IP-COM



User Guide

Ceiling AP Series

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.

Copyright statement

Copyright © 2024-2026 IP-COM Networks Co., Ltd. All rights reserved.

IP-COM is the registered trademark of IP-COM Networks Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to IP-COM Networks Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of IP-COM Networks Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for reference 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 ceiling APs.

- W63AP
- Pro-6-Mini
- Pro-6-LR
- Pro-6-Lite
- Pro-7-LR
- Pro-7-Lite

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-7-Lite V1.1.

Conventions

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

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

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 the 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 the user guide was first published.

Version	Date	Description
V2.1	2026.11.06	– Added the description of configuring portal authentication. – Optimized the description of getting started with AP, logging in to the web UI, and managing wireless settings. – Improved wording and sentence structure.
V1.0 – V2.0	2024.03 – 2025.01	Historical versions.

Contents

Getting started with AP **1**
1.1 Use with an IP-COM wireless controller (or a router that supports AP management) 1
1.2 Use without an IP-COM wireless controller 2

Login and logout **14**
2.1 Log in to the web UI 14
2.2 Log out of the web UI 16
2.3 View the layout of the web UI 16
2.4 Use common buttons 18

Manage internet settings **19**
3.1 Configure LAN settings 19
3.2 Configure management IP 21
3.3 Use the AP as a DHCP server 22

Change the working mode **26**
4.1 Switch to AP mode 26
4.2 Switch to bridge mode 27

Manage wireless settings **29**
5.1 Configure SSID settings 29
5.2 Configure radio frequency 50
5.3 Optimize radio frequency 53
5.4 Configure load balancing 58
5.5 Configure frequency analysis 62
5.6 Enable client type identification function 63
5.7 Configure broadcast and multicast packet control 64
5.8 Use the AP as a virtual controller 65
5.9 Configure roaming settings 65

Control internet access **68**
6.1 Add devices to the blocklist 68
6.2 Add devices to the whitelist 70
6.3 Remove devices from the blocklist/whitelist 71
6.4 Control internet access speed 71
6.5 Control internet usage time 73

Configure portal authentication **75**
7.1 Portal authentication configuration guide 75
7.2 Enable portal authentication 76
7.3 Configure authentication page 77
7.4 Configure authentication method 79
7.5 Configure authentication policy 84
7.6 Configure accounts for account password authentication 85
7.7 Configure accounts for random code authentication 86
7.8 Configure authentication exemption policy 87
7.9 User management 88
7.10 Portal authentication configuration example for a street-front shop 89

Maintain and monitor network **95**
8.1 View system status 95
8.2 View wireless status 97
8.3 View traffic statistics 98
8.4 View client list 99
8.5 View system log 100
8.6 Diagnose the network 101
8.7 Configure uplink detection 102
8.8 Control LED indicator 104
8.9 Configure system time 106
8.10 Configure login timeout interval 108
8.11 Change login password 109
8.12 Reboot the AP 110
8.13 Backup and restore 112
8.14 Reset the AP 115
8.15 Upgrade system software 116
8.16 Configure remote web management 117
8.17 Change the cloud management mode 119

Configure QVLAN **120**

Appendixes **124**

1 Getting started with AP

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.

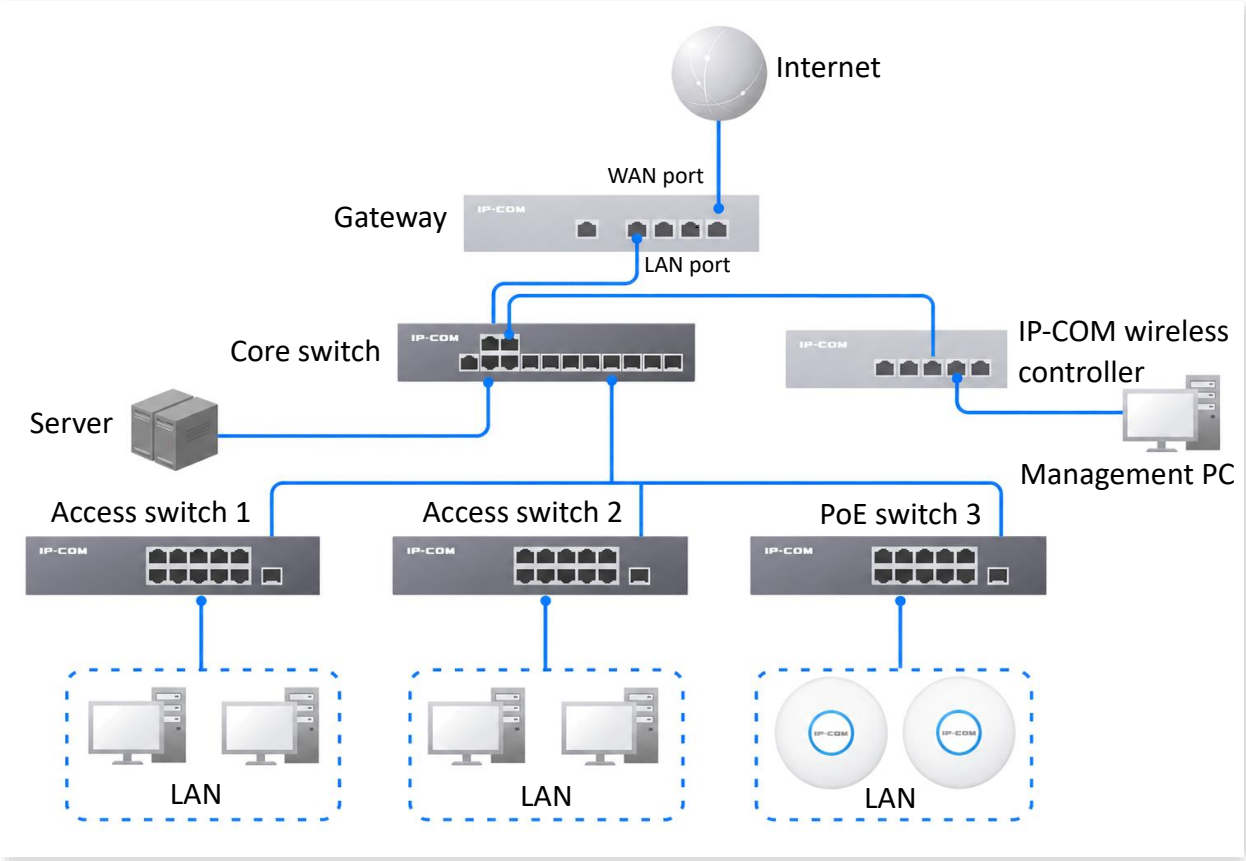
If you are using the AP for the first time or have restored it to factory settings, refer to the following instructions to configure the AP to quickly access the internet via Wi-Fi.

For more configuration options through the AP web UI, refer to other chapters of this guide.

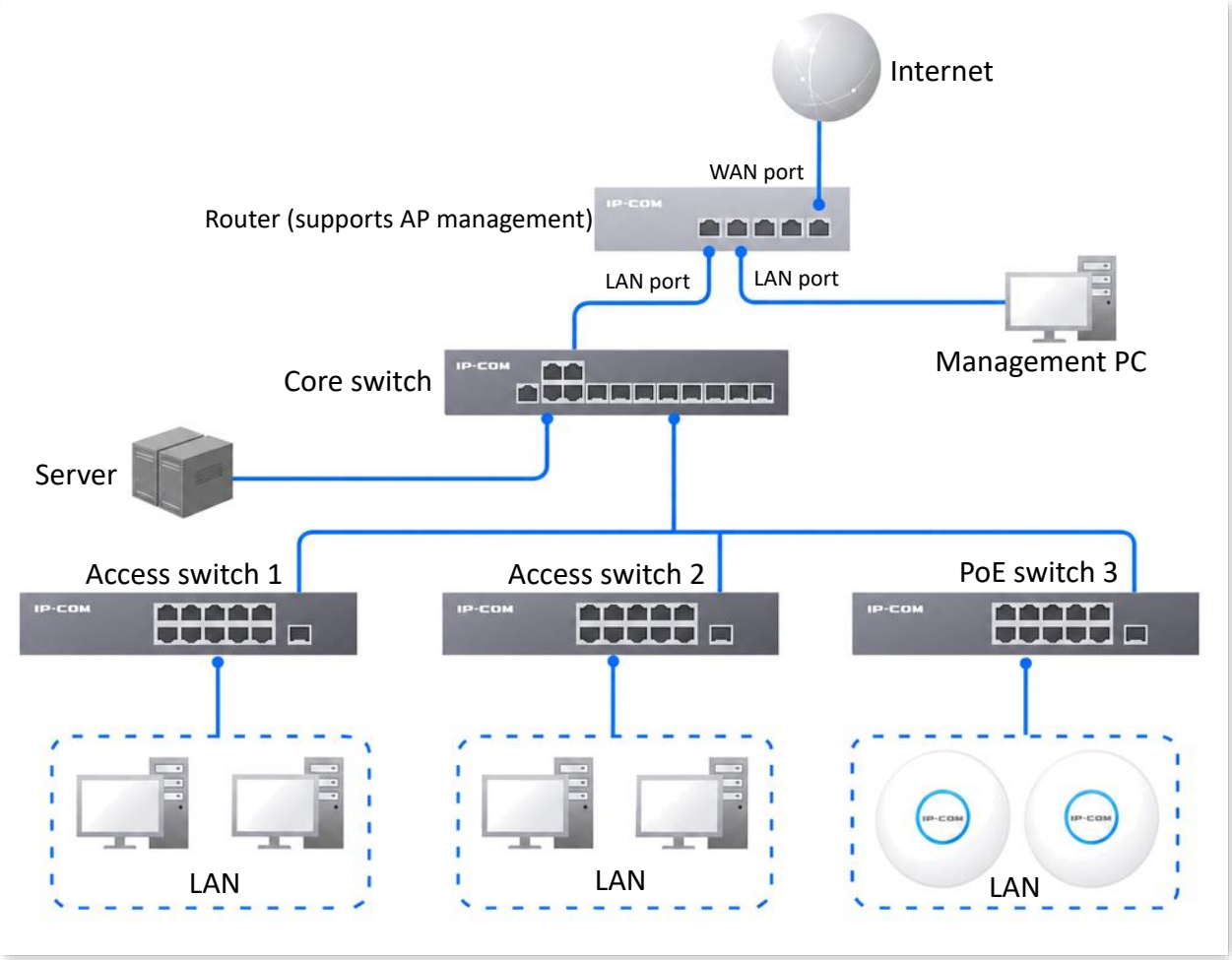
1.1 Use with an IP-COM wireless controller (or a router that supports AP management)

When an IP-COM wireless controller or an IP-COM router that supports AP management is available on the LAN, you can use the controller or router to centrally manage multiple APs. The network topology for this application scenario is shown below.

- **Use with an IP-COM wireless controller**



- **Use with a router that supports AP management**



Setup: Connect the management PC to the controller or router using an Ethernet cable. Then log in to the web UI of the controller or router to centrally manage the APs.

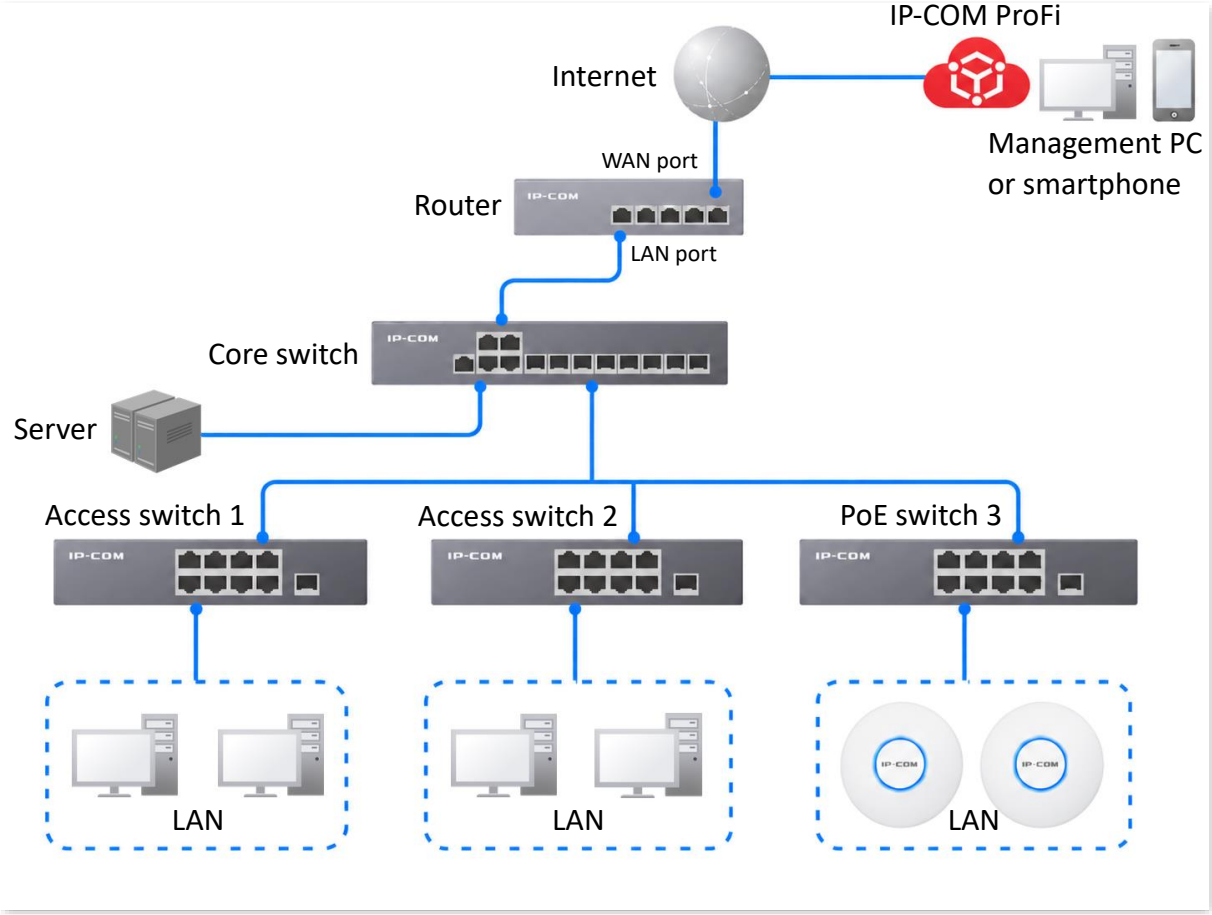
For details, visit the IP-COM official website (www.ip-com.com.cn) and refer to the user guide for the corresponding controller or router model.

1.2 Use without an IP-COM wireless controller

1.2.1 Manage APs through the cloud

IP-COM ProFi is a cloud platform provided by IP-COM for centrally managing IP-COM devices that support cloud management.

The IP-COM ProFi cloud platform is available as both a mobile app and a web version (https://imsen.ip-com.com.cn), and data is synchronized between the two. The network topology for this application scenario is shown below.



You can add the APs to the IP-COM ProFi cloud platform using either of the following methods to manage them anytime, anywhere.

Tip

Before managing the APs through the IP-COM ProFi cloud platform, ensure that the network where the APs are deployed has internet access.

- **Method 1: Add APs to the IP-COM ProFi cloud platform via Wi-Fi on the LAN (internal network)**

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

GET IT ON Google Play

Download on the App Store

Or

IP-COM ProFi

2. Connect your mobile device to the Wi-Fi of the AP.

Tip

- If you have configured the AP's Wi-Fi network through the AP's web UI, the AP's Wi-Fi name and password are those you set.
- If the AP is managed by an IP-COM wireless controller or router, log in to the controller or router's management page to view the AP's Wi-Fi name and password.
- If the AP is not managed by any network device, the AP's Wi-Fi network only has a default Wi-Fi name **IP-COM_*XXXXXX*** (***XXXXXX*** is the last six digits of the MAC address on the bottom label 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.

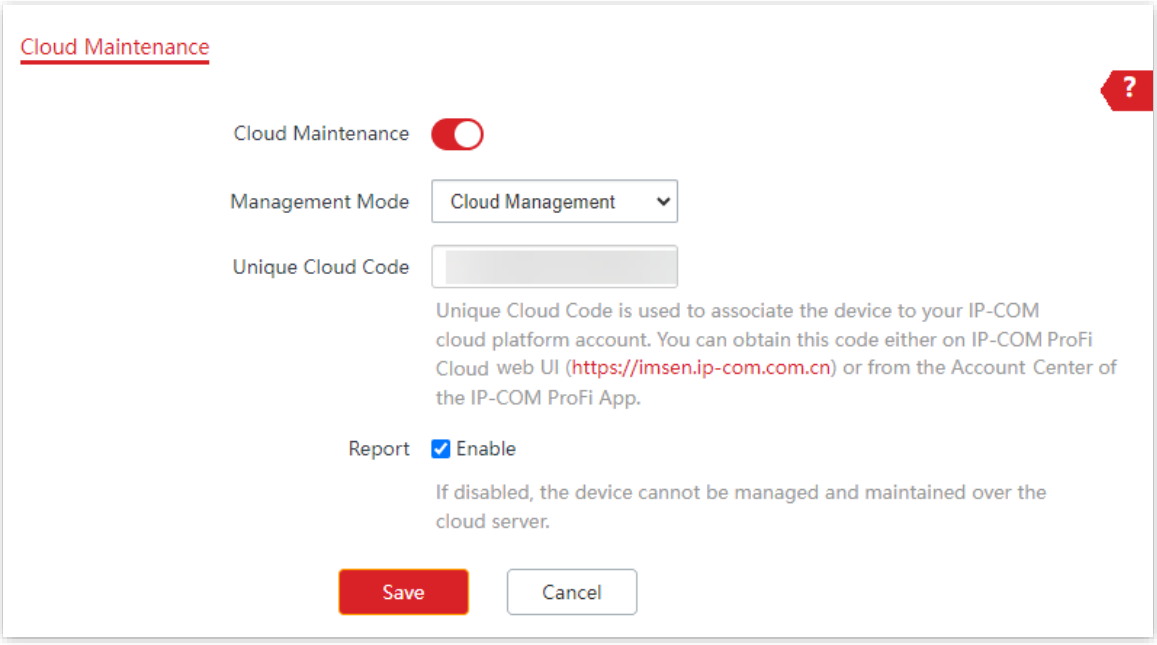
   If the pop-up window does not appear, tap  and follow the on-screen instructions.

---End

After an AP is successfully added to the IP-COM ProFi cloud platform using this method, the AP's cloud management function is enabled automatically. All AP configuration information is then delivered by the IP-COM ProFi cloud platform. Except for necessary settings such as cloud maintenance, no other configurations can be made on the AP's own web UI. This is referred to as **Cloud Management** mode. If you only want to view the AP configuration through the IP-COM ProFi cloud platform, you can change the cloud management mode on the **Advanced** > **Cloud Maintenance** page.

- **Method 2: Add APs to the IP-COM ProFi cloud platform using a unique cloud code**

1. Get the unique cloud code from **Account** in the IP-COM ProFi app, or click **Add** > **Unique Cloud Code** in the upper-right corner of the web UI of the IP-COM ProFi cloud platform (https://imsen.ip-com.com.cn).
2. Enable and configure the cloud maintenance function of the AP
   1) Log in to the web UI of the AP.
   2) Navigate to **Advanced** > **Cloud Maintenance**.
   3) Enable the **Cloud Maintenance** function.
   4) Set the parameters of the cloud maintenance function.
      - Set **Management Mode** as required.
      - Paste the **Unique Cloud Code** in the input box.
      - Enable the **Report** function.
   5) Click **Save**.



3. Add the AP to the project through **Device-joining Alert** on IP-COM ProFi app or on the web UI of the IP-COM ProFi cloud platform.

---End

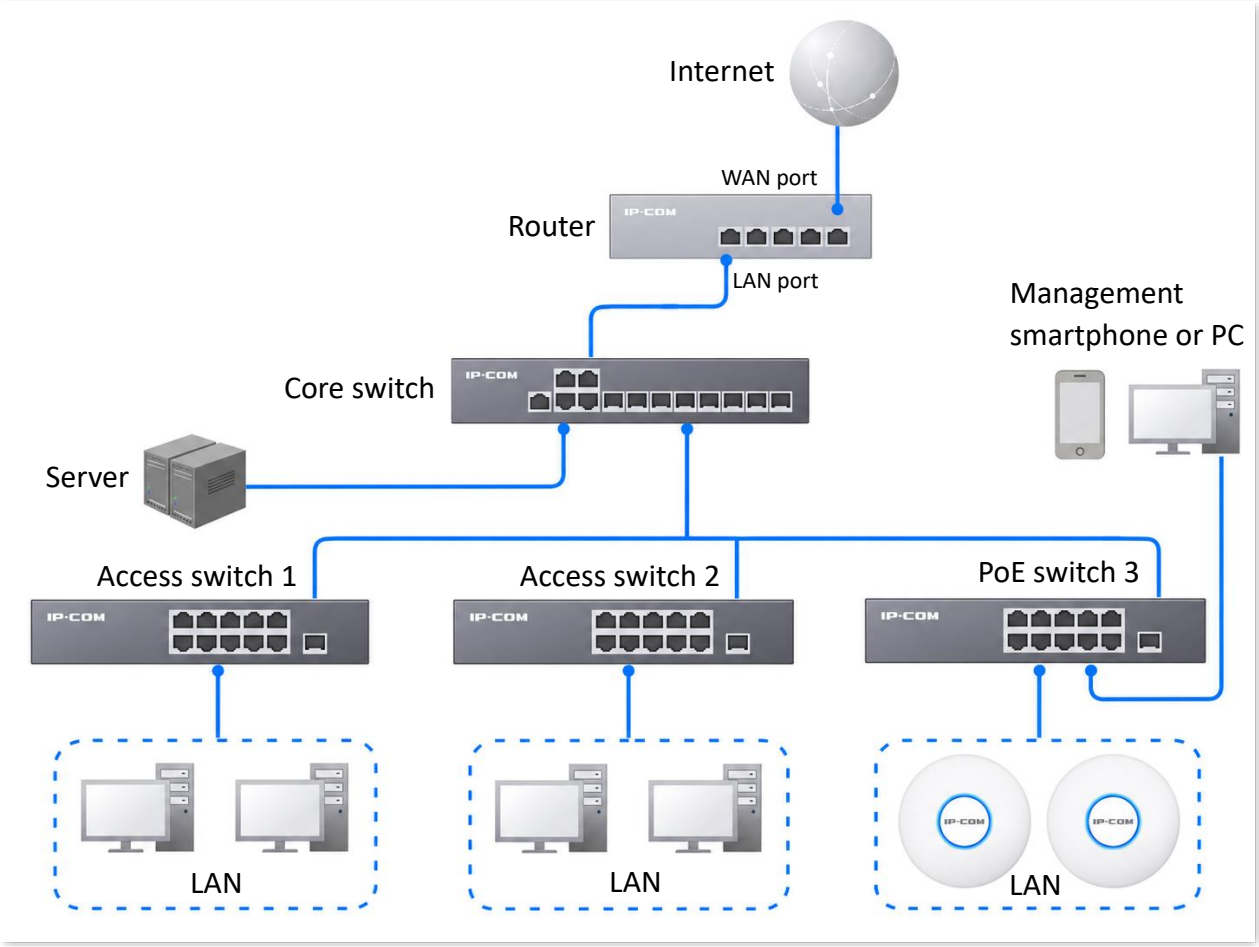
Parameter description

Parameter	Description
Cloud Maintenance	Specifies whether to enable the cloud maintenance function of the AP.
Management Mode	Specifies the modes under which your AP is managed. – **Cloud Management**: Applicable to scenarios that require unified configuration and maintenance through the IP-COM ProFi cloud platform. In this mode, 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. Except for necessary settings such as cloud maintenance, no other configurations can be made on the AP's own web UI. – **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 or local wireless controller, 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 the 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.

1.2.2 Manage APs through the AP web UI

The network topology for this application scenario is shown below.



Procedure for managing APs through the AP web UI

Step 1: Log in to the quick setup page of the AP.

1. Connect a management device to the AP.
   - Smartphone or laptop: Connect to the AP's Wi-Fi.

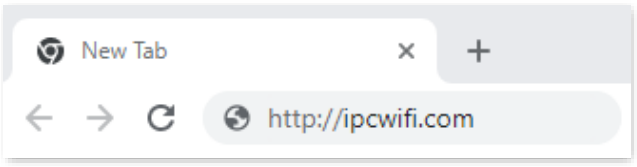
Tip

- If the AP is not managed by any network device or cloud platform, the AP's Wi-Fi network only has a default Wi-Fi name **IP-COM_*XXXXXX*** (***XXXXXX*** is the last six digits of the MAC address on the bottom label of the AP).
- When connecting to the AP's Wi-Fi, if an Unsecured network message appears, ignore it.

- Desktop computer: Connect the computer to the AP (or to a switch connected to the AP) using an Ethernet cable.

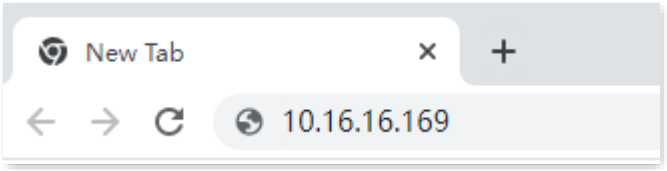
2. On the management device, use a web browser to access the AP's management address.

- Smartphone or laptop: After a successful connection, the Wi-Fi-enabled device will automatically open a browser and be redirected to the **Quick Setup** page. If it does not redirect automatically, start a browser manually and enter **http://ipcwifi.com** in the address bar to log in.



- Desktop computer: Open a web browser, enter the AP's management IP address or internet IP address in the address bar, and press **Enter**. (The following figure uses **10.16.16.169** as an example.)

  The default management IP address is **10.16.16.169**. By default, the internet IP address is obtained from the DHCP server on the LAN. If no DHCP server is available on the LAN where the AP is located, the default internet IP address is **192.168.0.254**.



Tip

If the quick setup page does not appear, try the following solutions:

- If you log in using a Wi-Fi-enabled device such as a laptop, ensure that it is successfully connected to the AP's Wi-Fi. If you log in using a smartphone, disable the cellular network (mobile data). If you log in using a computer over a wired connection, ensure that the Ethernet cable is connected correctly and securely.
- Try to use the IP address to log in to the web UI of 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. If not, use **192.168.0.254** 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, except 168 and 169, and is unused) of the computer or smartphone to the IP address within the same network segment as the AP.
- When logging in using the IP address, if there are at least two APs on the network, it is recommended to connect each AP to the network one by one and change its IP address to ensure that each AP has a unique IP address.
- Clear your browser's cache or use a different browser, and try logging in again.
- If you still cannot log in after performing the preceding steps, reset the AP and try again.

Step 2: Set the working mode of the AP.

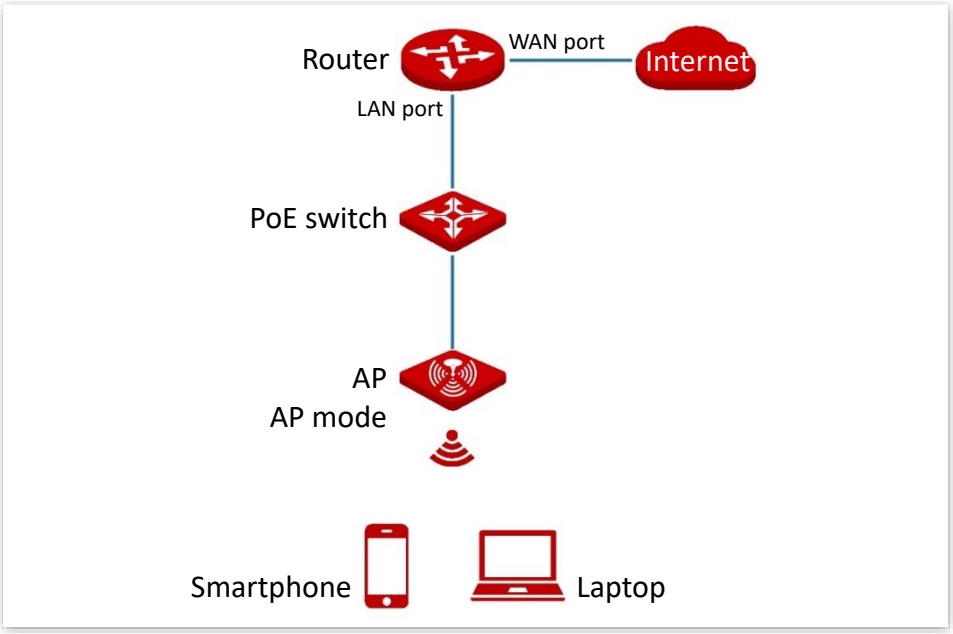
After logging in to the AP's quick setup page, you can set the working mode and wireless parameters.

Tip

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

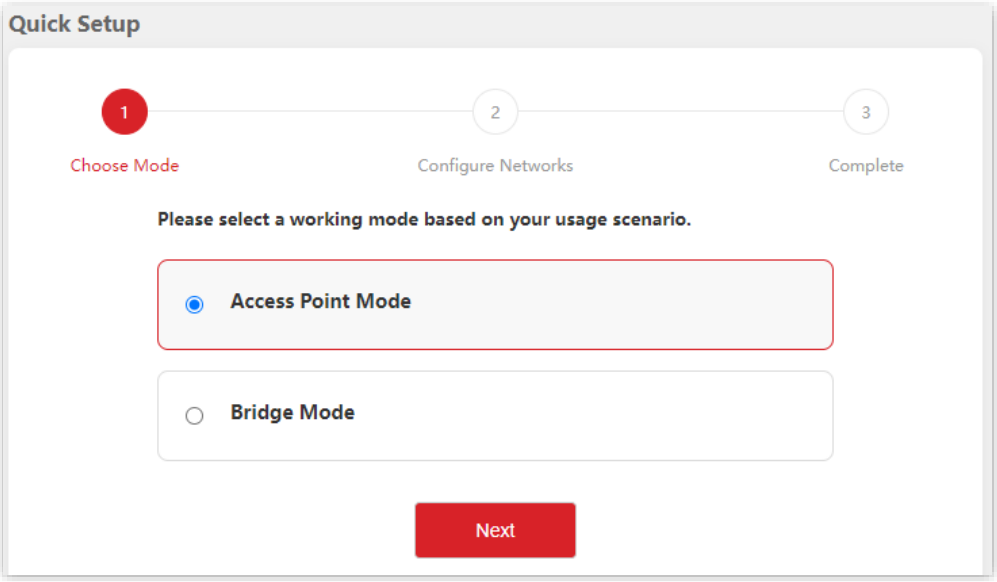
Configure AP mode

In this mode, the AP connects to the internet through an Ethernet cable and converts the wired network connection into Wi-Fi coverage. The application topology is shown below.



Procedure for configuring AP mode

1. Set the working mode of the AP to **Access Point Mode**, and click **Next**.



2. Enable or disable the **Dual-band same SSID** function as required. The following figure shows an example of enabling the **Dual-band same SSID**.

   - Enable **Dual-band same SSID**: The Wi-Fi name and password for the 2.4 GHz and 5 GHz networks of the primary Wi-Fi are the same, and only one name is displayed. When you connect to your AP's primary Wi-Fi, your device can automatically use the 2.4 GHz or 5 GHz network with the better connection quality.
   - Disable **Dual-band same SSID**: The 2.4 GHz and 5 GHz networks for the primary Wi-Fi are displayed separately. You can access the internet through either Wi-Fi network.

3. For the AP's primary Wi-Fi, customize the **WiFi Name**, WiFi Security Mode and specific parameters as required.

4. Enable or disable **Smart Home SSID** as required.

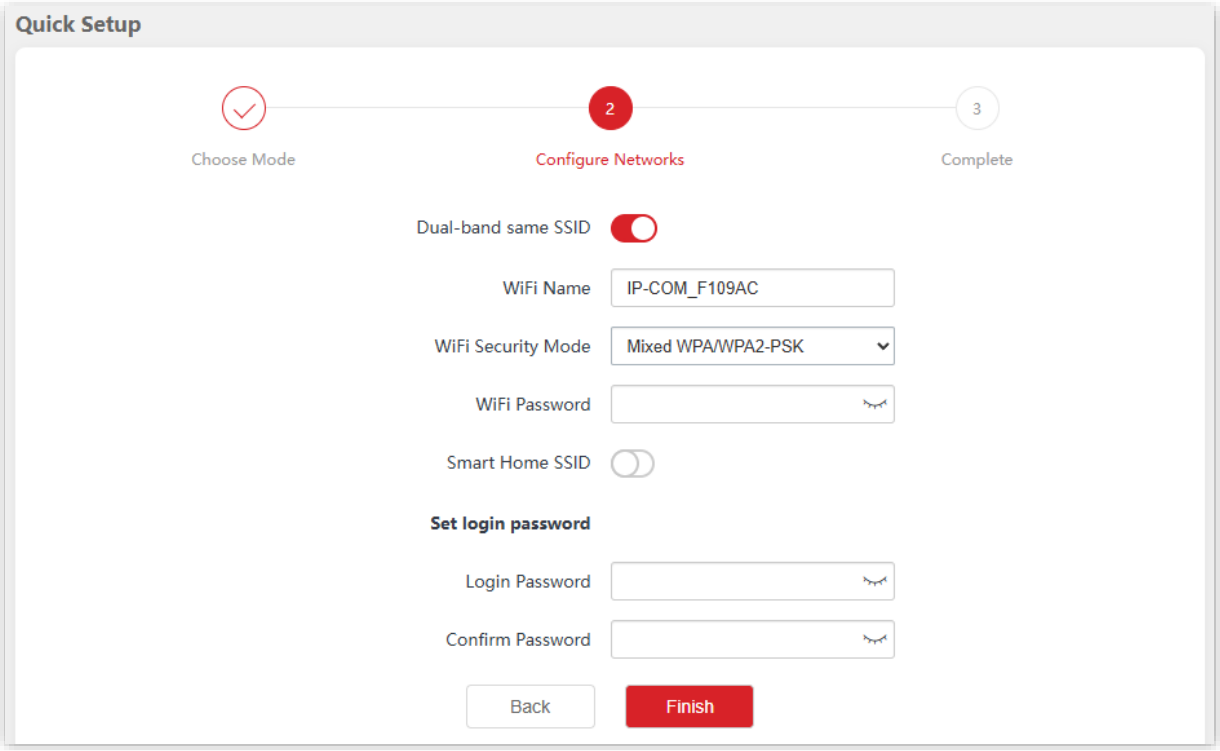
   If your deployment includes 2.4 GHz smart home devices, such as smart speakers or cameras, it is recommended to enable this option to help these devices access the network more smoothly. Then set the Wi-Fi name and password for the smart home devices to connect to.

5. Set the login password for the AP.

   Note

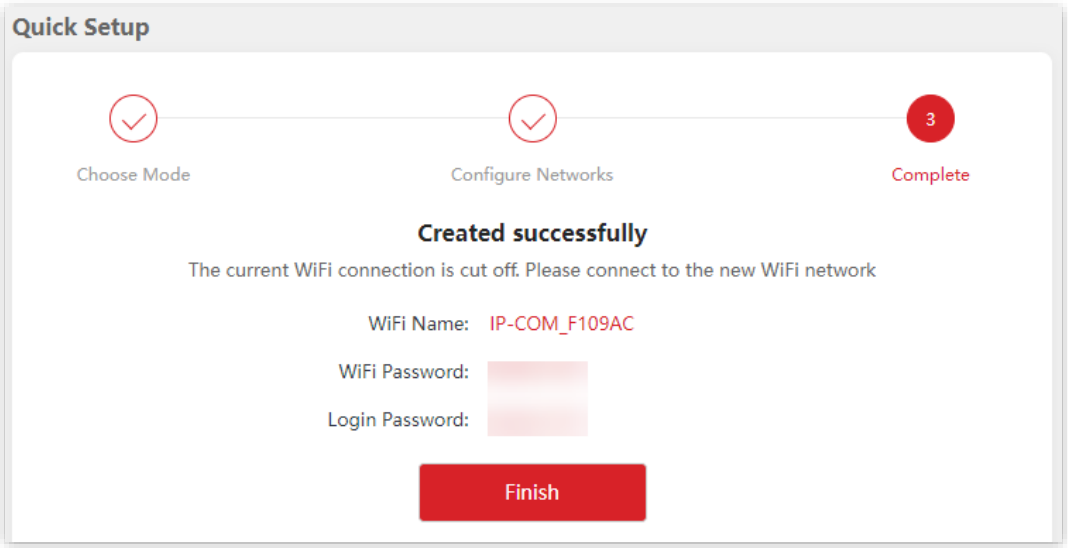
   For initial setup or after a reset, set new login and Wi-Fi passwords for privacy and security (The longer the password, the stronger the protection). The character limit and composition rules for passwords are subject to software user interface prompts.

6. Click **Finish**.



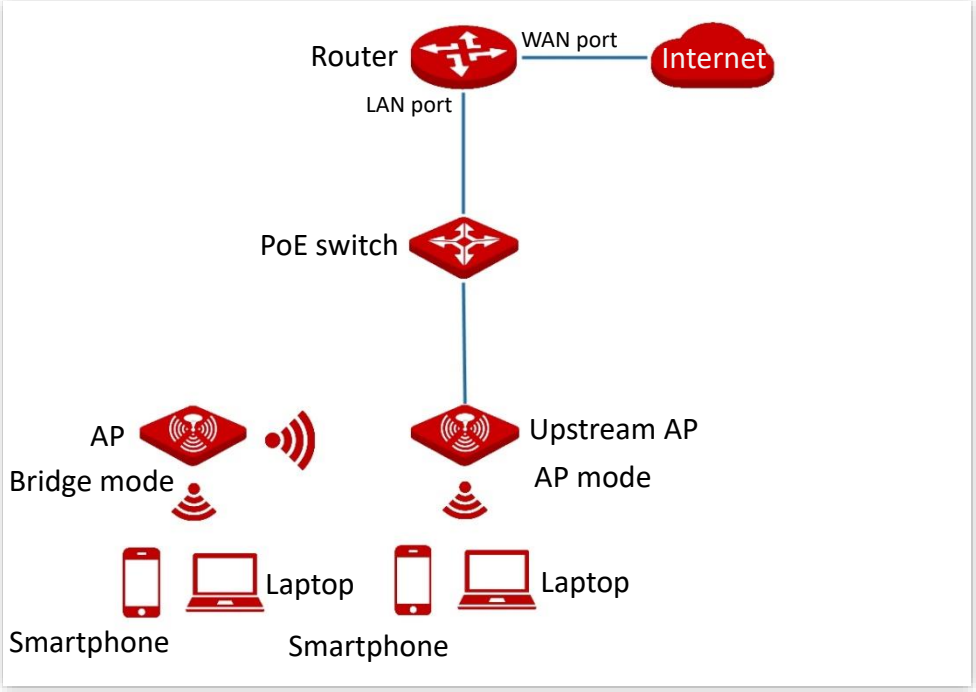
---End

After the quick setup is complete, Wi-Fi-enabled devices, such as smartphones and smart home devices, can connect to the AP Wi-Fi networks you configured to access the internet. If you want to use a Wi-Fi-enabled device to log in to the AP's web UI for further configuration (see Chapter 2 and subsequent sections), connect to the AP's newly configured Wi-Fi.



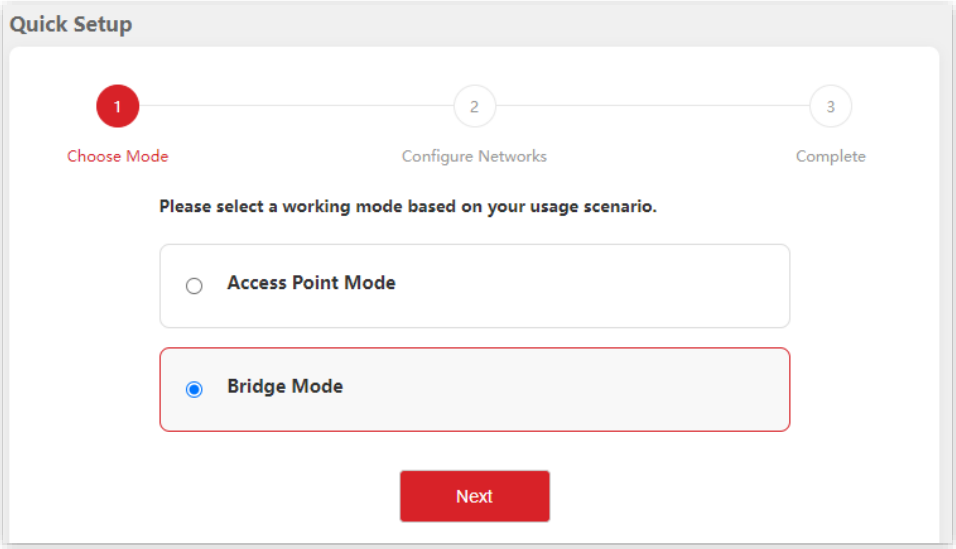
Configure bridge mode

In this mode, the AP is wirelessly bridged to the Wi-Fi network of the upstream device (such as a wireless router or AP) to extend the Wi-Fi network coverage of the upstream device. The application topology is shown below.



Procedure for configuring bridge mode

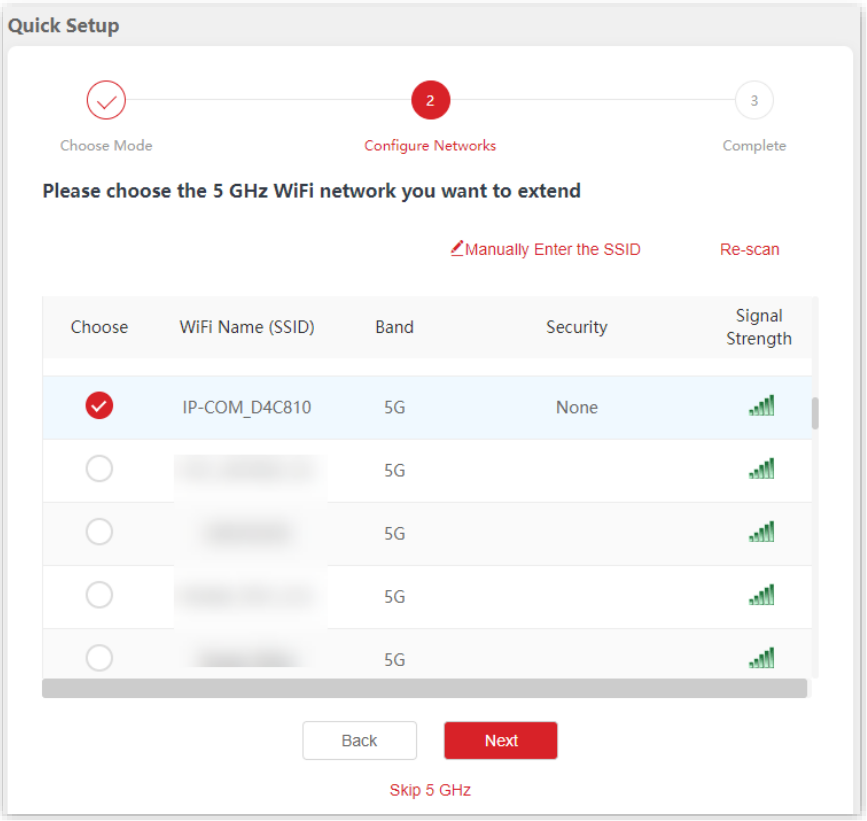
1. Set the working mode of the AP to **Bridge Mode**, and click **Next**.



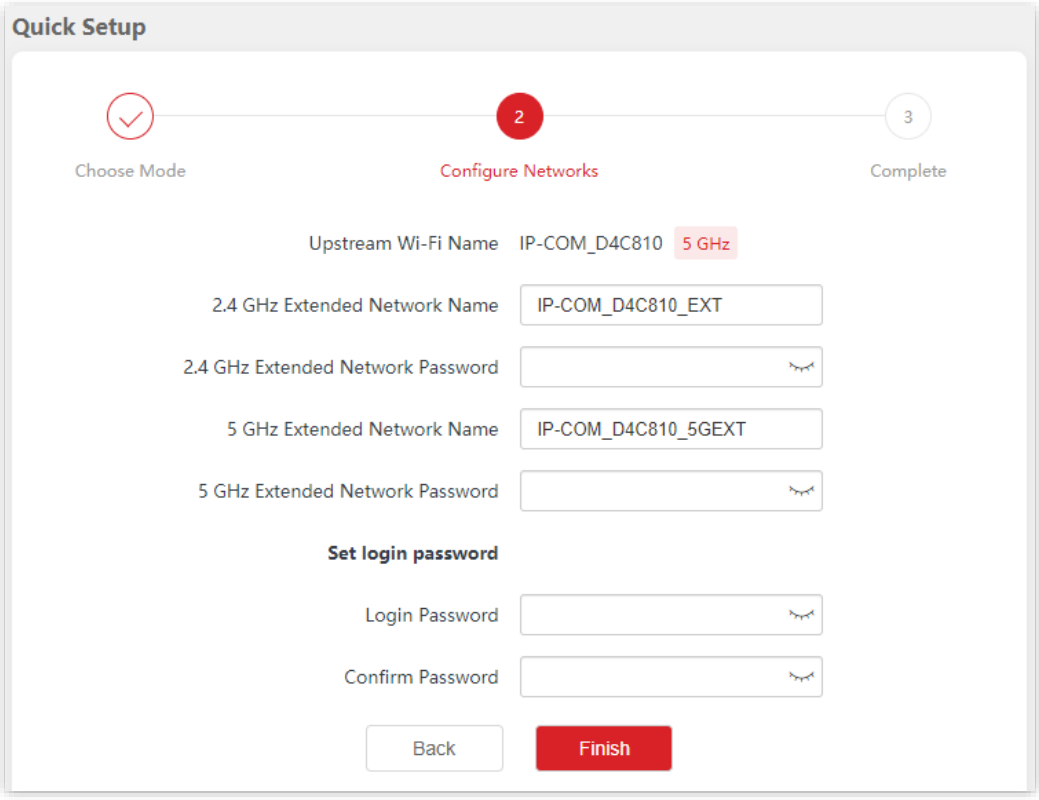
2. Select the upstream device's Wi-Fi to extend the network. If it has a password, enter its password below **Security**. Then click **Next**. Here, **IP-COM_D4C810** is used as an example of the 5 GHz Wi-Fi network to be extended.

Tip

- If you need to extend the 2.4 GHz Wi-Fi or if the upstream device's Wi-Fi only supports the 2.4 GHz frequency band, click **Skip 5 GHz** at the bottom of the page to extend the 2.4 GHz Wi-Fi.
- If the upstream Wi-Fi network is hidden, click **Manually Enter the SSID**, and enter the upstream Wi-Fi name and password manually.

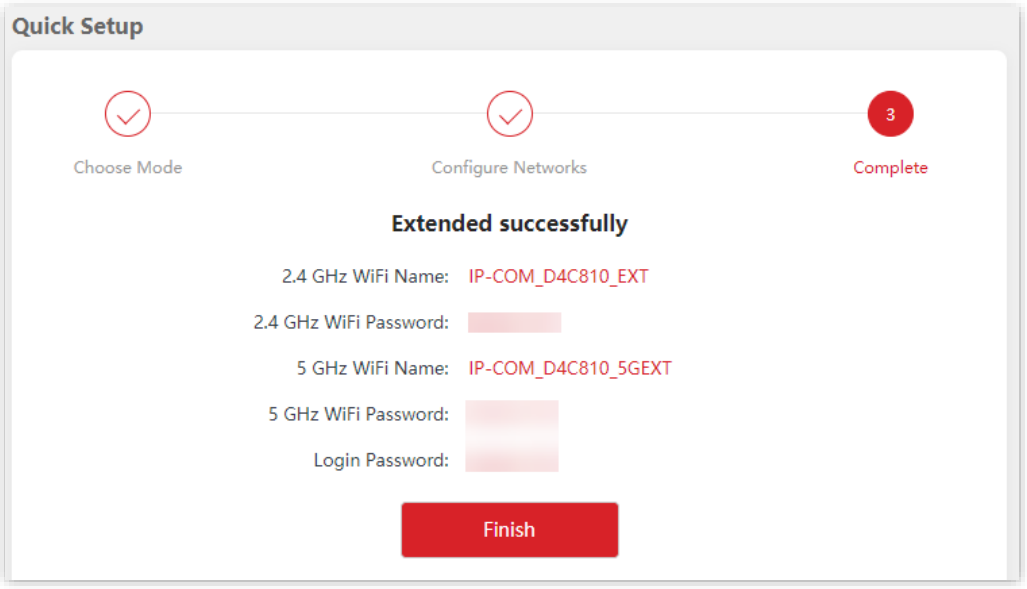


3. Confirm the name and password of the extended Wi-Fi and modify them as required.
4. Set the login password for the AP.
5. Click **Finish**.



---End

After the configuration is completed, you can use Wi-Fi-enabled devices (such as smartphones) to connect to the extended Wi-Fi you set up to access the internet. If you want to use a Wi-Fi-enabled device to log in to the AP's web UI for further configuration (see Chapter 2 and subsequent sections), connect to the AP's newly configured Wi-Fi.



2 Login and logout

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.

2.1 Log in to the web UI

If you are using the AP for the first time or have restored it to factory settings, and the AP is not managed by any network device or cloud platform, refer to the Getting started with AP section to log in to the web UI of the AP.

For other situations, refer to the following instructions to log in.

Procedure for logging in to the web UI of the AP

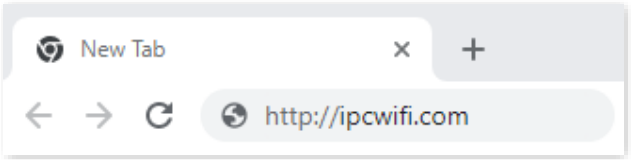
1. Connect a management device to the AP.
   - Smartphone or laptop: Connect to the AP's Wi-Fi.

   Tip

   - If you have configured the AP's Wi-Fi network through the AP web UI, the Wi-Fi name (SSID) and password are the ones you set.
   - If the AP is managed by a controller (including a router with AP management functions) or a cloud platform, log in to the controller's web UI or the cloud platform to check the AP's Wi-Fi name and password.

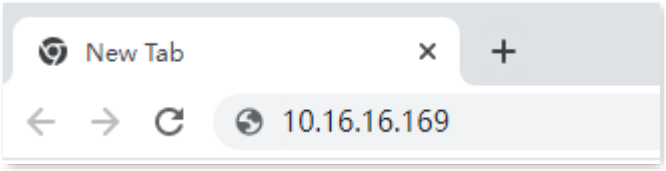
   - Desktop computer: Connect the computer to the AP (or to a switch connected to the AP) using an Ethernet cable.
2. Open a web browser on the management device, enter the AP's management address in the address bar, and access it.
   - Smartphone or laptop: Enter **http://ipcwifi.com**

     The following figure uses a laptop as an example.

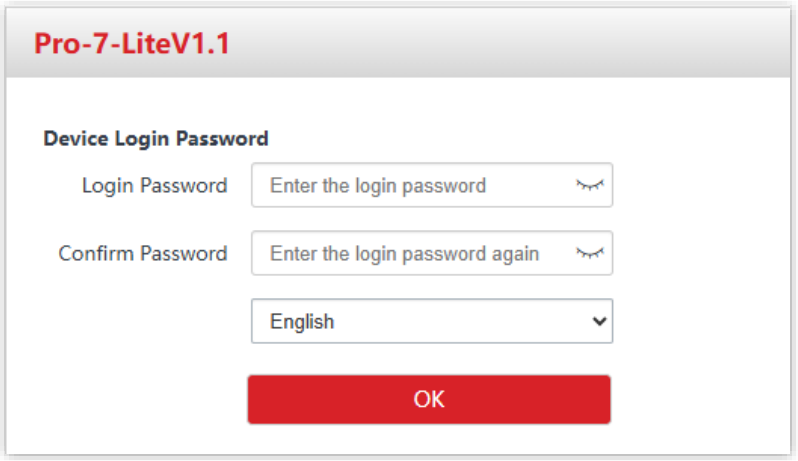


- Desktop computer: Enter the AP's management IP address or internet IP address.

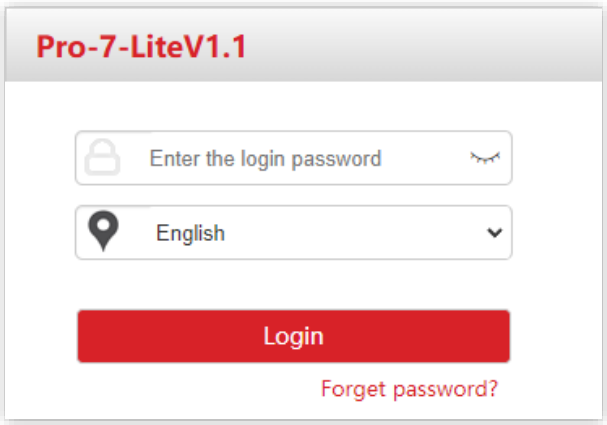
  The default management IP address is **10.16.16.169**. By default, the internet IP address is obtained from the DHCP server on the LAN (If no DHCP server is available on the LAN where the AP is located, the default internet IP address is **192.168.0.254**). The following figure uses **10.16.16.169** as an example.



3. When you log in for the first time, if prompted to set the AP login password, enter a password and click **OK**.



4. Enter the login password, and click **Logi**n to log in to the web UI of the AP.



---End

Tip

If the page for setting the login password or the login page does not appear, try the following solutions:

- If you log in using a Wi-Fi-enabled device such as a laptop, ensure that it is successfully connected to the AP's Wi-Fi. If logging in using your smartphone, ensure that the cellular network (mobile data) of the device is disabled.
- If you log in using a computer over a wired connection, ensure that the Ethernet cable is connected correctly and securely.
- Try to use the IP address to log in to the web UI of 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. If not, use **192.168.0.254** 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, except 168 and 169, and is unused) of the computer or smartphone to the IP address within the same network segment as the AP.
- When logging in using the IP address, if there are at least two APs on the network, it is recommended to connect each AP to the network one by one and change its IP address to ensure that each AP has a unique IP address.
- If the QVLAN function is enabled, ensure that the VLAN ID of the connected Wi-Fi matches the AP's management VLAN ID.
- Clear your browser's cache or use a different browser, and try logging in again.
- Reset the AP and try again.

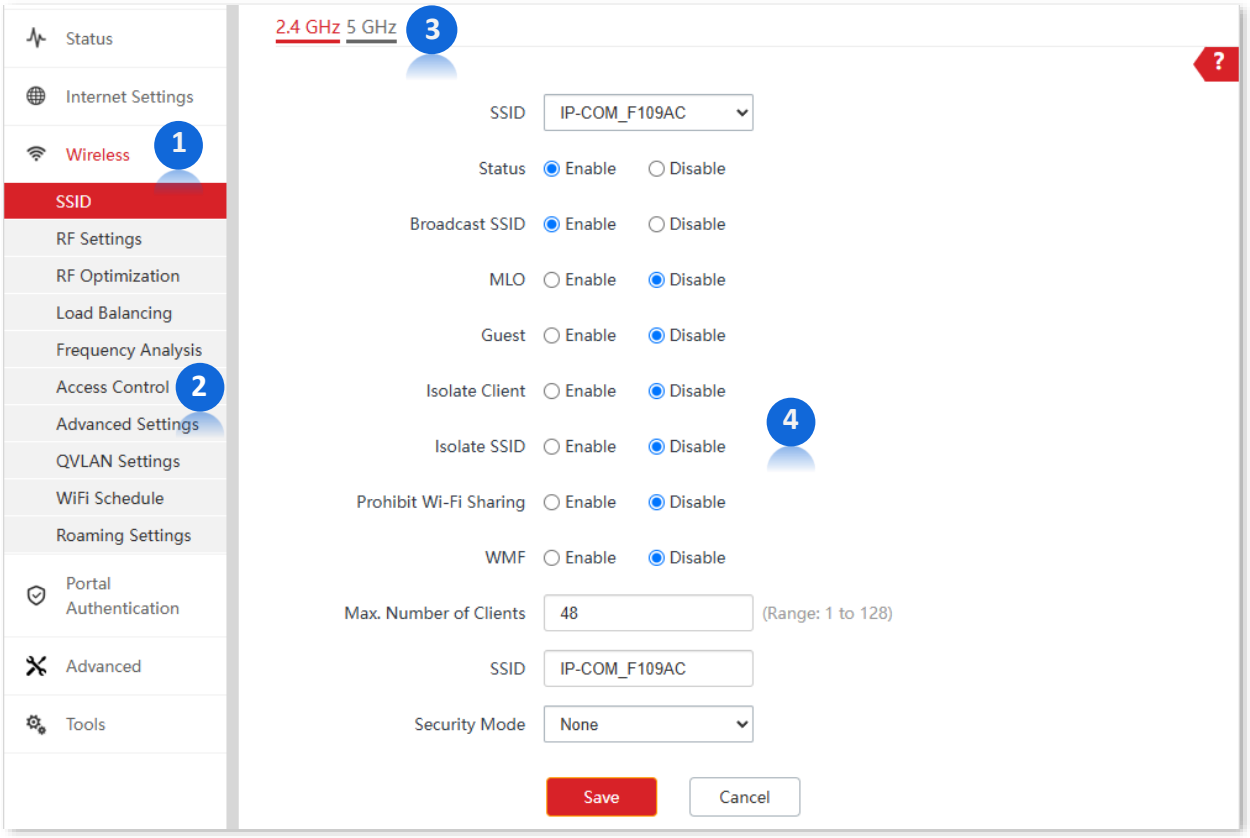
After logging in to the web UI of the AP, you can now configure the AP.

2.2 Log out of the web UI

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

2.3 View the layout of the web UI

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



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.

2.4 Use common buttons

Buttons commonly used on the web UI are illustrated 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.

3 Manage 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.

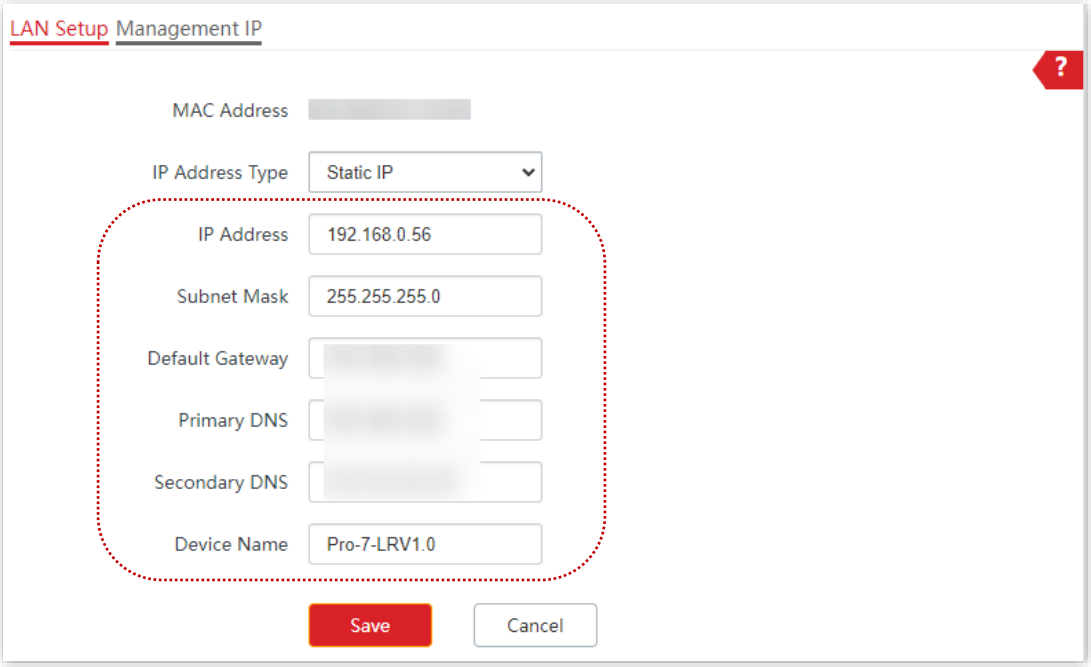
3.1 Configure LAN settings

By default, the AP obtains its internet IP address (LAN IP address) from a DHCP server on the LAN. If no DHCP server is available, the AP uses 192.168.0.254.

You can view the MAC address of the AP's LAN port and configure the IP address, device name, and other related parameters.

Procedure for configuring LAN settings (Pro-7-LR V1.0 is used as an example here.)

1. Log in to the web UI of the AP.
2. Navigate to **Internet Settings** > **LAN Setup** > **LAN Setup**.
3. Set the **IP Address Type** to specify how the AP obtains its internet IP address. If **Static IP** is selected, manually specify the AP's IP address, subnet mask, default gateway, and DNS server.
4. Click **Save**. The following figure is for reference only.



---End

Tip

If you have changed the AP's internet IP address, you need to use the new IP address to log in to the web UI of the AP.

Parameter description

Parameter	Description
MAC Address	Specifies the MAC address of the LAN port of the AP.
IP Address Type	Specifies how the AP obtains its IP address. – **Static IP**: It indicates that the IP address, subnet mask, gateway, and DNS server of the AP are set manually. This mode is suitable for networks with only one or a few APs. – **DHCP (Dynamic IP Address)**: It indicates that the IP address, subnet mask, gateway, and DNS server information of the AP are obtained from a DHCP server on your LAN. This mode is suitable for networks with a large number of APs. Tip When **DHCP (Dynamic IP Address)** is selected as the IP address type, the AP's IP address may change. Before logging in to the web UI of the AP, check the client list on the DHCP server in the network to find the IP address assigned to the AP, and then use that IP address to log in.
IP Address	Specifies the internet IP address (LAN IP address) of the AP. The web UI of the AP is accessible at this IP address. Tip – Before using this IP address to log in to the web UI of the AP, ensure that the IP address of the LAN user is in the same subnet as the AP's IP address. – If the QVLAN function is enabled, only users connected to the AP's management VLAN member ports can use this IP address to log in to the web UI of the AP.
Subnet Mask	Specifies the subnet mask corresponding to the AP's LAN port IP address. It is used to define the address range of the device's network segment.
Default Gateway	Specifies the default gateway corresponding to the AP's LAN port IP address. It is generally set to the LAN port IP address of the egress router.
Primary DNS	Specifies the primary DNS server of the AP. If the egress router has a DNS proxy function, you can enter the LAN port IP address of the egress router here. Otherwise, enter the correct IP address of the DNS server.

Parameter	Description
Secondary DNS	Specifies the IP address of the secondary DNS server of the AP. This parameter is optional. If there are two DNS server IP addresses, you can enter the secondary IP address in this field.
Device Name Remark	You are recommended to change the name of the AP to indicate the location of the AP (such as Hall), so that you can easily identify the AP when managing many APs.
AC Management IP	The AP that is configured with this option will be used as a lighthouse AP. The AP will discover the AC based on the AC address filled in. At the same time, it will guide other APs in the local area network to discover AC. If the current AP is offline, other APs that have been managed by AC in the same local area network will replace it and guide other APs in the LAN to add AC. There is only one lighthouse AP in a local area network. Tip This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.
Optimize Ethernet for	Specifies the Ethernet mode of the PoE power-supply port of this AP. – **Fast Speed (Auto Negotiation)**: This mode features a high transmission rate but short transmission distance. Generally, this mode is recommended. – **Longer Distance (10 Mbps Full Duplex)**: This mode features a long transmission distance but relatively low transmission rate (usually 10 Mbps). The **Longer Distance (10 Mbps Full Duplex)** mode is recommended only if the Ethernet cable that connects the PoE power-supply port of the AP to a peer device exceeds 100 meters. In this case, the connected LAN port of the peer device must work in auto-negotiation mode. Otherwise, the PoE power-supply port of the AP may not be able to properly transmit or receive data. Tip This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.

3.2 Configure management IP

Users within the LAN can access the AP’s management IP address to log in to its web UI. The default management IP address of the AP is 10.16.16.169.

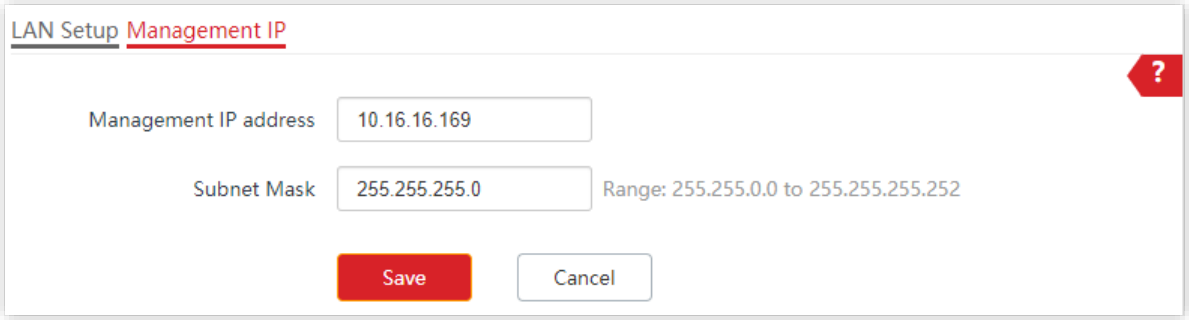
Tip

Before using this IP address to log in to the web UI of the AP:

- Ensure that the IP address of the LAN user is in the same subnet as the AP's IP address.
- If the QVLAN function is enabled, ensure that the VLAN ID of the user-connected AP Wi-Fi (or port) matches the AP's management VLAN ID.

Procedure for configuring management IP (Pro-7-LR V1.0 is used as an example here.)

1. Log in to the web UI of the AP.
2. Navigate to **Internet Settings** > **LAN Setup** > **Management IP**.
3. Modify the **Management IP address** and **Subnet Mask** as required.
4. Click **Save**.



---End

After the configuration is completed, you need to use the new management IP address to log in to the web UI of the AP.

3.3 Use the AP as a DHCP server

Tip

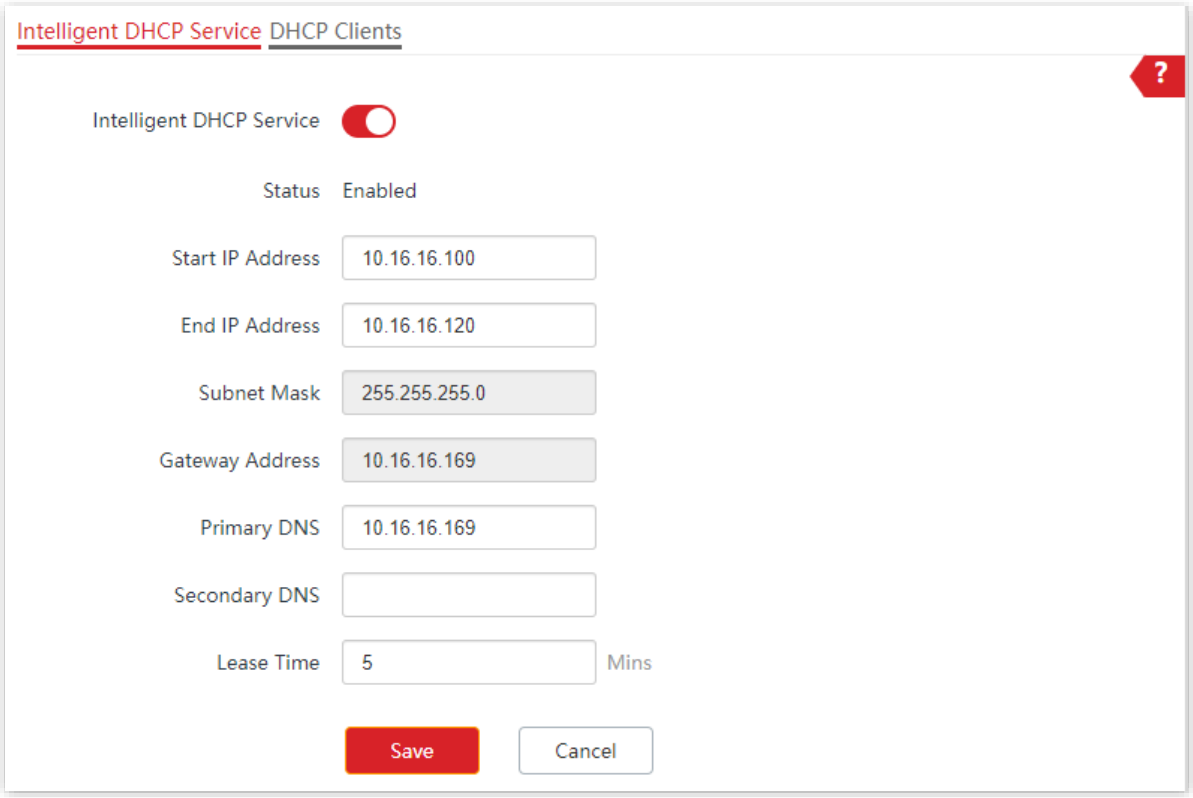
Pro-7-LR V1.0 is used as an example here. This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.

The DHCP service is used when there is no other DHCP server in the LAN where the AP is located. In this case, the AP acts as a DHCP server and automatically assigns IP addresses to devices on the LAN.

The intelligent DHCP service function is enabled by default. When there are other DHCP servers in the LAN where the AP is located, or when the AP is managed by an AC (IP-COM wireless controller or an IP-COM router that supports AP management), this function will be automatically disabled. If there are no other DHCP servers in the LAN and the AP is not managed by an AC, the AP must be restored to its factory settings to re-enable this function.

3.3.1 Change DHCP server settings

1. Log in to the web UI of the AP.
2. Navigate to **Internet Settings** > **Intelligent DHCP Service** > **Intelligent DHCP Service**.
3. Modify the AP's DHCP server parameters as required.
4. Click **Save**.



---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.

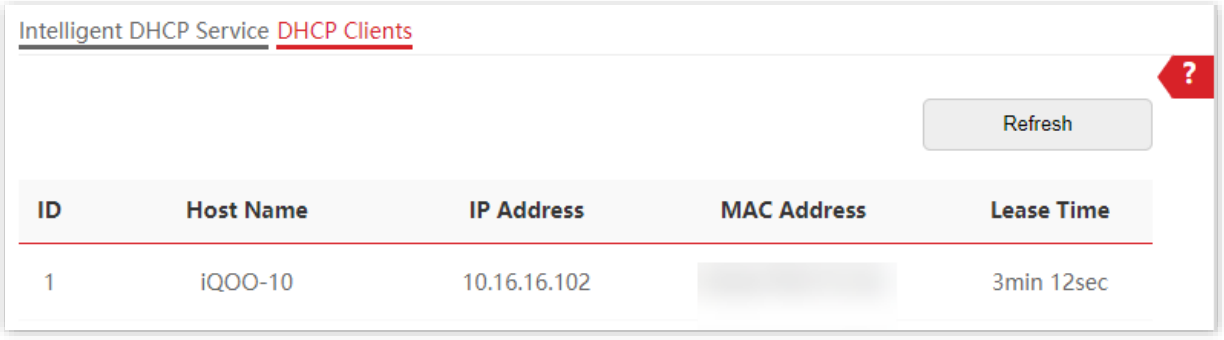
Parameter	Description
Start IP Address	Specify the start IP address or end IP address of the DHCP address pool. The DHCP address pool is the range of IP addresses that can be assigned to clients by the AP's intelligent DHCP server. Tip After changing the AP's management IP address, if the new management IP address is not in the same subnet as the original IP address, the system will automatically adjust the AP's DHCP address pool to match the subnet of the new management IP address.
End IP Address	
Subnet Mask	Specifies the subnet mask assigned by the AP's DHCP server to clients. By default, it is the subnet mask corresponding to the AP's management IP address.
Gateway Address	Specifies the gateway IP address assigned by the AP's 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 AP's DHCP server to clients.
Secondary DNS	Specifies the IP address of the secondary DNS server assigned by the AP's DHCP server to clients. This parameter is optional. Leave it blank if the DHCP server does not provide a secondary DNS server address.
Lease Time	Specifies the validity period of an IP address assigned by the AP's DHCP server to clients. When the lease time expires: – If a LAN client is still connected to the AP, the LAN client will renew the lease and continue to keep the IP address. – If a LAN client is no longer connected to the AP, the AP will release its IP address. If another LAN client requests an IP address, the AP can assign the released IP address to the new client.

3.3.2 View DHCP clients

When the AP is acting as a DHCP server, you can view information such as the host name and IP address of devices that obtained an IP address from the AP.

Procedure for viewing DHCP clients

1. Log in to the web UI of the AP.
2. Navigate to **Internet Settings** > **Intelligent DHCP Service** > **DHCP Clients**.
3. (Optional) Click **Refresh** to view the latest DHCP client list.


Intelligent DHCP Service
DHCP Clients
Refresh
ID
Host Name
IP Address
MAC Address
Lease Time
1
iQOO-10
10.16.16.102
3min 12sec

---End

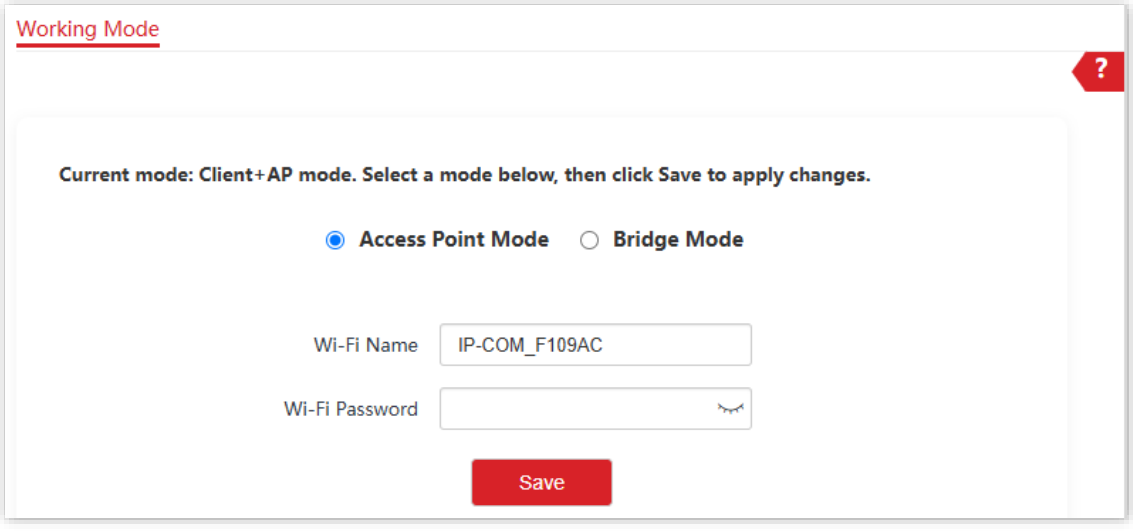
4 Change the working mode

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.

4.1 Switch to AP mode

To switch the working mode from **Client+AP** (**Bridge**) **Mode** to **Access Point Mode**, follow these steps.

1. Log in to the web UI of the AP.
2. Navigate to **Advanced** > **Working Mode**.
3. Select **Access Point Mode**.
4. Set the **Wi-Fi Name** and **Wi-Fi Password**. By default, the 2.4 GHz and 5 GHz bands use the same Wi-Fi name.
5. Click **Save**. The following figure is for reference only.



---End

After the configuration is completed, you can use Wi-Fi-enabled devices (such as smartphones) to connect to the AP Wi-Fi you configured to access the internet.

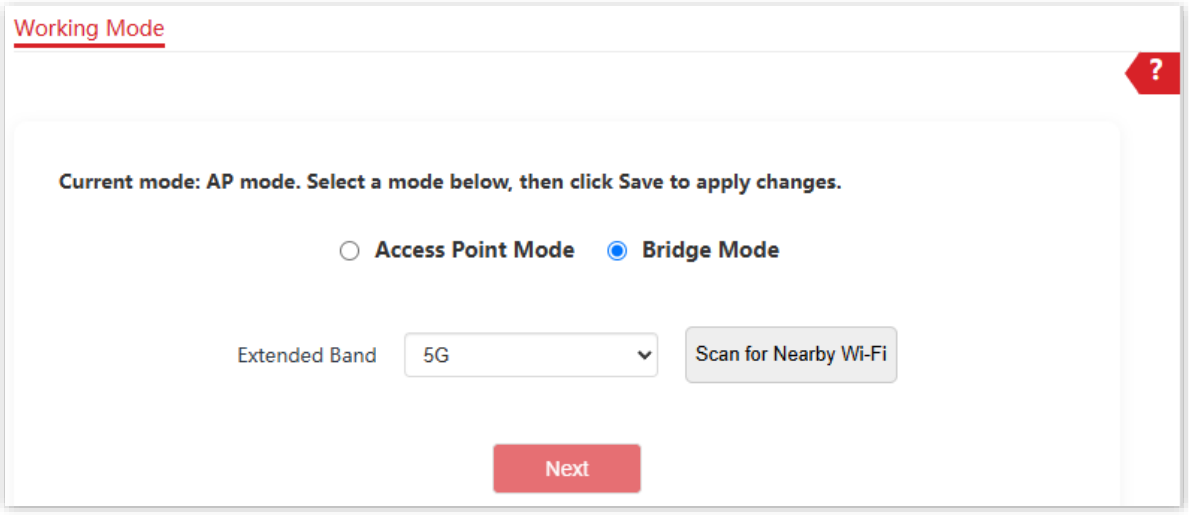
4.2 Switch to bridge mode

To switch the working mode from **Access Point Mode** to **Bridge Mode**, follow these steps.

1. Log in to the web UI of the AP.
2. Navigate to **Advanced** > **Working Mode**.
3. Select **Bridge Mode**.
4. Select **Extended Band** as required, and click **Scan for Nearby Wi-Fi**.

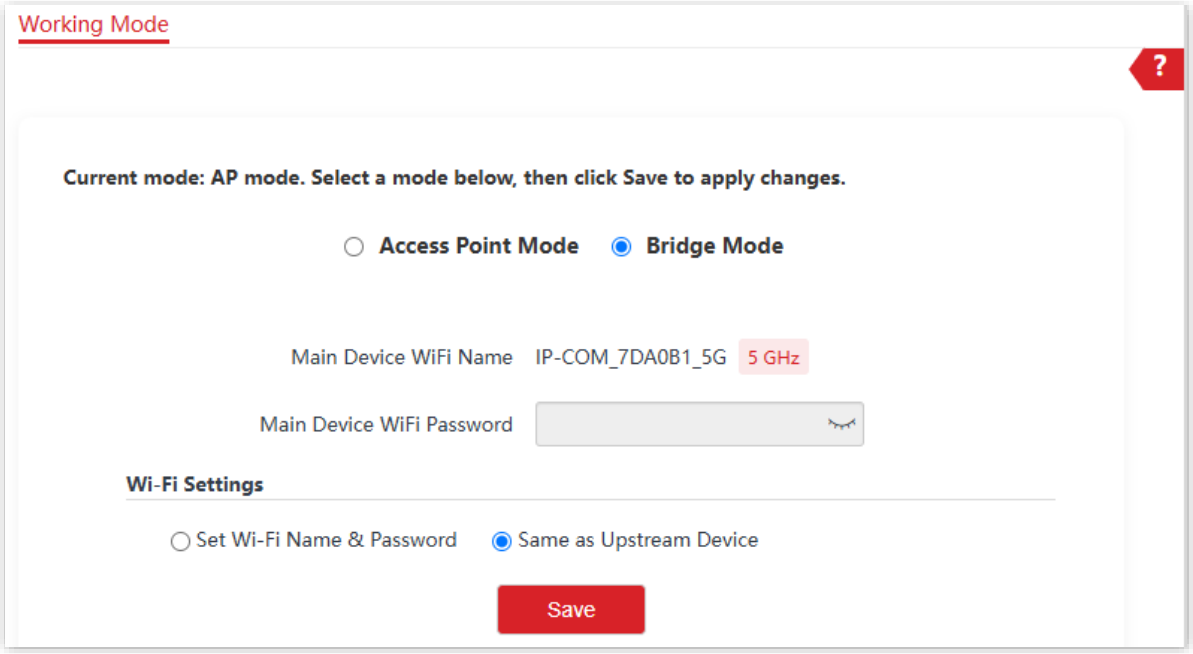
Tip

If no nearby Wi-Fi networks are found, navigate to **Wireless** > **RF Settings** and ensure that the Wi-Fi network for the corresponding frequency band is enabled. Then try again.



5. Select the Wi-Fi network to be extended (the primary device's Wi-Fi) from the scanned Wi-Fi list, and click **Next** at the bottom of the page.
6. If the primary device's Wi-Fi is encrypted, enter its Wi-Fi password. Configure this AP's Wi-Fi name and password as required, then click **Save**.

   You can configure a separate Wi-Fi network for this AP as required, or select **Same as Upstream Device** to use the same Wi-Fi name and password as the primary device.



---End

After the configuration is completed, you can use Wi-Fi-enabled devices (such as smartphones) to connect to the AP Wi-Fi you configured to access the internet.

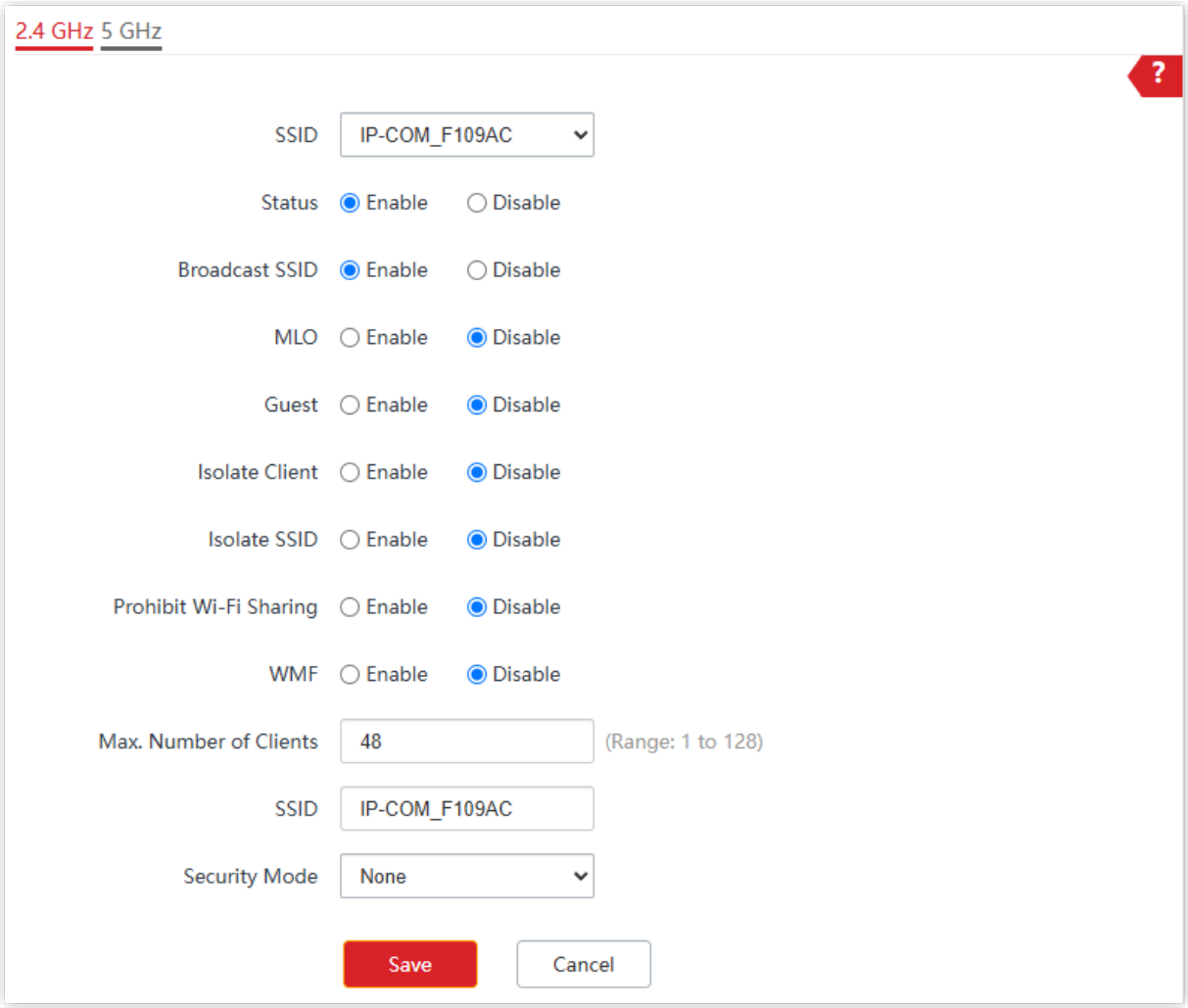
5 Manage wireless settings

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.

5.1 Configure SSID settings

5.1.1 Overview

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



Parameter description

Parameter	Description
2.4 GHz 5 GHz	Used to select the radio band of the AP to be configured.
SSID	Specifies the SSID to be configured. The first SSID displayed on the page under the radio band tab is the primary SSID of the radio band.
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 Wi-Fi network corresponding to the SSID. Disabling broadcast SSID can reduce the visibility of the Wi-Fi network name, but it is not a substitute for security encryption. It is still recommended to use WPA2 or WPA3 and set a strong password.
MLO	Specifies whether to enable the MLO function. Multi-Link Operation (MLO) is one of the core features of Wi-Fi 7 (IEEE 802.11be). After this function is enabled, the AP coordinates multiple links in different frequency bands to establish a multi-band connection with the client, achieving higher bandwidth and lower latency. Tip This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.
Guest	Specifies whether to enable the guest function. After this function is enabled, wireless clients connected to this Wi-Fi network can access the internet, but cannot access the AP's web UI or wireless clients connected to other networks. Setting up a guest network can meet the internet access needs of guests while ensuring the security of the primary network.
Isolate Client	Specifies whether to enable the isolate client function. After this function is enabled, all wireless clients connected to the same Wi-Fi network are completely isolated from one another. They can only access the internet and client devices connected to the AP via Ethernet, such as computers. This feature is suitable for public hotspots in places such as hotels and airports, where isolating wireless clients helps improve network security.

Parameter	Description
Isolate SSID	Specifies whether to enable the isolate SSID function. After this function is enabled, wireless clients connected to different SSIDs of the AP cannot communicate with each other, enhancing the security of the Wi-Fi network.
Prohibit Wi-Fi Sharing	Used to prevent wireless clients connected to this SSID from sharing the current Wi-Fi network with other devices. When enabled, connected clients cannot provide network access to other devices through Wi-Fi sharing. This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.
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 Wi-Fi 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 Wi-Fi network corresponding to an SSID. After this upper limit is reached, new clients cannot connect to the SSID unless some connected clients disconnect.
SSID	Used to change the selected SSID.
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 Wi-Fi network uses radio, which is open to the public, as its data transmission medium. If the Wi-Fi 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 Wi-Fi networks must be encrypted for protection.

The AP supports various security modes for network encryption, including None, 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.

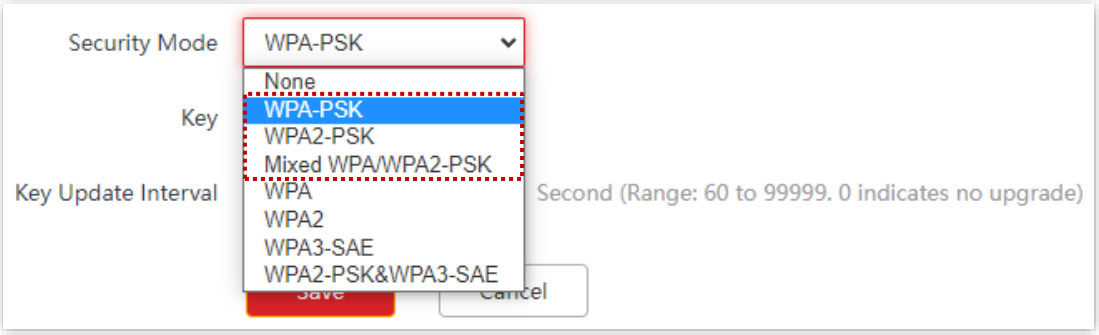
- **None**

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

- **WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK (Mixed WPA/WPA2-PSK)**

  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 Wi-Fi networks. Nevertheless, because the initial pre-shared key for authentication is manually set and all clients use the same key to connect to the same AP, the key may be disclosed unexpectedly. This makes the security modes not suitable for scenarios where high security is required.

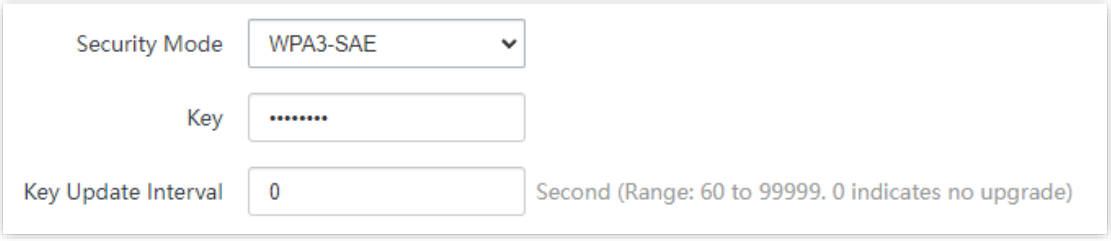


- **WPA3-SAE**

  WPA3-SAE (Simultaneous Authentication of Equals) is the security authentication mechanism used by WPA3-Personal. Compared with WPA2-PSK, it enhances the security of Wi-Fi password authentication and provides better protection against attacks such as offline password cracking. It uses AES encryption.

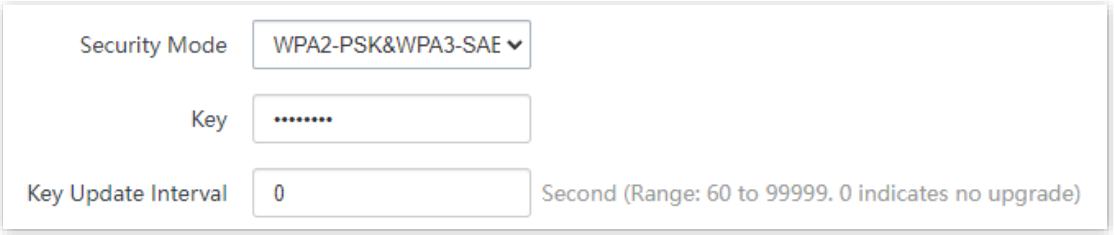
Tip

If your wireless clients do not support WPA3-SAE or you experience Wi-Fi connectivity issues, it is recommended that you set the security mode to WPA2-PSK.



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

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



Parameter description

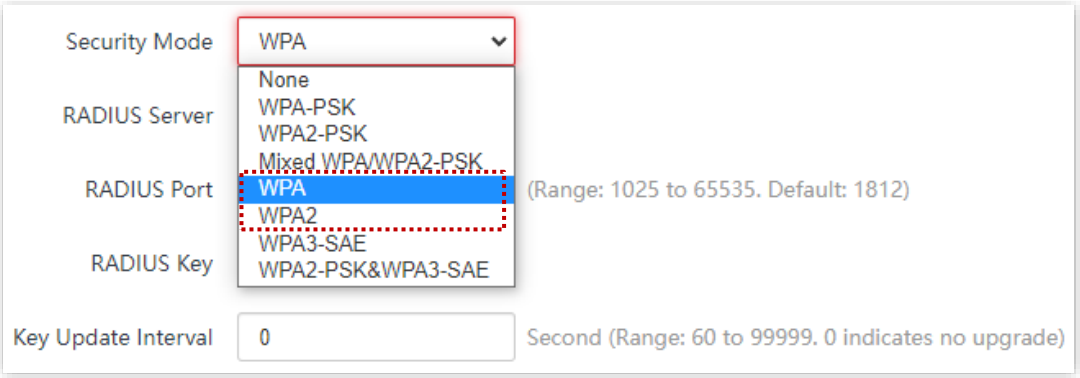
Parameter	Description
Security Mode	Specifies the personal or pre-shared key security mode, including **WPA-PSK**, **WPA2-PSK**, **WPA-PSK&WPA2-PSK (Mixed WPA/WPA2-PSK)**, **WPA3-SAE** and **WPA2-PSK&WPA3-SAE**. – **WPA-PSK**: It indicates that the Wi-Fi network corresponding to the selected SSID is encrypted with WPA-PSK. – **WPA2-PSK**: It indicates that the Wi-Fi 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 Wi-Fi network corresponding to the selected SSID using either WPA-PSK or WPA2-PSK. – **WPA3-SAE**: It indicates that the Wi-Fi network corresponding to the selected SSID is encrypted with WPA3-SAE. – **WPA2-PSK&WPA3-SAE**: The Wi-Fi network adopts the mixed encryption mode of WPA2-PSK/AES and WPA3-SAE/AES to ensure safety.
Key	Specifies a pre-shared WPA key, that is, the password clients use to connect to the Wi-Fi 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**

WPA and WPA2 (Enterprise mode) authenticate users or devices through IEEE 802.1X and EAP instead of using a pre-shared key (PSK) shared by all users. Enterprise mode is typically used with a RADIUS server to centrally manage user identities and wireless access permissions.

Each user authenticates using individual credentials. After successful authentication, the system establishes security keys for each wireless session to protect wireless communications. Therefore, compared with WPA/WPA2-PSK modes that use a shared PSK, WPA and WPA2 in Enterprise mode can reduce the security risks caused by the disclosure of a shared Wi-Fi password.

This mode is suitable for enterprise, school, and other network environments that require centralized management of wireless users and access permissions.



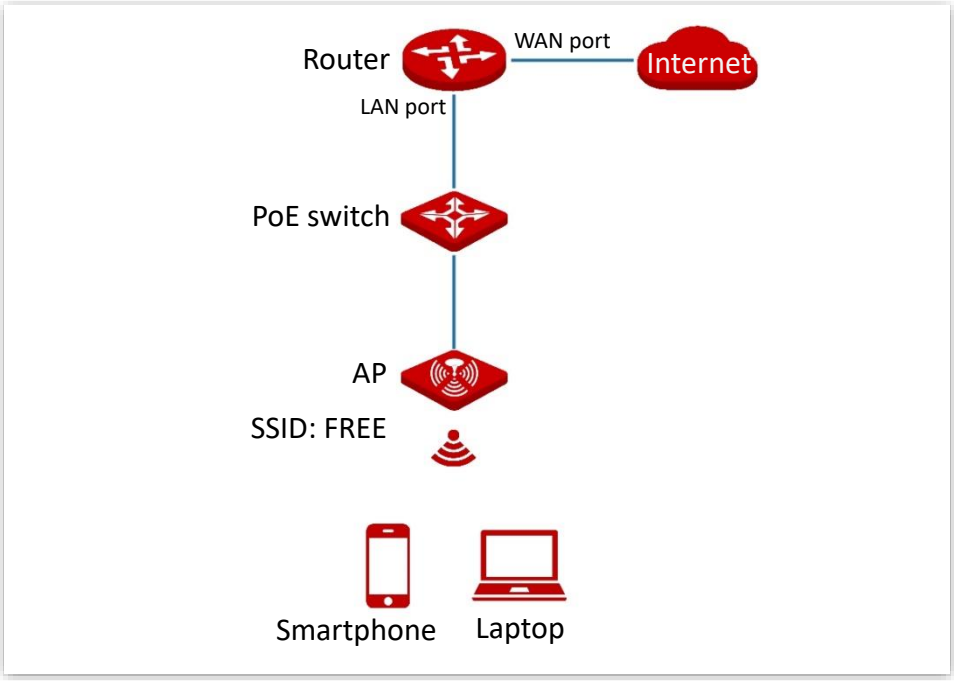
Parameter description

Parameter	Description
Security Mode	The **WPA** and **WPA2** options are available for network protection with a RADIUS server. – **WPA**: It indicates that the Wi-Fi network corresponding to the selected SSID is encrypted with WPA. – **WPA2**: It indicates that the Wi-Fi 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.
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.

5.1.2 Example of setting up an open Wi-Fi network

Networking requirements

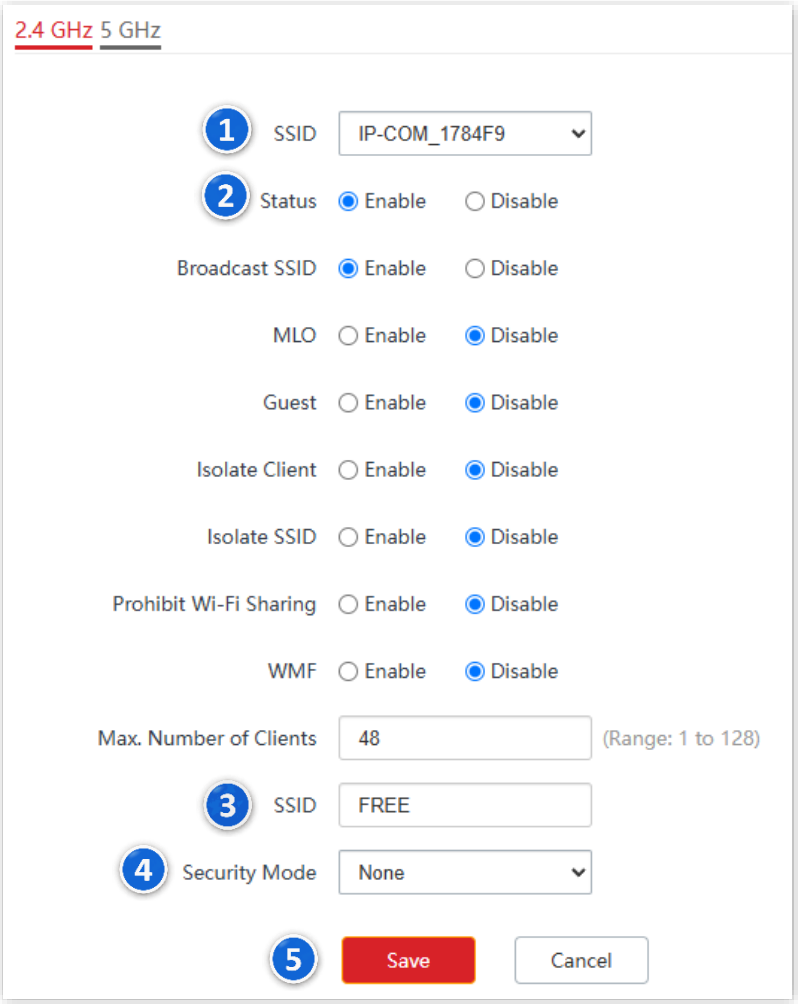
In a hotel lounge, guests can connect to the Wi-Fi network without a password and access the internet through the Wi-Fi network.



Procedure for setting up an open Wi-Fi network

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.
2. Navigate to **Wireless** > **SSID**.
3. Select the second SSID from the **SSID** drop-down list box.
4. Set **Status** to **Enable**.
5. Set **SSID** to **FREE**.
6. Set **Security Mode** to **None**.
7. Click **Save**.



---End

Verification

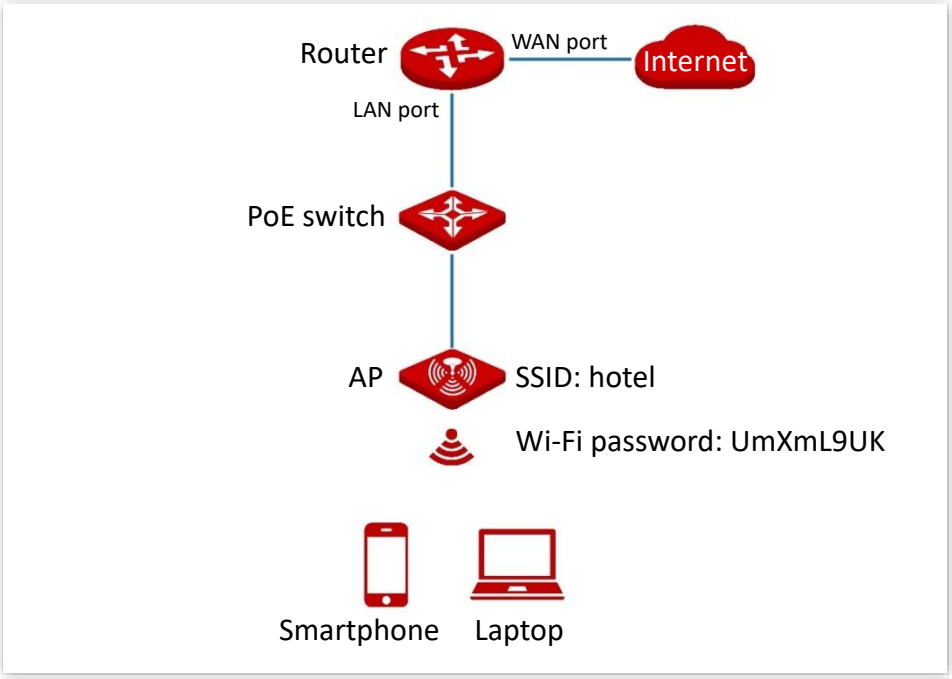
Verify that Wi-Fi-enabled devices can connect to the **FREE** Wi-Fi network without a password.

5.1.3 Example of setting up a Wi-Fi network encrypted with PSK

Networking requirements

A hotel Wi-Fi 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.

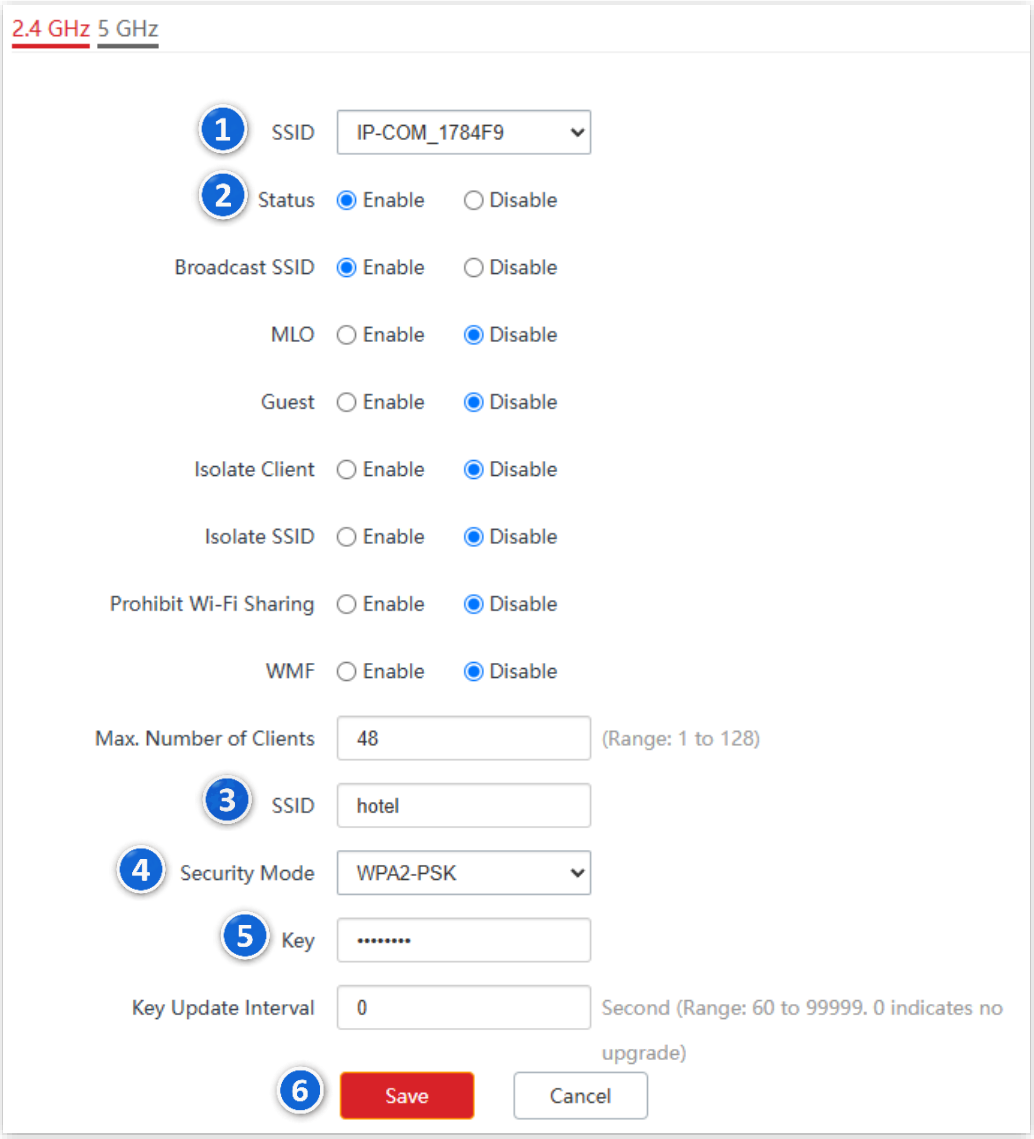
Assume that the SSID is **hotel** and the Wi-Fi password is **UmXmL9UK**. See the following topology.



Procedure for setting up a Wi-Fi network encrypted with PSK

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.
2. Navigate to **Wireless** > **SSID**.
3. Select the second SSID from the **SSID** drop-down list box.
4. Set **Status** to **Enable**.
5. Set **SSID** to **hotel**.
6. Set **Security Mode**, which is **WPA2-PSK** in this example.
7. Set **Key** to **UmXmL9UK**.
8. Click **Save**.



---End

Verification

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

5.1.4 Example of setting up a Wi-Fi network encrypted with WPA or WPA2

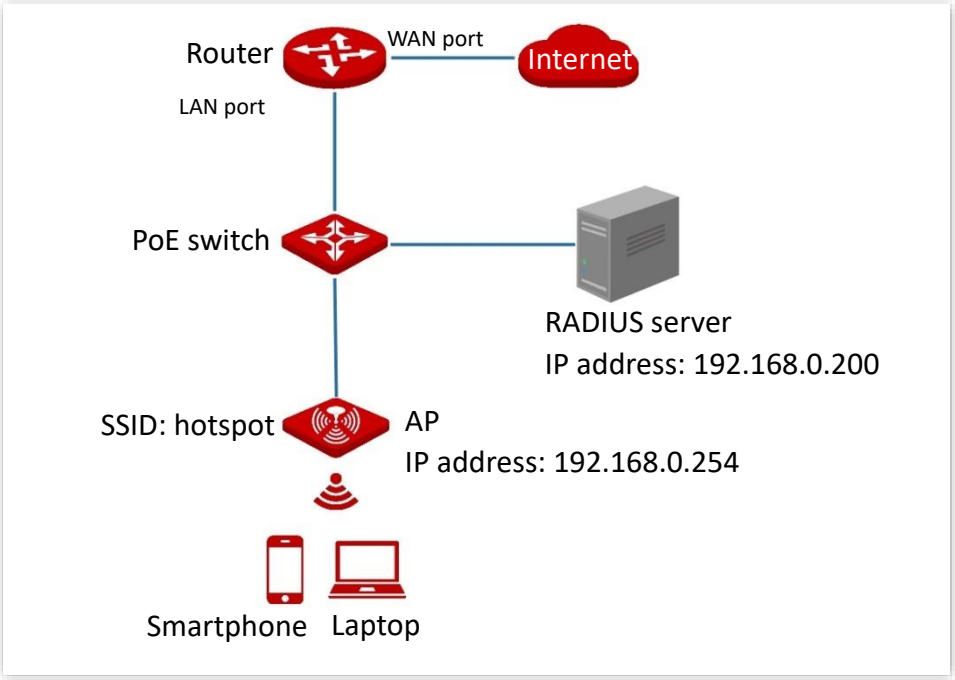
Networking requirements

A highly secure Wi-Fi 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: **UmXmL9UK**

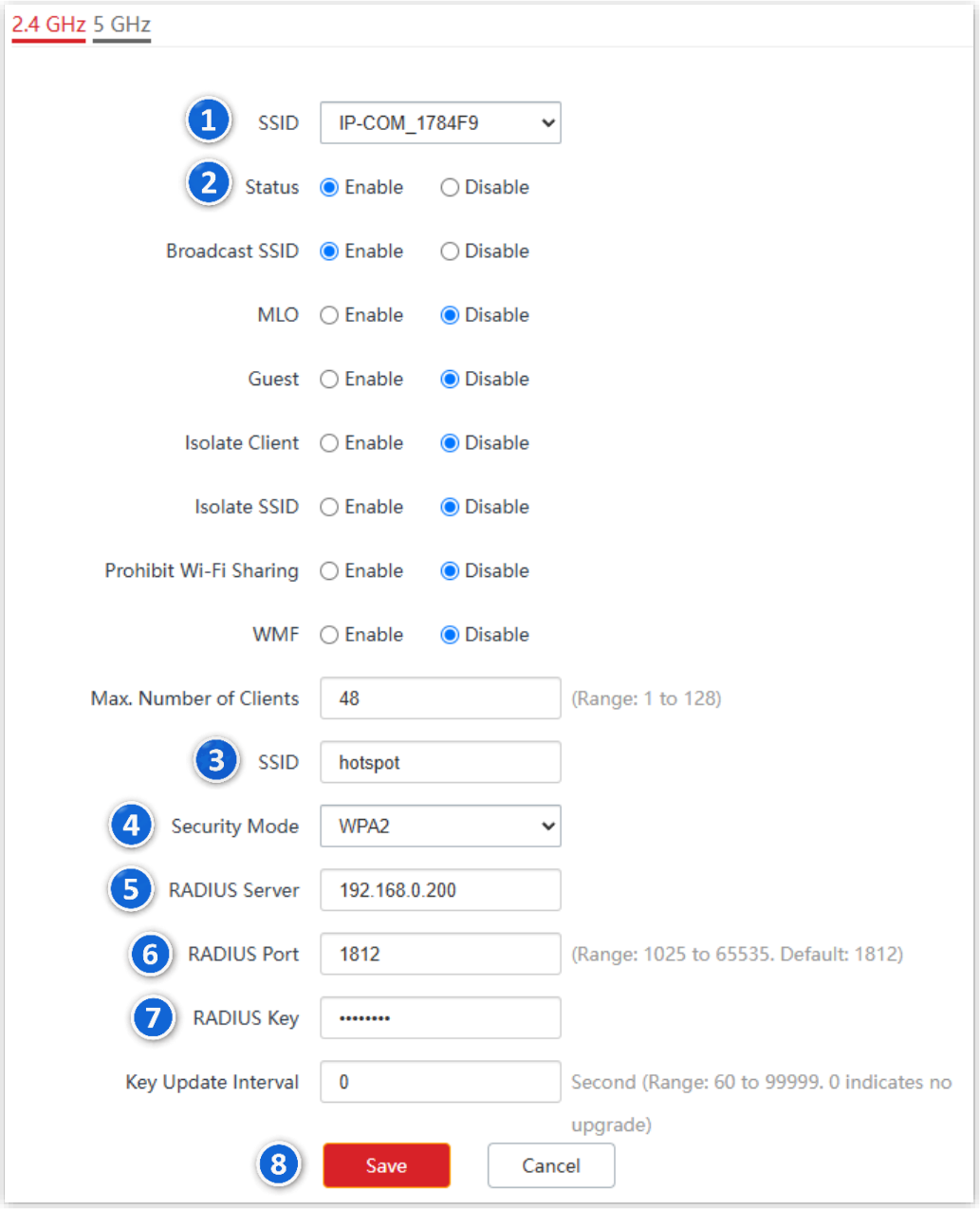


Procedure for setting up a Wi-Fi network encrypted with WPA or WPA2

I. Configure the AP

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.
2. Navigate to **Wireless** > **SSID**.
3. Select the second SSID from the **SSID** drop-down list box.
4. Set **Status** to **Enable**.
5. Set **SSID** to **hotspot**.
6. Set **Security Mode**, which is **WPA2** in this example.
7. Set **RADIUS Server**, **RADIUS Port**, and **RADIUS Key** to **192.168.0.200**, **1812**, and **UmXmL9UK** respectively.
8. Click **Save**.



II. Configure the RADIUS server

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

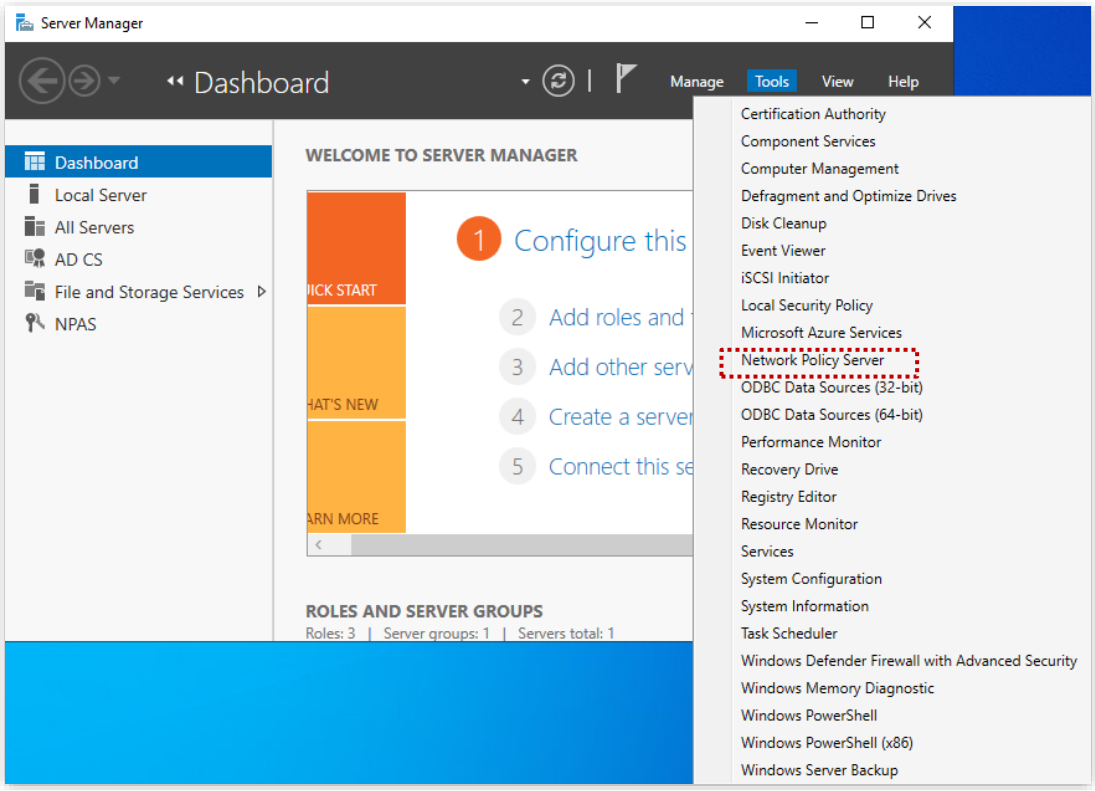
1. Install **Active Directory Certificate Services** and **Network Policy and Access Services**, and deploy the certificate.

   On the **Start** > **Server Manager** > **Dashboard** page, navigate to **Add roles and features** > **Server Selection** > **Server Roles**, and select the **Active Directory Certificate Services** check box. According to the operation wizard, install the **Certification Authority** of **Active Directory Certificate Services** and **Network Policy and Access Services**.

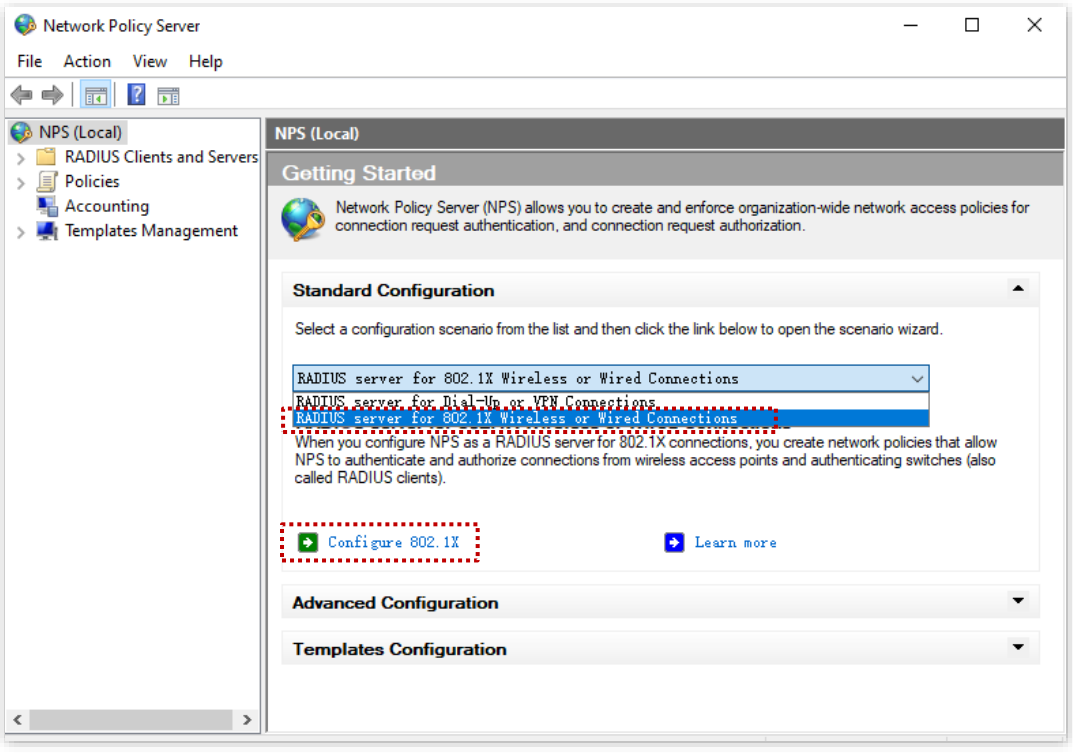
   After the service installation is completed, click in the upper right corner and follow the prompts to deploy the certificate.

2. Configure 802.1X.

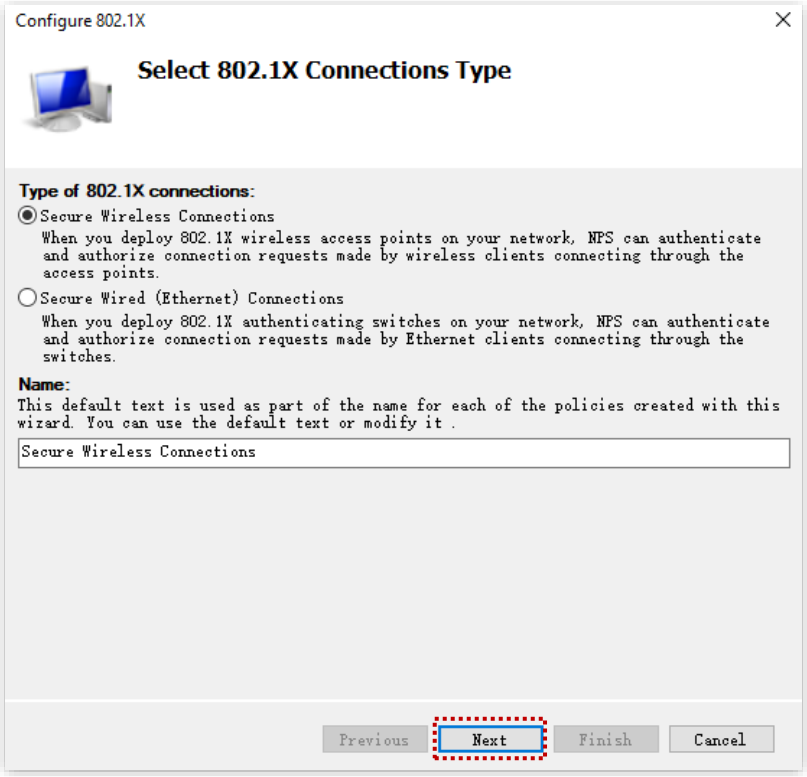
1) Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, and click **Network Policy Server**.



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

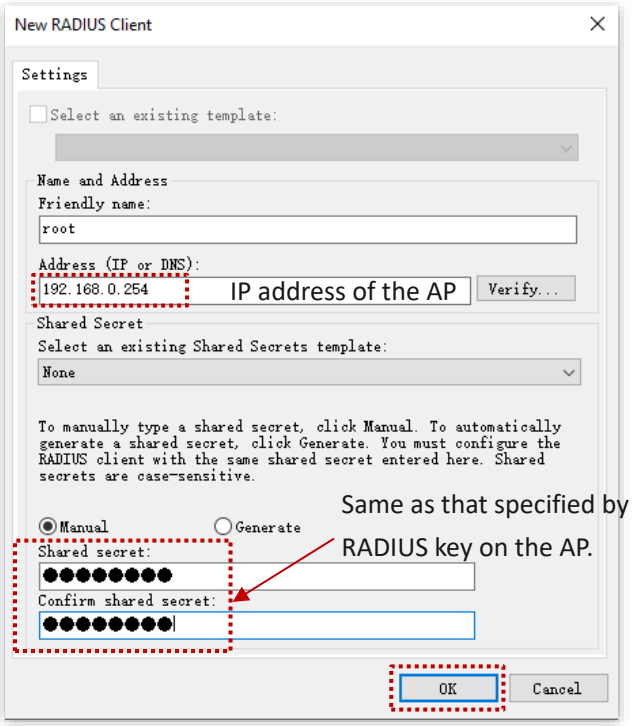


3) Select **Secure Wireless Connections** for **Type of 802.1X connections**. Modify the name as required, which is **Secure Wireless Connections** in this example, and click **Next**.

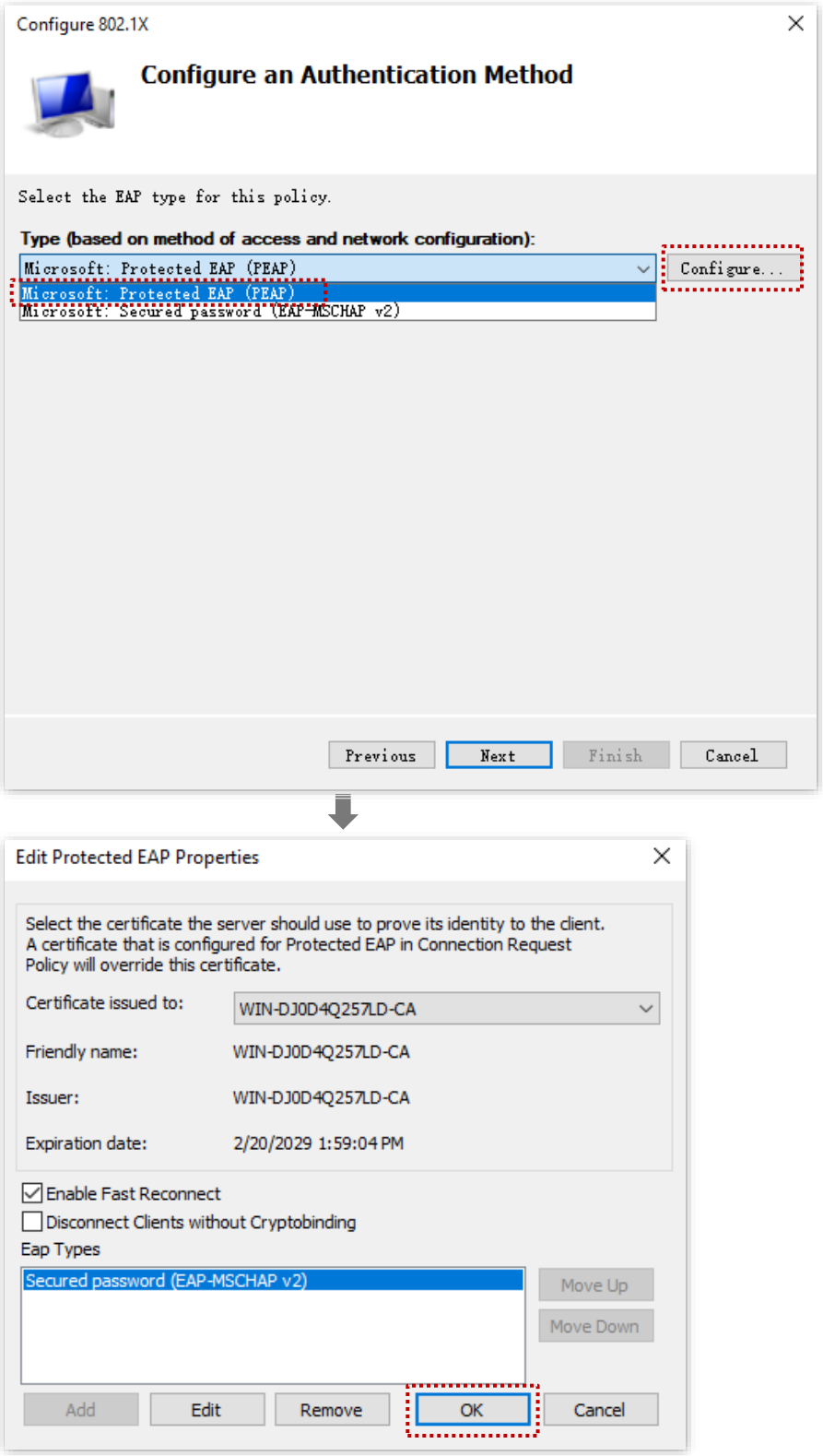


4) On the **Specify 802.1X Switches** page, click **Add**.

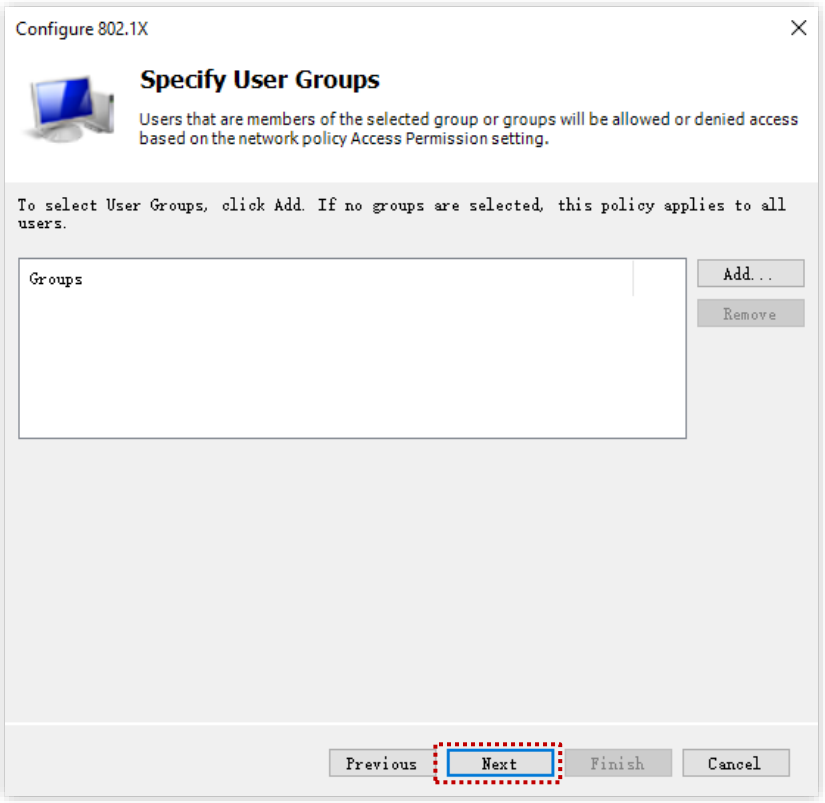
5) Set a RADIUS client name (which can be the name of the AP) and the IP address of the AP. Enter **UmXmL9UK** in the **Shared secret** and **Confirm shared secret** text boxes, and click **OK**.



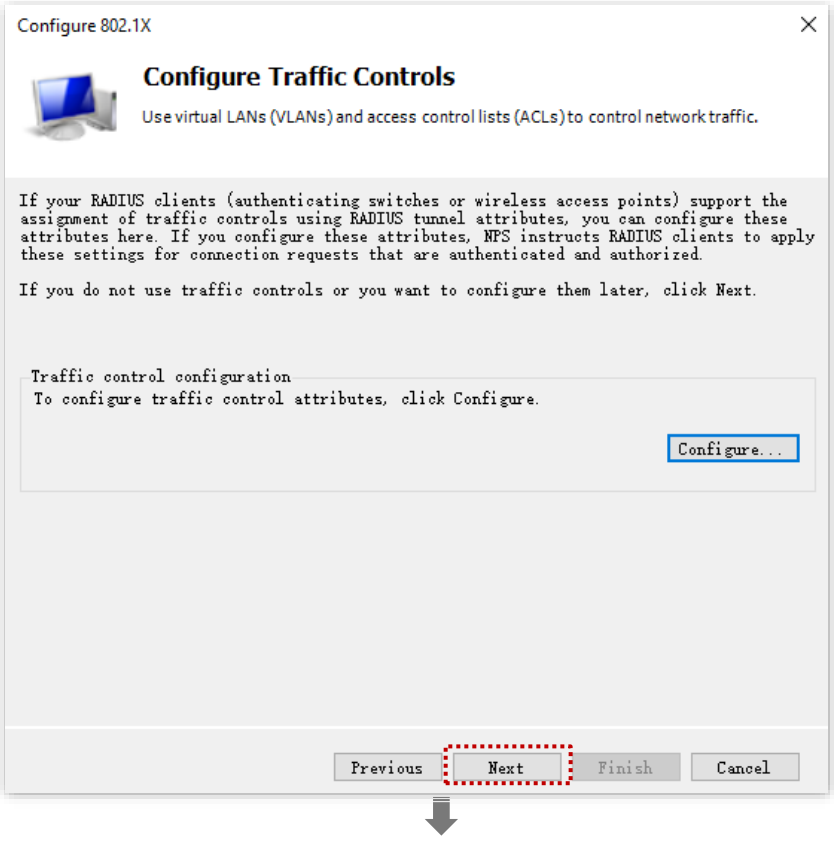
6) Select **Microsoft: Protected EAP (PEAP)** from **Type**, and click **Configure**. Select the certificate deployed in the certificate authority in the previous step, click **OK**, and click **Next** after the configuration is completed.

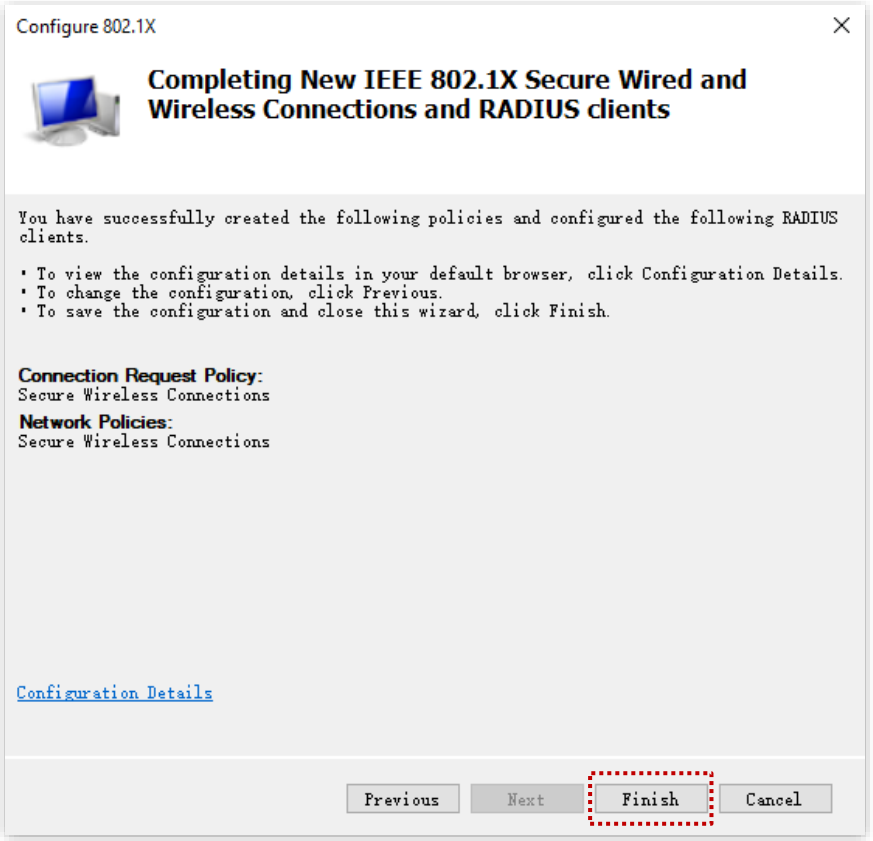


7) Click **Next** on the **Specify User Groups** page.



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



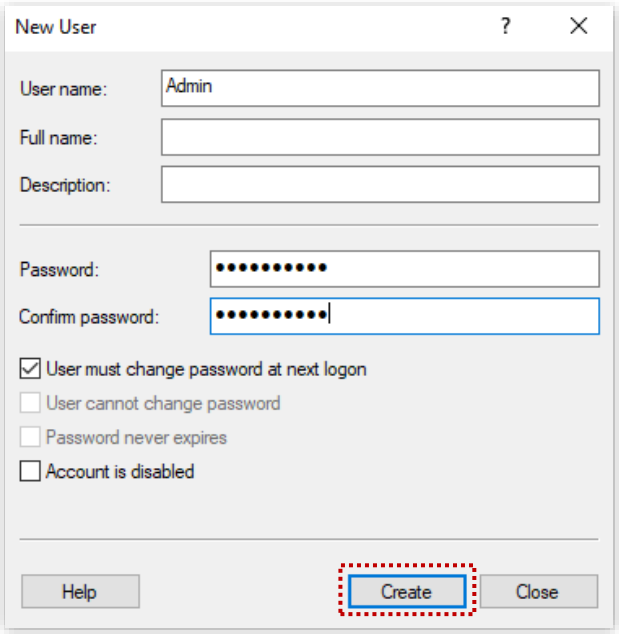


3. Configure the user and user group.

1) Create a user.

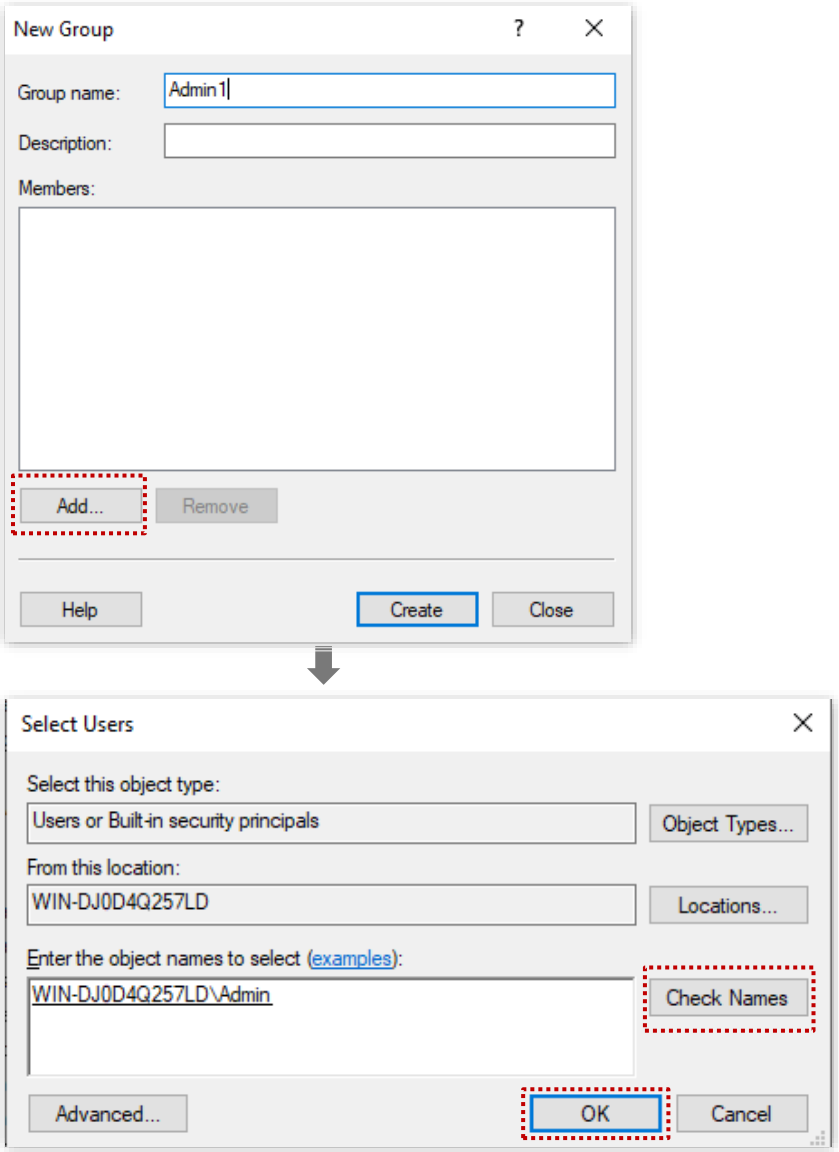
Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, click **Computer Management**, and double-click **Local Users and Groups**.

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



2) Create a user group.

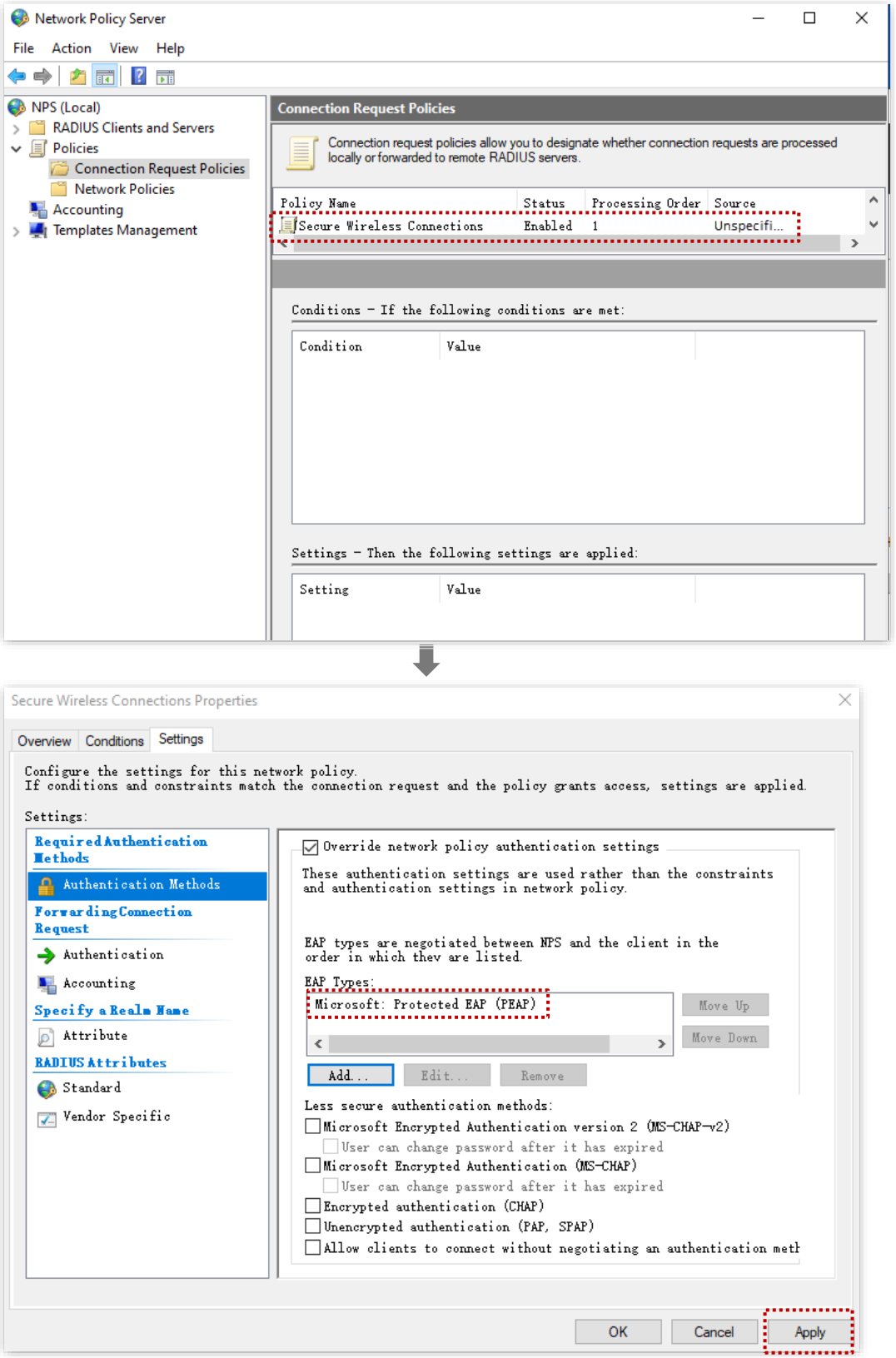
Right-click **Groups**, and select **New Group**. Set **Group name**, which is **Admin1** in this example, and click **Add**. In the **Enter the object names to select** column, enter the created user name, click **Check Names**, and click **OK**. In the **New Group** window, click **Create**.



4. Configure the policies.

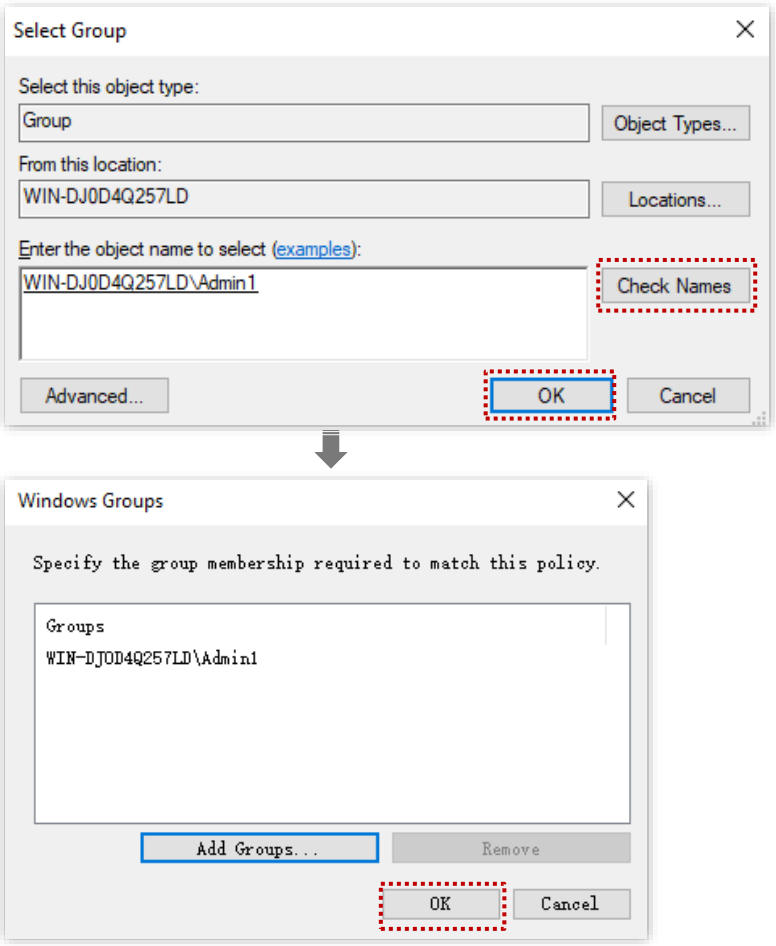
1) Navigate to **Start** > **Server Manager** > **Dashboard**, click **Tools** in the upper right corner, click **Network Policy Server**, and double-click **Policies**.

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



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

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



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 Wi-Fi network, named **hotspot** in this example.
2. Enter the username and password, and tap **Join**.

Tip

If a certificate trust prompt appears, verify that the server certificate is issued by a trusted authority and that the server name and certificate information match the information provided by the administrator. Then click **Trust**.



---End

Verification

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



Tip

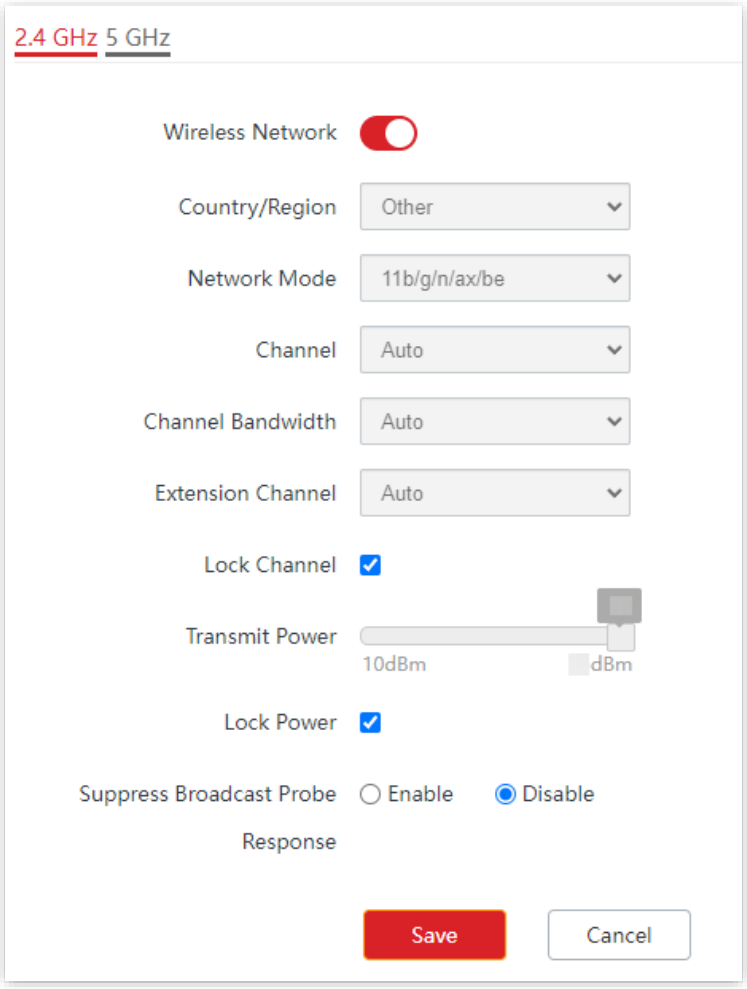
If the connection fails, please:

- Ensure that the RADIUS server and AP can communicate normally (ping each other).
- Try modifying the firewall settings on the RADIUS server: add inbound and outbound rules to allow connections on UDP ports **1812** and **1813**, which are used by RADIUS. For compatibility with legacy ports, also allow connections on UDP ports **1645** and **1646**.

5.2 Configure radio frequency

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.



Parameter description

Parameter	Description
2.4 GHz 5 GHz	Used to select the radio band of the AP to be configured.
Wireless Network	Specifies whether to enable the Wi-Fi 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 Wi-Fi 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**, **11b/g/n/ax** and **11b/g/n/ax/be**, and available options for 5 GHz are **11a**, **11ac**, **11a/n**, **11a/n/ac/ax** and **11a/n/ac/ax/be**. – **11b**: The AP works in 802.11b mode. – **11g**: The AP works in 802.11g mode. – **11b/g**: The AP works in 802.11b/g mode. – **11b/g/n**: The AP works in 802.11b/g/n mode. – **11b/g/n/ax**: The AP works in 11b/g/n/ax mode. – **11b/g/n/ax/be**: The AP works in 11b/g/n/ax/be mode. – **11a**: The AP works in 802.11a mode. – **11ac**: The AP works in 802.11ac mode. – **11a/n**: The AP works in 802.11a/n mode. – **11a/n/ac/ax**: The AP works in 11a/n/ac/ax mode. – **11a/n/ac/ax/be**: The AP works in 11a/n/ac/ax/be mode. Tip The Wi-Fi network modes of the AP may differ with different models of APs. The actual product prevails.
Channel	Specifies the operating channel of the AP. This parameter can be set if Lock Channel is not selected. **Auto**: It indicates that the AP automatically adjusts its operating channel according to the ambient environment. If you frequently experience disconnections, lag, or slow internet speeds when connecting to the AP's Wi-Fi network, try changing the AP's channel. You can use the frequency analysis function to detect channels that are less used and have less interference in the surrounding area.

Parameter	Description
Channel Bandwidth	Specifies the wireless channel bandwidth of the AP. This parameter can be set if 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. – **80 MHz**: 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. – **Auto**: The AP automatically adjusts its channel bandwidth according to the surrounding environment.  The wireless channel bandwidths of the AP may differ with different models of APs. The actual product prevails.
Extension Channel	Used to set the extension channel used when the AP operates in 802.11n mode with a 40 MHz channel bandwidth on the 2.4 GHz band. This parameter can be set if Lock Channel is not selected.
Lock Channel	Used to lock the channel settings of the AP. If this parameter is selected, channel settings including **Country/Region**, **Network Mode**, **Channel**, **Channel Bandwidth**, and **Extension Channel** cannot be changed.
Transmit Power	Specifies the transmit power of the AP. This parameter can be set if Lock Power is not selected. A greater transmit power of the AP offers broader network coverage. You can slightly reduce the transmit power to improve the Wi-Fi 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.
Preamble	Specifies a group of bits located at the beginning of a packet to enable a receiver of the packet to perform synchronization and prepare for receiving data. By default, the **Long Preamble** is selected for compatibility with old network adapters installed on wireless clients. To achieve better synchronization performance of networks, you can select the **Short Preamble**.  This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.

Parameter	Description
Short GI	Specifies whether to enable the short guard interval function. Short GI is short for Short Guard Interval. When wireless channel conditions are good, Short GI shortens the guard interval between adjacent data symbols, thereby improving wireless transmission efficiency and throughput. Actual performance gains depend on factors such as the wireless channel environment and the capabilities of the AP and client devices. Tip This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.
Suppress Broadcast Probe Response	Specifies whether to enable the suppress broadcast probe response function. Wi-Fi-enabled devices may send Probe Request frames to scan for nearby Wi-Fi networks. A Probe Request may contain an SSID field. After receiving a Probe Request, the AP determines whether to respond based on the information in the request and sends a Probe Response containing Wi-Fi network information. Frequent probe exchanges may consume wireless airtime. After this function is enabled, the AP does not respond to broadcast Probe Request frames, reducing wireless airtime overhead.

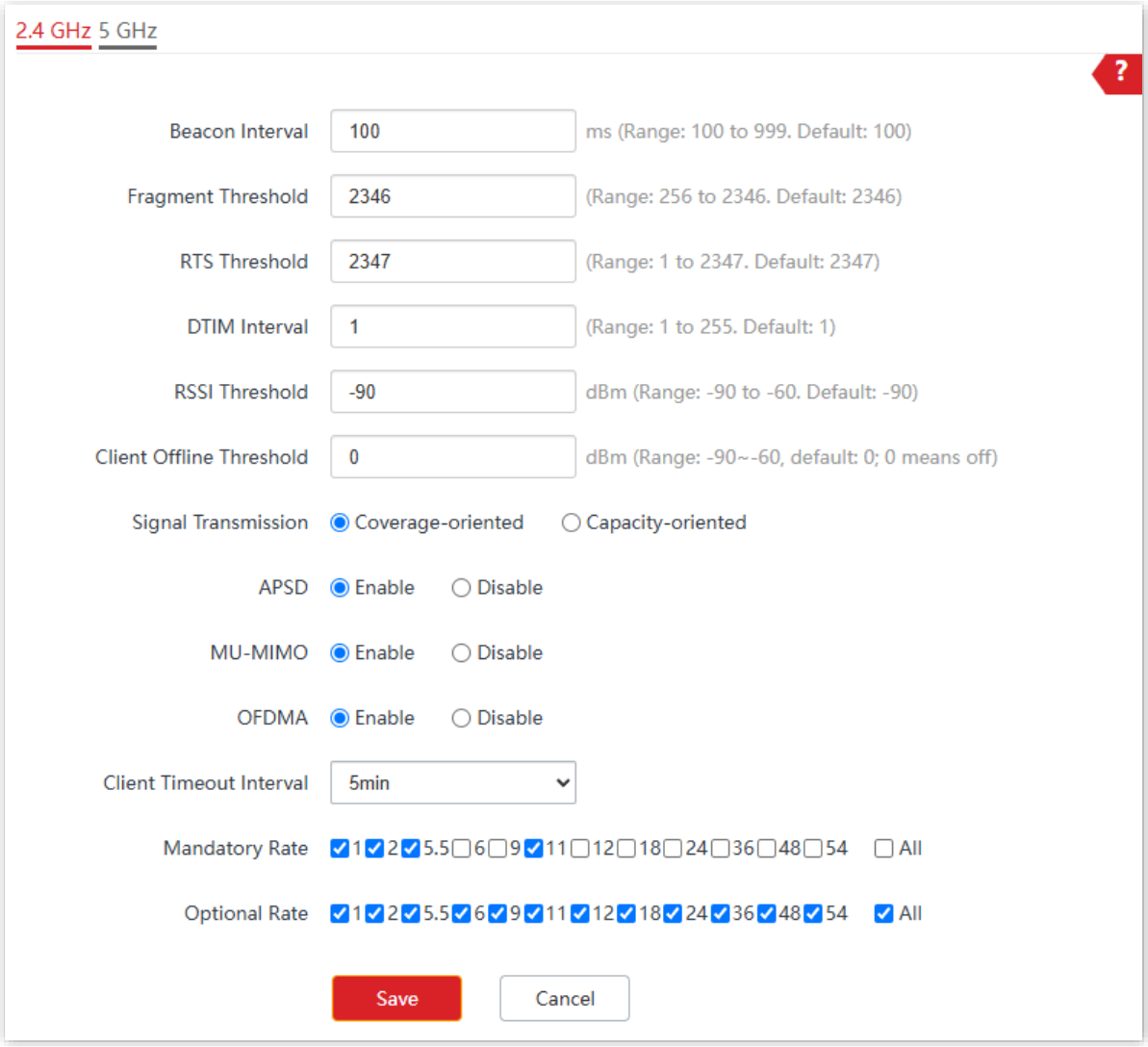
5.3 Optimize radio frequency

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

It is recommended to retain the default settings without professional guidance to avoid reducing the AP's wireless performance.



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 the AP sends Beacon frames. Beacon frames are sent at the interval to announce the existence of a Wi-Fi network. Generally, a smaller interval allows wireless clients to discover the AP sooner, while a larger interval reduces beacon overhead.

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 bytes. 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 Wi-Fi network to recover from conflicts quicker. For a Wi-Fi 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 the AP transmits broadcast and multicast frames in its cache. The unit is Beacon interval. For example, if **DTIM Interval** is set to **1**, the AP transmits all cached frames at one Beacon interval.
RSSI Threshold	Used to set the minimum strength of received signals acceptable to the 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 the AP. A proper value helps Wi-Fi-enabled devices connect to an AP with a stronger signal when multiple APs are available.
Client Offline Threshold	Used to set the minimum signal strength required for a client to maintain connection to the AP. If a client's access signal strength falls below the configured threshold, the AP will disconnect it.
Signal Transmission	Select the option based on your actual situation. – **Coverage-oriented**: This mode broadens AP wireless coverage and is typically used in deployments with fewer APs, such as offices, warehouses, and hospitals. – **Capacity-oriented**: This mode reduces mutual interference among APs and is typically used in high-density deployments with many APs, such as conference venues, exhibition halls, banquet halls, stadiums, universities, and airports.

Parameter	Description
Air Interface Scheduling	Specifies whether to enable the air interface scheduling function of the AP. If this function is enabled, users with different data rates are allocated equal airtime, improving the experience of high-rate users.  This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.
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):** Suppresses mild interference in low-interference environments. – **2 (Suppress moderate interference):** Suppress moderate interference for bad radio environment. – **3 (Suppress critical interference):** Suppress critical interference for heavy loading radio environment.  This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.
Anti-interference	When the device transmits using a wide channel bandwidth (such as 80 MHz or 160 MHz), the bandwidth is formed by bonding multiple subchannels. If some subchannels experience significant interference, conventional transmission can only reduce the overall rate and fall back to a narrower bandwidth. When this feature is enabled, the device automatically skips the interfered subchannels when transmitting packets and bonds only the clean subchannels, helping maintain higher wireless rates even in the presence of interference. This feature is suitable for scenarios using a channel bandwidth of 80 MHz or greater where surrounding wireless interference is significant.
APSD	Specifies whether to enable the automatic power save delivery function. If this function is enabled, the AP can work with wireless clients that support APSD or U-APSD (Unscheduled Automatic Power Save Delivery) to transmit data. This reduces wireless receiving activity when continuous data reception is not required, thereby lowering the power consumption of the client devices.
MU-MIMO	Multi-User Multiple-Input Multiple-Output. If this function is enabled, the AP can communicate with multiple users concurrently, avoiding Wi-Fi network congestion and improving communication.

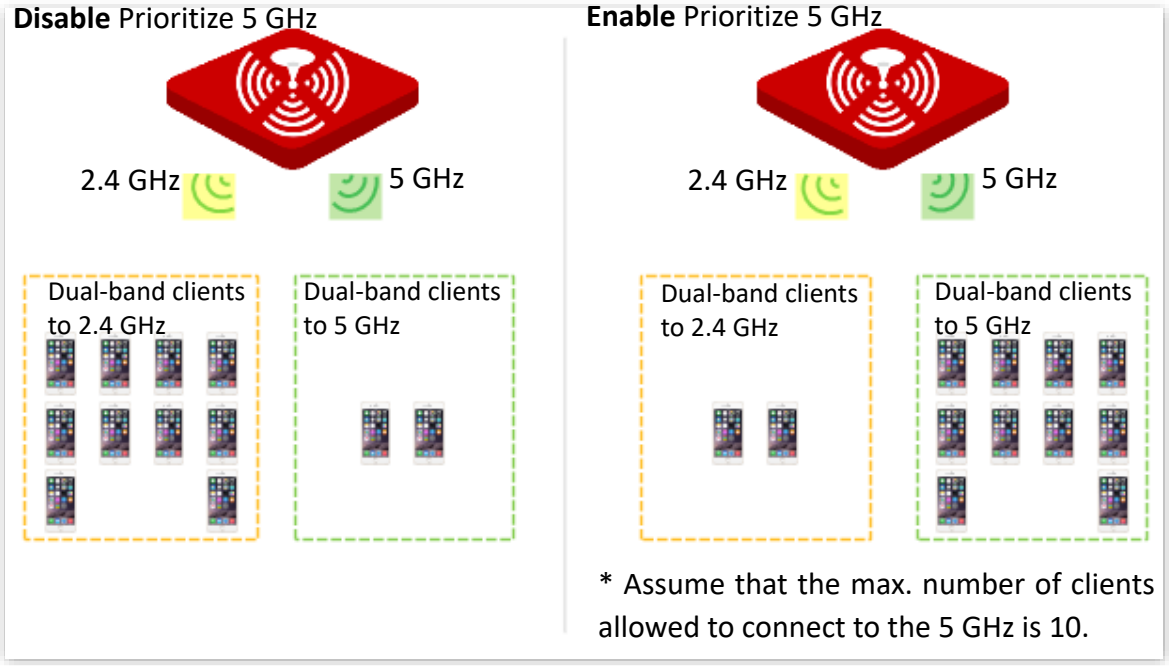
Parameter	Description
OFDMA	Orthogonal Frequency Division Multiple Access. If this function is enabled, multiple clients can transmit data at the same time, so that the transmission efficiency is improved, delay is reduced, and user experience is enhanced.
Client Timeout Interval	Used to set the wireless client disconnection interval of the 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 Wi-Fi networks of the AP.
Optional Rate	Specifies the additional rates that the AP supports, which are optional to wireless clients. Clients that support the mandatory rates can connect to the AP using higher optional rates when supported.
Prioritize 5 GHz	Specifies whether to enable the prioritize 5 GHz function. If this function is enabled, dual-band Wi-Fi-enabled devices preferentially connect to the AP's 5 GHz Wi-Fi network when the received 5 GHz signal strength is greater than or equal to the **Prioritize 5 GHz Threshold**.
Prioritize 5 GHz Threshold	With this function enabled, if the strength of the signals transmitted by a Wi-Fi-enabled device is greater than or equal to this threshold, the Wi-Fi-enabled device connects to the 5 GHz Wi-Fi network. Otherwise, it connects to the 2.4 GHz Wi-Fi network.

- **Prioritize 5 GHz**

  Although the 2.4 GHz band is more widely used than the 5 GHz band in many Wi-Fi deployments, it is more susceptible to congestion and interference because it has only three non-overlapping channels in typical deployments. The 5 GHz band could provide more non-overlapping communication channels. The quantity could reach more than 20 in some countries.

  As Wi-Fi networks evolve, clients that support both the 2.4 GHz and 5 GHz bands have become more common. By default, some dual-band clients may connect to the 2.4 GHz band, increasing congestion on 2.4 GHz and leaving 5 GHz underutilized.

  The Prioritize 5 GHz function encourages dual-band wireless clients to connect to the 5 GHz band during network initialization when the received 5 GHz signal strength reaches or exceeds the configured threshold, helping improve 5 GHz utilization and reduce load and interference on the 2.4 GHz band.



Note

The Prioritize 5 GHz function takes effect only when both the 2.4 GHz and 5 GHz wireless networks are enabled and the two bands use the same SSID, security mode, and password.

- **Air interface scheduling**

Tip

This feature is supported only on certain models. For actual feature availability, refer to the AP's web UI.

In a mixed-rate wireless environment, traditional first-in, first-out (FIFO) scheduling allocates more airtime to clients with low transmission rates and low spectral efficiency, reducing AP throughput and overall system utilization.

The air interface scheduling function evenly allocates downlink airtime to clients, allowing clients with higher transmission rates to transmit more data and thereby improving AP throughput and client capacity.

5.4 Configure load balancing

5.4.1 Configure load balancing between APs

In an actual Wi-Fi 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

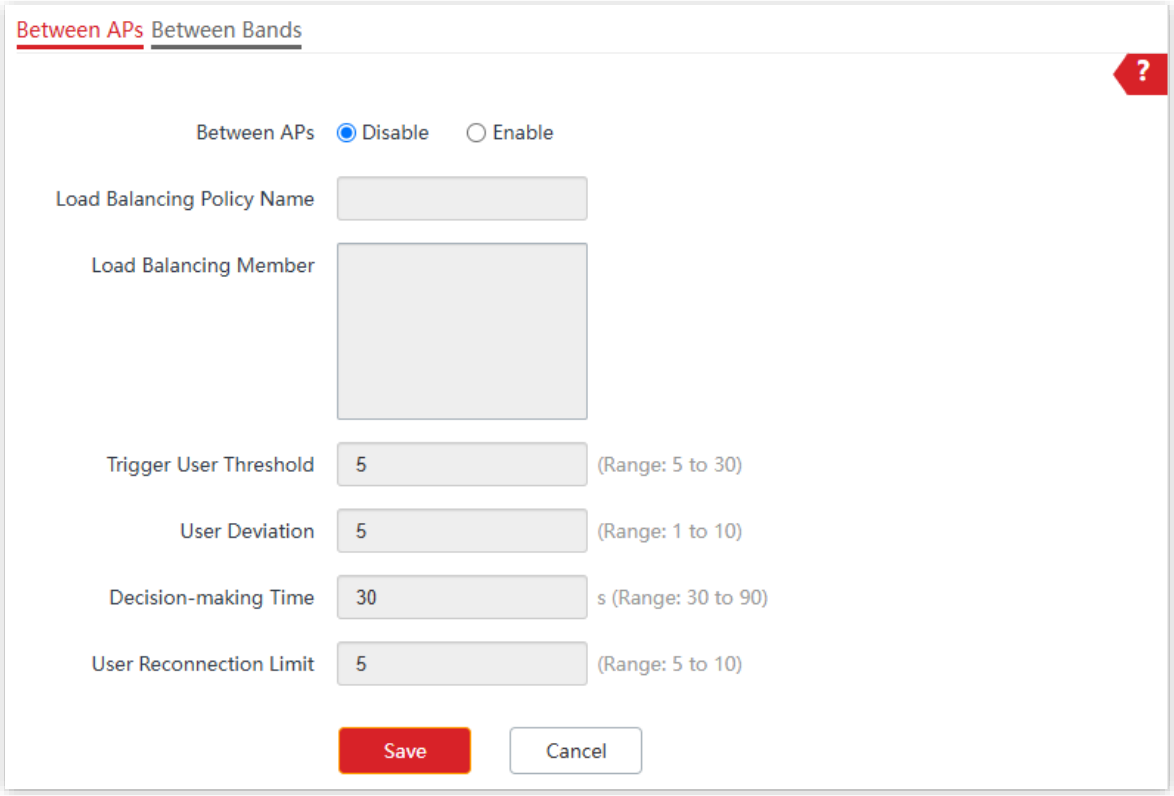
APs. In this way, the utilization of network resources can be maximized and the utilization rate of system resources can be effectively improved.

Tip

The load balancing policy takes effect only when APs use the same load balancing policy name and have identical SSIDs and Wi-Fi passwords.

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. The following figure is for reference only.



Parameter description

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

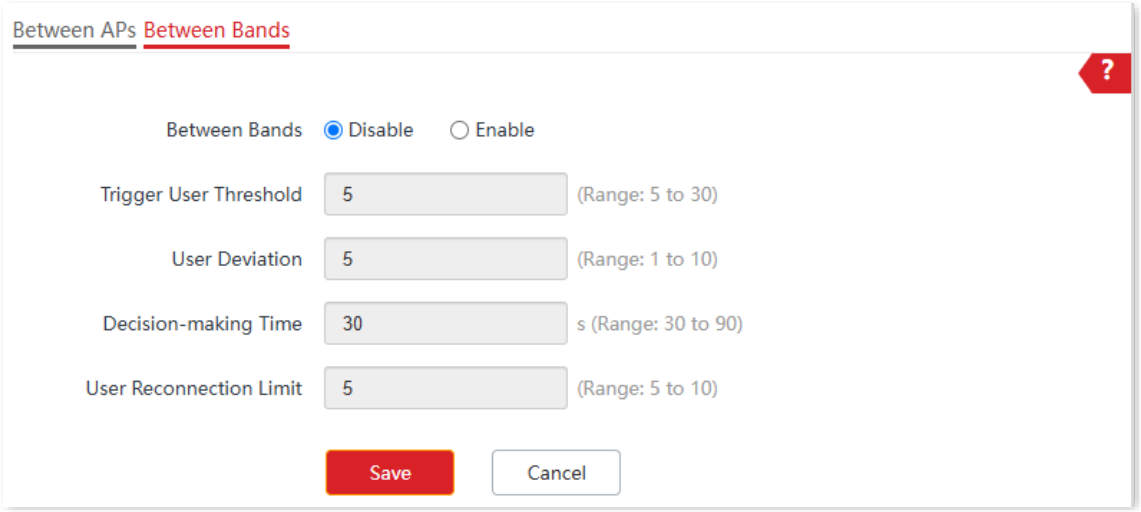
Parameter	Description
Load Balancing Policy Name	Specifies the load balancing policy between APs applied by the AP. It supports load balancing based on the number of users. This policy can be delivered to the AP via the controller (a device with AP management and AP load balancing functions) or configured directly through the AP's web UI. Tip If there is no controller in the LAN where the APs are located, APs with 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. The MAC addresses of APs with the same load balancing policy name enabled in the network will be automatically filled in here.
Trigger User Threshold	Specifies the threshold to trigger load balancing between APs. When the number of 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 period during which the AP refuses user connection requests. It is recommended to keep the default settings. If within this period, the number of AP refusals has reached the **User Reconnection Limit**, AP allows access from this user. If within this 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.

5.4.2 Configure load balancing between bands

The AP supports Wi-Fi 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 Wi-Fi network, the 2.4 GHz radio band is selected by default. Therefore, the 2.4 GHz radio band may be overloaded while the 5 GHz radio band may be relatively idle. To prevent this situation, enable load balancing between bands to distribute clients more evenly between the AP's radio bands and improve users' 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. The following figure is for reference only.



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 period during which the AP refuses user connection requests. It is recommended to keep the default settings. If within this period, the number of AP refusals has reached the **User Reconnection Limit**, AP allows access from this user. If within this 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.

5.5 Configure frequency analysis

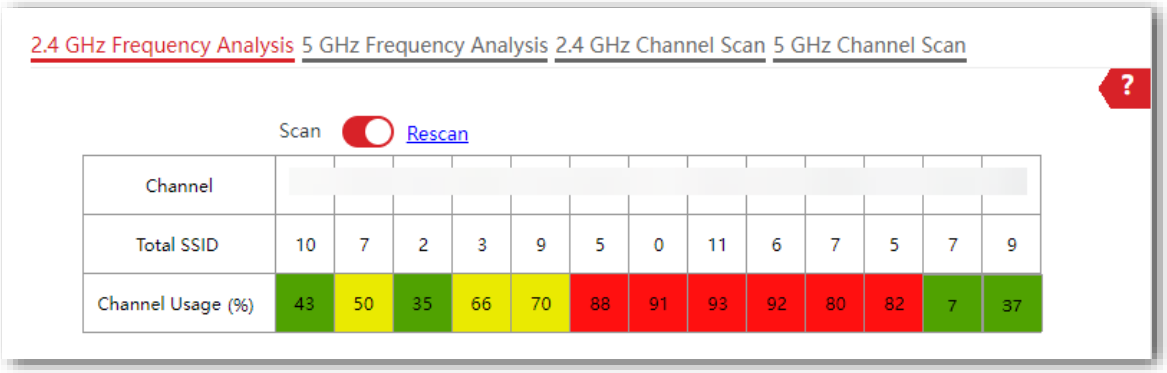
5.5.1 View frequency analysis

You can view the number of signals and channel utilization of each channel, and then select a channel with lower utilization as the working channel of the AP to improve wireless transmission efficiency.

Procedure for viewing frequency analysis

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

---End



After scanning, you can select a channel with lower utilization as the AP working channel.

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

5.5.2 Perform channel scan

The scan result list presents you with information about nearby Wi-Fi networks, including SSID, MAC address, channel, channel bandwidth, and signal strength.

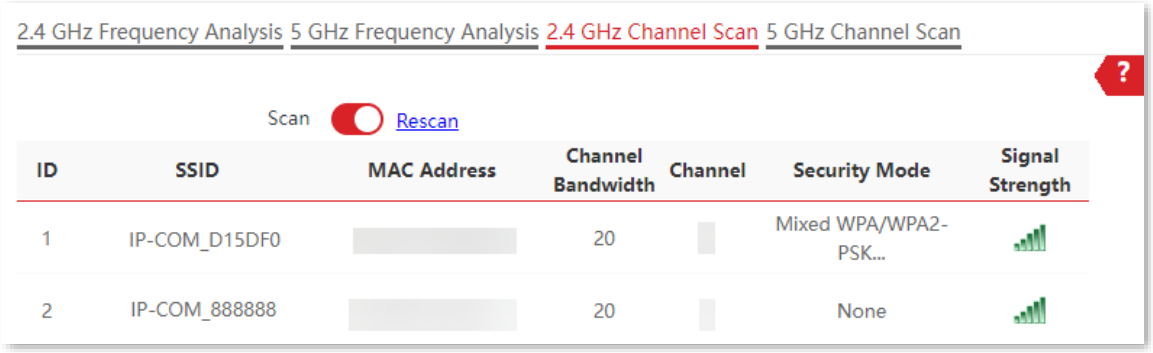
Procedure for performing channel scan

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Frequency Analysis**.

3. Click **2.4 GHz Channel Scan** or **5 GHz Channel Scan** tab to select the Wi-Fi network radio band for channel scan, which is **2.4 GHz Channel Scan** in this example.
4. Enable **Scan**.

---End

Scan results are as shown in the figure below.



5.6 Enable client type identification function

After enabling this function, the AP can identify the operating system types of Wi-Fi-enabled devices connected to its Wi-Fi network, making Wi-Fi network management more effective. The client types that the AP can identify include: Android, iOS, WPhone, Windows, macOS, and so on.

Procedure for enabling client type identification function

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Advanced Settings**.
3. Enable the **Identify Client Type** function.
4. Click **Save**.

---End

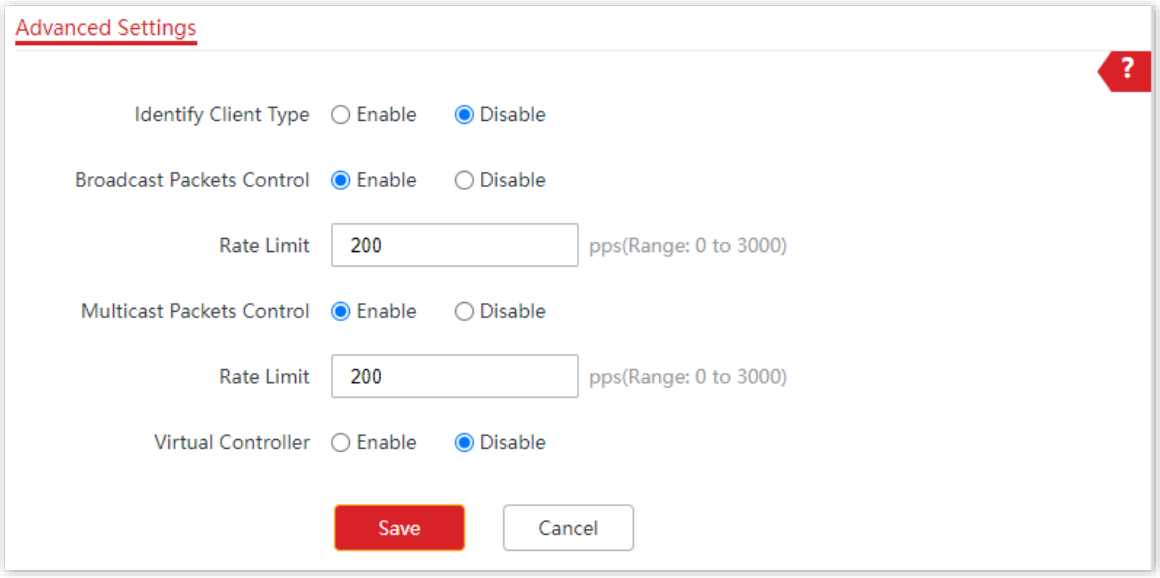
After the configuration is completed, if the client connects to the AP Wi-Fi and has accessed HTTP websites, you can view the client's operating system type on the **Status** > **Client List** page.

5.7 Configure broadcast and multicast packet control

Limiting the transmission rate of broadcast or multicast packets can prevent excessive broadcast or multicast traffic from consuming too much airtime, helping reduce wireless resource usage and interference.

Procedure for configuring broadcast and multicast packet control

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Advanced Settings**.
3. Enable the **Broadcast Packets Control** function.
4. Set the **Rate Limit** for broadcast packets. It is 200 pps by default.
5. Enable the **Multicast Packets Control** function. It is recommended to enable the WMF function simultaneously.
6. Set the **Rate Limit** for multicast packets. It is 200 pps by default.
7. Click **Save**.



---End

5.8 Use the AP as a virtual controller

When there is no AC controller or router supporting AP management in the network, 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.



This function can be used only in a network with at least two APs. The primary AP information is displayed in the virtual controller list.

Procedure for enabling the virtual controller function

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Advanced Settings**.
3. Enable the **Virtual Controller** function.
4. Click **Save**.

---End

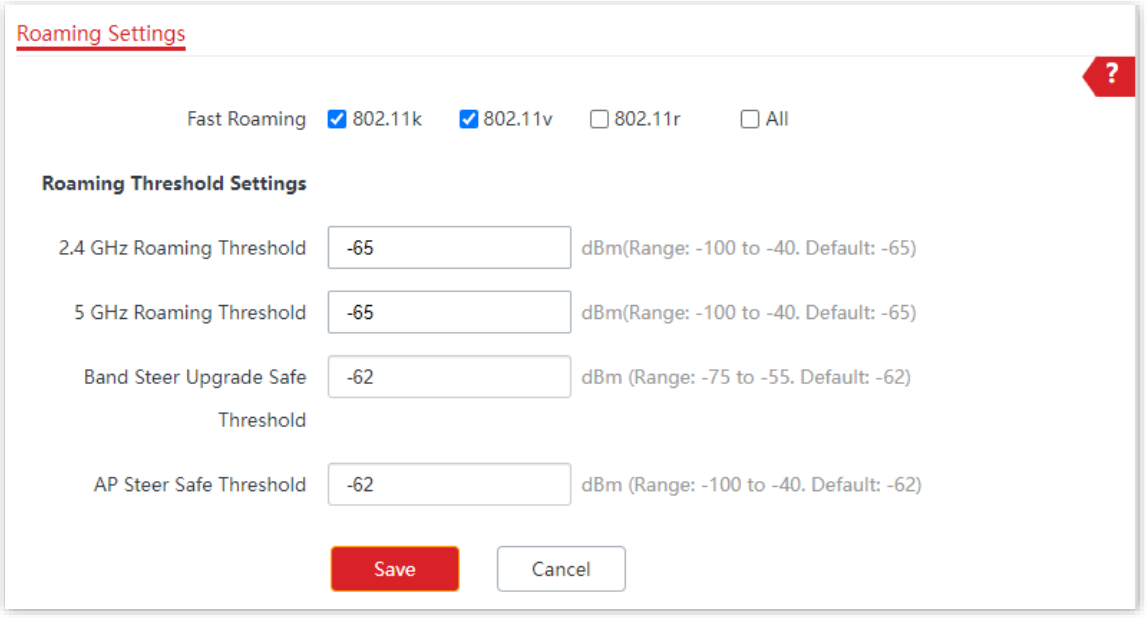
5.9 Configure roaming settings

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

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

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

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



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:** Wi-Fi 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 Transition (FT) protocol. When enabled, 802.11r reduces the authentication and key-management overhead during roaming, helping shorten roaming time.
2.4 GHz Roaming Threshold 5 GHz Roaming Threshold	Used to set 2.4 GHz or 5 GHz roaming threshold, which means setting the sensitivity of the client to roaming. When the signal strength received by the client from the AP falls below the roaming threshold, the roaming is triggered and the AP with better link quality is switched over.
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.

Parameter	Description
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.

6 Control internet access

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 Add devices to the blocklist

Devices on the blocklist cannot access the corresponding AP's Wi-Fi network for internet access.

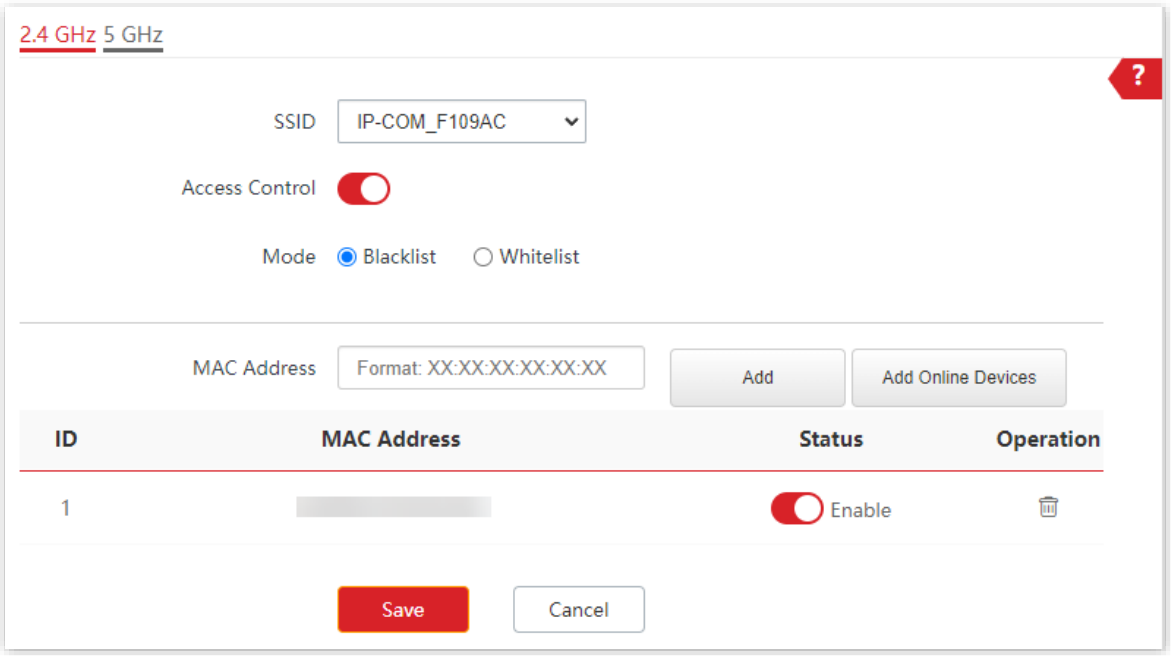
6.1.1 Through the access control function

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Access Control**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Select the **SSID** from the drop-down list.
5. Enable the **Access Control** function, and set **Mode** to **Blacklist**.
6. Enter MAC addresses of the Wi-Fi-enabled devices to which the policy applies, and 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.

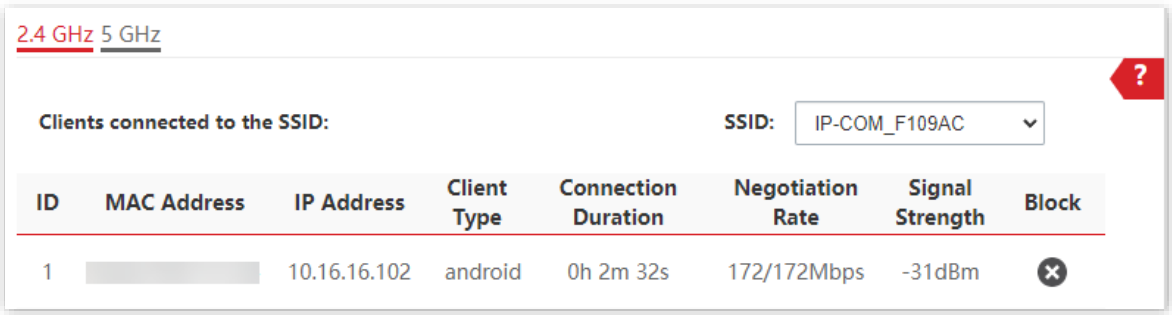
7. Click **Save**.



---End

6.1.2 Through the client list

1. Log in to the web UI of the AP.
2. Navigate to **Status** > **Client List**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Find the device to add to the blocklist, and click ⊗ to add it to the blocklist.



---End

After the configuration is completed, the device is added to the access control blocklist. The device cannot connect to the AP again by reconnecting to the Wi-Fi network. To unblock a device, you can remove it from the blocklist.

6.2 Add devices to the whitelist

Devices on the whitelist can connect to the AP's Wi-Fi network to access the internet, while other devices cannot connect to this Wi-Fi network.

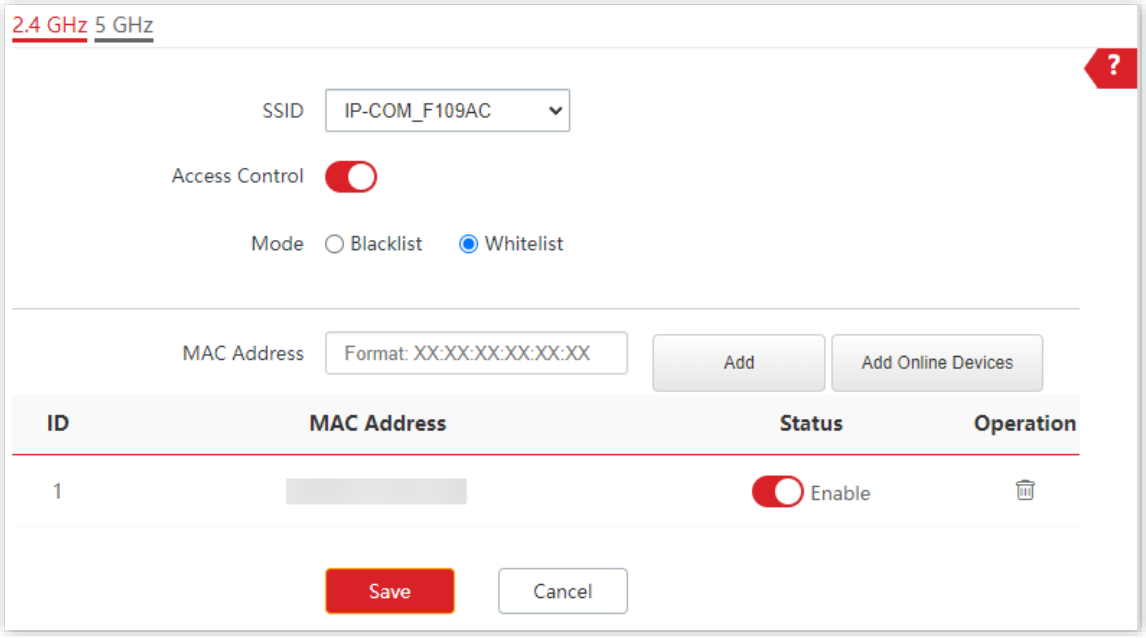
Procedure for adding devices to the whitelist

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Access Control**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Select the **SSID** from the drop-down list.
5. Enable the **Access Control** function, and set **Mode** to **Whitelist**.
6. Enter MAC addresses of the Wi-Fi-enabled devices to which the policy applies, and 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**.



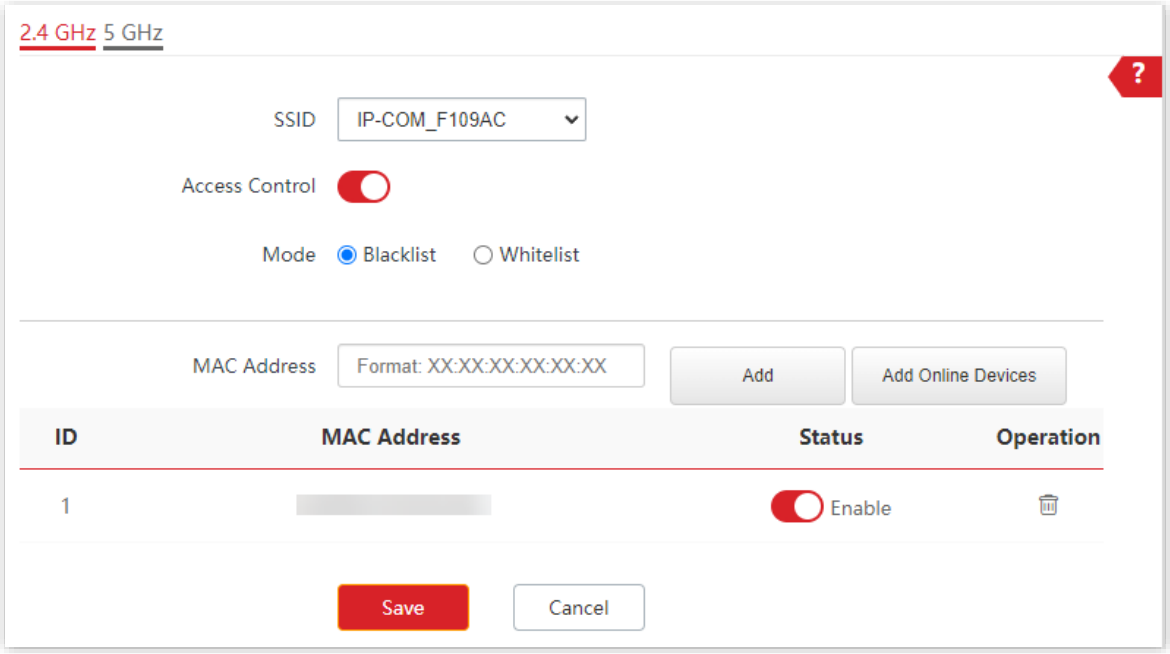
---End

6.3 Remove devices from the blocklist/whitelist

The steps for removing devices from the blocklist and whitelist are similar. Take removing from the blocklist as an example.

Procedure for removing devices from the blocklist

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **Access Control**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Select the **SSID** from the drop-down list.
5. In the access control list, find the device to be removed from the blocklist, then disable the **Enable** toggle or click .
6. Click **Save**.



---End

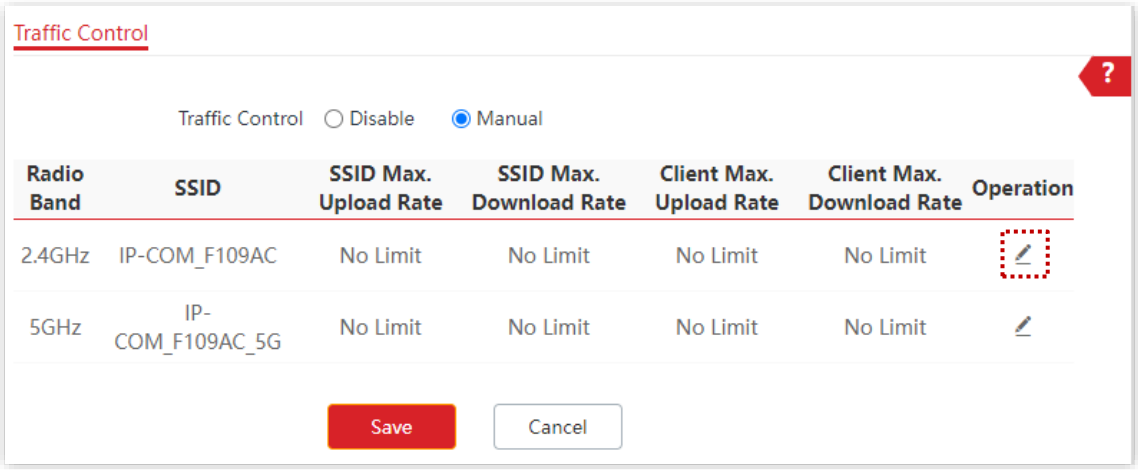
6.4 Control internet access speed

Through the traffic control function, you can set the maximum upload or download rate of SSIDs and user devices to limit the total bandwidth of SSID and evenly allocate bandwidth to users. This prevents a low-priority network, such as a guest network, or an individual user from consuming excessive bandwidth and degrading internet access for other users.

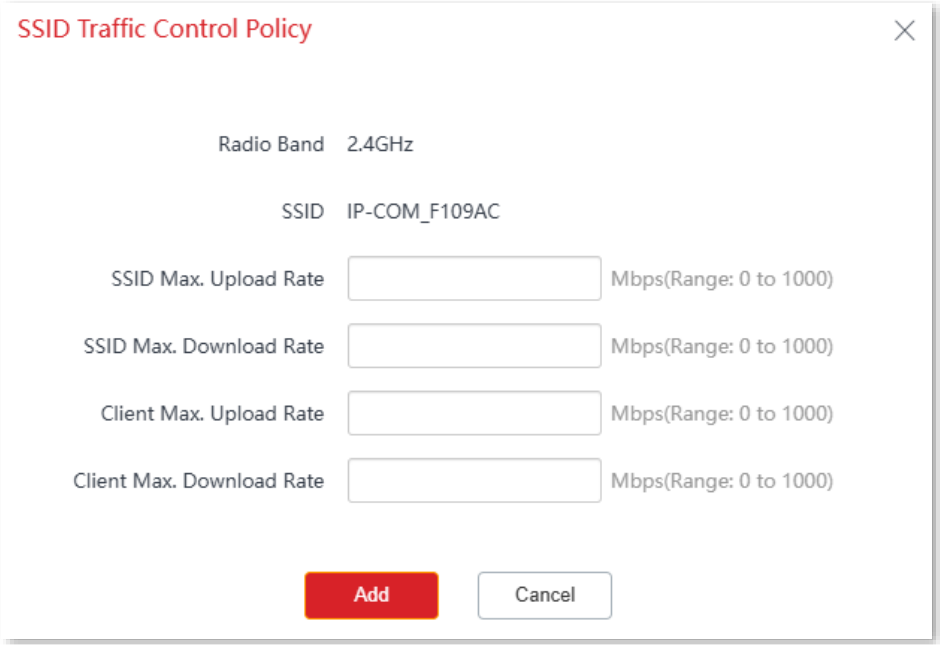
By default, the traffic control function is disabled.

Procedure for controlling internet access speed

1. Log in to the web UI of the AP.
2. Navigate to **Advanced** > **Traffic Control**.
3. Set **Traffic Control** to **Manual**.
4. Click ✎ on the row where the Wi-Fi network to be controlled resides.



5. Set the maximum upload or download rate allowed for the Wi-Fi network and the maximum upload or download rate allowed for every user device connected to the Wi-Fi network.
6. Click **Add**.



---End

Parameter description

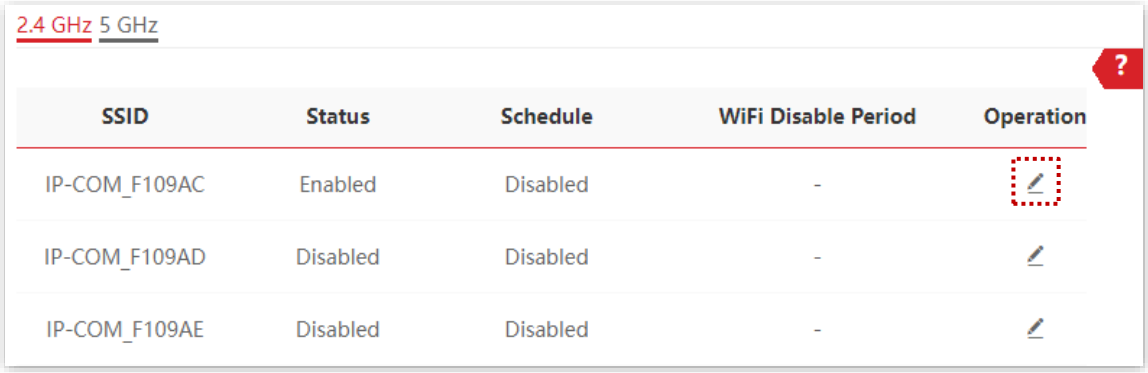
Parameter	Description
Traffic Control	Specifies whether to enable the traffic control function.
Radio Band	Specifies the radio band of the Wi-Fi network on which you manually set a traffic control rule.
SSID	Specifies the name of the Wi-Fi network on which you manually set a traffic control rule.
SSID Max. Upload Rate	Specify the maximum upload or download rate allowed for a Wi-Fi network. If you leave it blank, the maximum upload or download rate of the target Wi-Fi network is 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 Wi-Fi network. If you leave it blank, the maximum upload or download rate of every user device connected to the target Wi-Fi network is not limited. It is available only when you manually set a traffic control rule.
Client Max. Download Rate	
Operation	Click to set the maximum upload or download rate allowed for the target Wi-Fi network and the maximum upload or download rate allowed for every user device connected to the target Wi-Fi network. It is available only when you manually set a traffic control rule.

6.5 Control internet usage time

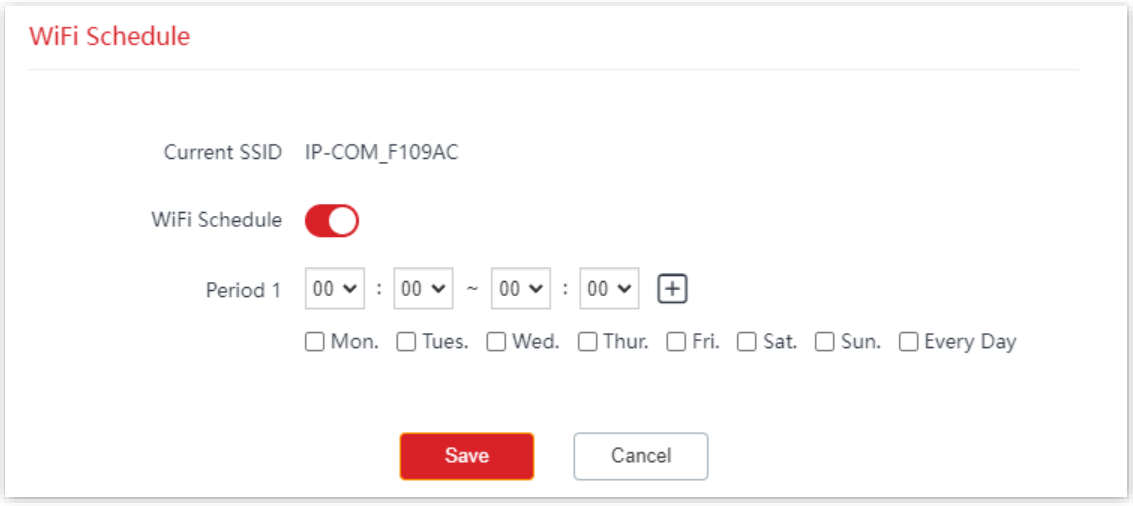
You can disable the Wi-Fi network of the AP during a specified period. During the scheduled disable period, Wi-Fi-enabled devices such as smartphones cannot search for the Wi-Fi networks.

Procedure for controlling internet usage time

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **WiFi Schedule**.
3. Select a Wi-Fi radio band where the policy must be implemented, which is **2.4 GHz** in this example.
4. Click on the row where the Wi-Fi network to be controlled resides.



5. Enable the **WiFi Schedule** function, and set the period for the Wi-Fi network to automatically disable.



6. Click **Save**.

---End

Parameter description

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

7 Configure portal authentication

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.

Portal authentication is a web-based Wi-Fi access authentication service. When users connect to Wi-Fi and attempt to access the network, they are redirected to a portal page and can access the internet only after authentication. Enterprises can use the page for brand presentation, information promotion, and access authentication management.

7.1 Portal authentication configuration guide

Step	Task	Task Description
1	Enable portal authentication	**Required.** Enable portal authentication and select a role for the AP.
2	Configure authentication page	**Required.** Manually create an authentication page template.
3	Configure authentication method	**Required.** Configure one or more authentication method policies as required by the actual scenario.
4	Configure authentication policy	**Required.** Apply the configured authentication page and authentication method to the specified SSID.
5	Configure accounts for account password authentication	**Optional.** If account password authentication is used, authentication accounts must be configured.
6	Configure accounts for random code authentication	**Optional.** If random code authentication is used, random code accounts must be configured.
7	Configure authentication exemption policy	**Optional.** Configure an authentication exemption policy if devices need to access the internet without authentication.

7.2 Enable portal authentication

After the portal authentication function is enabled, users who connect to Wi-Fi and attempt to access the network are redirected to a portal page and can access the internet only after authentication. Pro-7-Lite V1.1 supports up to 100 simultaneously authenticated users. The limit may vary by model. Refer to the product specifications for the actual limit.

Note

After portal authentication is enabled, both the primary node and secondary nodes support only **Local Management** mode for cloud management.

Procedure for enabling portal authentication

1. Log in to the web UI of the AP.
2. Navigate to **Portal Authentication** > **Portal Authentication**.
3. Enable **Portal Authentication**.
4. Select the AP role for the portal authentication.
   - **Main node**: The AP acts as the primary node for the portal authentication and automatically synchronizes the SSID configuration and authentication policies to secondary nodes. When Pro-7-Lite V1.1 acts as the primary node, it can manage up to 7 secondary nodes. The limit may vary by model. Refer to the product specifications for the actual limit.
   - **Child node**: After joining the portal authentication group, the AP receives only the SSID configuration and authentication policies delivered by the primary node. It does not receive AC configurations.
5. If you set the AP as the primary node in the previous step, click **Scan**. After the AP scans for other APs on the LAN, locate the AP to be added as a secondary node of the portal authentication, and click ⊞ on the right of the corresponding entry.

---End

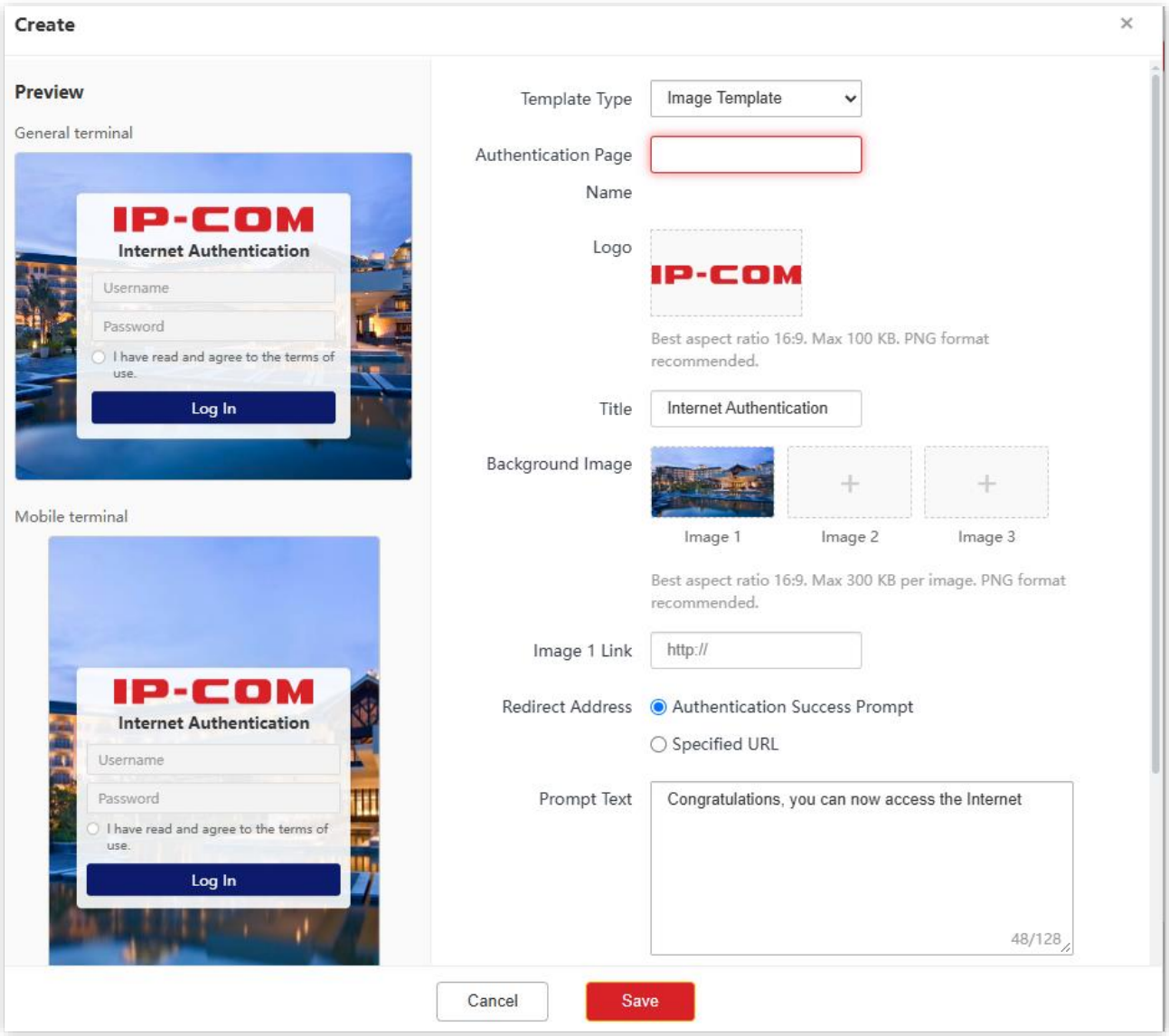
Tip

When a secondary node is managed by a primary node, it can switch to the primary node role only in any of the following three cases:

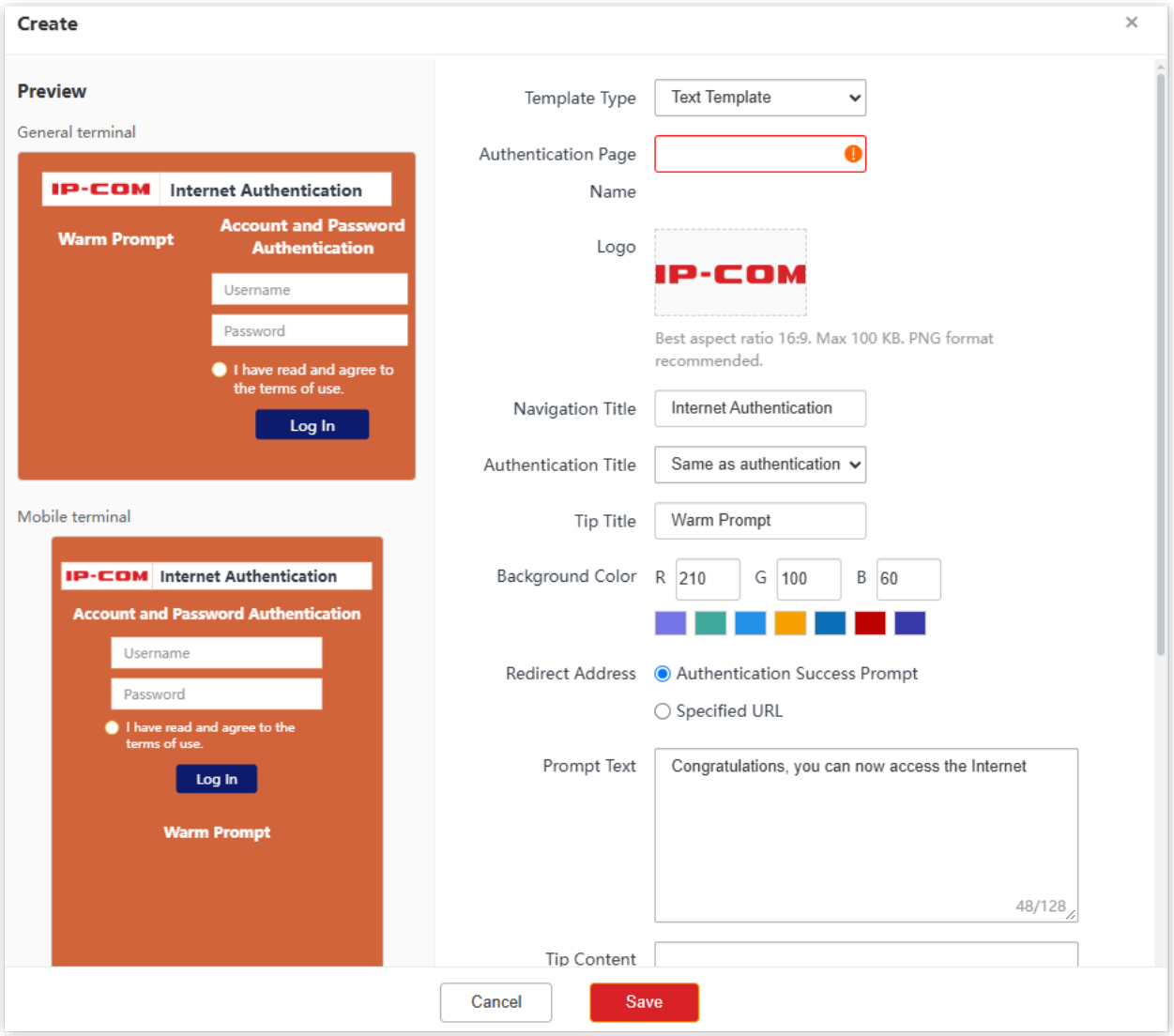
- The secondary node is removed by the primary node.
- The primary node remains offline for an extended period or is restored to factory settings.
- The secondary node is restored to factory settings.

7.3 Configure authentication page

1. Log in to the web UI of the AP.
2. Navigate to **Portal Authentication** > **Authentication Page**.
3. Click **+ Manual Creation**.
4. Select a **Template Type** as required, and then configure the parameters on the authentication page.
5. Click **Save**.



Or



----End

Parameter description

Parameter	Description
Template Type	Specifies the template type including image templates and text templates.
Authentication Page Name	Specifies the name of the authentication page.
Background Image	Specifies the background image of the authentication page. Image aspect ratio: 16:9 (recommended) or 19.5:9 (suitable for smartphones). Each image must not exceed 300 KB. PNG format is recommended. Tip If multiple background images are uploaded (up to 3), the authentication page rotates through them.

Parameter	Description
Image X Link (X is the image number)	Specifies the URL linked to the background image (HTTP and HTTPS are supported). After configuration, clicking the background image on the authentication page opens the URL.
Redirect Address	Specifies the URL to which the browser automatically redirects after the user is authenticated. – **Authentication Success Prompt**: Displays the configured message after successful authentication. – **Specified URL**: After successful authentication, the browser redirects to the URL configured here.
Prompt Text	When **Redirect Address** is set to **Authentication Success Prompt**, you can customize the message.
Specified URL	When **Redirect Address** is set to **Specified URL**, enter the destination URL here (HTTP and HTTPS are supported).
Disclaimer	Specifies the disclaimer displayed on the authentication page. Users must select the checkbox to accept the disclaimer before they can log in.

7.4 Configure authentication method

7.4.1 One-click authentication, random code authentication, and account password authentication

- **One-Click Authentication**

  After the one-click authentication is enabled, users only need to click **Connect to Internet** on the displayed authentication page to access the internet.

- **Random Code Authentication**

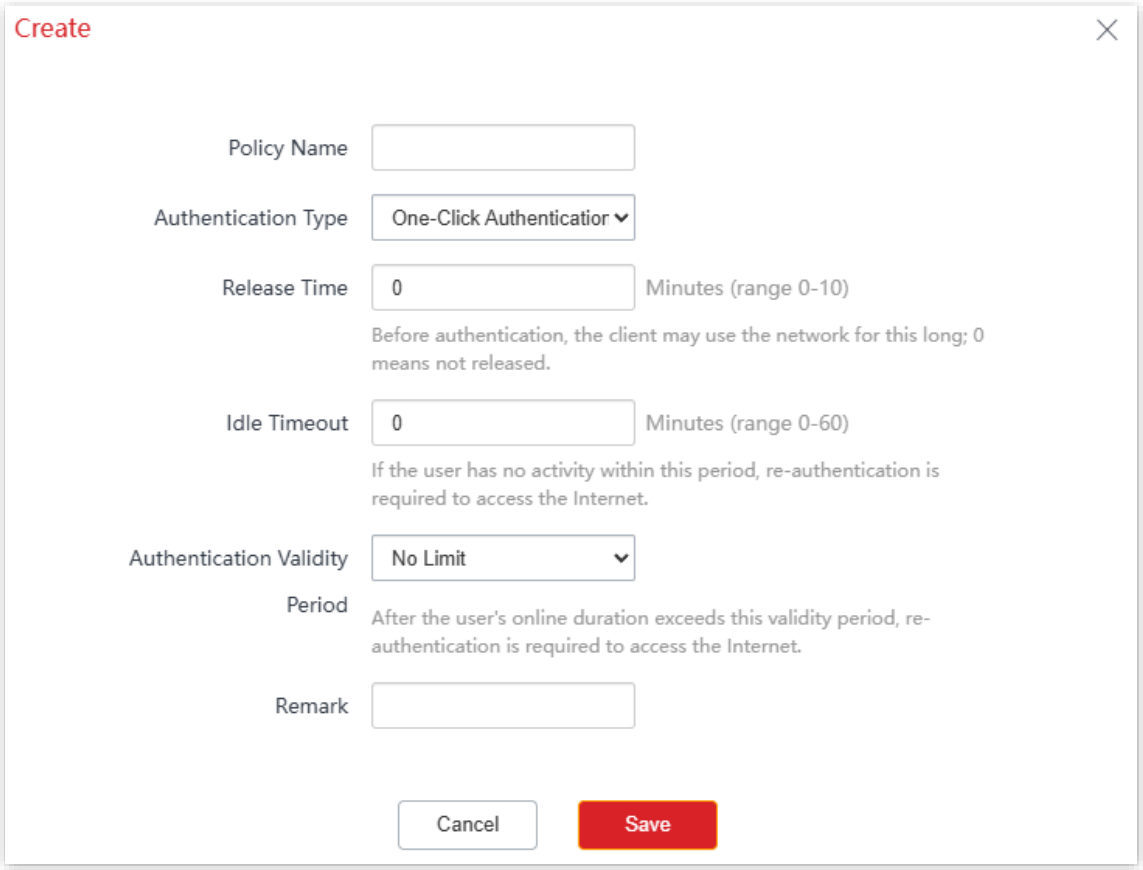
  After the random code authentication is enabled, users must enter a random code on the authentication page and can access the internet only after successful authentication. Random codes must be configured in Random Code Account in advance.

- **Account Password Authentication**

  After the account password authentication is enabled, users must enter a username and password on the authentication page and can access the internet only after successful authentication. Configure the usernames and passwords in Authentication Account in advance.

Procedure for configuring one-click authentication, random code authentication, or account password authentication

1. Log in to the web UI of the AP.
2. Navigate to **Portal Authentication** > **Authentication Method**.
3. Click **Create**.
4. Set the **Policy Name**, select **One-Click Authentication**, **Random Code Authentication**, or **Account Password Authentication** as the **Authentication Type**, and configure the other authentication parameters.
5. Click **Save**.



----End

Parameter description

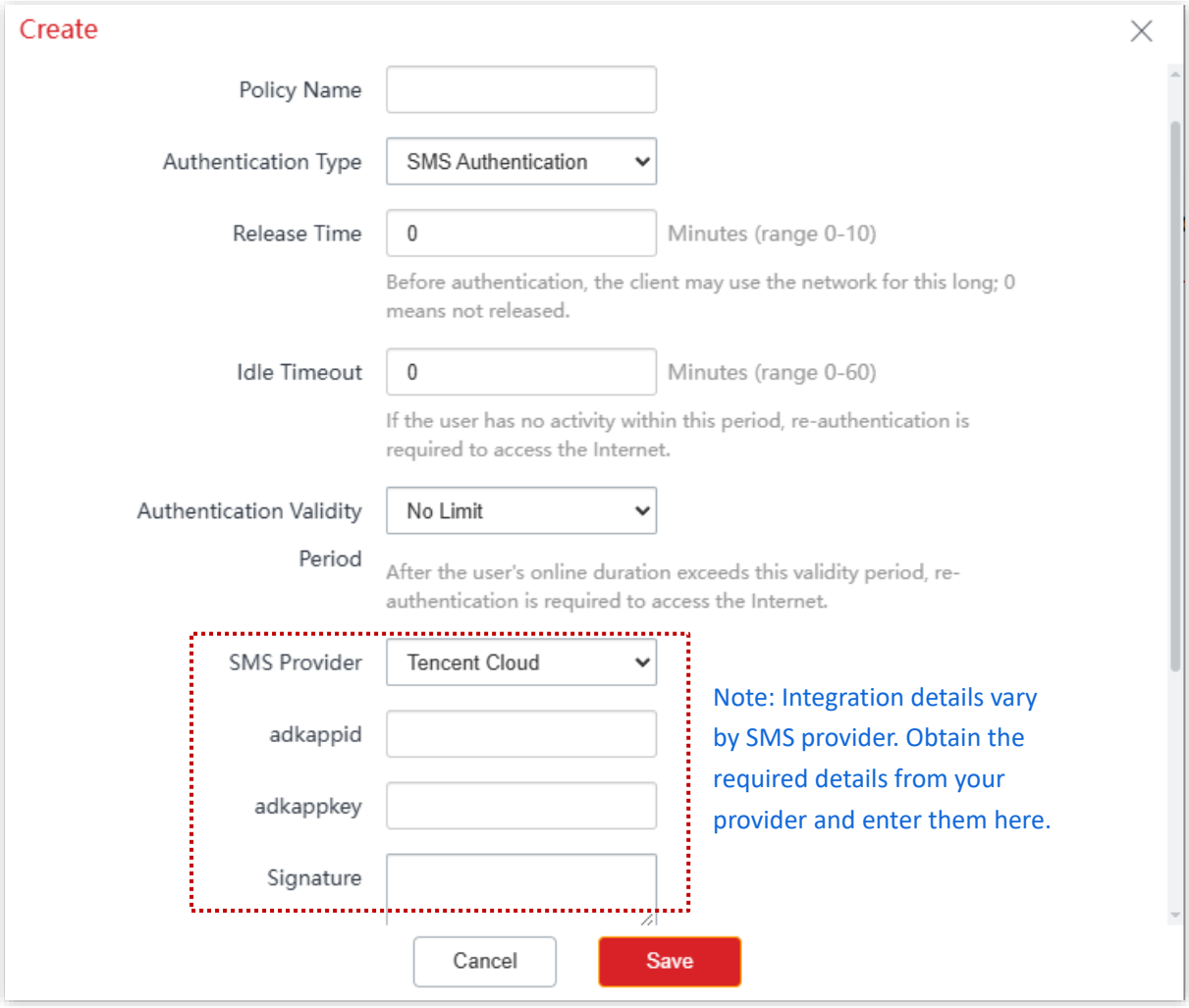
Parameter	Description
Release Time	Specifies the amount of time users can use the network before authentication. 0 indicates no access is allowed.
Idle Timeout	After successful authentication, users must authenticate again if the network is not used within the idle timeout. 0 disables idle-timeout reauthentication.
Authentication Validity Period	Specifies that users must authenticate again after the authentication validity period expires.
Remark	Specifies the remark for the policy.

7.4.2 SMS authentication

After the SMS authentication is enabled, users must enter a valid smartphone number on the authentication page to obtain a verification code, which is sent by the SMS provider configured by the administrator. Users can access the internet only after successful authentication.

Procedure for configuring SMS authentication

1. Purchase an SMS package from an SMS provider and record the required provider information. The AP currently supports **Alibaba Cloud**, **Tencent Cloud**, **Jixintong**, and **NEXMO**. Other SMS providers can also be integrated through **Custom HTTP Integration**.
2. Log in to the web UI of the AP.
3. Navigate to **Portal Authentication** > **Authentication Method**.
4. Click **Create**.
5. Set the policy name, select **SMS Authentication** as the **Authentication Type**, and configure the related SMS authentication parameters. The following figure is for reference only.
6. Click **Save**.



----End

Parameter description

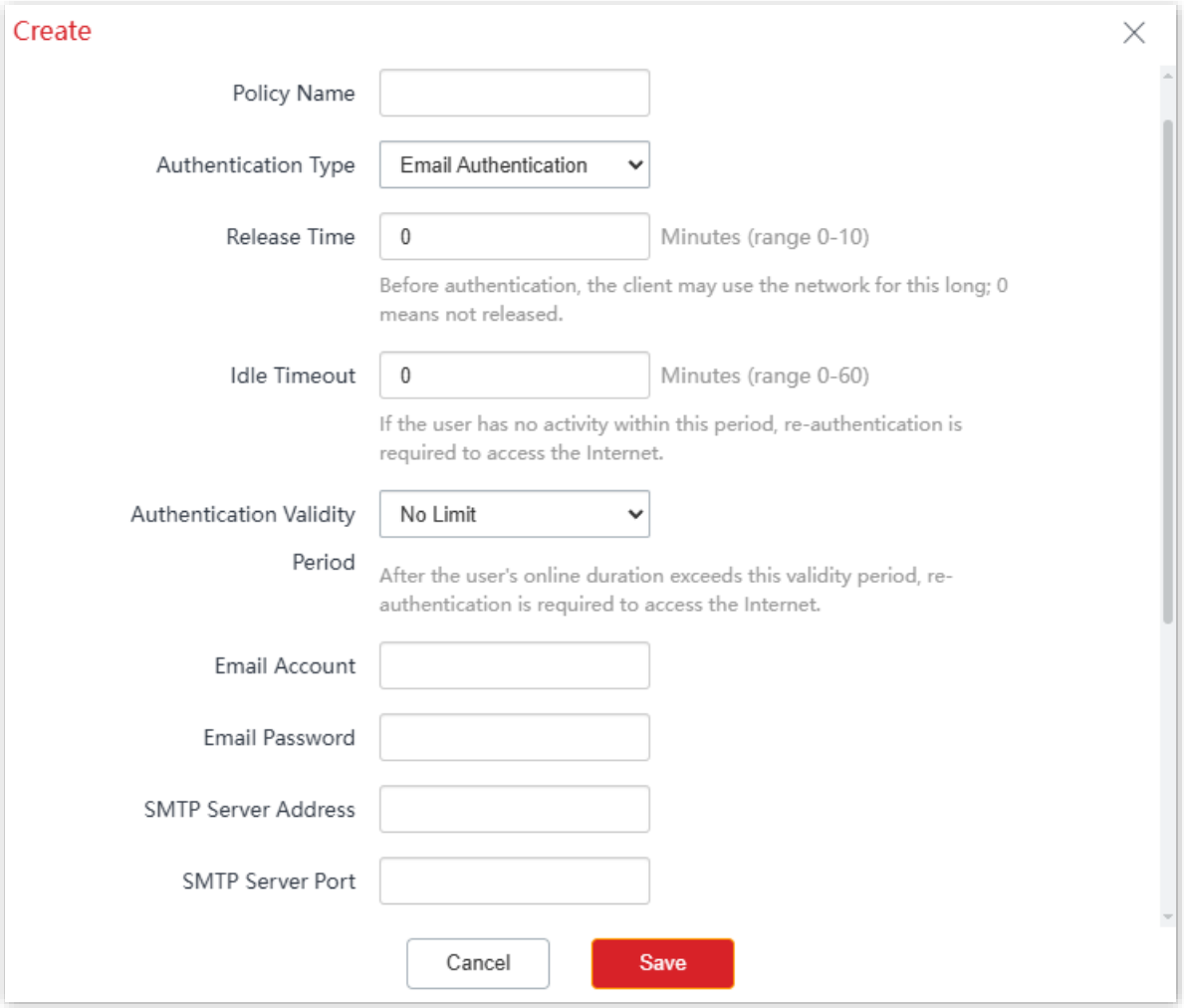
Parameter	Description
Release Time	Specifies the amount of time users can use the network before authentication. 0 indicates no access is allowed.
Idle Timeout	After successful authentication, users must authenticate again if the network is not used within the idle timeout. 0 disables idle-timeout reauthentication.
Authentication Validity Period	Specifies that users must authenticate again after the authentication validity period expires.
Validity Test	Used to test whether the AP is successfully connected to the SMS provider. Enter a smartphone number and click **Test**. If the connection is successful, the smartphone number receives an SMS containing a verification code.

7.4.3 Email authentication

After the email authentication is enabled, users must enter an email address on the authentication page to obtain a verification code and can access the internet only after successful authentication.

Procedure for configuring email authentication

1. Log in to the web UI of the AP.
2. Navigate to **Portal Authentication** > **Authentication Method**.
3. Click **Create**.
4. Set the **Policy Name**, select **Email Authentication** as the **Authentication Type**, and configure the other authentication parameters.
5. Click **Save**.



----End

Parameter description

Parameter	Description
Release Time	Specifies the amount of time users can use the network before authentication. 0 indicates no access is allowed.
Idle Timeout	After successful authentication, users must authenticate again if the network is not used within the idle timeout. 0 disables idle-timeout reauthentication.
Authentication Validity Period	Specifies that users must authenticate again after the authentication validity period expires.
Email Account	Specifies the email account used to send verification-code emails.
Email Password	Specifies the password of the email account used to send verification-code emails.
SMTP Server Address	– **SMTP Server Address**: Specifies the address of the SMTP server used to send verification-code emails. – **SMTP Server Port**: Specifies the port number used by the SMTP server. SMTP stands for Simple Mail Transfer Protocol. An SMTP server is a mail relay server. SMTP server addresses and ports vary by email service provider; obtain the required information from your provider.
SMTP Server Port	
Validity Test	Used to test whether the AP is successfully connected to the mail server. Enter an email address and click Test. If the connection is successful, the address receives an email containing a verification code.
Email Content	Specifies the content of the verification-code email.
Shared User Count	Specifies the number of users that can use the same email address to authenticate and access the internet at the same time.

7.5 Configure authentication policy

You can configure an authentication policy for an SSID.

Procedure for configuring authentication policy

1. Log in to the web UI of the AP.
2. Navigate to **Portal Authentication** > **Authentication Policy**.
3. Click **Create**.
4. Configure the authentication policy parameters.
5. Click **Save**.

----End

Parameter description

Parameter	Description
Application Interface (Wireless Name)	Specifies the SSID of the Wi-Fi network to which the authentication policy applies.
Authentication Page (Template Name)	Specifies the authentication page used by the authentication policy. Configure it on the Authentication Page in advance.
Authentication Method (Policy Name)	Specifies the authentication method used by the authentication policy. Configure it on the Authentication Method page in advance.
Status	Displays whether the authentication policy is active.

7.6 Configure accounts for account password authentication

1. Log in to the web UI of the AP.
2. Navigate to **Portal Authentication** > **Authentication Account**.
3. Click **Create**.
4. Configure the account parameters.
5. Click **Save**.

----End

Button and parameter description

Item	Description
Delete	Click to delete the selected account information.
Import	Click to import previously exported authentication account information to this AP.
Export	Click to export the authentication account information configured on the current AP to the local device. File: exportAuthAccountList.csv
Account	Specifies the username of the authentication account.
Password	Specifies the password of the authentication account.
Validity Period	Specifies the validity period for internet access using this account. If the authenticated online time exceeds the validity period, the user must authenticate again to access the internet.

Item	Description
Bind MAC	After this function is enabled, the AP binds the account to the MAC addresses of the first several devices that successfully authenticate using this account.
Shared Users	Specifies the number of users that can use the account to authenticate and access the internet at the same time. Note If **Bind MAC** is enabled, the AP binds the account to the MAC addresses of the first several devices that successfully authenticate using the account. Devices with other MAC addresses cannot use the account for authentication. For example, if **Shared Users** is set to **2**, the AP binds the account to the MAC addresses of the first two devices that successfully authenticate using the account. Devices with other MAC addresses cannot share the account for authentication.
Upload Speed Limit	Specify the maximum upload or download speed for the account.
Download Speed Limit	
Remark	Specifies the remark for the account.

7.7 Configure accounts for random code authentication

1. Log in to the web UI of the AP.
2. Navigate to **Portal Authentication** > **Random Code Account**.
3. Click **Create**.
4. Configure the account parameters.
5. Click **Save**.

----End

Button and parameter description

Item	Description
Print	Click to print the selected random code account information.
Delete	Click to delete the selected random code account information.
Random Code	Specifies the random code used for authentication.

Item	Description
Creation Time	Specifies the time when the random code was created.
Expired Time	Specifies the time when the random code expires and becomes invalid. The AP calculates it automatically based on **Account Validity Period** and **Creation Time**.
Traffic Limit	Specifies the total download traffic allowed for the random code account. Once the limit is reached, the random code can no longer be used to access the internet and is automatically deleted by the system.
Available Duration (Account Usage Duration)	Specifies how long the random code account can access the internet. When the remaining time reaches zero, the system automatically deletes the random code.
Shared Users	Specifies the number of users that can use the random code to authenticate and access the internet at the same time. Note Random code accounts bind MAC addresses by default. For example, if **Shared Users** is set to 2, the AP binds the first two MAC addresses that successfully authenticate with the random code to that code. Devices with other MAC addresses cannot use the random code for internet access.
No. of Used	Specifies the number of users that have used the random code to authenticate and access the internet.
Remark	Specifies the remark for the random code.
No. of Created Codes	Specifies the number of random codes to be created this time.
Account Validity Period	Specifies the validity duration of the random code.

7.8 Configure authentication exemption policy

You can configure an authentication exemption policy for special devices, such as network cameras, so that these devices can access the internet without authentication.

Procedure for configuring authentication exemption policy

1. Log in to the web UI of the AP.
2. Navigate to **Portal Authentication** > **Exemption Authentication Policy**.
3. Click **Create**.
4. Enter the **MAC Address** of the authentication exemption host and configure the remarks.

Separate multiple non-consecutive MAC addresses with semicolons (;). A maximum of 16 MAC addresses can be added to each policy.

5. Click **Save**.

----End

Parameter Description

Parameter	Description
Exemption Authentication Condition	Specifies the condition of the authentication exemption policy. Only clients that meet this condition can access the internet without authentication. Currently, authentication exemption conditions based on MAC addresses are supported. **By MAC**: Matches authentication exemption devices by device MAC address.
Exemption Authentication Content	Only devices that match this content can access the internet without authentication. The AP first checks the authentication exemption condition and then the authentication exemption content. Authentication is bypassed only when both checks pass.

7.9 User management

You can view and export authenticated user information, disconnect online users in batches, and delete information about offline authenticated users in batches.

To access the page, log in to the web UI of the AP, and navigate to **Portal Authentication** > **User Management**.

Button and parameter description

Item	Description
Disconnect	Used to disconnect the selected online users. Authenticated online users must authenticate again before accessing the internet. Authentication exemption online users reconnect automatically to access the internet.
Delete	Used to delete the selected offline user information.
Authentication Type	Specifies the authentication type used by the authenticated user. Users configured as authentication exemption hosts are displayed as **Free Authentication**.

Item	Description
Authentication Account	Specifies the authentication account, email address, smartphone number, random code, or other credential used by the user.

7.10 Portal authentication configuration example for a street-front shop

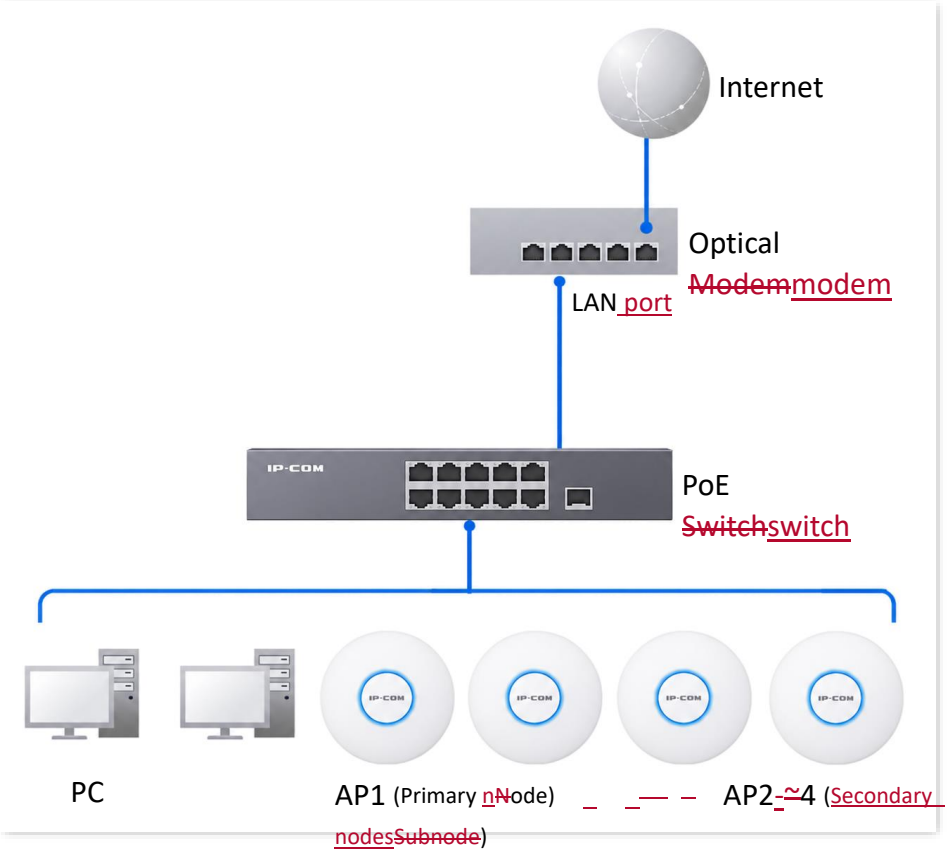
7.10.1 Network requirements

A street-front shop, such as a restaurant or coffee shop, uses an ISP optical modem to access the internet and has four APs installed to provide Wi-Fi for customers. The optical modem does not support the portal authentication, and the shop owner wants to promote the shop brand while customers connect to Wi-Fi, for example by displaying a shop introduction, menu, promotions, and an official-account QR code. Portal authentication is therefore enabled on the APs, with the authentication page serving as the promotion entry point.

The shop network has the following requirements:

- After customers connect to the shop Wi-Fi, the portal authentication page is displayed automatically. Customers can access the internet only after successful authentication.
- The authentication page displays shop branding posters and promotional information. Customers can click a background image to go to the shop promotion website.
- After successful authentication, the browser automatically redirects to a URL specified by the shop owner, such as a new-product promotion page, membership registration page, or official-account page.
- An authentication validity period of at least 2 hours is recommended to cover the average dining or stay duration and avoid repeated authentication pop-ups.
- Use a simple authentication method so that customers can get online quickly.
- In-store devices such as the shop owner's smartphone and wireless smart speakers can access the internet without authentication.

The network topology is shown below:



7.10.2 Solution

- Use a portal authentication network consisting of a primary AP and secondary APs. Enable the portal authentication on the primary AP and use it as the authentication gateway. Add the other APs to the authentication group as secondary nodes so that they use the same SSID and authentication policies, reducing repeated configuration.
- Configure an image-template authentication page. Upload shop promotional posters as background images, with multiple images rotating if needed, and link the background images to the shop promotion website. Set the post-authentication redirect to a specified URL to guide customers to online ordering, membership registration, or the official-account page.
- Configure the one-click authentication. Customers can access the internet by clicking **Connect to Internet**. Keep the authentication process short; the time customers spend on the authentication page serves as promotional exposure for the shop.
- Configure an authentication policy: Apply one-click authentication to the customer SSID **Cafe**.
- For in-store devices such as the shop owner's smartphone and wireless smart speakers, add the relevant MAC addresses to the authentication exemption whitelist. As long as the authentication exemption policy remains active, these devices do not need portal authentication on subsequent connections.

- Keep the optical modem in router mode with the internet connection already established. Connect the primary AP to a LAN port of the optical modem and obtain an IP address automatically through DHCP. It is recommended that you disable the optical modem's built-in Wi-Fi to avoid conflicts with the shop SSID.

Benefits:

- Brand exposure: Every customer first sees the customized branded authentication page when connecting to Wi-Fi, increasing brand touchpoints and awareness.
- Marketing conversion: Background-image links and post-authentication redirects guide customers to promotion pages, online ordering pages, or membership registration pages.
- Promotion: Rotating background images can be updated with the latest posters and coupon information as marketing campaigns change.

7.10.3 Configuration procedure

I. Enable portal authentication and add secondary nodes

1. Log in to the web UI of AP1 (primary node).
2. Navigate to **Portal Authentication** > **Portal Authentication**.
3. Enable **Portal Authentication** and set the AP role to **Main node**.
4. Click **Scan**. After the AP scans for other APs on the LAN, locate the APs to be added as the secondary nodes (AP2-AP4) of the portal authentication, and click ⊞ on the right of each corresponding entry.

   AP2-AP4 join the portal authentication group as secondary nodes and receive only the SSID configuration and authentication policies delivered by the primary node.

II. Configure the authentication page

Example authentication page parameters are shown in the following table. Leave any parameters not mentioned at their default settings.

Parameter	Example
Template Type	Image Template
Authentication Page Name	Shop Wi-Fi Authentication Page
Logo	Upload the shop logo image

Parameter	Example
Background Image	Upload 2–3 shop promotional poster images for rotation on the authentication page Image aspect ratio: 16:9 (recommended) or 19.5:9 (suitable for mobile phones). Each image must not exceed 300 KB in size. PNG format is recommended.
Image 1 Link	Product 1 link Example URL: https://www.ip-com.com.cn/en/product/M35.html
Image 2 Link	Product 2 link Example URL: https://www.ip-com.com.cn/en/product/M30.html
Redirect Address	Specified URL Example URL: https://www.ip-com.com.cn/en
Disclaimer	Internet access notice and personal information protection statement. Users must select the checkbox to accept it before login

Procedure:

1. Log in to the web UI of AP1 (primary node).
2. Navigate to **Portal Authentication** > **Authentication Page**.
3. Click **+ Manual Creation** and select **Image Template** as the **Template Type**.
4. Configure the authentication page parameters according to the table above, and click **Save**.

III. Configure the authentication method

Example one-click authentication parameters are shown in the following table. Leave any parameters not mentioned at their default settings.

Parameter	Example
Policy Name	Guest One-Click Authentication
Authentication Type	One-Click Authentication
Release Time	0 (no access before authentication)
Idle Timeout	30 minutes
Authentication Validity Period	2 hours (Covers the customer dining duration. After the validity period expires, reauthentication is required and the latest promotional page is displayed again)
Remark	Shop Customer Wi-Fi Authentication

Procedure:

1. Log in to the web UI of AP1 (primary node).
2. Navigate to **Portal Authentication** > **Authentication Method**.
3. Click **Create**.
4. Set **Policy Name** to **Guest One-Click Authentication**, select **One-Click Authentication** as the **Authentication Type**, and configure the other authentication parameters according to the table above.
5. Click **Save**.

IV. Configure the authentication policy

Example authentication policy parameters are shown in the following table.

Parameter	Example
Application Interface	SSID corresponding to the customer Wi-Fi, **Cafe** in this example
Authentication Page	Shop Wi-Fi Authentication Page
Authentication Method	Guest One-Click Authentication

Procedure:

1. Log in to the web UI of AP1 (primary node).
2. Navigate to **Portal Authentication** > **Authentication Policy**.
3. Click **Create** and configure the authentication policy parameters according to the table above.
4. Click **Save** and confirm that the policy status is **Enabled**.

V. Configure the authentication exemption policy

Assume that the MAC address of the wireless smart speaker is 44:37:E6:12:34:56 and that of the shop owner's smartphone is 44:37:E6:12:34:78.

1. Log in to the web UI of AP1 (primary node).
2. Navigate to **Portal Authentication** > **Exemption Authentication Policy**.
3. Click **Create**, enter the MAC address of the authentication exemption host, add remarks such as **Speaker** or **Shop Owner's Smartphone**, and click **Save**.

----End

7.10.4 Verification

- After a customer's smartphone connects to the shop Wi-Fi, the authentication page is displayed automatically and rotates through the shop promotional posters.
- Clicking a background image on the authentication page opens the shop promotion website.
- After the customer clicks **Connect to Internet** and authentication succeeds, the browser automatically redirects to the specified URL, such as the shop website, and the customer can access the internet normally.
- Customers must authenticate again after the authentication validity period (2 hours) expires.
- The wireless smart speaker and the shop owner's smartphone can access the internet without authentication.
- You can view and export authenticated user information on **Portal Authentication** > **User Management** to evaluate the number of customers reached by the promotional page.

Note

Process or export authentication information only after users have been adequately informed and the necessary authorization has been obtained. Limit the purpose and retention period, and implement access control and data masking measures.

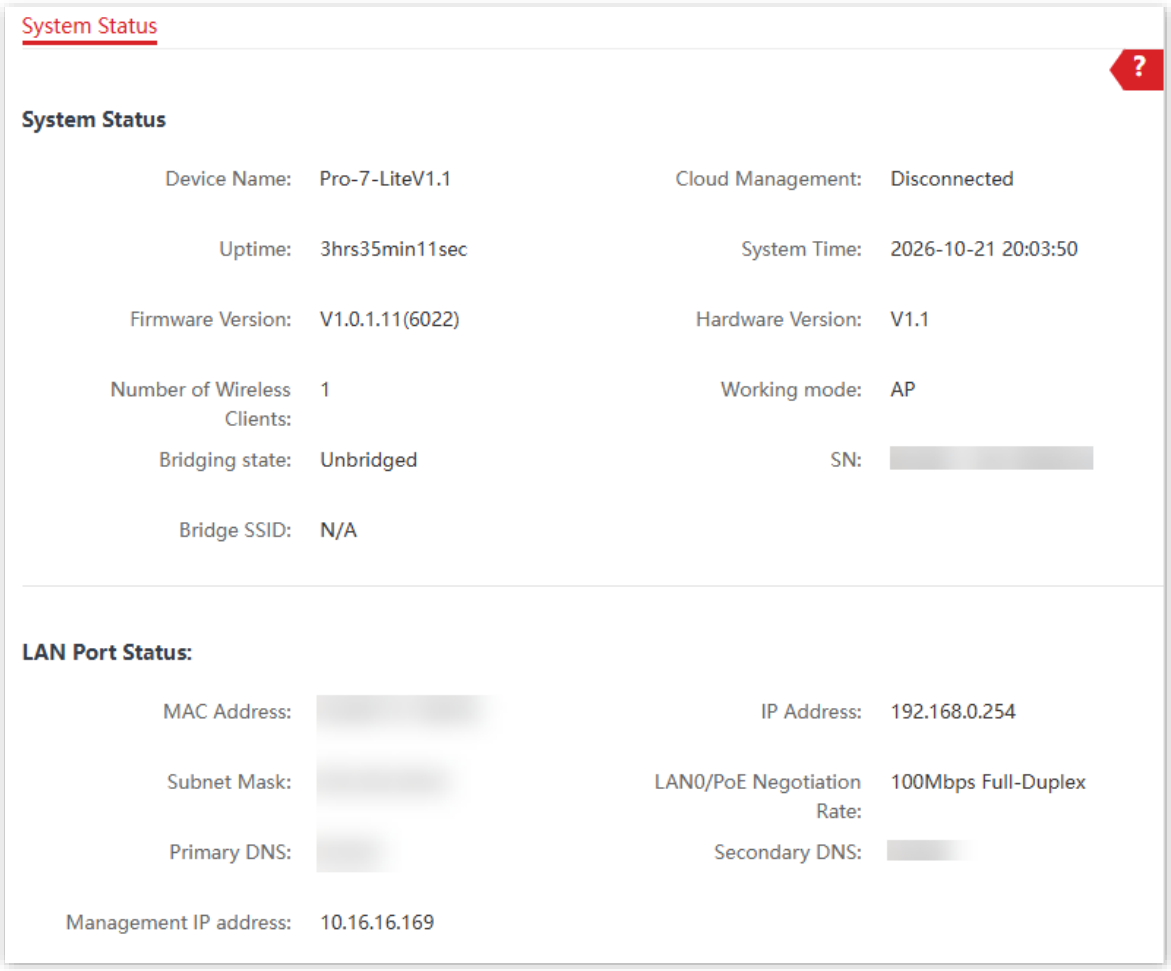
8 Maintain and monitor network

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.

8.1 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. The following figure is for reference only.



Parameter description

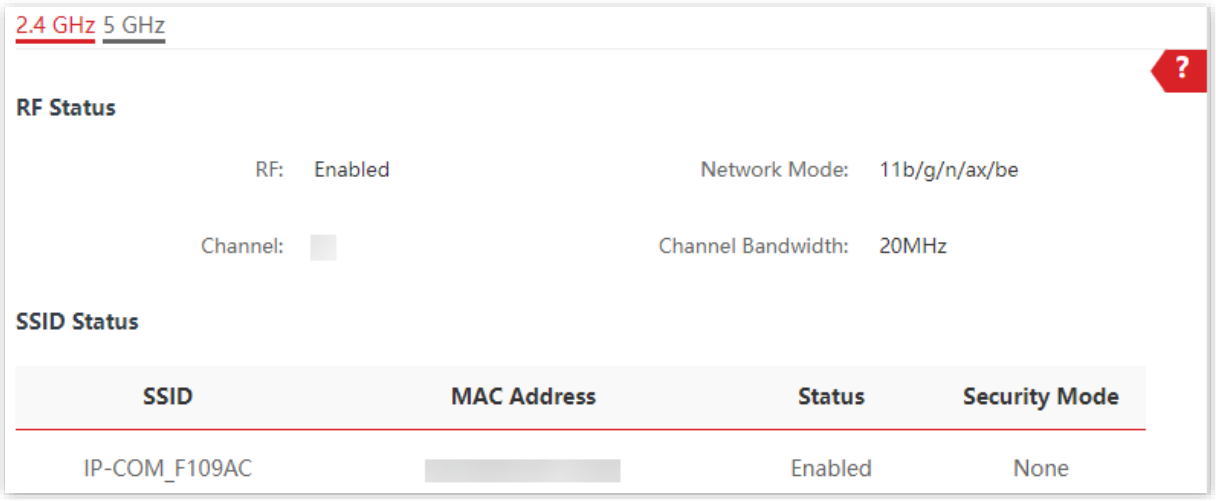
Parameter		Description
System Status	Device Name	Specifies the name of the AP. You can change the AP name on the LAN setup module. You are recommended to change the name of the AP to indicate the location of the AP (such as Hall), so that you can easily identify the AP when managing many APs.
	Cloud 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.
	Bridging SSID	Specifies the SSID of the upstream device for AP bridging.
	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 (internet IP address) of the AP. Users within the LAN can log in to the web UI of the AP using this IP address. This IP address is obtained from the LAN's DHCP server by default. If there is no DHCP server in the LAN where the AP is located, the default IP address will be 192.168.0.254. You can change the IP address on the LAN setup module. Tip – Before using this IP address to log in to the web UI of the AP, ensure that the IP address of the LAN user is in the same subnet as the AP's IP address. – If the QVLAN function is enabled, only users connected to the AP's management VLAN member ports can use this IP address to log in to the web UI of the AP.

Parameter		Description
	Subnet Mask	Specifies the subnet mask corresponding to the LAN port IP address of the AP.
	Primary DNS	Specifies the IP address of the primary DNS server of the AP.
	Secondary DNS	Specifies the IP address of the secondary DNS server of the AP.
	LAN0/PoE Negotiation Rate	Specifies the network rate negotiated with the peer device by the AP's PoE power input and data transmission multiplexing interface.
	LAN1 Negotiation Rate	Specifies the network rate negotiated between the AP's intranet network interface and the peer device. Tip This parameter is available on some APs. The actual product prevails.
	Management IP address	Specifies the management IP address of the AP. Users within the LAN 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 module. Tip – Before using this IP address to log in to the web UI of the AP, ensure that the IP address of the LAN user is in the same subnet as the AP's IP address. – If the QVLAN function is enabled, only users connected to the AP's management VLAN member ports can use this IP address to log in to the web UI of the AP.

8.2 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 wireless status for the 2.4 GHz band. To view the wireless status for the 5 GHz band, click **5 GHz**.



Parameter description

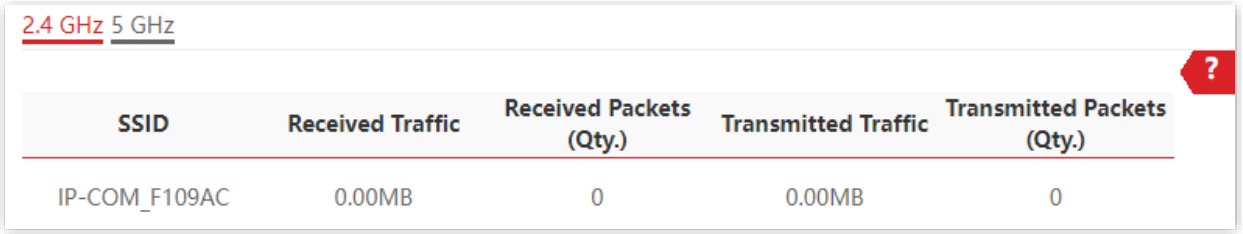
Parameter		Description
RF Status	RF	Specifies the status of the wireless function of the AP.
	Network Mode	Specifies the Wi-Fi network mode of the AP.
	Channel	Specifies the working channel of the AP.
	Channel Bandwidth	Specifies the channel bandwidth of the AP.
SSID Status	SSID	Specifies the names of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

8.3 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 Wi-Fi network of the AP.

By default, the page displays traffic statistics for the 2.4 GHz band. To view statistics for the 5 GHz band, click **5 GHz**.



Parameter description

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

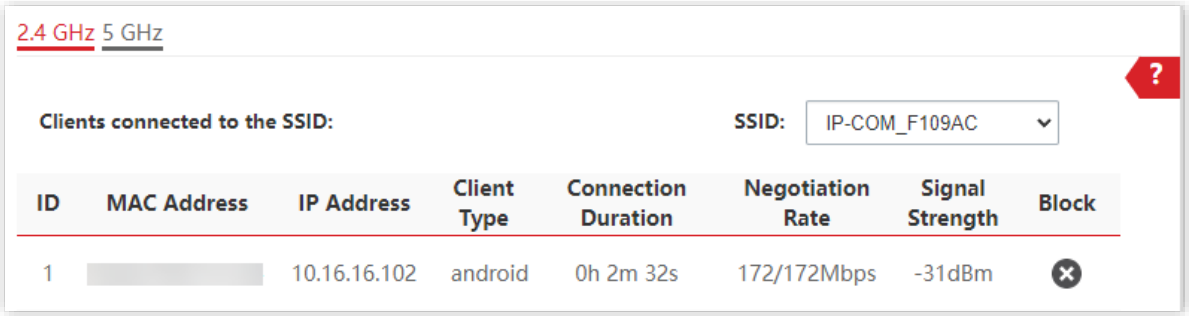
Note

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

8.4 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 Wi-Fi networks corresponding to the SSIDs of the AP.



By default, the page displays information about the wireless clients connected to the 2.4 GHz Wi-Fi 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 Wi-Fi 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 Wi-Fi 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.  The AP can correctly identify the client's operating system type only when the Identify Client Type function is enabled and the client has accessed an HTTP website.
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.

8.5 View system log

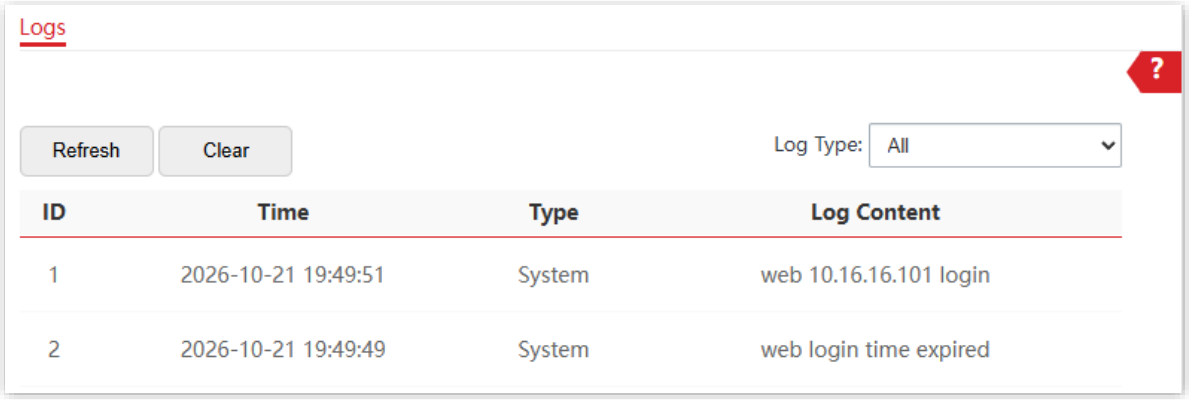
The logs of the AP record various events that occur and the operations that users perform after the AP starts. In case of a system fault, you can refer to the logs during troubleshooting.



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

Procedure for viewing system log

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **System Log**.
3. (Optional) Click **Refresh** to view the latest logs of the AP, or click **Clear** to clear the existing logs of the AP.



---End

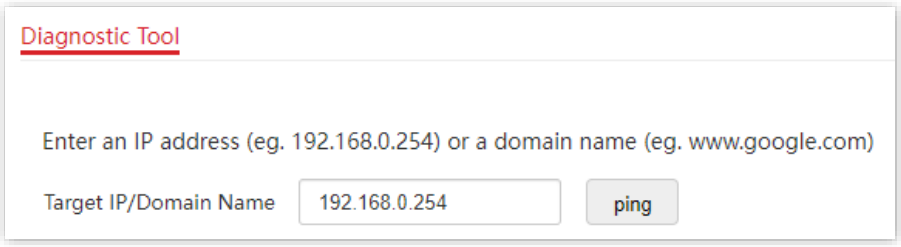
8.6 Diagnose the network

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

Procedure for diagnosing the network

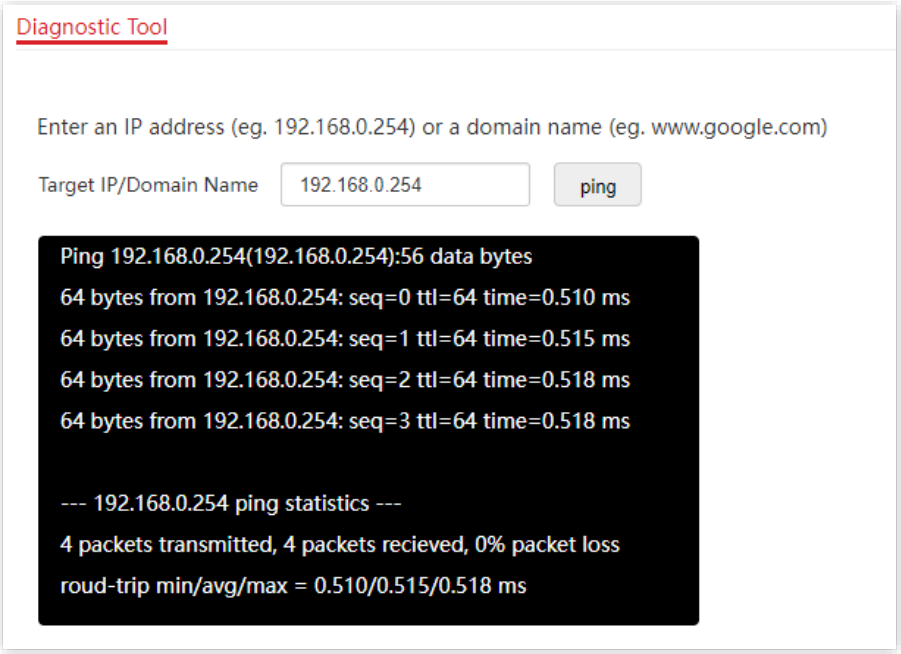
The connection to **192.168.0.254** is used as an example.

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Diagnostic Tool**.
3. 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.
4. Click **ping**.



---End

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

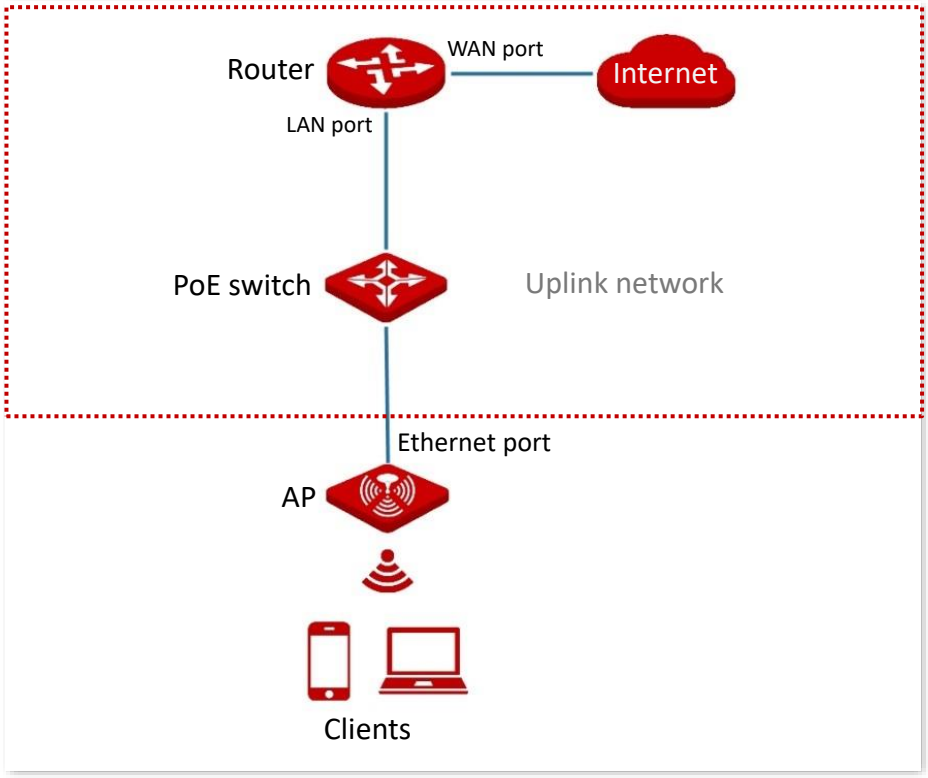


8.7 Configure uplink detection

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. Wireless clients can reconnect to the AP only after the connection between the AP and the upstream network is restored.

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).



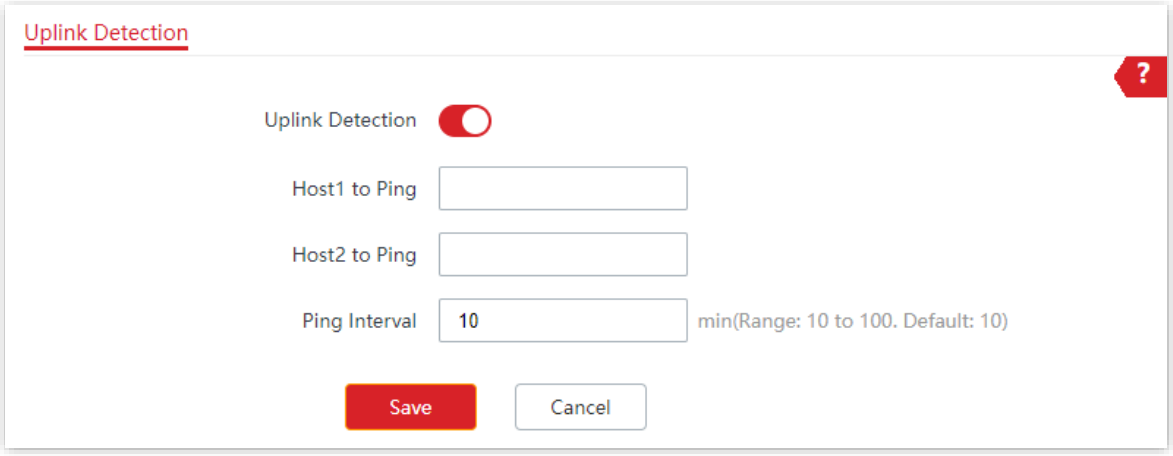
Procedure for configuring uplink detection

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Uplink Detection**.
3. Enable the **Uplink Detection** function.
4. Enter the IP address of the host to be pinged in **Host1 to Ping** or **Host2 to Ping**, such as the IP address of the switch or router directly connected to the AP.

Tip

If there is only one destination host address, enter that address for both **Host1 to Ping** and **Host2 to Ping**.

5. Set **Ping Interval** to the interval at which the AP detects its uplink.
6. Click **Save**.



---End

Parameter description

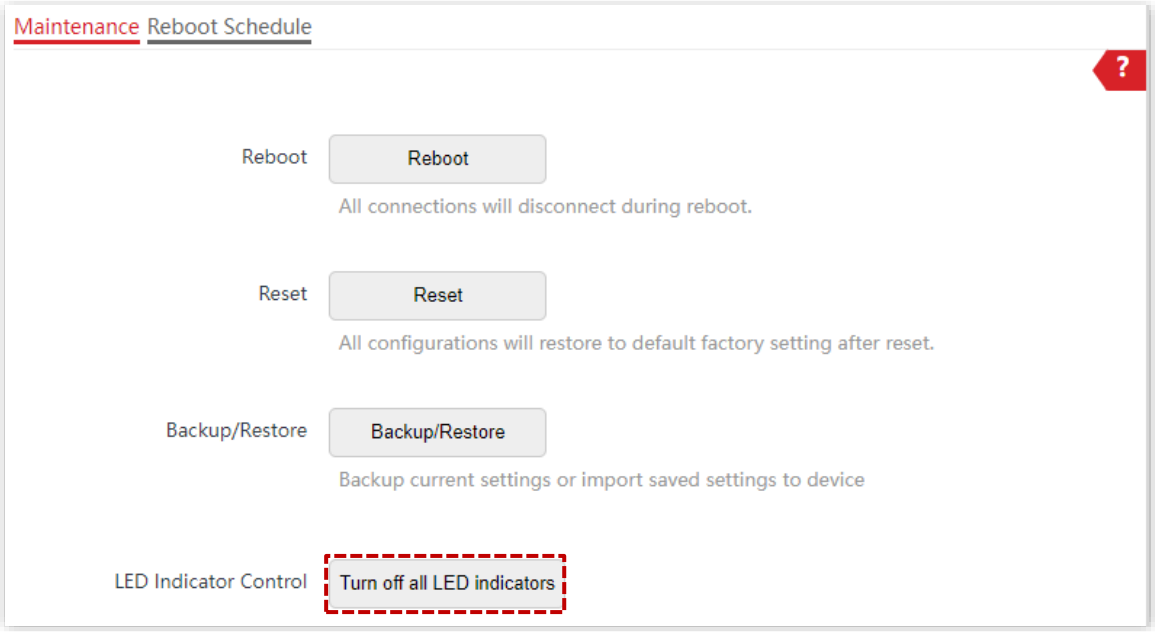
Parameter	Description
Uplink Detection	Specifies whether to enable the uplink detection function of the AP.
Host1 to Ping	Specify the IP address of the host to be pinged through the Ethernet port of the AP. It is available only when the uplink detection function is enabled.
Host2 to Ping	
Ping Interval	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**.

8.8 Control LED indicator

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

8.8.1 Turn off the LED indicator

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

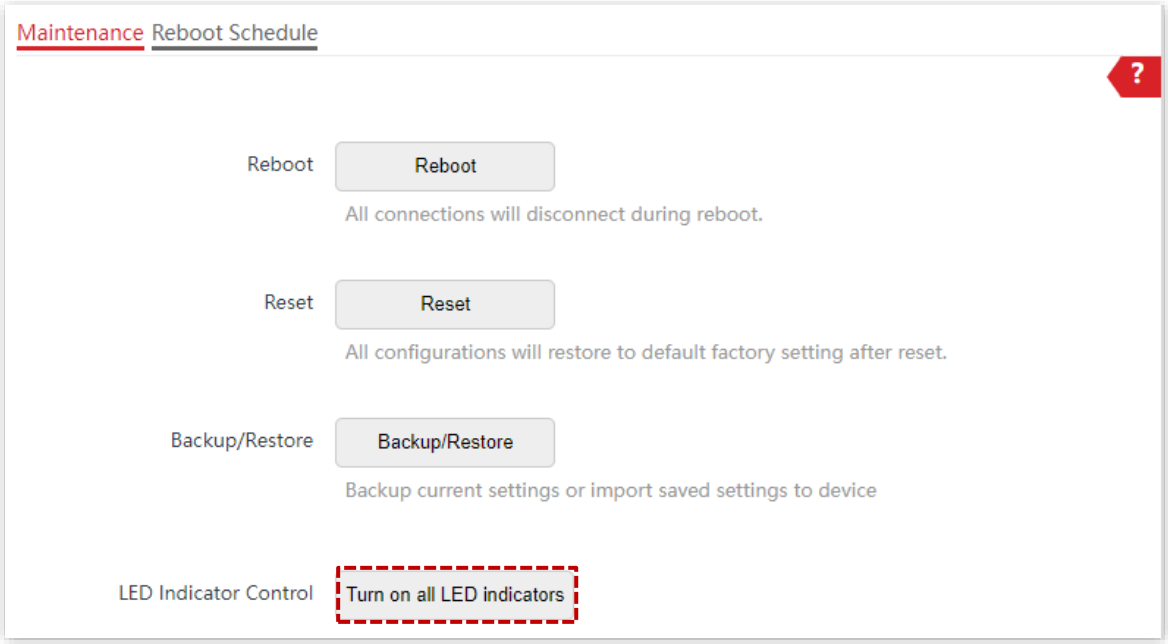


---End

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

8.8.2 Turn on the LED indicator

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



---End

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

8.9 Configure system time

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

8.9.1 Sync the time with the internet

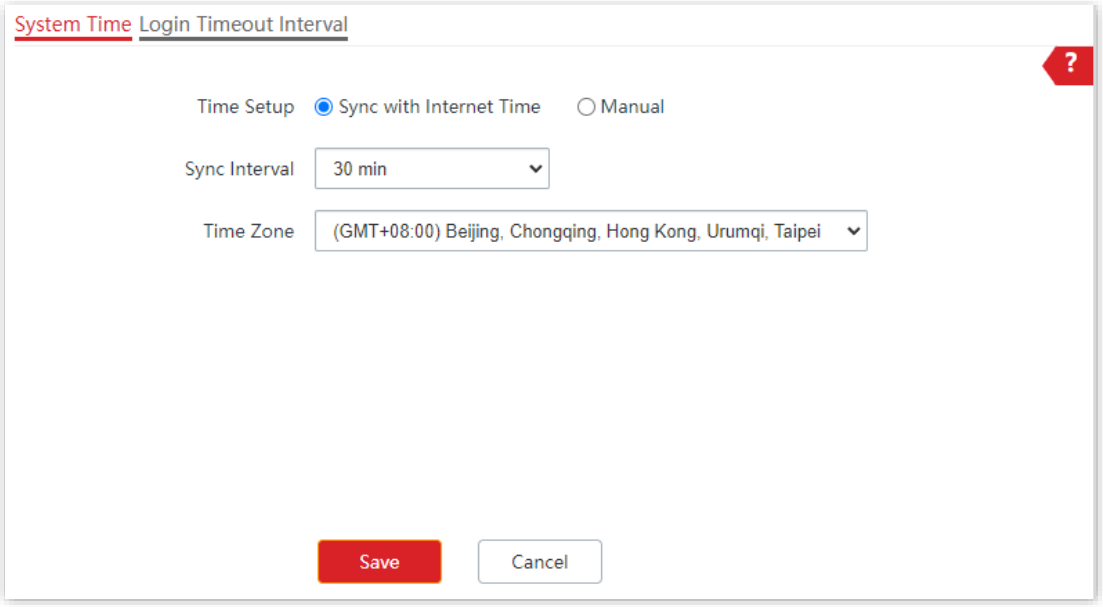
The AP automatically synchronizes its system time with an internet time server. This enables the AP to automatically correct its system time after being connected to the internet. For details about how to connect the AP to the internet, refer to Internet settings.

Tip

When **Sync with Internet Time** is enabled, the AP can automatically synchronize its time after a reboot without requiring reconfiguration.

Procedure for synchronizing the time with the internet

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Date & Time** > **System Time**.
3. Set **Time Setup** to **Sync with Internet Time**.
4. Set the interval at which the AP will automatically synchronize with a time server of the internet, which is **30 min** in this example.
5. Set the time zone for the region in which the AP is located.
6. Click **Save**.



---End

After the configuration is completed, the AP automatically synchronizes with the internet time every 30 minutes.

8.9.2 Manually set the time

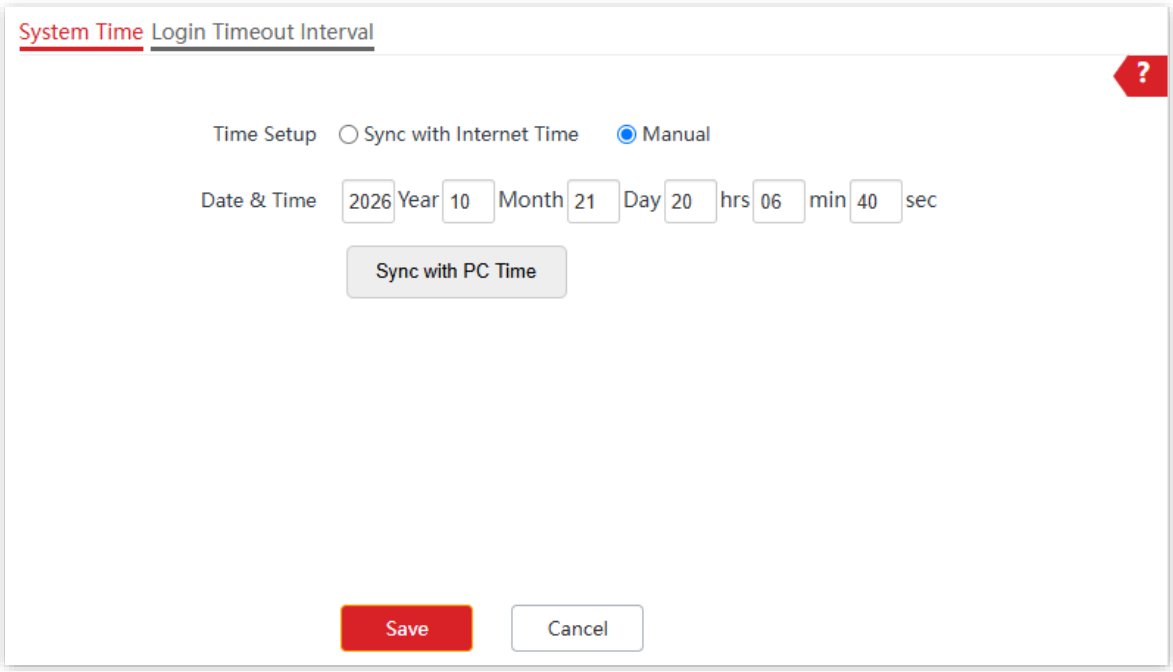
You can manually set the system time of the AP.

Tip

If the time is set manually, the AP's system time must be set again after each reboot.

Procedure for manually setting the time

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Date & Time** > **System Time**.
3. Set **Time Setup** to **Manual**.
4. Manually enter the date and time, or click **Sync with PC Time** to synchronize the system time of the AP with the system time of the management computer.
5. Click **Save**.



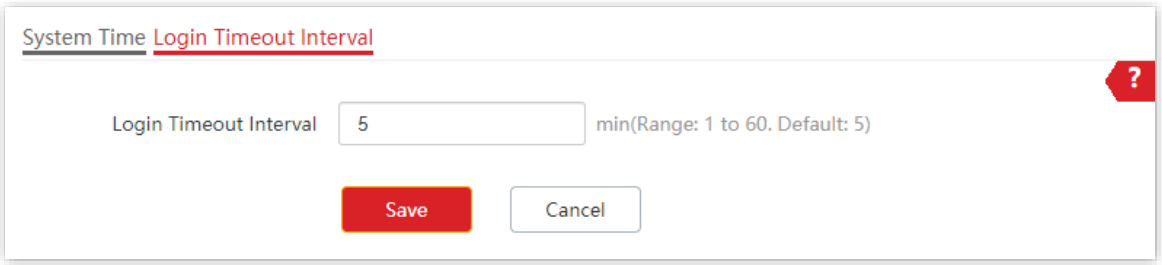
---End

8.10 Configure login timeout interval

You can set the login timeout interval. If you log in to the web UI of the AP and perform no operation within the login timeout interval, the AP logs you out for network security. The default login timeout interval is 5 minutes.

Procedure for configuring login timeout interval

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Date & Time** > **Login Timeout Interval**.
3. Set the **Login Timeout Interval** as required.
4. Click **Save**.



---End

8.11 Change login password

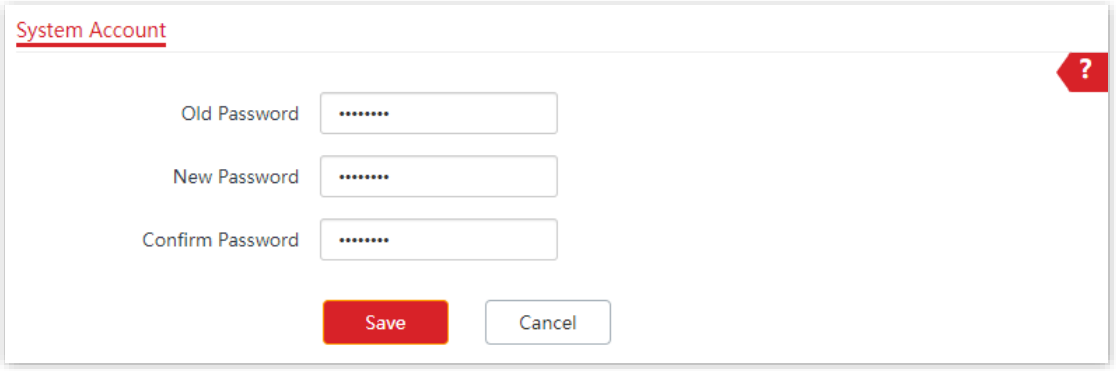
When logging in to the AP's web UI for the first time, set a login password as required to ensure security. Additionally, during AP usage, regularly change the web UI password to maintain ongoing security.

Procedure for changing login password

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **System Account**.
3. Enter the current password in **Old Password**.
4. Enter the new password in **New Password**.

> Note
>
> For initial setup or after a reset, set the new login password to ensure privacy and security. The longer the password, the higher the security. The character limit and composition rules for passwords are subject to software user interface prompts.

5. Re-enter the new password in **Confirm Password**.
6. Click **Save**.



---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.

8.12 Reboot the AP

Tip

Rebooting the AP will disconnect all connections. It is recommended that you reboot the AP during off-peak hours.

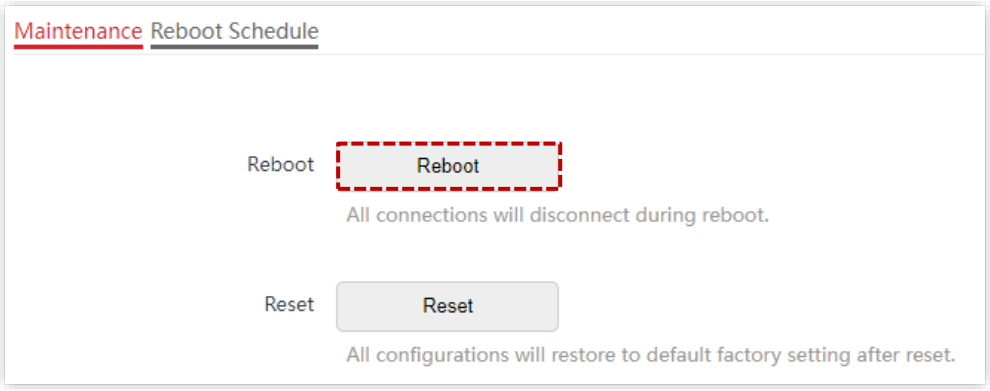
If a setting does not take effect or the AP works improperly, you can try rebooting the AP manually to resolve the problem.

You can also configure the AP to reboot automatically as required for maintenance. The AP supports the following reboot schedule types:

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

8.12.1 Manual reboot

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Reboot**.



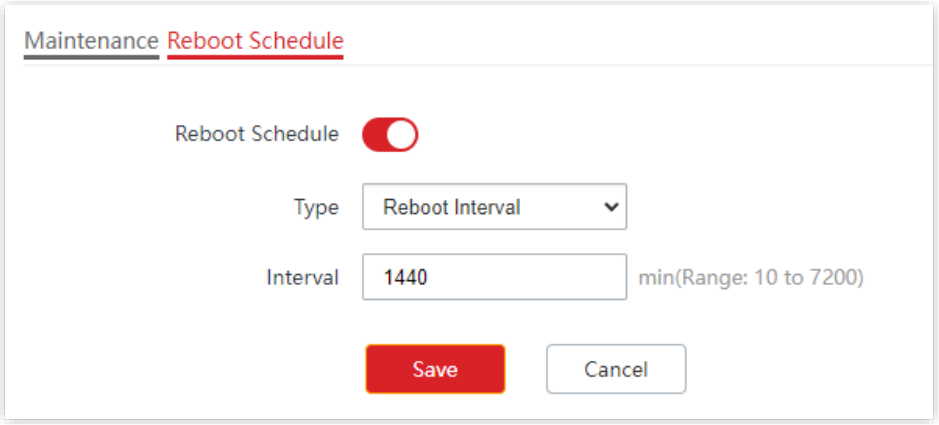
4. Confirm the prompt information, and click **OK**.

---End

8.12.2 Configure the AP to reboot at an interval

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Reboot Schedule**.
3. Enable the **Reboot Schedule** function.
4. Set **Type** to **Reboot Interval**.

5. Set **Interval** to a value in minutes, which is **1440** in this example.
6. Click **Save**.



---End

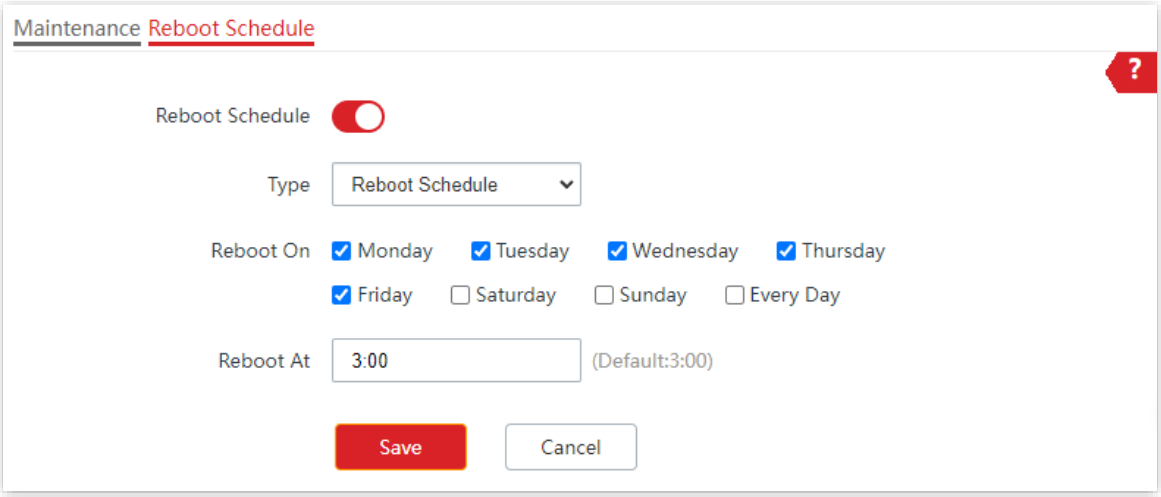
After the configuration is completed, the AP will automatically reboot every 24 hours.

8.12.3 Configure the AP to reboot at a specified time

Tip

Rebooting at a specified time is based on the system time. To ensure that the AP reboots at the specified time, make sure that the system time is correct.

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Reboot Schedule**.
3. Enable the **Reboot Schedule** function.
4. Set **Type** to **Reboot Schedule**.
5. Select the days on which the AP will reboot: **Monday** through **Friday** in this example.
6. Set the time when the AP reboots, which is **3:00** in this example.
7. Click **Save**.



---End

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

8.13 Backup and restore

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

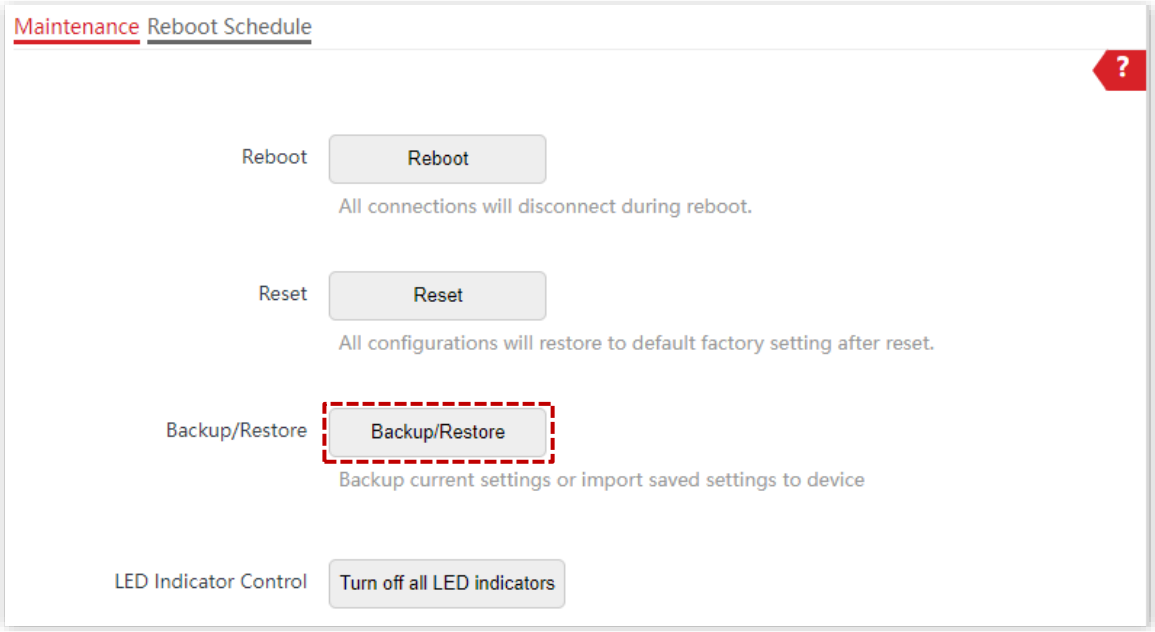
If the AP operates as expected after significant configuration changes, it is recommended that you back up the new configuration so that you can restore it after an upgrade or reset.

Tip

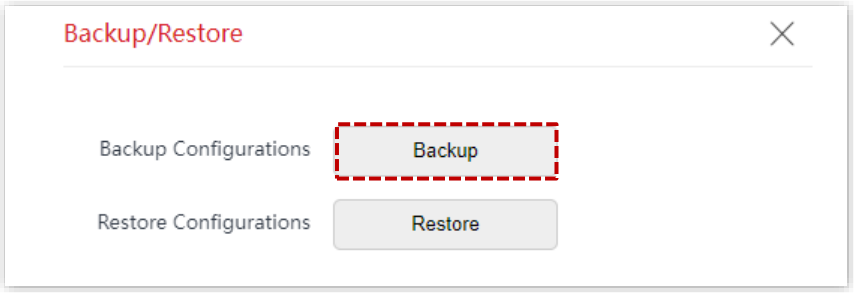
If you need to apply the same or similar configurations to many APs, you can configure one of the APs, back up the configuration of the AP, and use the backup to restore the configuration on the other APs. This improves configuration efficiency.

8.13.1 Back up the current configuration

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Backup/Restore**.



4. Click **Backup**.



---End

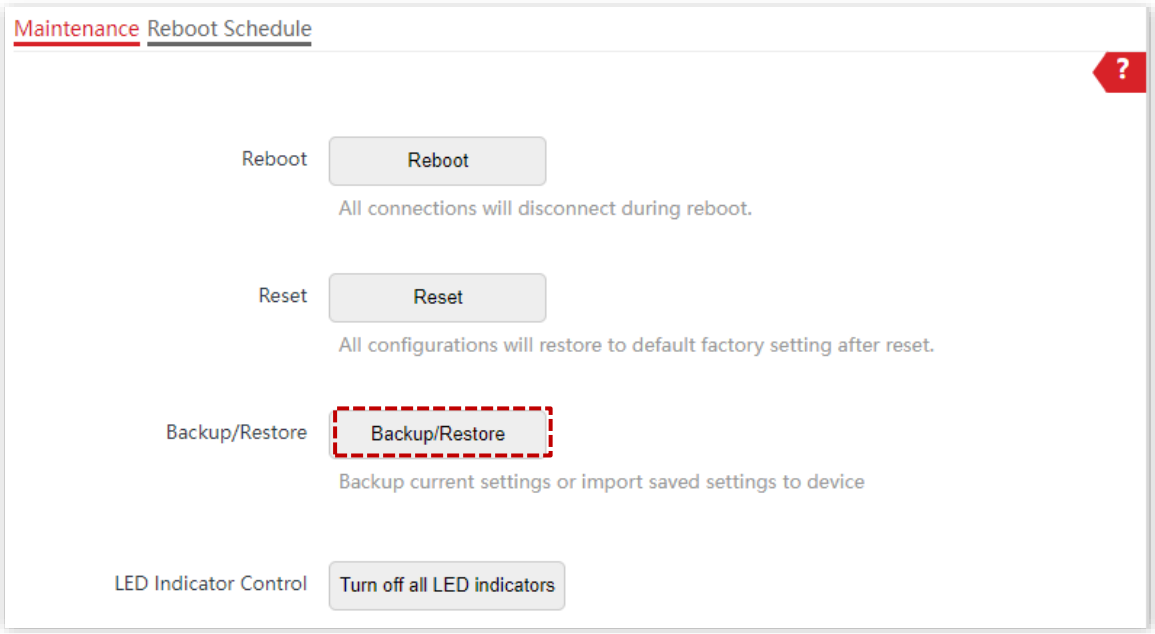
A configuration file named **APCfm.cfg** is downloaded.

Tip

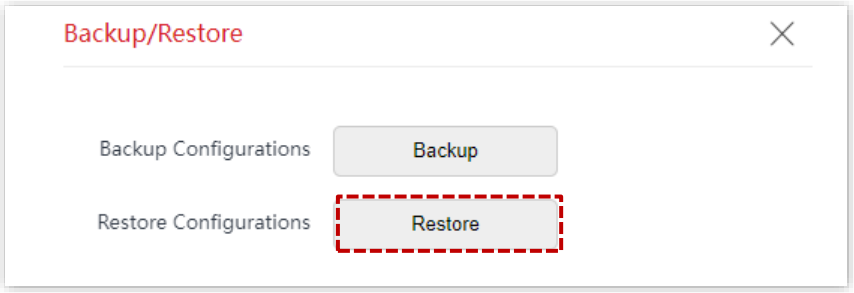
If the prompt “This type of file can harm your computer. Do you want to keep APCfm.cfg anyway?” appears, click “Keep”.

8.13.2 Restore a configuration

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Backup/Restore**.



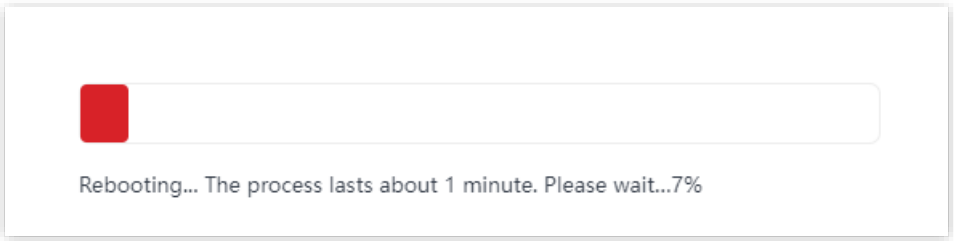
4. Click **Restore**.



5. Select and upload the configuration file (suffixed with .**cfg**) to be restored.

---End

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



8.14 Reset the AP

If you cannot resolve an AP issue or you forget the AP web UI password, you can reset the AP to restore its factory settings and then configure it again.

Note

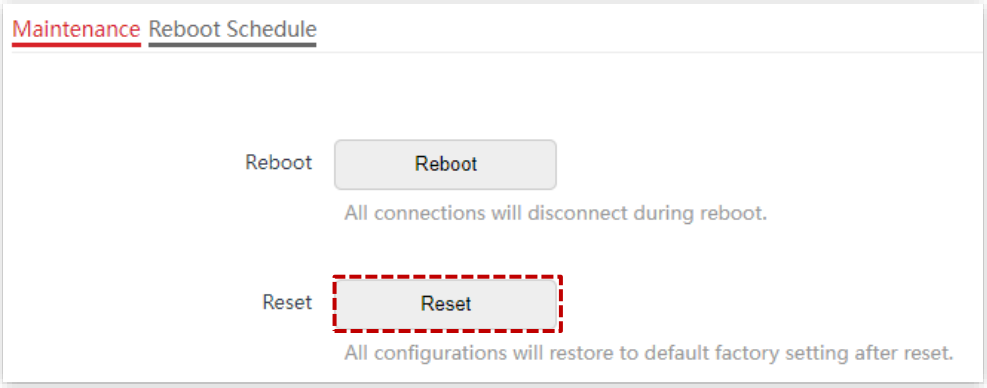
- When the factory settings are restored, your configuration will be cleared. Therefore, you need to reconfigure the AP to reconnect to the internet. Restore the factory settings of the AP only when necessary.
- You are recommended to back up the configuration before restoring the factory settings.
- To prevent damage to the AP, ensure that the AP has a stable power supply while it is being reset.

Method 1: Reset the AP using the reset button

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

Method 2: Reset the AP on the web UI

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **Maintenance** > **Maintenance**.
3. Click **Reset**.



4. Confirm the prompt information, and click **OK**.

---End

8.15 Upgrade system software

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

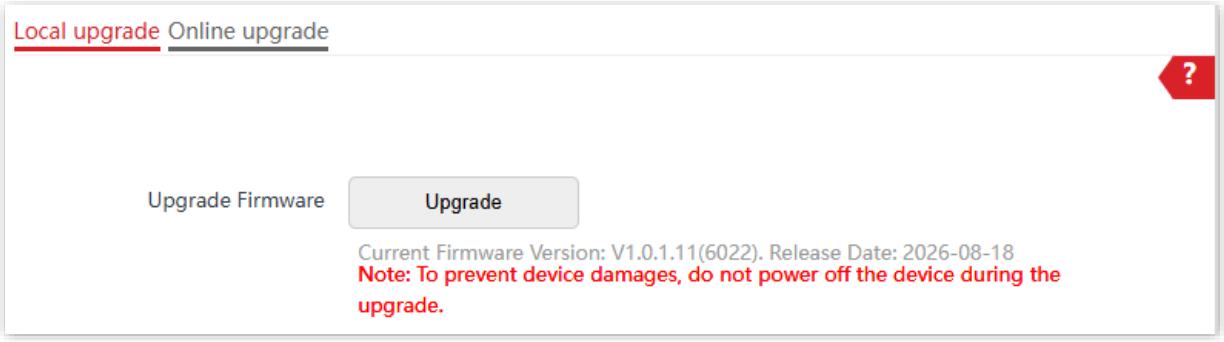
Note

To ensure a correct upgrade and avoid damage:

- Ensure that the new firmware is applicable to the AP. Generally, the decompressed firmware file has a **.bin** filename extension.
- Keep a proper power supply to the AP during the upgrade. For an online upgrade, ensure that the AP maintains a stable internet connection throughout the upgrade.

8.15.1 Local upgrade

1. Download the package of the latest firmware version for the AP from www.ip-com.com.cn to your local computer, and decompress the package. Generally, the firmware file in the downloaded package has a **.bin** filename extension.
2. Log in to the web UI of the AP.
3. Navigate to **Tools** > **System Software Upgrade** > **Local upgrade**.
4. Click **Upgrade**. The following figure is for reference only.



5. Select and upload the upgrade file in the pop-up window.

---End

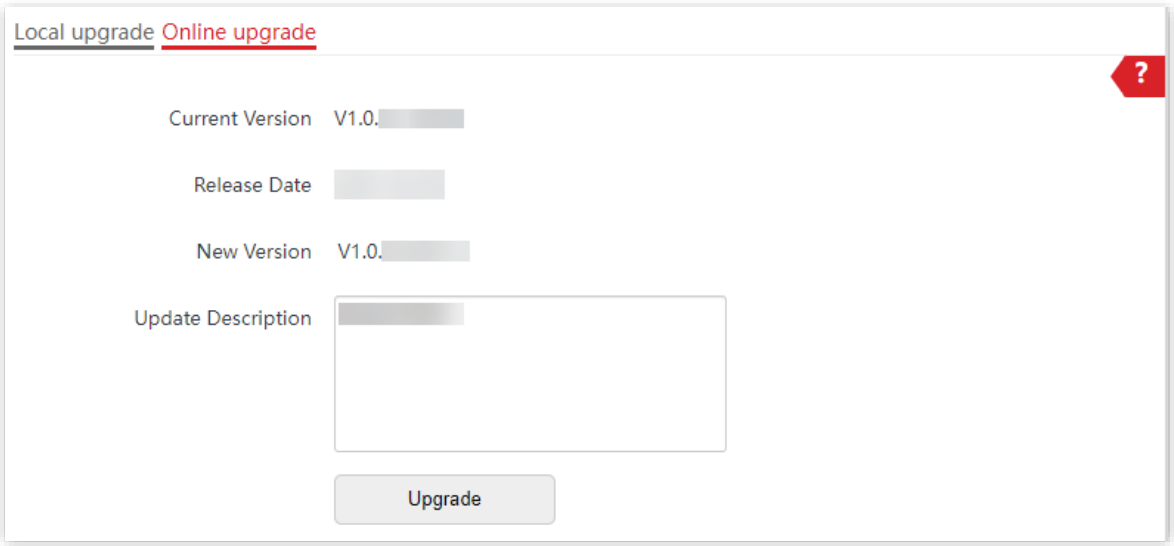
Wait until the progress bar is complete. Log in to the web UI of the AP again, navigate to **Status** > **System Status** and check whether the upgrade is successful based on **Firmware Version**.

8.15.2 Online upgrade

After the AP connects to the internet, the system automatically checks for new firmware and displays information about any available version. When a new upgrade firmware is displayed on the page, you can upgrade the AP as required.

Procedure for performing online upgrade

1. Log in to the web UI of the AP.
2. Navigate to **Tools** > **System Software Upgrade** > **Online upgrade**.
3. Wait until a new firmware version is detected. The following figure is for reference only.



4. Click **Upgrade**.

---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**.

8.16 Configure remote web management

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 authorized remote access to the AP web UI for scenarios such as remote technical support.

The remote web management function is disabled by default.

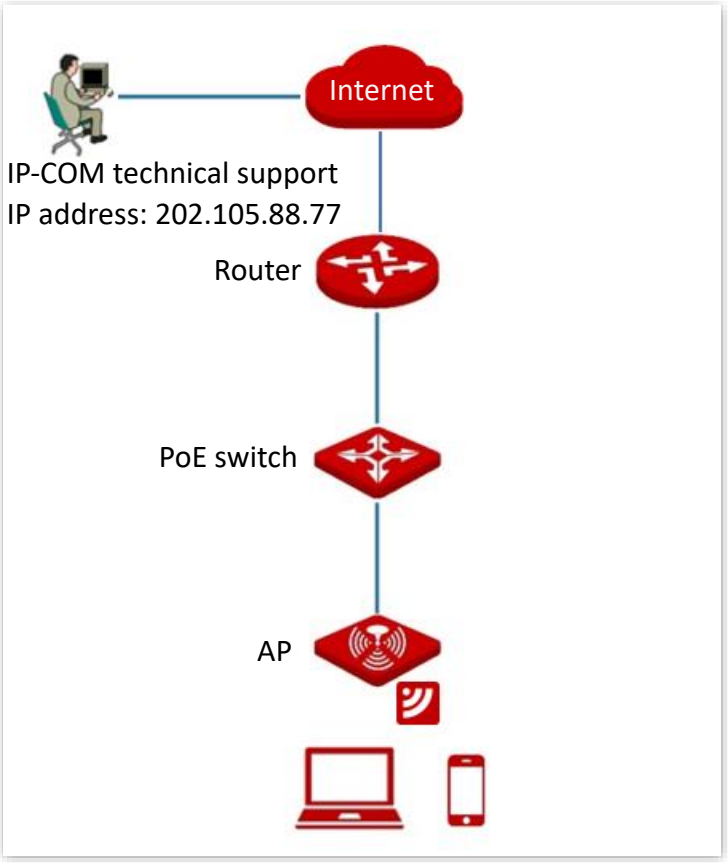
Example of configuring remote management

Networking requirements

An enterprise uses the AP to set up a network and has connected to the internet. The network administrator encounters a configuration problem and needs IP-COM technical support to remotely log in to the AP web UI for analysis and troubleshooting.

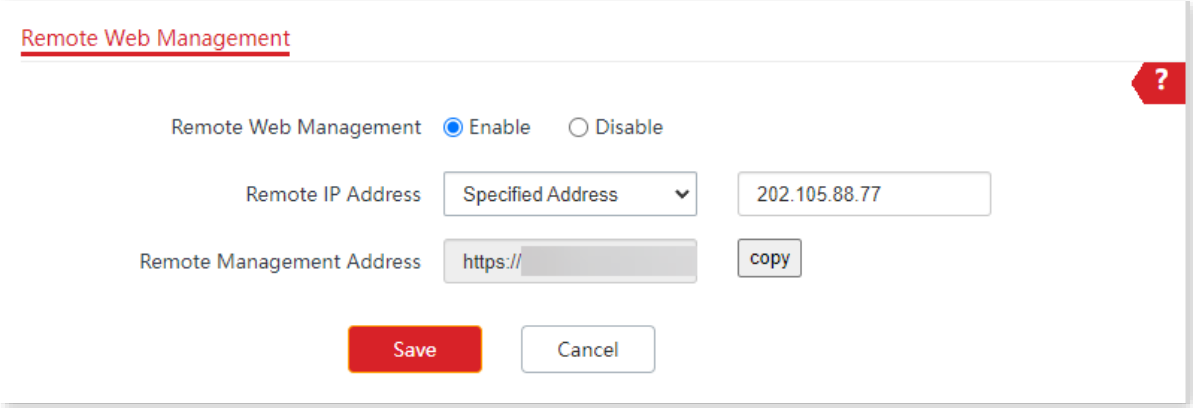
Solution

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



Procedure for configuring remote management

1. Log in to the web UI of the AP.
2. Navigate to **Advanced** > **Remote Management**.
3. Enable the **Remote Web Management** function.
4. Set **Remote IP Address** to **Specified Address.** Enter the public IP address used by the IP-COM technician, which is **202.105.88.77** in this example.
   - **All Addresses**: Devices with any IP address on the internet can access the web UI of the AP. For network security, this option is not recommended.
   - **Specified Address**: Only devices with specified IP addresses can access the web UI of the AP. If the device is in the local area network, the IP address (public IP address) of the gateway of the device should be filled in.
5. Click **Save**.



---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).

8.17 Change the cloud management mode

After the AP is successfully added to the cloud platform, you can change the cloud management mode as required.

Procedure for changing the cloud management mode

1. Log in to the web UI of the AP.
2. Navigate to **Advanced** > **Cloud Maintenance**.
3. Change the **Management Mode** as required.
   - **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. Except for necessary settings such as cloud maintenance, no other configurations can be made on the AP's own web UI.
   - **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 or local wireless controller, and the information is reported to the IP-COM ProFi cloud platform.
4. Click **Save**.

---End

9 Configure QVLAN

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.

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.

Example of configuring QVLAN settings

Networking requirements

A hotel has the following Wi-Fi network coverage requirements:

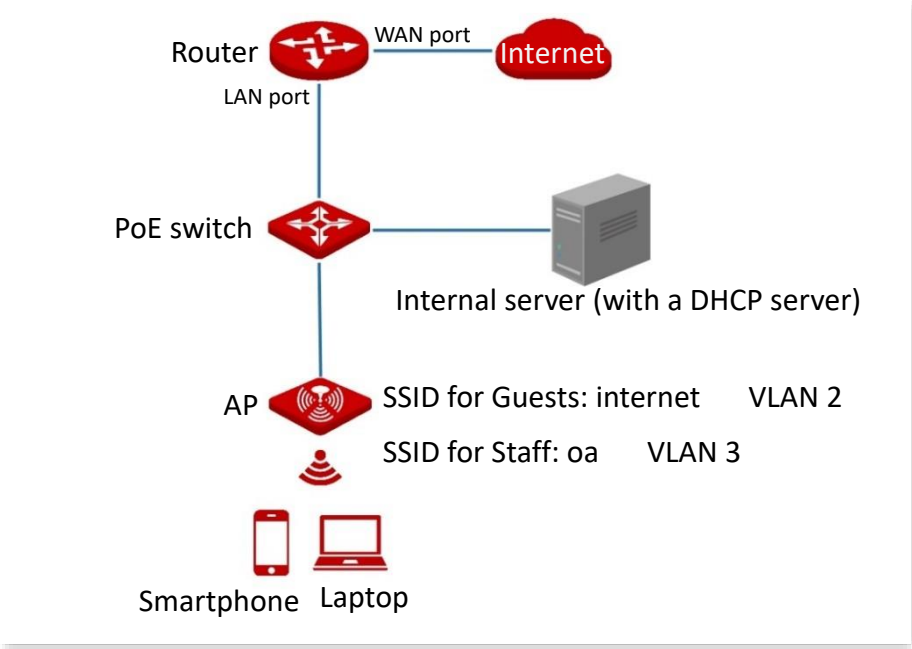
- Guests are connected to VLAN 2 and can access only the internet.
- Staff are connected to VLAN 3 and can access only the intranet.

Solution

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

Tip

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



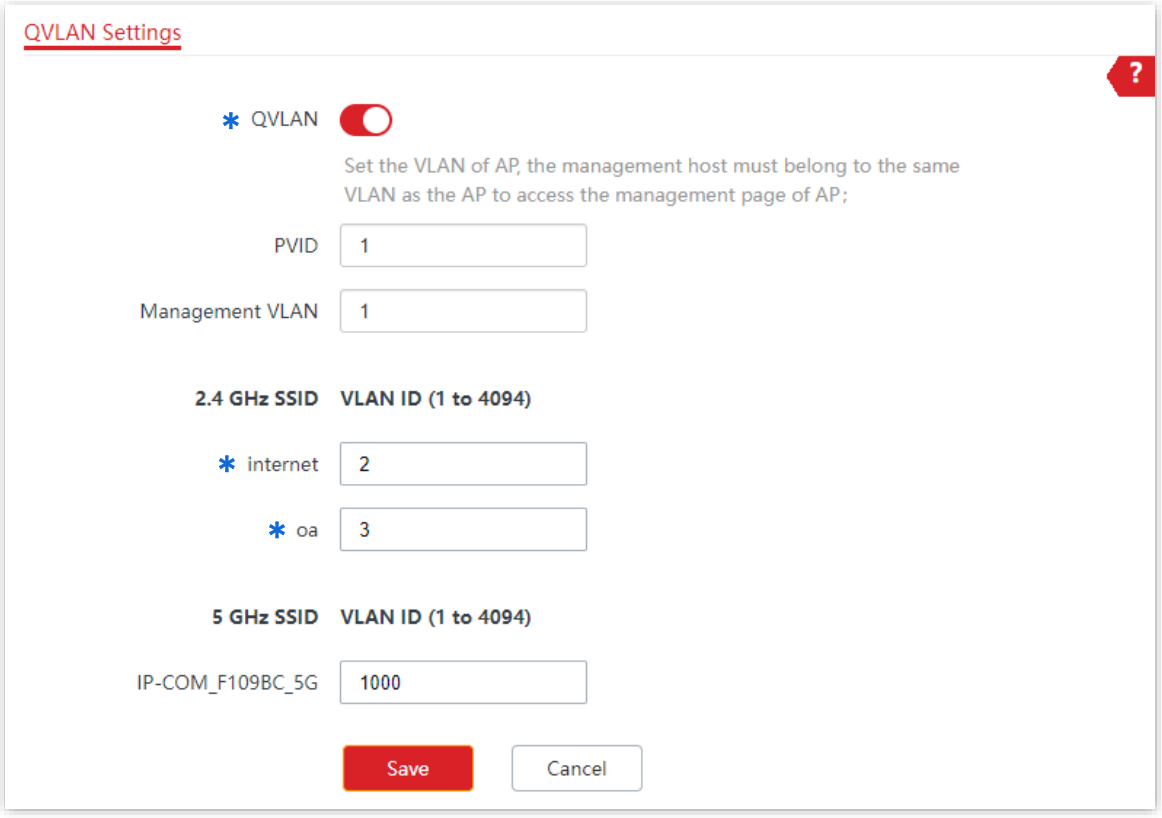
Procedure for configuring QVLAN settings

I. Configure the AP

1. Log in to the web UI of the AP.
2. Navigate to **Wireless** > **QVLAN Settings**.
3. Enable the **QVLAN** function.
4. Modify the VLAN IDs of the SSIDs on the 2.4 GHz band. Set the VLAN ID of **internet** to **2** and **oa** to **3** respectively.
5. Click **Save**.

Tip

For some AP models, after you click **Save**, a confirmation dialog box appears. Confirm the operation as prompted. The AP then automatically reboots for the configuration to take effect.



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

Parameter description

Parameter	Description
QVLAN	Specifies whether to enable the 802.1Q VLAN function of the AP. By default, it is disabled.

Parameter	Description
PVID	Specifies the ID of the default native VLAN of the trunk port of the AP.
Management VLAN	Specifies the ID of the AP management VLAN. After changing the management VLAN, you can manage the AP only after connecting your computer or AP controller to the new management VLAN.
Trunk Port	Used to select the port to be set to trunk mode. A trunk port allows traffic from all VLANs to pass. Note When you enable the 802.1Q VLAN function, choose at least one LAN port as the trunk port. If the AP has only one Ethernet port, this port serves as the trunk port by default.
Wired LAN Port	Specifies the Ethernet port of the AP and the ID of the VLAN to which a LAN port belongs. – **LAN0**: The PoE power and data transmission multi-functional port of the AP. – **LAN1**: The data transmission port of the AP. Tip An Ethernet port that is not set as a trunk port operates as an access port, and you can set its VLAN ID.
2.4 GHz SSID	Specify the currently enabled SSIDs on the 2.4 GHz or 5 GHz band and the VLAN IDs corresponding to the SSIDs. Tip After the QVLAN function is enabled, the wireless ports corresponding to the SSIDs function as access ports. The PVID and VLAN ID of an access port are the same.
5 GHz SSID	
VLAN ID	

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 Mode
SSID Settings	SSID	2.4 GHz	The AP allows *X* SSIDs. X may vary with APs of different models. For details, you can log in to the web UI of the AP and view the related parameters on the **Wireless** > **SSID** page. Except for the Smart Home SSID, the SSIDs are **IP-COM_*XXXXXX***, where ***XXXXXX*** ranges from the last six digits of the AP's LAN port MAC address to the last six digits + **X** − **1**. Smart home SSID: **IP-COM_*XXXXXX*+3-IOT** By default, the first SSID is enabled, and the other SSIDs are disabled.
		5 GHz	The AP allows *Y* SSIDs. Y may vary with APs of different models. For details, you can log in to the web UI of the AP and view the related parameters on the **Wireless** > **SSID** page. The SSIDs are **IP-COM_*XXXXXX*_5G**, where ***XXXXXX*** ranges from the last six digits of the AP's LAN port MAC address + ***X*** to the last six digits + ***X*** + ***Y*** − **1**. By default, the first SSID is enabled, and the other SSIDs are disabled.
RF Settings	Wireless Network		Enable

A.2 Acronyms & Abbreviations

Acronym or Abbreviation	Full Spelling
AC	Access Point Controller
ACK	Acknowledgment
AES	Advanced Encryption Standard
AP	Access Point
APSD	Automatic Power Save Delivery
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DTIM	Delivery Traffic Indication Map
DNS	Domain Name System
FIFO	First-in First-out
GI	Guard Interval
ID	Identifier
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MLO	Multi-Link Operation
MU-MIMO	Multi-User Multiple-Input Multiple-Output
OFDMA	Orthogonal Frequency Division Multiple Access
PoE	Power over Ethernet
PSK	Pre-shared Key
PVID	Port VLAN ID
RF	Radio Frequency

Acronym or Abbreviation	Full Spelling
RTS	Request To Send
SAE	Simultaneous Authentication of Equals
Short GI	Short Guard Interval
SSID	Service Set Identifier
U-APSD	Unscheduled Automatic Power Save Delivery
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMF	Wireless Multicast Forwarding
WPA	Wi-Fi Protected Access