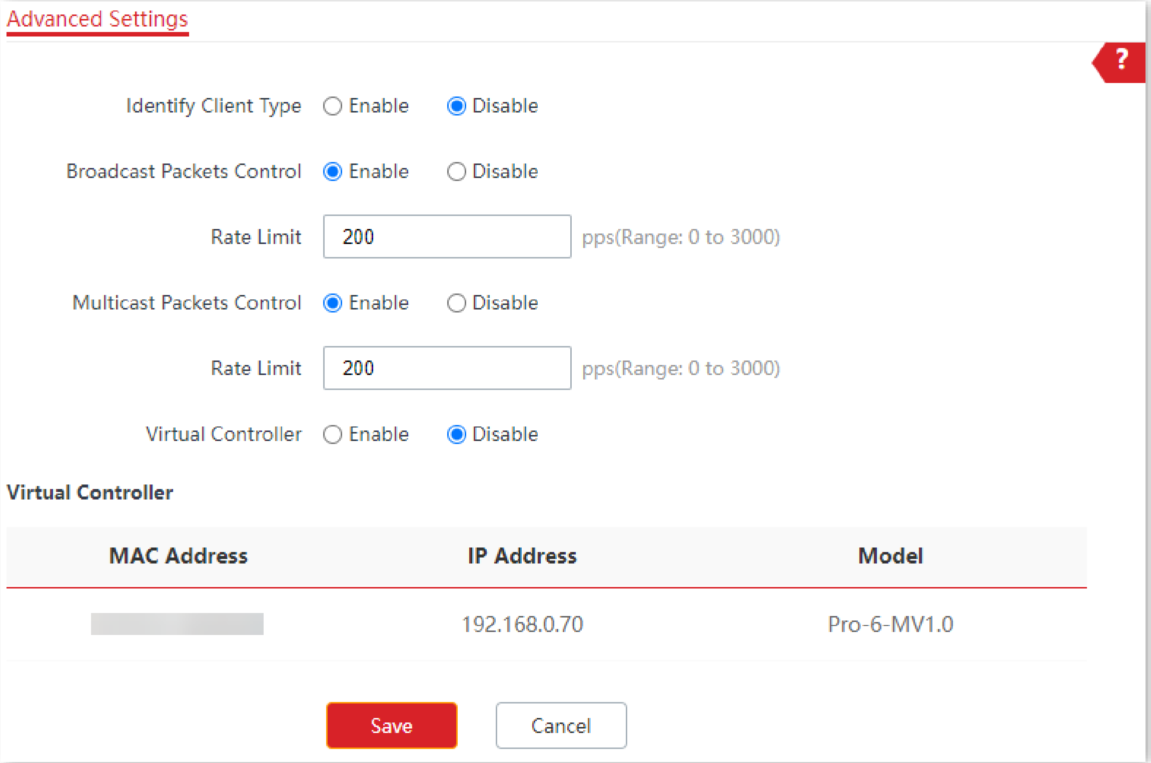
  It specifies whether to identify operating system types of wireless clients connected to this AP. Client types that the AP can identify include: Android, iOS, WPhone, Windows, Mac OS and HarmonyOS.

- **Broadcast and multicast packet control**

  By limiting the transmission rate of broadcast or multicast packets, channel congestion caused by non-essential broadcasts is prevented. This reduces air interface resources usage, minimizes interference, enhances transmission efficiency, and improves the user experience.

- **Virtual controller**

  In an AC-less network environment, you can configure one AP as a virtual wireless controller to automatically discover and manage other APs with the same SSID, ensuring seamless roaming stability. Only one virtual controller can be configured within the same local area network.



Advanced Settings

Identify Client Type ○ Enable ● Disable

Broadcast Packets Control ● Enable ○ Disable

Rate Limit 200 pps(Range: 0 to 3000)

Multicast Packets Control ● Enable ○ Disable

Rate Limit 200 pps(Range: 0 to 3000)

Virtual Controller ○ Enable ● Disable

Virtual Controller

MAC Address	IP Address	Model
[redacted]	192.168.0.70	Pro-6-MV1.0

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 Wi-Fi-enabled devices connected to the AP’s wireless network can be viewed by navigating to **Status** > **Client List**.
Broadcast Packets Control	Used to limit the transmission rate of broadcast packets. It is 200 pps by default. Excessive broadcast packets may cause a broadcast storm, leading to network paralysis. Configure this setting appropriately.
Rate Limit	
Multicast Packets Control	Used to limit the transmission rate of multicast packets. It is 200 pps by default. Excessive multicast traffic may degrade the overall network performance. It is recommended to enable the WMF function simultaneously.
Rate Limit	
Virtual Controller	Specifies whether to enable the virtual controller function. Tip This function can only be used in a network environment with no less than 2 APs. The primary AP information is displayed in the virtual controller list.

7.9 QVLAN settings

7.9.1 Overview

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

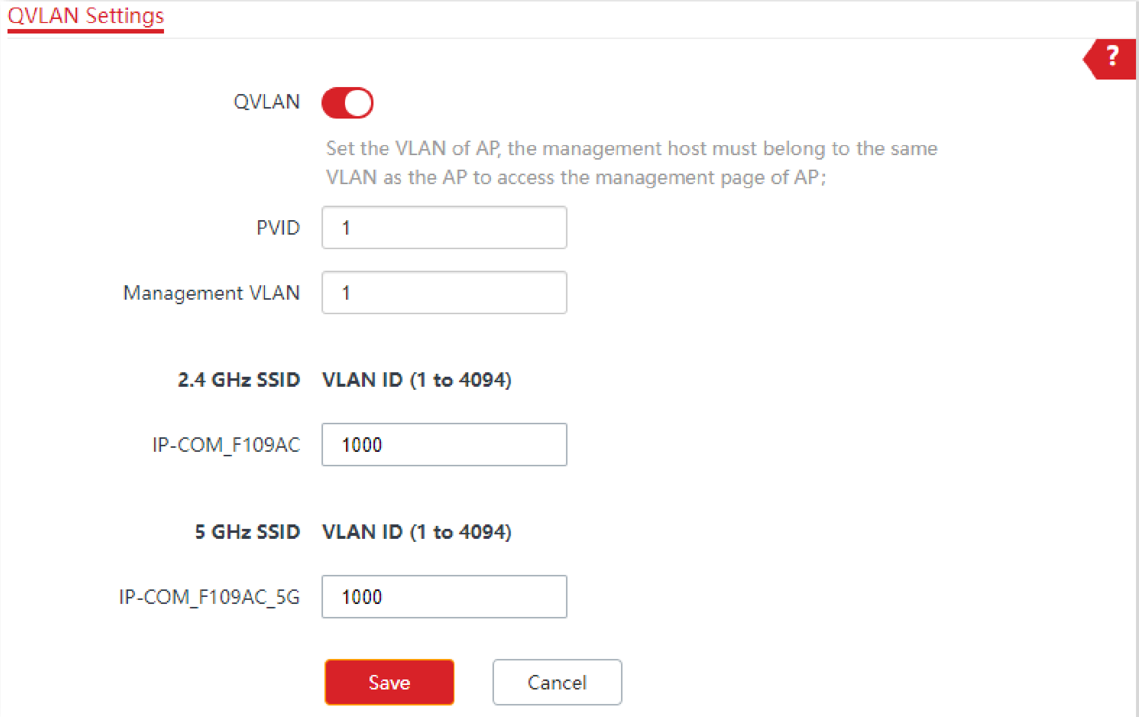
If the QVLAN function is enabled, tagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the VID in the data, whereas untagged data received by a port of the AP is forwarded to the other ports of the VLAN corresponding to the PVID of the port that receives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

You can set VLAN IDs of all wireless networks.



QVLAN Settings

QVLAN ●

Set the VLAN of AP, the management host must belong to the same VLAN as the AP to access the management page of AP;

PVID: 1

Management VLAN: 1

2.4 GHz SSID	VLAN ID (1 to 4094)
IP-COM_F109AC	1000

5 GHz SSID	VLAN ID (1 to 4094)
IP-COM_F109AC_5G	1000

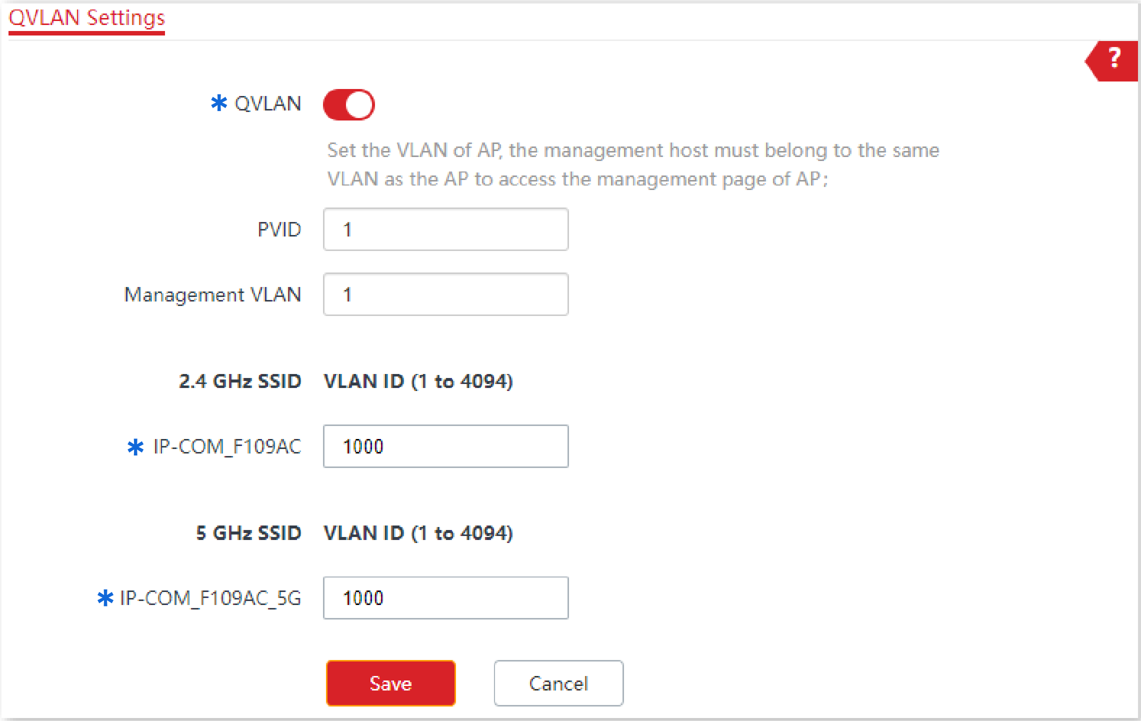
Parameter description

Parameter	Description
QVLAN	Specifies whether to enable the QVLAN function of the AP. By default, it is disabled.
PVID	Specifies the default VLAN ID of the AP's trunk port. 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
2.4 GHz SSID	Specify the currently enabled SSIDs over the 2.4 GHz or 5 GHz band of the AP, and the VLAN IDs corresponding to SSIDs. Tip After the QVLAN function is enabled, the wireless ports corresponding to SSIDs function as access ports. The PVID of an access port is the same as its VLAN ID.
5 GHz SSID	
VLAN ID	

7.9.2 Configure QVLAN

1. Log in to the web UI of the AP and navigate to **Wireless** > **QVLAN Settings**.
2. Enable the **QVLAN** function.
3. Change 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**.



QVLAN Settings

* QVLAN ●

Set the VLAN of AP, the management host must belong to the same VLAN as the AP to access the management page of AP;

PVID: 1

Management VLAN: 1

2.4 GHz SSID **VLAN ID (1 to 4094)**

* IP-COM_F109AC: 1000

5 GHz SSID **VLAN ID (1 to 4094)**

* IP-COM_F109AC_5G: 1000

---End

7.9.3 Example of configuring QVLAN settings

Networking requirements

An industrial park has the following wireless network coverage requirements:

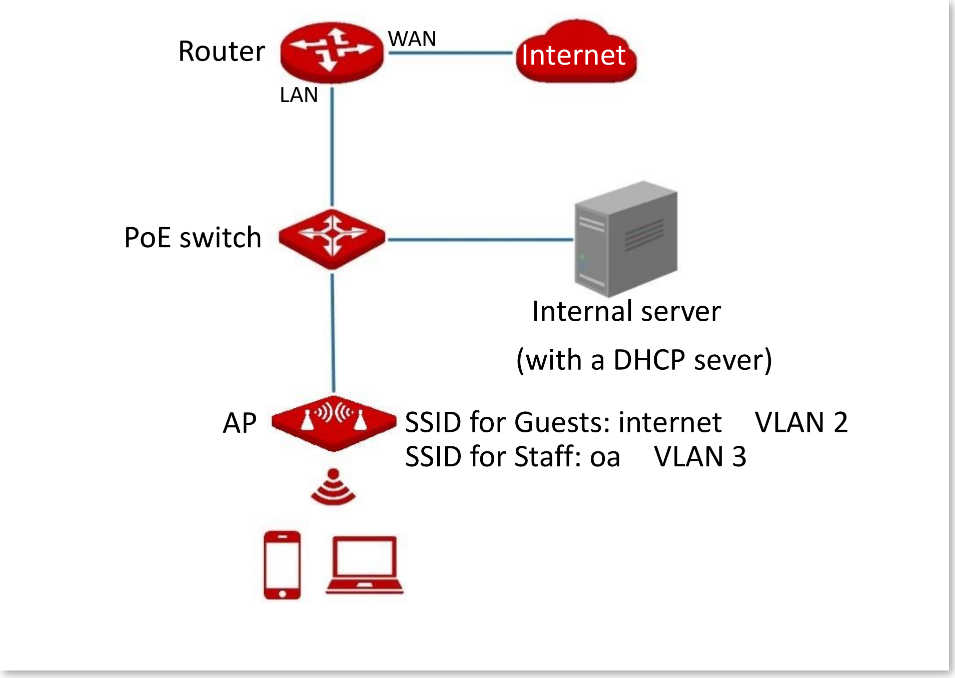
- Guests are connected to VLAN 2 and can access only the internet.
- Staffs are connected to VLAN 3 and can access only the intranet.

Solution

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

Tip

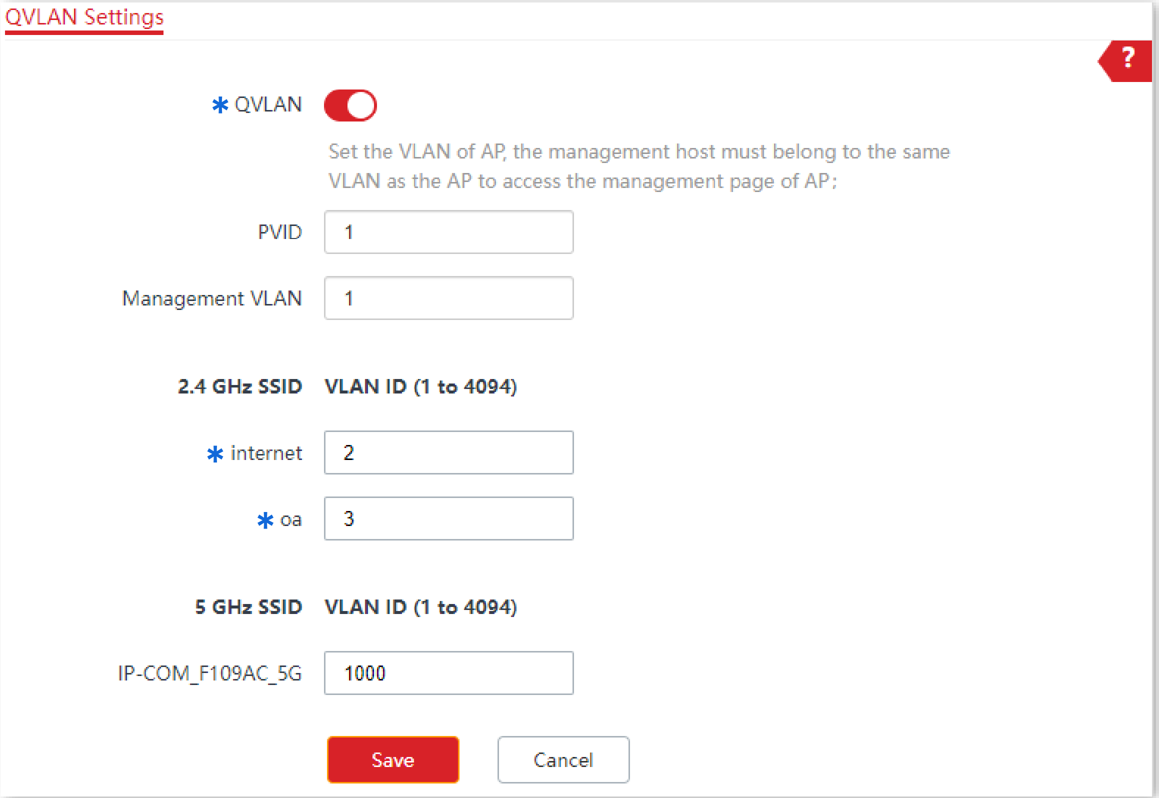
The internal server must be deployed with a DHCP server in the LAN to assign IP addresses to downlink devices.



Configuration procedure

I. Configure the AP

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 ID of **internet** to **2** and the VLAN of **oa** to **3**.
4. Click **Save**.



QVLAN Settings

✱ QVLAN ●

Set the VLAN of AP, the management host must belong to the same VLAN as the AP to access the management page of AP;

PVID: 1

Management VLAN: 1

2.4 GHz SSID **VLAN ID (1 to 4094)**

✱ internet: 2

✱ oa: 3

5 GHz SSID **VLAN ID (1 to 4094)**

IP-COM_F109AC_5G: 1000

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

7.10 Set WiFi schedule

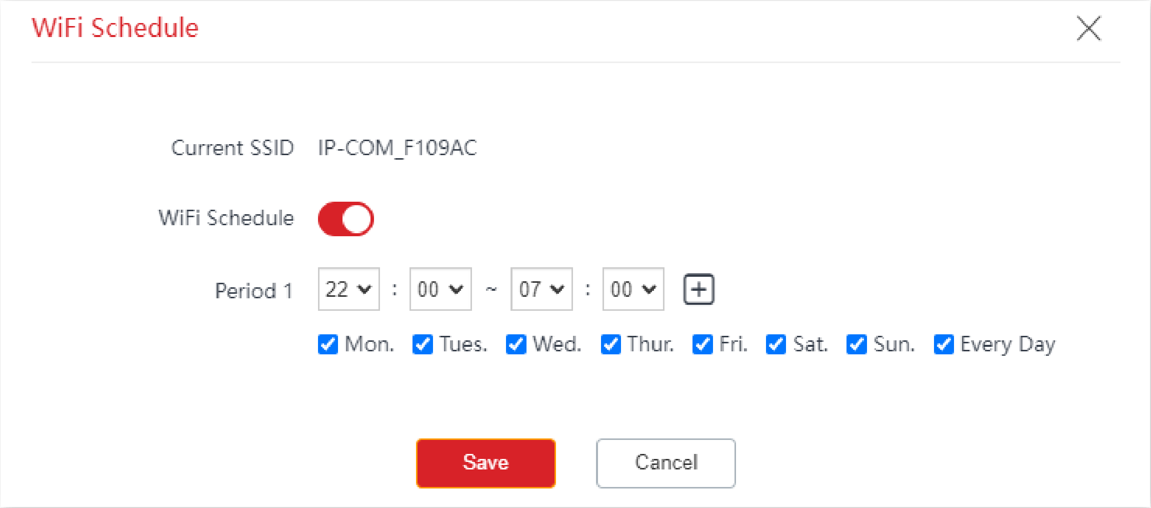
You can disable the wireless network of the AP during a specified period. During the scheduled disable period, Wi-Fi-enabled devices such as smartphones cannot search for the wireless networks.

Tip

To make the WiFi schedule work properly, ensure that the system time is correct and the SSID for which the WiFi schedule is to be set is enabled.

Configuration procedure

1. Log in to the web UI of the AP, and navigate to **Wireless** > **WiFi Schedule**.
2. Click ✎ in the line of the **SSID** to set WiFi schedule.
3. Enable **WiFi Schedule**.
4. Set the period for the wireless network to automatically disable, which are **22:00** - **07:00** and **Every Day** in this example.
5. Click **Save**.



WiFi Schedule

Current SSID IP-COM_F109AC

WiFi Schedule ●

Period 1 22 : 00 ~ 07 : 00

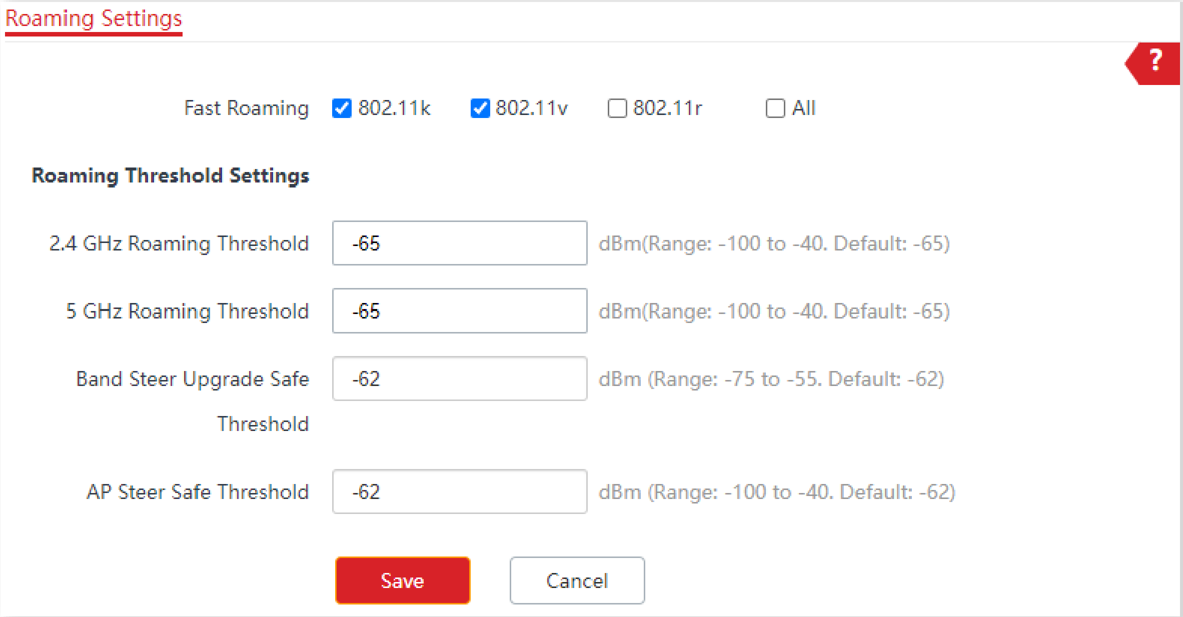
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur. ☑ Fri. ☑ Sat. ☑ Sun. ☑ Every Day

---End

After the configuration is completed, the wireless network will be disabled from 22:00 to 7:00 every day.

7.11 Roaming settings

To access the page, log in to the web UI of the AP, and navigate to **Wireless** > **Roaming Settings**. You can set roaming parameters of the AP.



Roaming Settings

Fast Roaming ☑ 802.11k ☑ 802.11v ☐ 802.11r ☐ All

Roaming Threshold Settings

2.4 GHz Roaming Threshold	-65	dBm(Range: -100 to -40. Default: -65)
5 GHz Roaming Threshold	-65	dBm(Range: -100 to -40. Default: -65)
Band Steer Upgrade Safe Threshold	-62	dBm (Range: -75 to -55. Default: -62)
AP Steer Safe Threshold	-62	dBm (Range: -100 to -40. Default: -62)

Parameter description

Parameter	Description
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	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 falls below the roaming threshold, the roaming is triggered and the AP with better link quality is switched over.
5 GHz Roaming Threshold	
Band Steer Upgrade Safe Threshold	Used to set band steer upgrade safe threshold. When a client is connected to either the 2.4 GHz or 5 GHz band of an AP, it will automatically connect to another frequency band if the received signal strength from the current band falls below the configured threshold.
AP Steer Safe Threshold	Used to set AP steer upgrade safe threshold. When connected to an AP, the client will automatically switch to the other AP with better signal if the client moves and the received signal strength falls below the configured threshold.

8 Advanced settings

8.1 Deployment mode

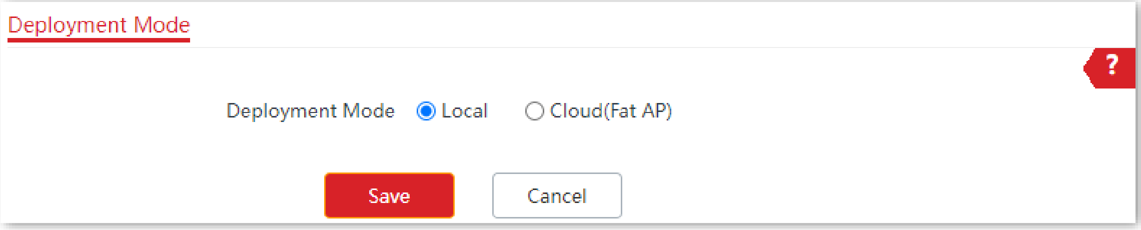
Tip

iUAP-AC-M V2.0 is used for illustration here.

8.1.1 Overview

If a large number of APs are to be deployed in a network, it is recommended that you integrate an IP-COM AC in order to achieve a unified AP management.

Unified AP management includes local deployment and cloud deployment. The default mode is local deployment mode.

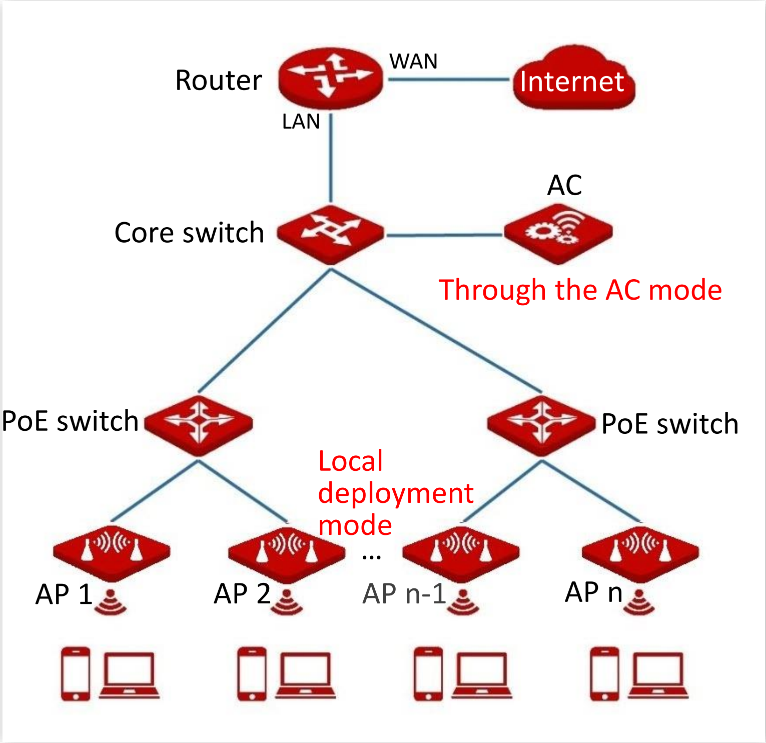


Deployment Mode

Deployment Mode ● Local ○ Cloud(Fat AP)

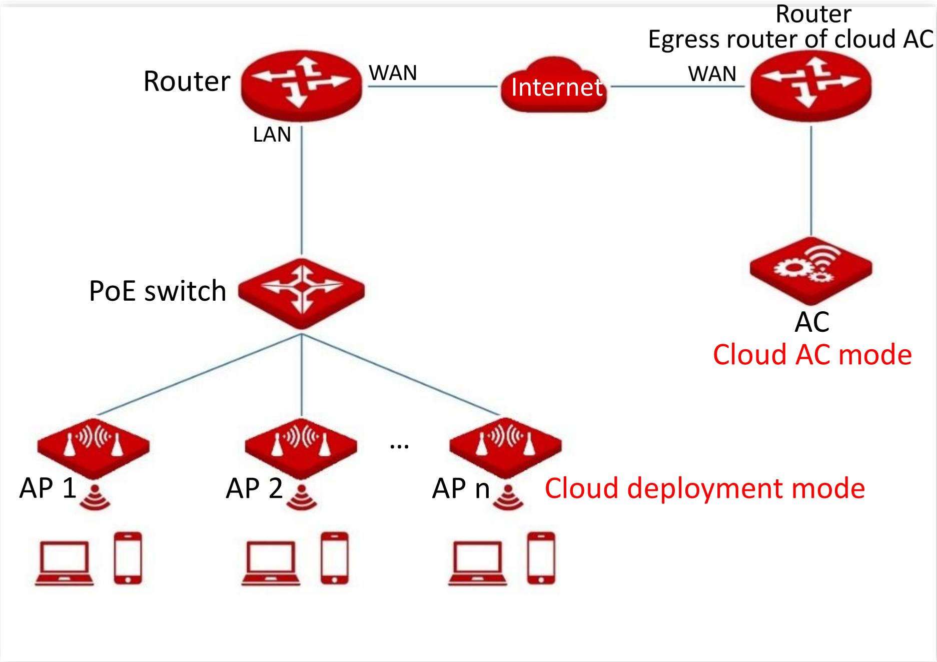
- **Local deployment**

If the network is concentrated and involves a large number of APs, it is recommended that you adopt the local deployment mode to enable unified management by AC through the AC mode. See the following topology.



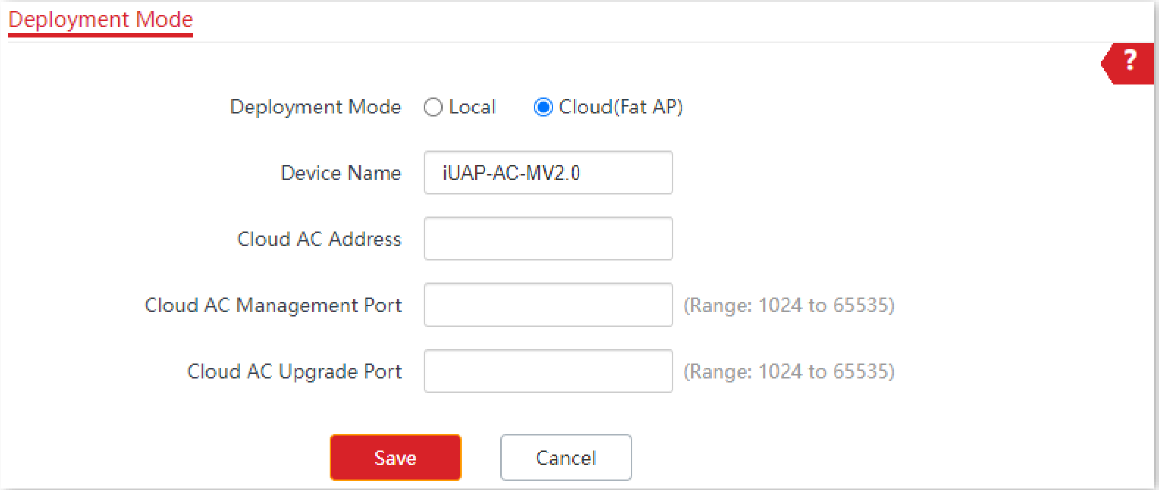
- **Cloud deployment**

  If the wireless network is dispersed and involves a large number of APs in total but these APs are scattered in small numbers, it is recommended that you adopt the cloud deployment mode in which ACs on the internet manage the scattered cloud APs in a unified manner through the cloud AC mode. See the following topology.



8.1.2 Configure deployment mode

To access the page, log in to the web UI of the AP, and navigate to **Advanced** > **Deployment Mode**. You can change the deployment mode of AP.



Deployment Mode ○ Local ● Cloud(Fat AP)

Device Name iUAP-AC-MV2.0

Cloud AC Address

Cloud AC Management Port (Range: 1024 to 65535)

Cloud AC Upgrade Port (Range: 1024 to 65535)

Parameter description

Parameter	Description
Deployment Mode	Specifies the deployment mode of AP. **Local** is selected by default. – **Local**: AP can be managed only by AC on the LAN. – **Cloud(Fat AP)**: AP can be managed only by the remote AC with the specified IP address on the internet or in other networks.
Device Name	Specifies the name of the AP. When multiple APs with the same model exist in the network, different device names can help you differentiate them.
Cloud AC Address	Specifies the WAN IP address (must be a pubic IP address) of the egress router of the remote AC or the domain name bound by the IP address.
Cloud AC Management Port	Specifies the available port of the egress router of the remote AC, which is used to manage the AP.
Cloud AC Upgrade Port	Specifies the available port of the egress router of the remote AC, which is used to upgrade the AP.

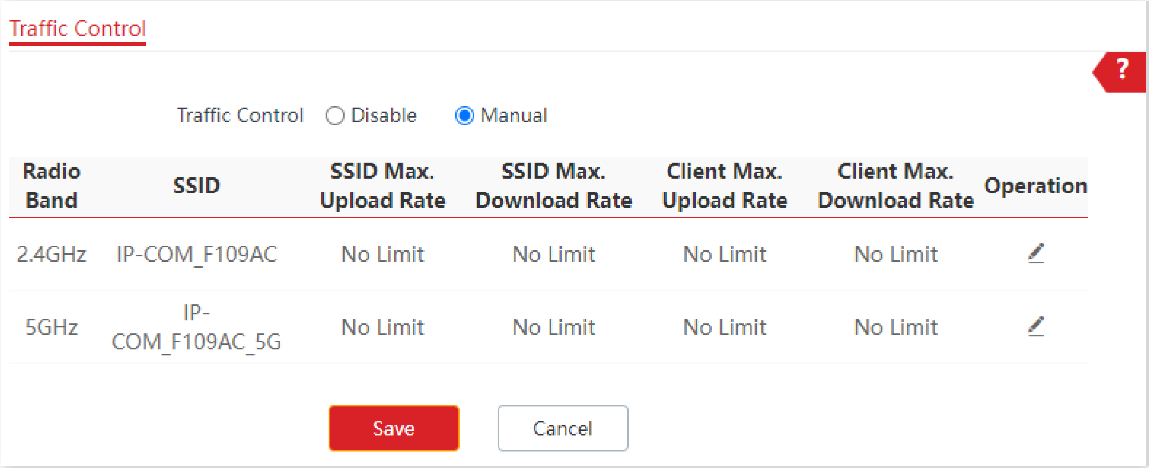
8.2 Traffic control

8.2.1 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.



Traffic Control ○ Disable ● Manual

Radio Band	SSID	SSID Max. Upload Rate	SSID Max. Download Rate	Client Max. Upload Rate	Client Max. Download Rate	Operation
2.4GHz	IP-COM_F109AC	No Limit	No Limit	No Limit	No Limit	✎
5GHz	IP-COM_F109AC_5G	No Limit	No Limit	No Limit	No Limit	✎

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 SSID and the maximum upload/download rate of user devices to limit the total bandwidth of SSID and evenly allocate bandwidth to users. In this way, if multiple SSIDs are enabled, and a user network with a lower priority (such as guest network) occupies an excessively high internet speed or a user occupies too much bandwidth, such circumstances as excessively low internet speed or even internet unavailability for other users will not occur.
Radio Band	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.

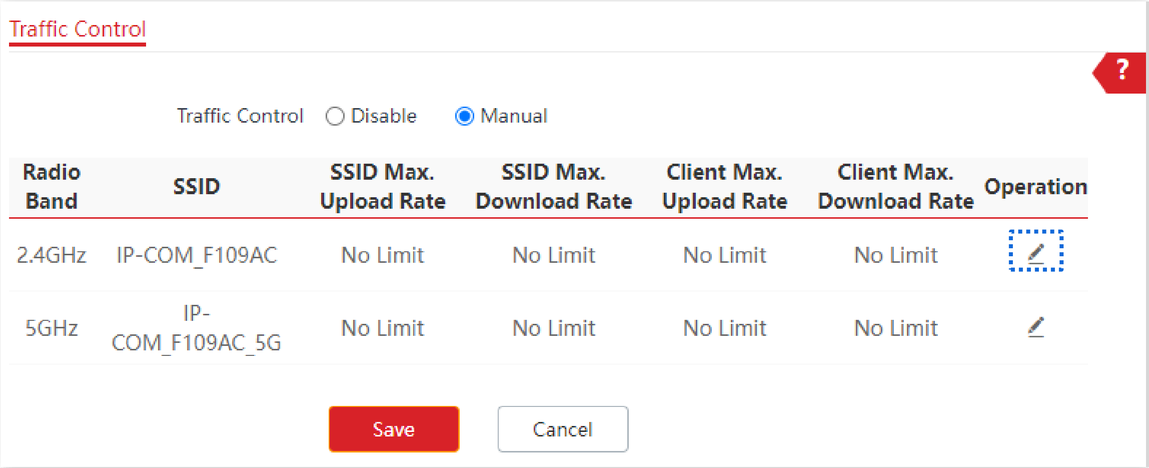
Parameter	Description
SSID Max. Upload Rate	Specify the maximum upload or download rate allowed for a wireless network. If you leave it blank, the maximum upload or download rate of the target wireless network are not limited. It is available only when you manually set a traffic control rule.
SSID Max. 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	Used to 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.

8.2.2 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.

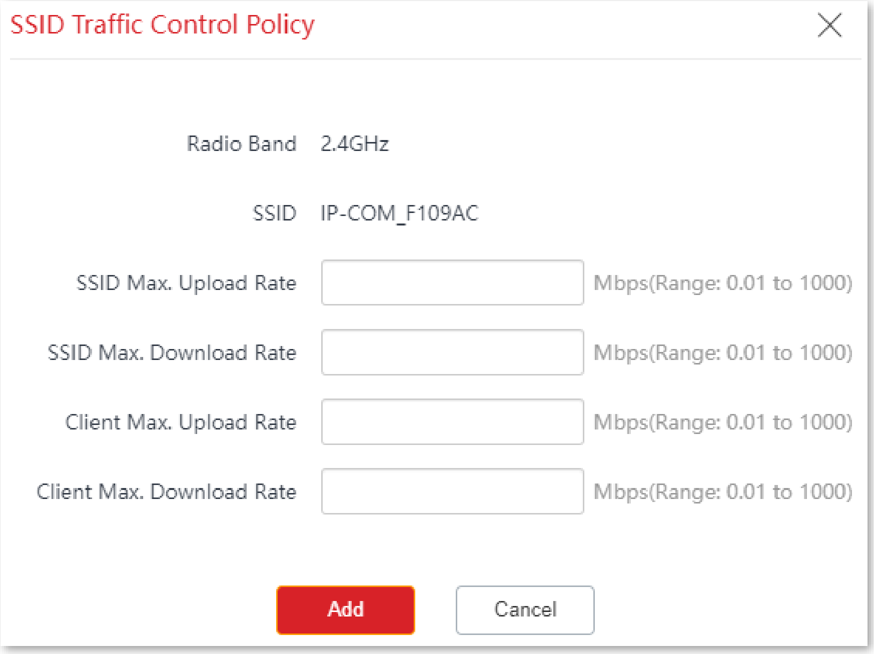


Traffic Control ○ Disable ● Manual

Radio Band	SSID	SSID Max. Upload Rate	SSID Max. Download Rate	Client Max. Upload Rate	Client Max. Download Rate	Operation
2.4GHz	IP-COM_F109AC	No Limit	No Limit	No Limit	No Limit	✎
5GHz	IP-COM_F109AC_5G	No Limit	No Limit	No Limit	No Limit	✎

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**.



SSID Traffic Control Policy

Radio Band	2.4GHz	
SSID	IP-COM_F109AC	
SSID Max. Upload Rate		Mbps(Range: 0.01 to 1000)
SSID Max. Download Rate		Mbps(Range: 0.01 to 1000)
Client Max. Upload Rate		Mbps(Range: 0.01 to 1000)
Client Max. Download Rate		Mbps(Range: 0.01 to 1000)

---End

8.3 SNMP

Tip

iUAP-AC-M V2.0 is used for illustration here.

8.3.1 Overview

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

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

SNMP management framework

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

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

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

Basic SNMP operations

The AP allows the following basic SNMP operations:

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

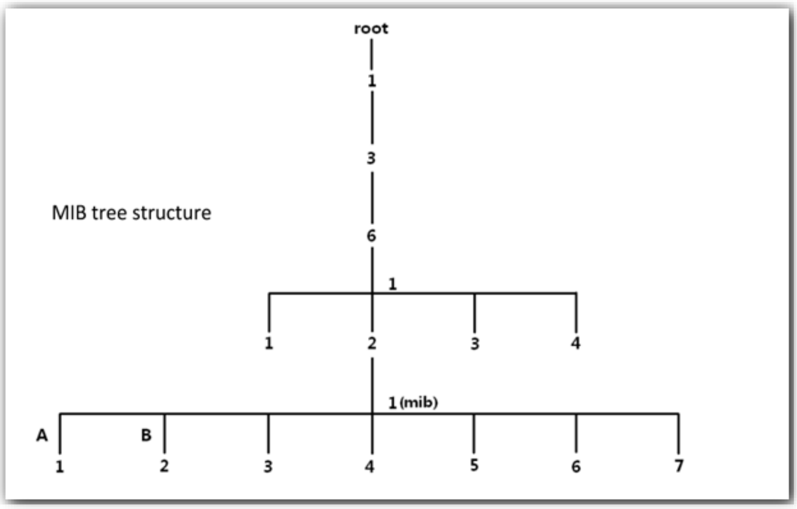
SNMP protocol version

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

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

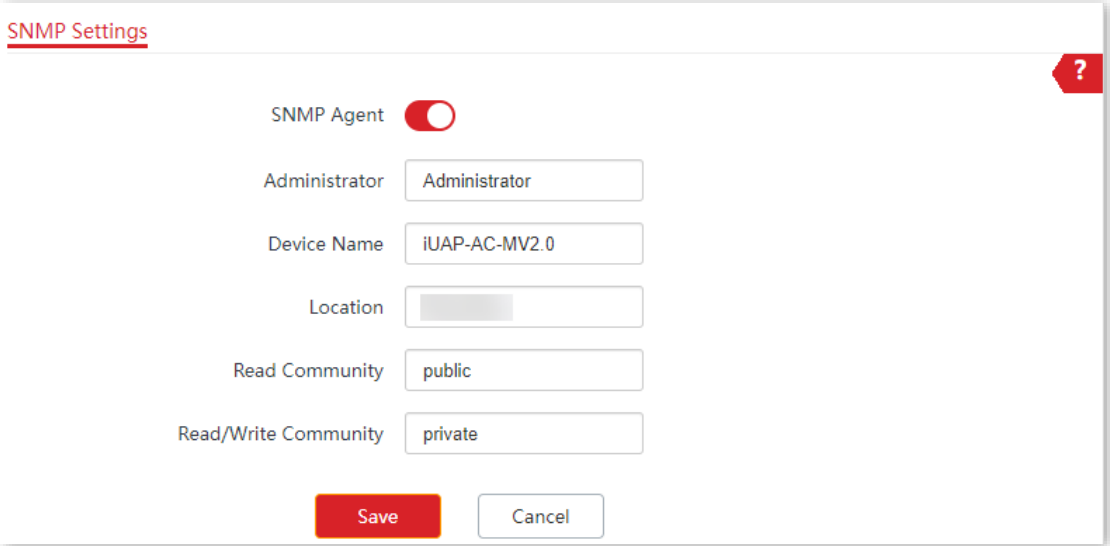
MIB introduction

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



8.3.2 Configure SNMP agent

To access the page, log in to the web UI of the AP, and navigate to **Advanced** > **SNMP**. You can configure the SNMP agent function of the AP.



SNMP Agent ●

Administrator	Administrator
Device Name	iUAP-AC-MV2.0
Location	
Read Community	public
Read/Write Community	private

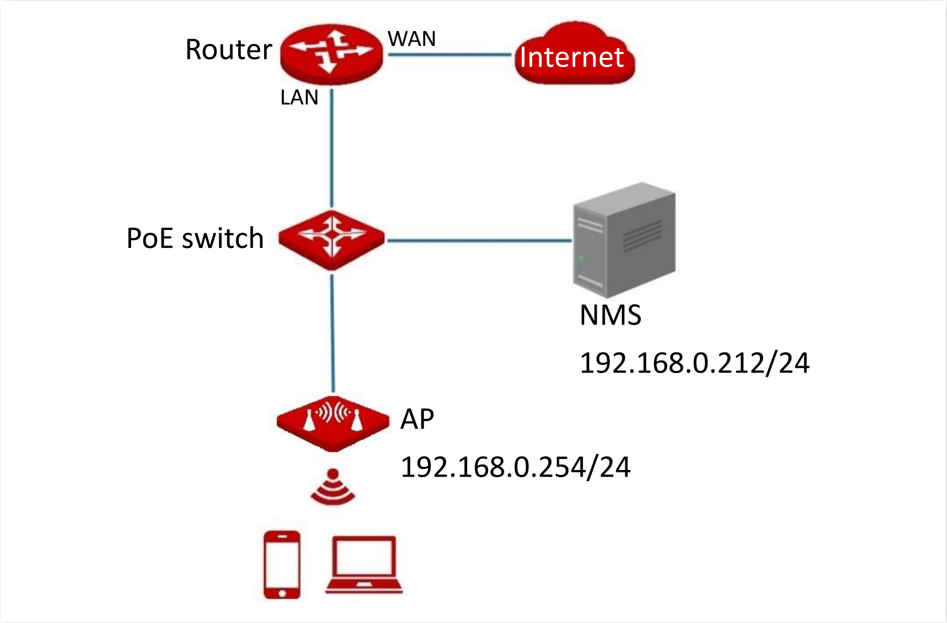
Parameter description

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

8.3.3 Example of configuring the SNMP function

Networking requirements

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

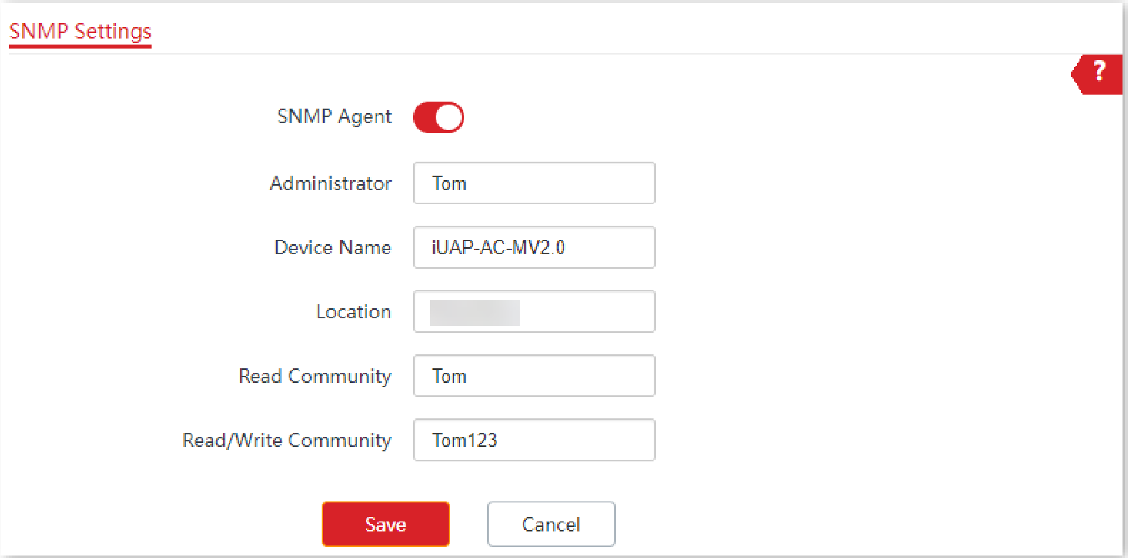


Configuration procedure

I. Configure the AP

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

1. Log in to the web UI of the AP., and navigate to **Advanced** > **SNMP**.
2. Enable the **SNMP Agent** function.
3. Set the SNMP parameters of **Administrator**, **Device Name**, **Location**, **Read Community** and **Read/Write Community**.
4. Click **Save**.



SNMP Settings

SNMP Agent: ●

Administrator: Tom

Device Name: iUAP-AC-MV2.0

Location: [redacted]

Read Community: Tom

Read/Write Community: Tom123

II. Configure the NMS

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

---End

Verification

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

8.4 Cloud maintenance

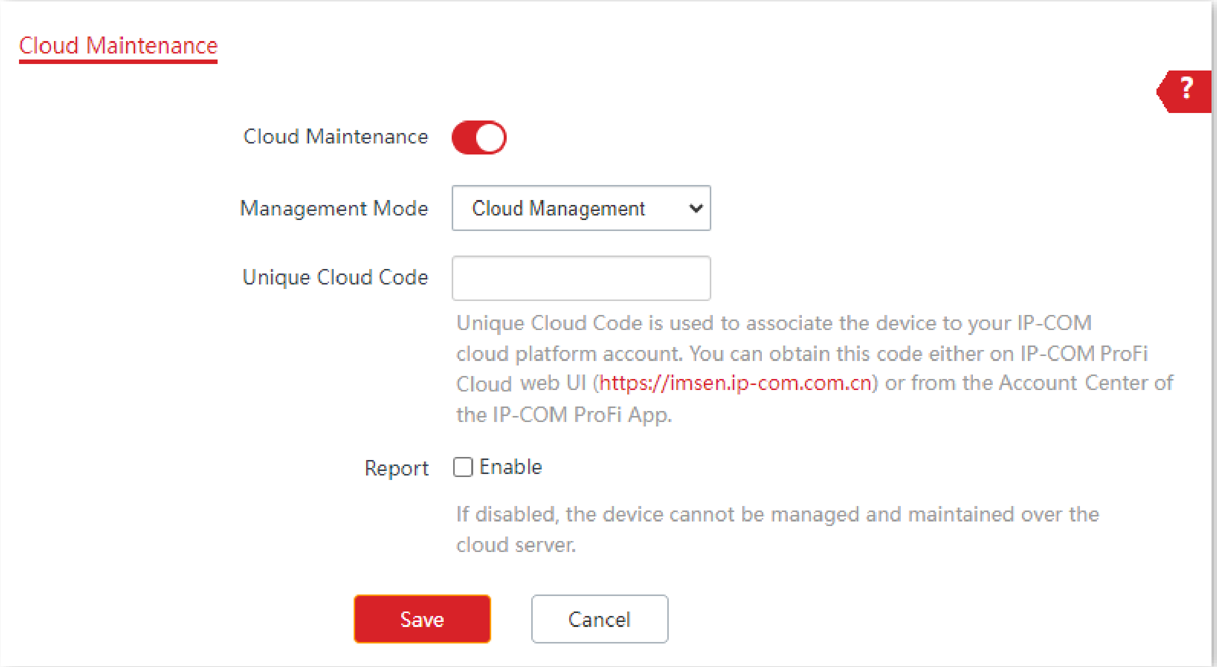
8.4.1 Overview

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

The AP can be managed by the IP-COM ProFi cloud platform. You can configure and check the parameters of the AP on the web UI of the IP-COM ProFi cloud platform (https://imsen.ip-com.com.cn) or IP-COM ProFi App.

To access the page, log in to the web UI of the AP, and navigate to **Advanced** > **Cloud Maintenance**. You can configure the cloud maintenance function of the AP.

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



Cloud Maintenance ●

Management Mode: Cloud Management

Unique Cloud Code:

Unique Cloud Code is used to associate the device to your IP-COM cloud platform account. You can obtain this code either on IP-COM ProFi Cloud web UI (https://imsen.ip-com.com.cn) or from the Account Center of the IP-COM ProFi App.

Report: □ Enable

If disabled, the device cannot be managed and maintained over the cloud server.

Parameter description

Parameter	Description
Cloud Maintenance	Specifies whether to enable the Cloud Maintenance function of the AP.
Management Mode	Specifies the mode 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, the AP can be managed by the IP-COM ProFi cloud platform and the configuration of relevant functions 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, the AP can be managed on the IP-COM ProFi cloud platform, but all configurations of the AP are completed on its own web UI, and the information is reported to the IP-COM ProFi cloud platform.
Unique Cloud Code	Specifies the IP-COM ProFi cloud platform account associated with the device. You can obtain this code from the web UI of the IP-COM ProFi cloud platform (https://imsen.ip-com.com.cn) or IP-COM ProFi App.

Parameter	Description
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.

8.4.2 Example of configuring cloud maintenance

Networking requirements

The AP can be managed through the web UI of the IP-COM ProFi cloud platform or IP-COM 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.

– Before managing the AP on the cloud, add the AP to the IP-COM ProFi App or IP-COM ProFi Cloud (https://imsen.ip-com.com.cn) first. For more details, see help document in **Help Center** of IP-COM ProFi App or IP-COM ProFi Cloud.

- **Method 1: Add the AP over Wi-Fi**

1. Get the **IP-COM ProFi** from **Google Play**, **App Store** or QR code.

2. Connect your mobile device to the Wi-Fi of the AP.
3. Open the App, and tap an existing project or create a new one.
4. Tap the pop-up window that shows the AP is detected, and add it to the project.

If the pop-up window does not appear, tap ⊕ and follow the on-screen instructions.

---End

- **Method 2: Add the AP with Unique Cloud Code**

1. Get the **Unique Cloud Code** from IP-COM ProFi App or IP-COM ProFi Cloud.
2. 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.

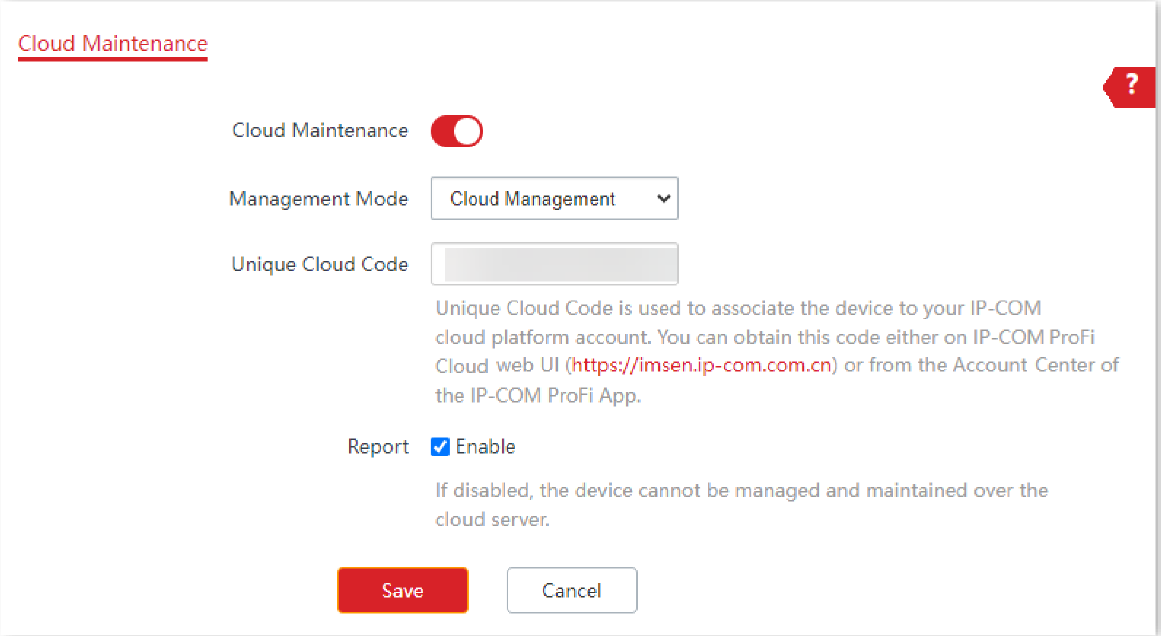
   3) Set the parameters of the cloud maintenance function.

   – Set **Cloud Management Type** to **Cloud Configuration**.

   – Paste the **Unique Cloud Code** in the input box.

   – Enable the **Report** function.

   4) Click **Save**.



Cloud Maintenance

Cloud Maintenance: ●

Management Mode: Cloud Management

Unique Cloud Code: [redacted]

Unique Cloud Code is used to associate the device to your IP-COM cloud platform account. You can obtain this code either on IP-COM ProFi Cloud web UI (https://imsen.ip-com.com.cn) or from the Account Center of the IP-COM ProFi App.

Report: ☑ Enable

If disabled, the device cannot be managed and maintained over the cloud server.

3. Add the AP to the project through **Device-joining Alert** on IP-COM ProFi App or IP-COM ProFi Cloud.

---End

Verification

After the configuration is completed, the AP can be managed through the web UI of the IP-COM ProFi cloud platform (https://imsen.ip-com.com.cn) or IP-COM ProFi App, and all its configuration is delivered by the IP-COM ProFi cloud platform.

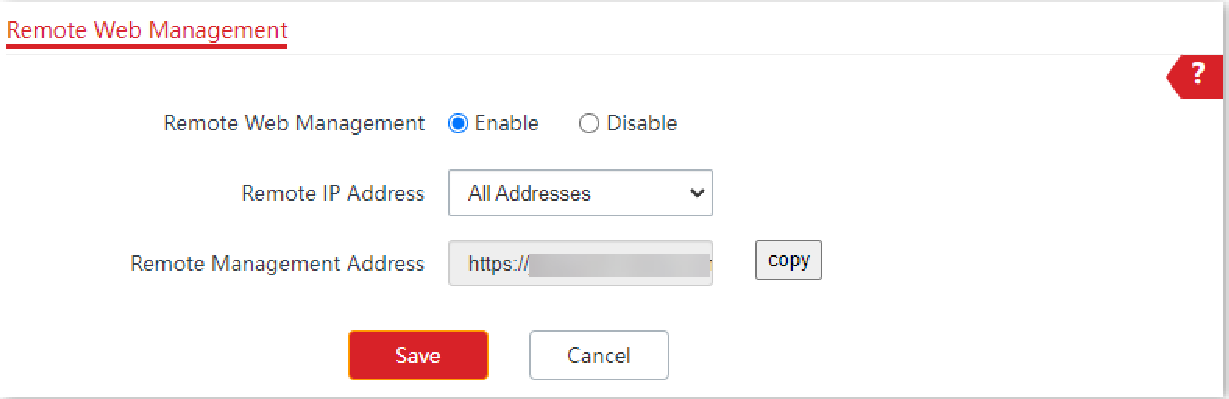
8.5 Remote web management

8.5.1 Overview

Generally, the web UI of the AP can only be accessed on clients that are connected to the AP by a LAN port or wirelessly. 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**. You can enable 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.


Remote Web Management

Remote Web Management ● Enable ○ Disable

Remote IP Address: All Addresses

Remote Management Address: https://[redacted]

Parameter description

Parameter	Description
Remote Web Management	Specifies whether to enable the remote web management function of the AP.

Parameter	Description
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 LAN, 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.

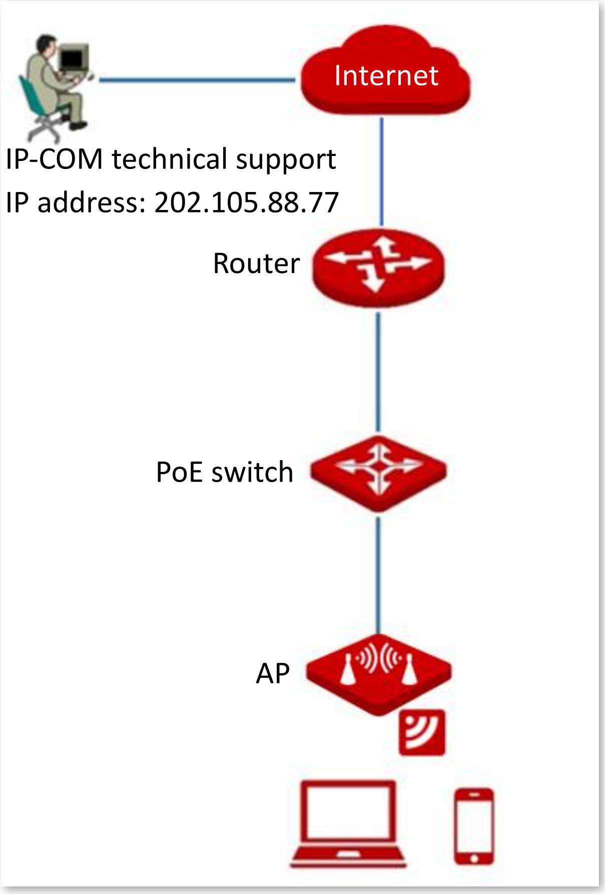
8.5.2 Example of configuring remote management

Networking requirements

An industrial park 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.

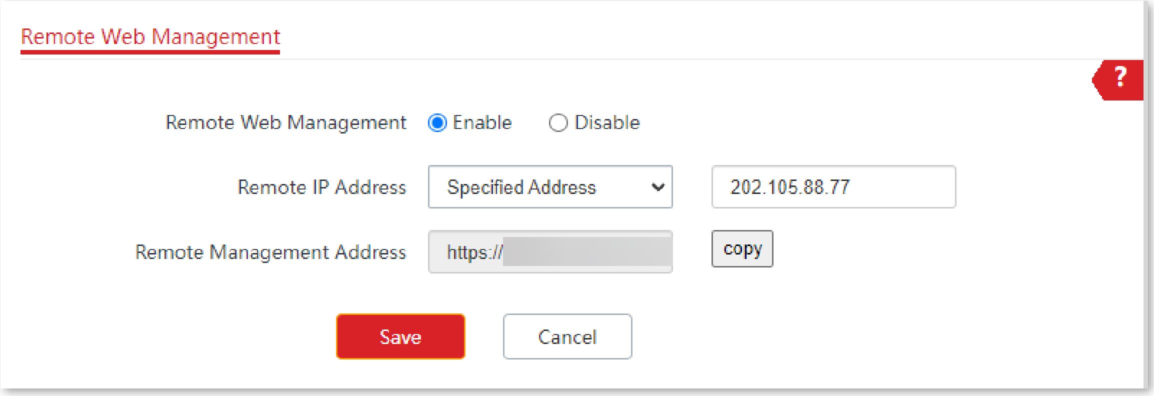
Solution

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



Configuration procedure

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



Remote Web Management

Remote Web Management ● Enable ○ Disable

Remote IP Address: Specified Address, 202.105.88.77

Remote Management Address: https://[redacted]

---End

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 (IP address: 202.105.88.77).

9 Tools

Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual AP experience.

9.1 Date & Time

You can set the system time and login timeout interval of the AP.

9.1.1 Configure system time

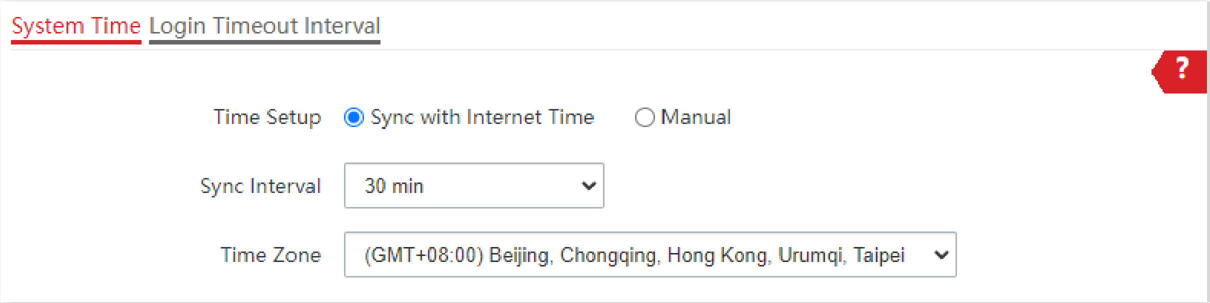
To access the page, log in to the web UI of the AP, and navigate to **Tools** > **Date & Time** > **System Time**. You can set the system time of your AP.

To make the time-related functions effective, ensure that the system time of the AP is set correctly. 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 LAN setup.



Time Setup ● Sync with Internet Time ○ Manual

Sync Interval: 30 min

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Taipei

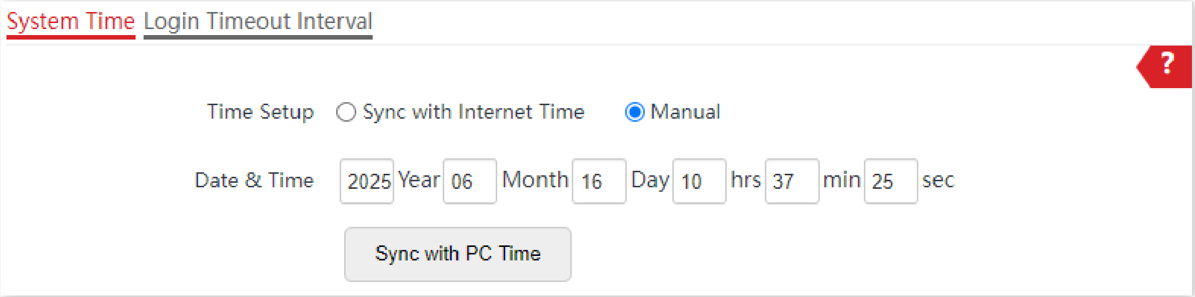
Parameter description

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 chosen.
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 chosen.

Manually set the time

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

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



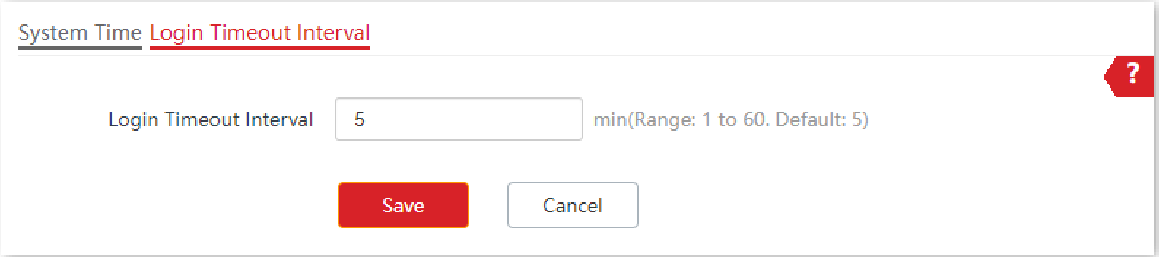
Time Setup ○ Sync with Internet Time ● Manual

Date & Time 2025 Year 06 Month 16 Day 10 hrs 37 min 25 sec

9.1.2 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**. You can modify 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.



Login Timeout Interval: 5 min(Range: 1 to 60. Default: 5)

9.2 Maintenance

To access the page, log in to the web UI of the AP, and navigate to **Tools** > **Maintenance** > **Maintenance**. You can reboot and reset AP, back up or restore settings, and control LED indicator.

9.2.1 Reboot

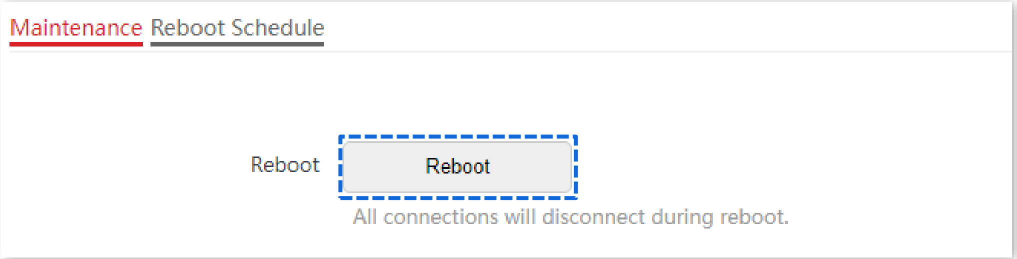
Tip

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, and navigate to **Tools** > **Maintenance** > **Maintenance** and click **Reboot**.



All connections will disconnect during reboot.

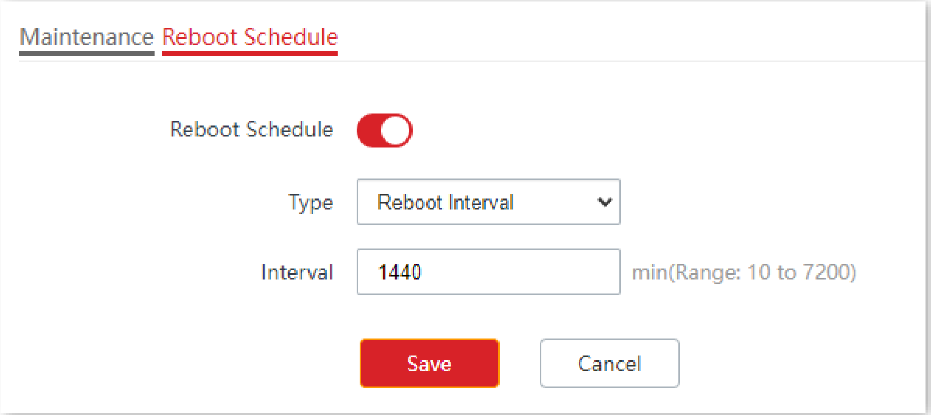
Reboot schedule

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

- Reboot interval: The AP reboots at the interval you set.
- Reboot schedule: The AP 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**.



Maintenance Reboot Schedule

Reboot Schedule: on

Type: Reboot Interval

Interval: 1440 min(Range: 10 to 7200)

---End

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

Configure the AP to reboot at a specified time

Tip

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

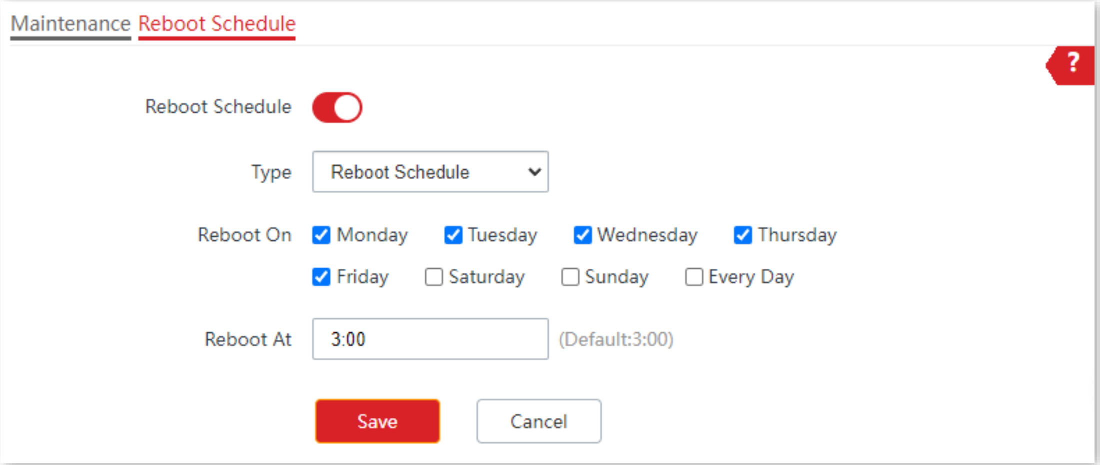
1. Log in to the web UI of the AP, and navigate to **Tools** > **Maintenance** > **Reboot Schedule**.
2. Enable the **Reboot Schedule** function.

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

4. Select the day or days 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**.



Reboot Schedule ●

Type: Reboot Schedule

Reboot On: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday □ Every Day

Reboot At: 3:00 (Default:3:00)

---End

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

9.2.2 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, the configuration data 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.

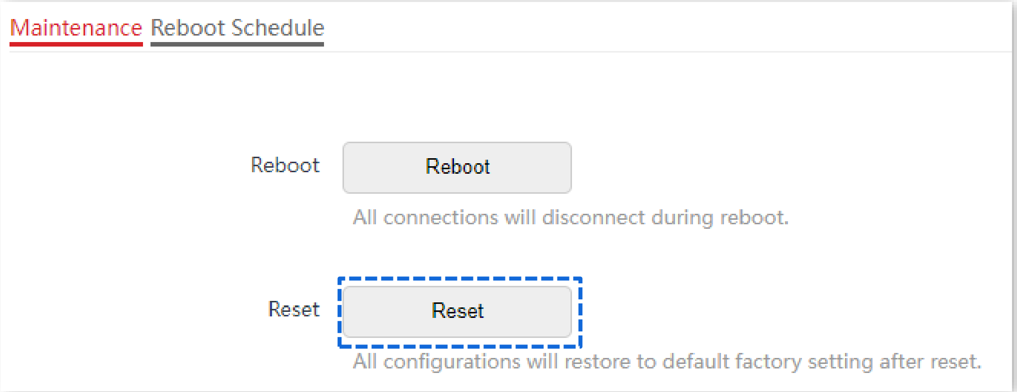
– To prevent AP damages, ensure that the power supply of the AP is normal when the AP is reset.

Method 1

When the AP is idle, hold down the reset button (**Reset**) for about 8 seconds. 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**.



All connections will disconnect during reboot.

All configurations will restore to default factory setting after reset.

9.2.3 Backup/Restore

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

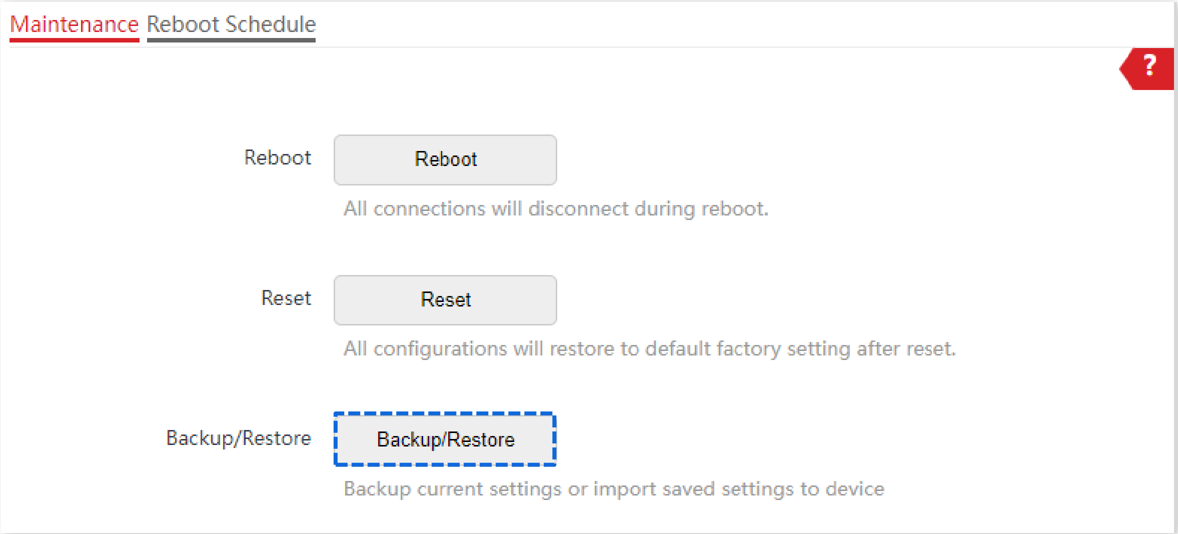
If the AP enters the optimum condition after you greatly change the configuration of the AP, you are recommended to back up the new configuration, so that you can restore it after upgrading or resetting the AP.

Tip

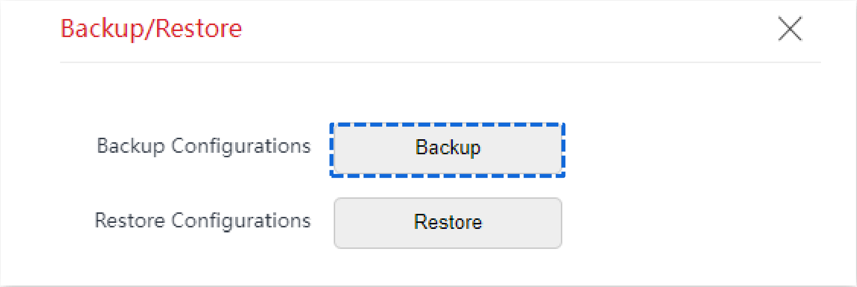
If you need to apply same or similar configurations to many APs, you can configure one of the APs, back up the configuration of the AP, and use the backup to restore the configuration on the other APs. This improves configuration efficiency.

Back up the current configuration

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


Maintenance
Reboot Schedule
?
Reboot
Reboot
All connections will disconnect during reboot.
Reset
Reset
All configurations will restore to default factory setting after reset.
Backup/Restore
Backup/Restore
Backup current settings or import saved settings to device

3. Click **Backup**.



---End

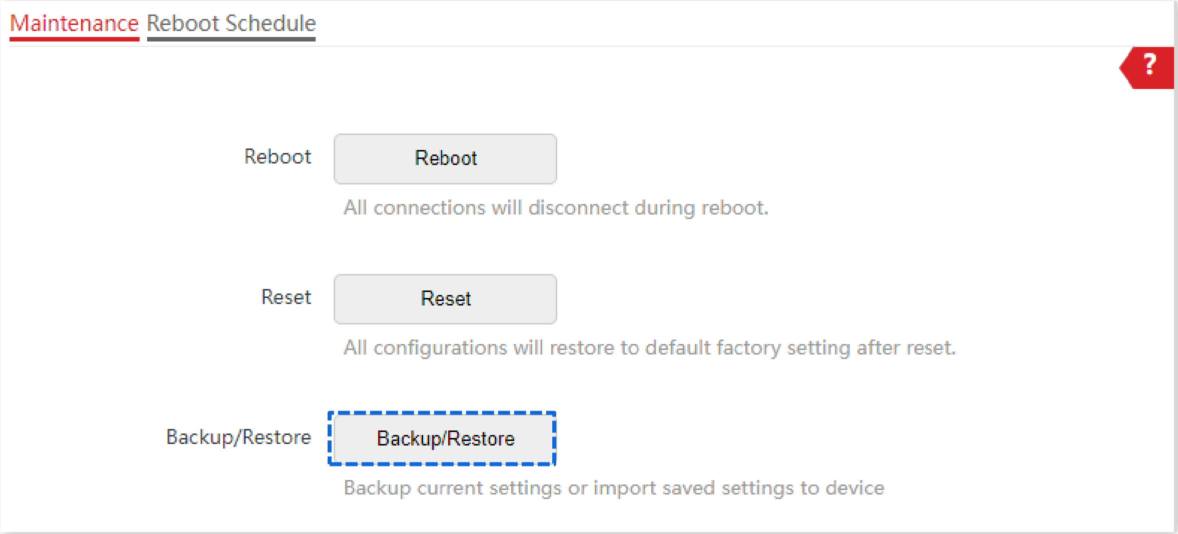
A configuration file named **APCfm.cfg** will be downloaded.

Tip

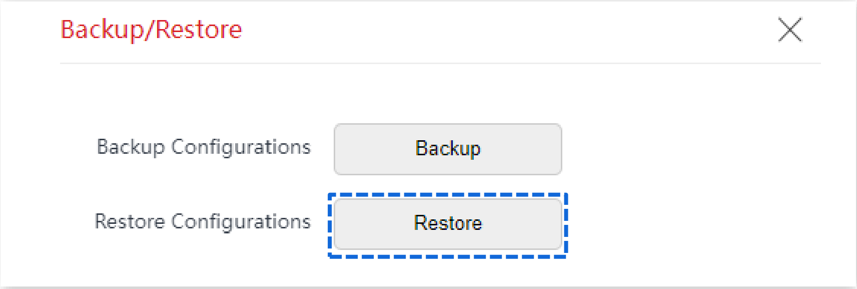
If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click **Keep**.

Restore the configuration

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


Maintenance
Reboot Schedule
?
Reboot
Reboot
All connections will disconnect during reboot.
Reset
Reset
All configurations will restore to default factory setting after reset.
Backup/Restore
Backup/Restore
Backup current settings or import saved settings to device

3. Click **Restore**.



4. Select the configuration file you backed up.

   ---End

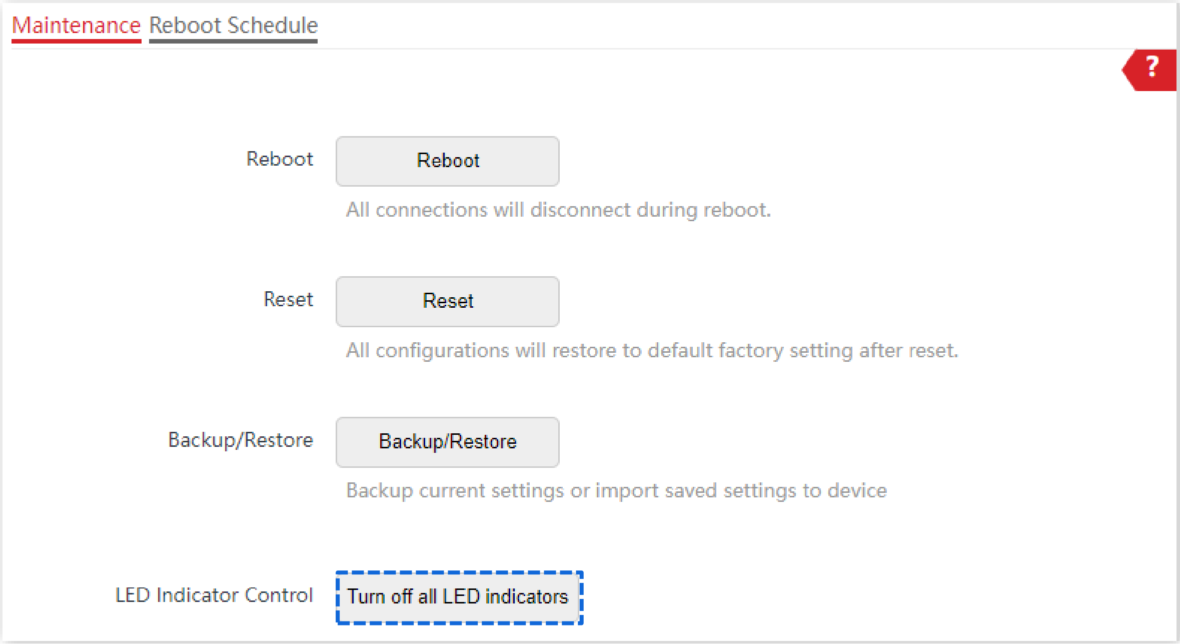
The AP restores the configurations successfully when the progress bar is done.

9.2.4 LED indicator control

This function allows 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

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



Reboot

All connections will disconnect during reboot.

Reset

All configurations will restore to default factory setting after reset.

Backup/Restore

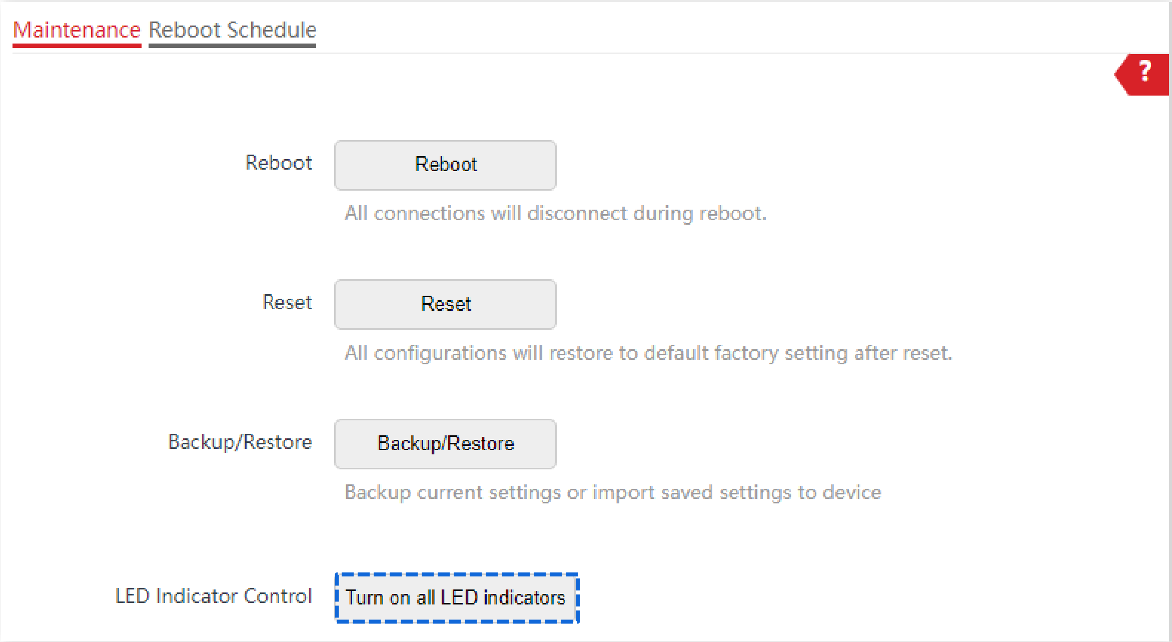
Backup current settings or import saved settings to device

LED Indicator Control

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

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



Reboot: Reboot
All connections will disconnect during reboot.

Reset: Reset
All configurations will restore to default factory setting after reset.

Backup/Restore: Backup/Restore
Backup current settings or import saved settings to device

LED Indicator Control: Turn on all LED indicators

After the configuration is completed, the LED indicator is turned on and you can judge the working status of the AP.

9.3 System software upgrade

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

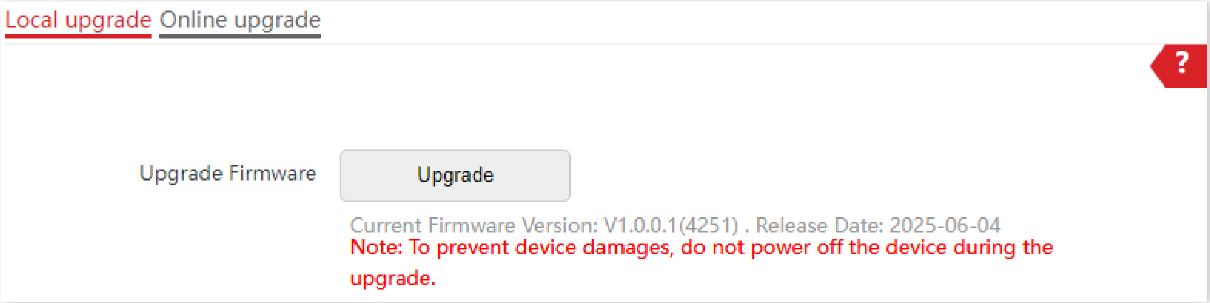
9.3.1 Local upgrade

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.

1. Download the latest 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** > **System Software Upgrade** > **Local upgrade**.
3. Click **Upgrade**. The following figure is for reference only.



Current Firmware Version: V1.0.0.1(4251) . Release Date: 2025-06-04
Note: To prevent device damages, do not power off the device during the 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**.

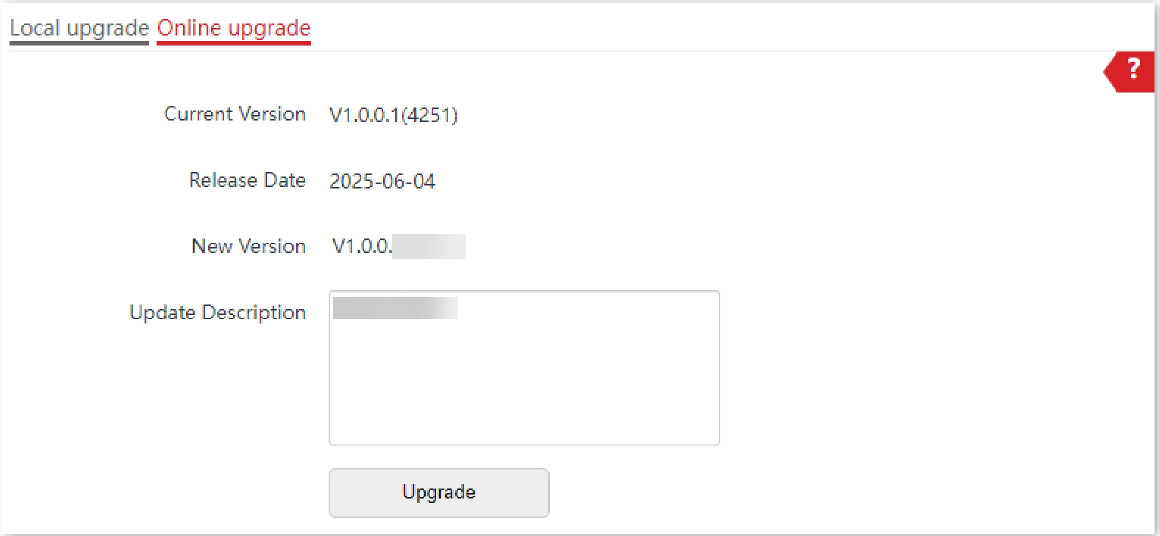
9.3.2 Online upgrade

To access the page, log in to the web UI of the AP, and navigate to **Tools** > **System Software Upgrade** > **Online upgrade**.

After the AP is connected to the internet, the system automatically detects whether there is a new upgrade firmware and displays the relevant information of the detected upgrade firmware. When a new upgrade firmware is displayed on the page, you can upgrade the AP as required. The following figure is for reference only.

Note

To ensure a correct upgrade and avoid damage, keep a proper power supply to the AP during the upgrade.



Current Version V1.0.0.1(4251)

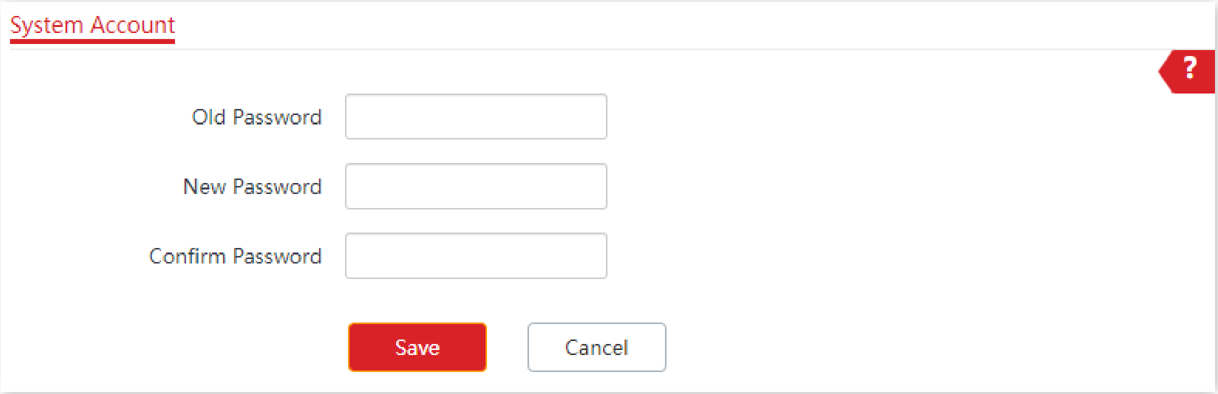
Release Date 2025-06-04

New Version V1.0.0.

9.4 System account

9.4.1 Overview

To access the page, log in to the web UI of the AP, and navigate to **Tools** > **System Account**. You can modify the password of the login account to keep unauthorized users from entering the web UI and modifying configurations, thus protecting the wireless network.



9.4.2 Change the password of login account

1. Log in to the web UI of the AP, and navigate to **Tools** > **System Account**.
2. Enter the current password in **Old Password**.

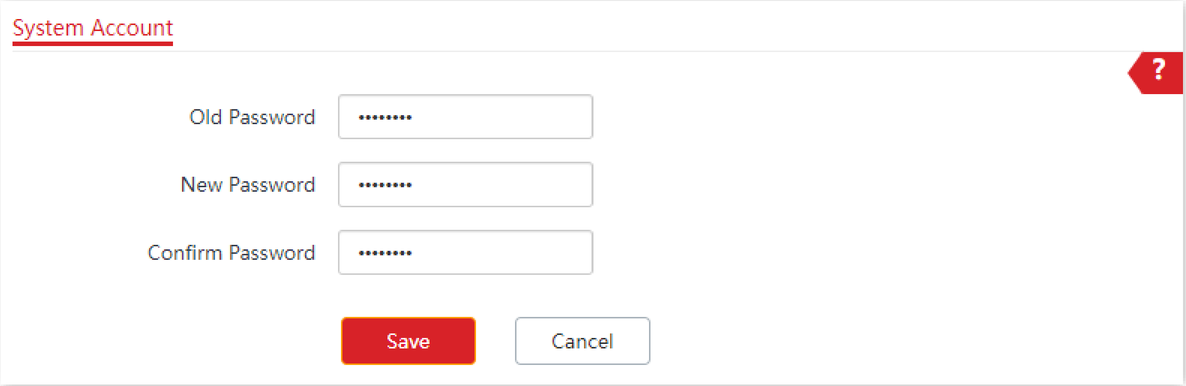
3. Enter the new password in **New Password**.

Note

For initial setup or after a reset, set new login password for privacy and security (The longer the password, the stronger the protection). The character limit and composition rules for the password are subject to software user interface prompts.

4. Enter again the new password in **Confirm Password**.

5. Click **Save**.



System Account

Old Password ••••••••

New Password ••••••••

Confirm Password ••••••••

---End

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

9.5 System log

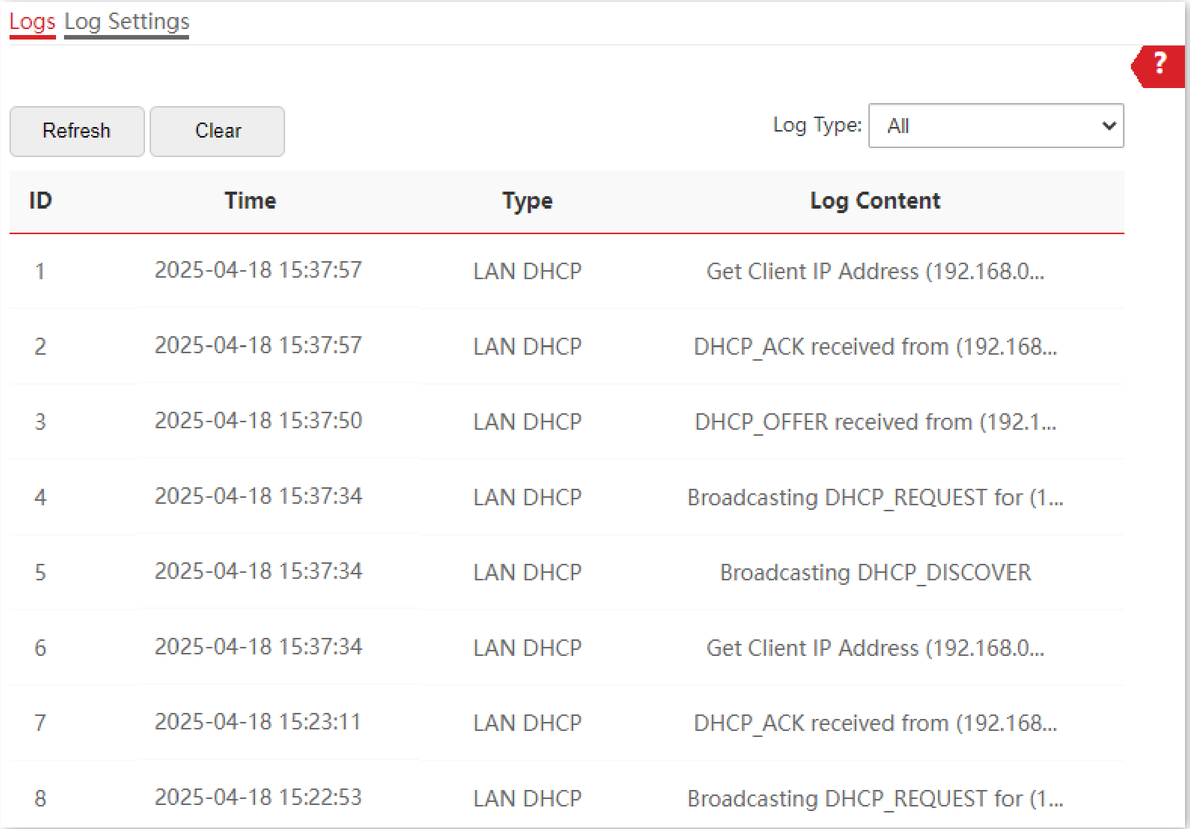
Tip

iUAP-AC-M V2.0 is used for illustration here.

9.5.1 View system logs

To access the page, log in to the web UI of the AP, and navigate to **Tools** > **System Log** > **Logs**. You can view system logs.

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



ID	Time	Type	Log Content
1	2025-04-18 15:37:57	LAN DHCP	Get Client IP Address (192.168.0...
2	2025-04-18 15:37:57	LAN DHCP	DHCP_ACK received from (192.168...
3	2025-04-18 15:37:50	LAN DHCP	DHCP_OFFER received from (192.1...
4	2025-04-18 15:37:34	LAN DHCP	Broadcasting DHCP_REQUEST for (1...
5	2025-04-18 15:37:34	LAN DHCP	Broadcasting DHCP_DISCOVER
6	2025-04-18 15:37:34	LAN DHCP	Get Client IP Address (192.168.0...
7	2025-04-18 15:23:11	LAN DHCP	DHCP_ACK received from (192.168...
8	2025-04-18 15:22:53	LAN DHCP	Broadcasting DHCP_REQUEST for (1...

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

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.

9.5.2 Log settings

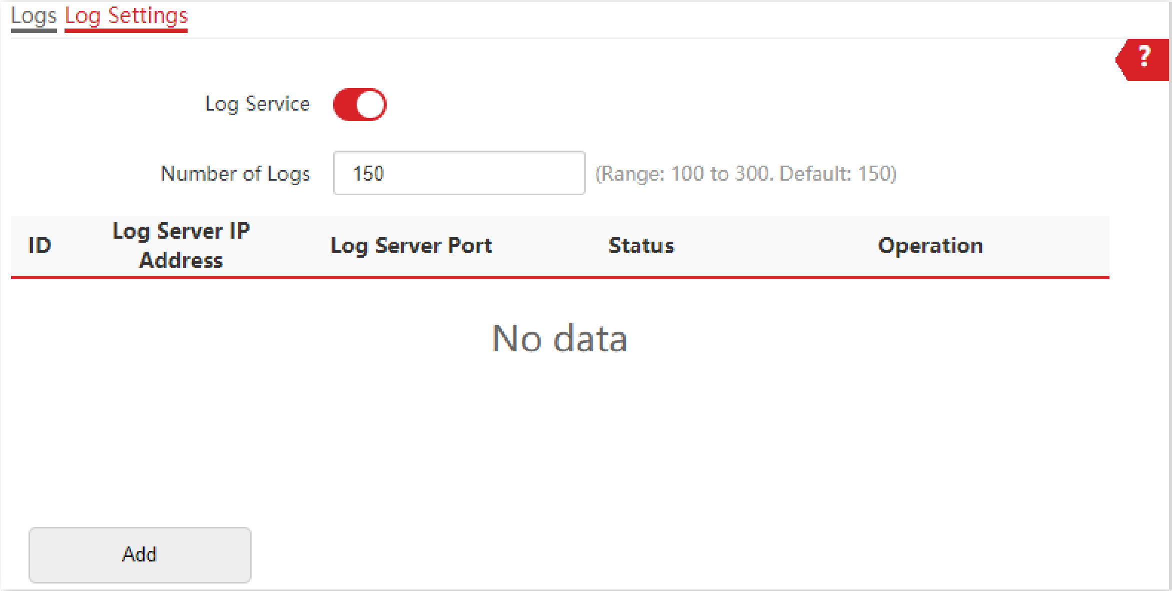
Tip

If the log number exceeds the maximum number of logs that can be displayed, the AP will automatically clear the older logs.

To access the page, log in to the web UI of the AP, and navigate to **Tools** > **System Log** > **Logs Settings**. You can set the number of logs to be displayed and configure log servers.

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

The log service function is disabled by default. The following figure displays the page when log service is enabled.



Log Service: ●

Number of Logs: 150 (Range: 100 to 300. Default: 150)

ID	Log Server IP Address	Log Server Port	Status	Operation

No data

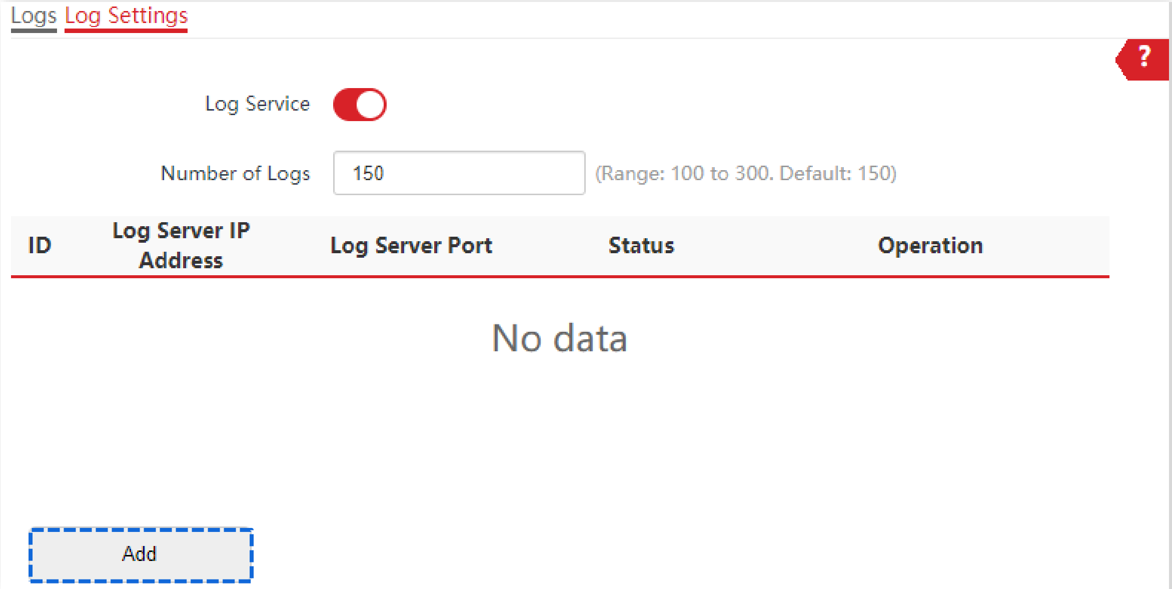
Parameter description

Parameter	Description
Log Service	Specifies whether to enable the Log Service function. This function is disabled by default. You can modify the number of logs to be displayed and configure log server only if the log service function is enabled.
Number of Logs	Specifies the largest number of logs that can be displayed on the web UI.
Log Server IP Address	Specifies the IP address of the log server. To ensure that system logs can be sent to the log server, deploy the log server within the LAN where the AP is located so that communication can be established between the AP and the log server.
Log Server Port	Specifies the port used by the log service. It should be the same port with the port configured by the log server.
Status	Specifies the status of the log server rule.

Parameter	Description
Operation	Specifies the operations you can perform on the log server: – Click ✎ to modify the IP address, port, or status of the log server. – Click 🗑 to delete the target log server.
Add	Used to click it to add a log server.

Add the log server

1. Log in to the web UI of the AP, and navigate to **Tools** > **System Log** > **Log Settings**.
2. Enable the **Log Service** function.
3. Click **Add**.



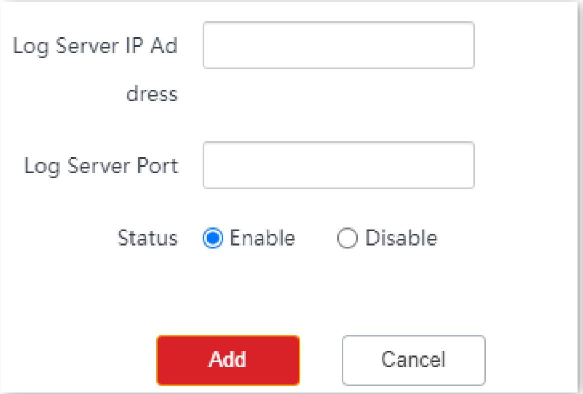
Log Service ●

Number of Logs: 150 (Range: 100 to 300. Default: 150)

ID	Log Server IP Address	Log Server Port	Status	Operation

No data

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



Status ● Enable ○ Disable

5. Click **Save**.

---End

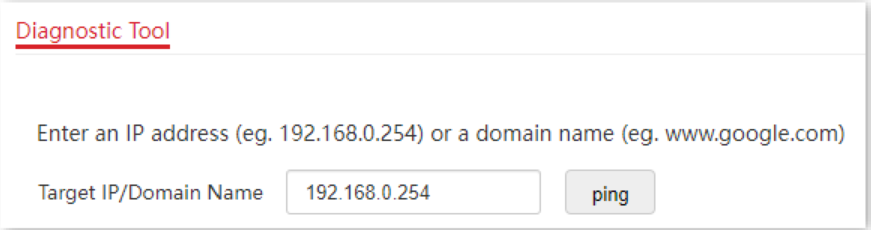
9.6 Diagnostic tool

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**.

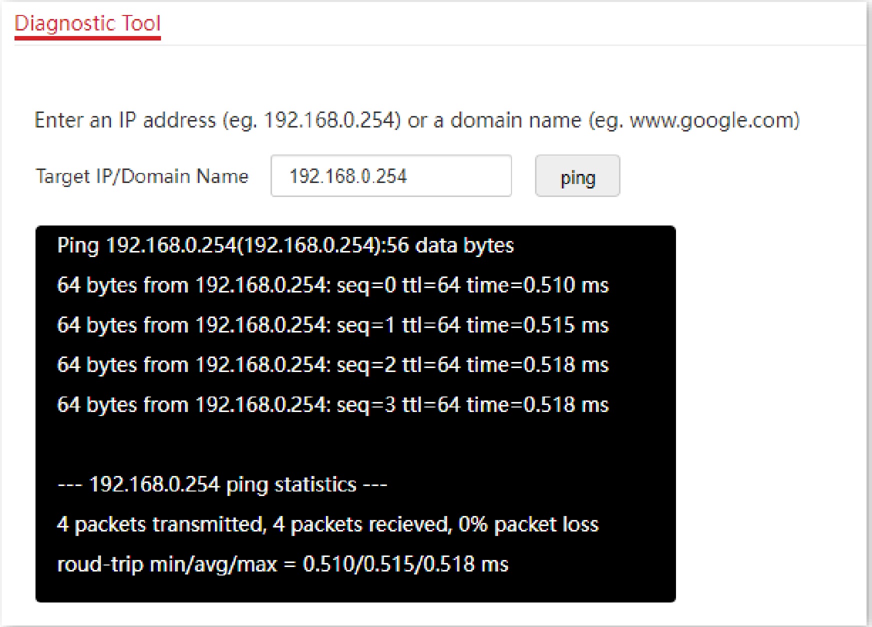


Enter an IP address (eg. 192.168.0.254) or a domain name (eg. www.google.com)

Target IP/Domain Name 192.168.0.254

---End

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


Diagnostic Tool
Enter an IP address (eg. 192.168.0.254) or a domain name (eg. www.google.com)
Target IP/Domain Name
ping

Target IP/Domain Name: 192.168.0.254

```
Ping 192.168.0.254(192.168.0.254):56 data bytes
64 bytes from 192.168.0.254: seq=0 ttl=64 time=0.510 ms
64 bytes from 192.168.0.254: seq=1 ttl=64 time=0.515 ms
64 bytes from 192.168.0.254: seq=2 ttl=64 time=0.518 ms
64 bytes from 192.168.0.254: seq=3 ttl=64 time=0.518 ms

--- 192.168.0.254 ping statistics ---
4 packets transmitted, 4 packets recieved, 0% packet loss
roud-trip min/avg/max = 0.510/0.515/0.518 ms
```

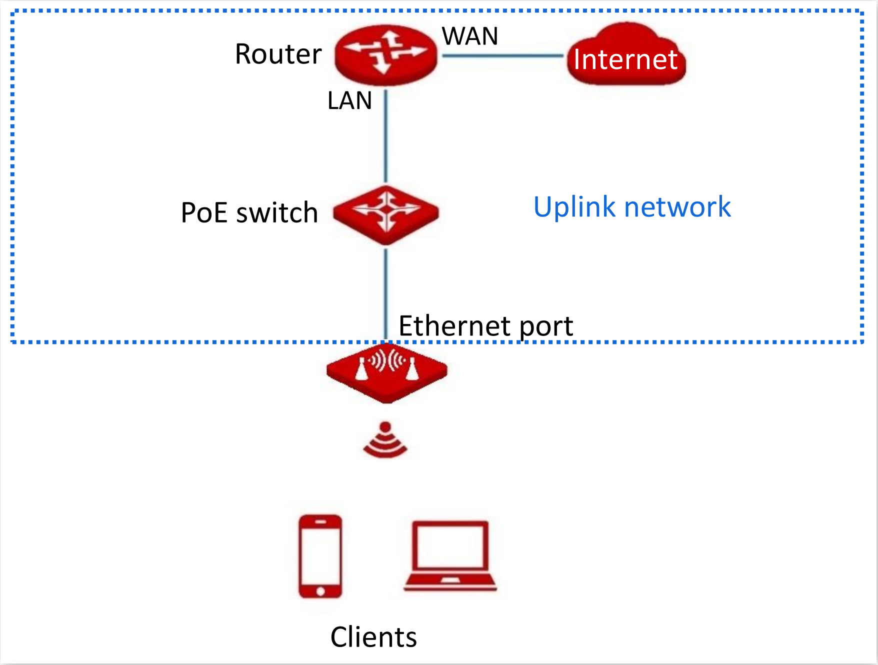
9.7 Uplink detection

9.7.1 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.

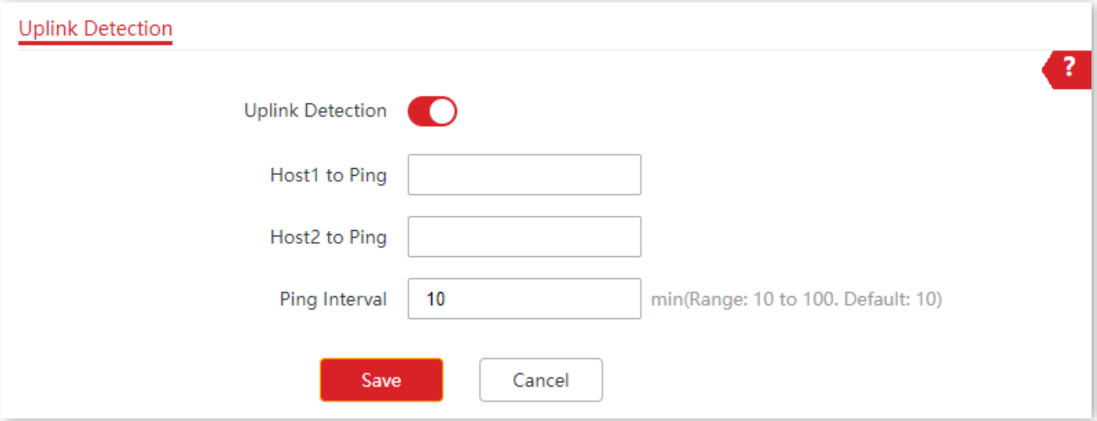
If the uplink of the AP with uplink detection enabled is faulty, wireless clients can connect to the upstream network through another nearby AP that works properly.

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



9.7.2 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 Ethernet 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 detects its uplink.
5. Click **Save**.



Uplink Detection

Uplink Detection	●
Host1 to Ping	
Host2 to Ping	
Ping Interval	10 min(Range: 10 to 100. Default: 10)

---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 Ethernet 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	LAN 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.
	Management IP address		10.16.16.169
Quick Setup	Working Mode		AP
SSID	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. 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. By default, the first SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network		Enable

A.2 Acronyms & Abbreviations

Acronyms & Abbreviations	Full Name
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
DTIM	Delivery Traffic Indication Map
DNS	Domain Name System
EDCA	Enhanced Distributed Channel Access
FIFO	First-in First-out
ID	Identity Document
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NMS	Network Management System
OID	Object Identifier
OFDMA	Orthogonal Frequency Division Multiple Access
PoE	Power over Ethernet
PSK	Pre-shared Key
PVID	Port-base VLAN ID
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTS	Request to Send
SAE	Simultaneous Authentication of Equals
Short GI	Short Guard Interval

Acronyms & Abbreviations	Full Name
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TXOP	Transmission Opportunity
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMF	Wireless Multicast Forwarding
WMM	WiFi Multimedia
WPA	Wi-Fi Protected Access