



Wireless Access Point

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY

RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Applicable Models

This manual is applicable to the wireless access point.

Symbol Conventions

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

Symbol	Description
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause overheating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Power Supply
 - Device powered by Safety Extra-Low Voltage (SELV): The power source should meet limited power source or PS2 requirements according to IEC 60950-1 or IEC 62368-1 standard.
 - Device powered by AC mains supply voltage: The equipment must be connected to an earthed mains socket-outlet. An appropriate readily accessible disconnect device shall be incorporated external to the equipment. An appropriate overcurrent protective device shall be incorporated external to the equipment, not exceeding the specification of the building. An all-pole mains switch shall be incorporated in the electrical installation of the building. If the device is powered by terminals connected to the power cord, ensure correct voltage and wiring of the

terminals for connection to mains supply. The equipment has been designed, when required, modified for connection to an IT power distribution system.

TABLE OF CONTENTS

Chapter 1 Activation & Login	1
1.1 Activation	1
1.2 Login.....	2
Chapter 2 Configuration Guide	3
2.1 Network Configuration	3
2.2 Wireless Network Settings.....	3
Chapter 3 General Toolbar	5
Chapter 4 Overview Information	6
Chapter 5 User Terminal Management	7
Chapter 6 Network Management	8
6.1 Uplink Port Configuration	8
6.2 LAN Settings.....	9
6.3 Port VLAN.....	9
Chapter 7 Wireless Network Management	11
7.1 Wireless Network Settings.....	11
7.2 Wireless Optimization.....	12
7.2.1 Quick Optimization	12
7.2.2 Scheduled Optimization.....	13
7.2.3 Optimization Record	14
7.3 Wireless Access Control.....	14
7.3.1 Blocklist	14
7.3.2 Allowlist.....	15
7.4 Wireless Speed Limit.....	16
7.5 RF Configuration	18
Chapter 8 Behavior Management	21
8.1 QoS.....	21
8.2 DSCP	21
Chapter 9 Fault Diagnosis	24
9.1 Network Self-Test	24
9.2 Fault Alarm.....	24
9.3 Network Tool	25
9.3.1 PING	25
9.3.2 Search Route	25
9.3.3 Search Domain Name	26
9.4 Faults Collection.....	26
9.5 SSH	27
Chapter 10 System Configuration	28
10.1 System Configuration.....	28
10.1.1 Basic Information	28
10.1.2 Time Settings	28

10.2 Hik-Connect Configuration	29
10.3 AP Status Indicator	30
Chapter 11 Maintenance and Security	31
11.1 System Maintenance	31
11.1.1 Restart	31
11.1.2 Upgrade	31
11.1.3 Restore	32
11.1.4 Security Audit Log	32
11.2 Login Management	33

Chapter 1 Activation & Login

After device networking, you may go to activate and log in to the wireless access point for remote management and configuration.

1.1 Activation

For the security of your privacy and system data, you are required to set a password for your first use. After the password has been set, you can log in to the web interface for further configuration.

Steps

Step 1 Connect your terminal to the Wi-Fi network of the access point.

Step 2 Start a browser.

Step 3 Enter the default IP address of the access point in the address bar and press **Enter**.

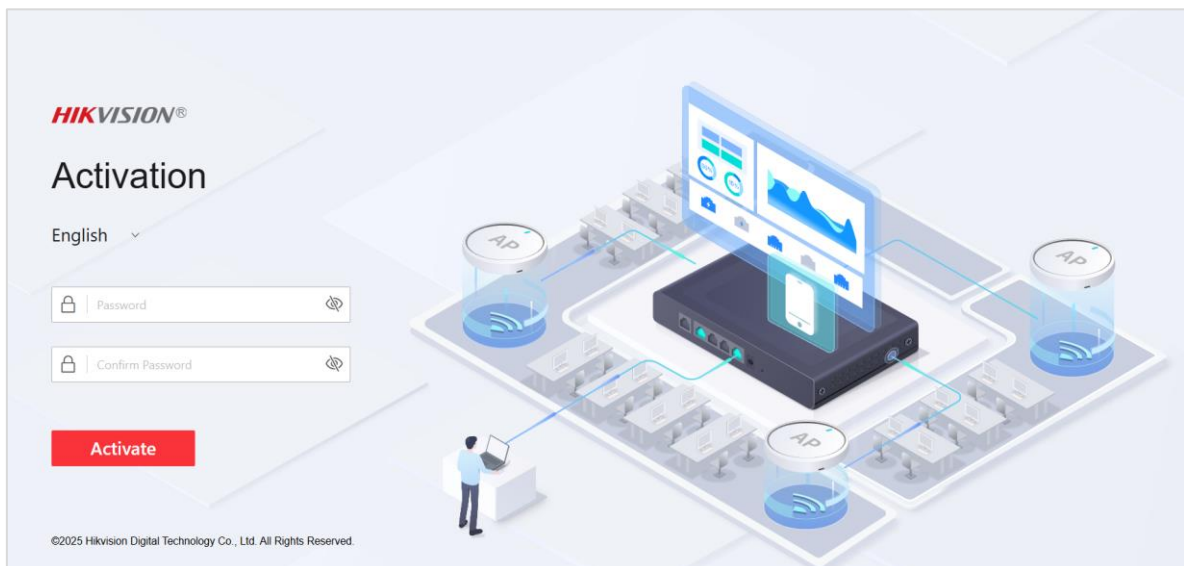


Figure 1-1 Activate

Note

Refer to the label on the back of the device for default IP address.

Step 4 Set your password and confirm it.

Caution

- The password strength of the device is automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: uppercase letters, lowercase letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system. Changing the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Step 5 Click **Activate**.

1.2 Login

After activating the device, you can log in to the device for management and configuration.

Steps

Step 1 Start a browser.

Step 2 Enter the IP address of the access point in the address bar and press **Enter**.

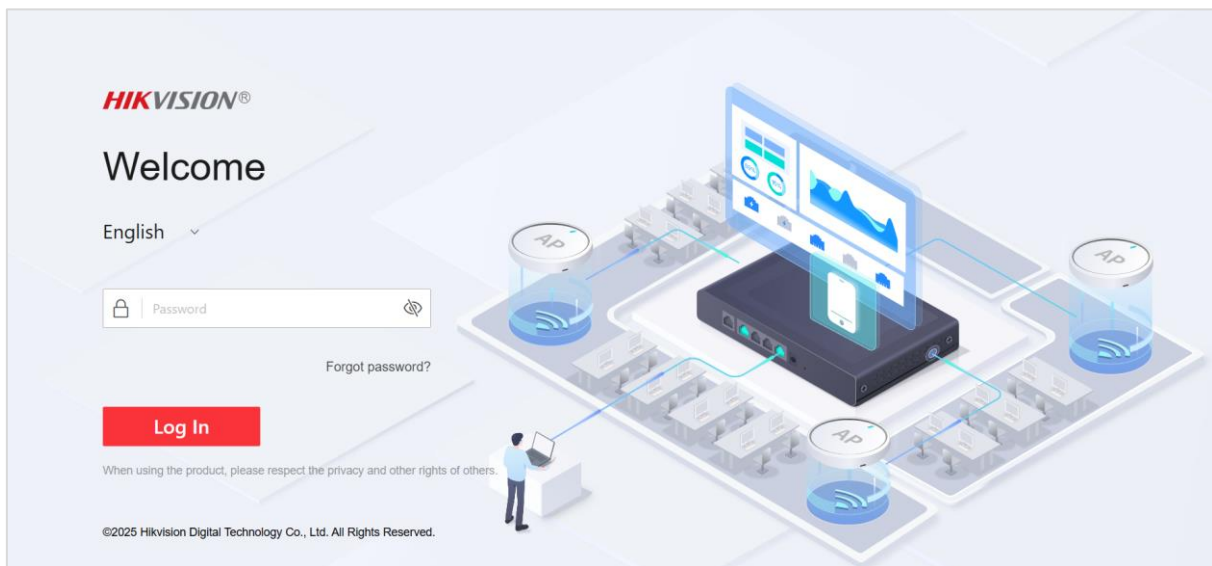


Figure 1-2 Log In

Step 3 Enter **Password**.

Note

If the password is forgotten, manually restore the device to factory defaults and set a new one. While the device is powered on, press and hold the reset button with a pointed object (e.g., a pin) for over 5 seconds. The factory reset is complete when the indicator light flashes rapidly.

Step 4 Click **Log In**.

Chapter 2 Configuration Guide

After logging in to the device for the first time, you will enter the configuration guide, which aims to lead you to finish the basic network and wireless network configuration. The whole configuration is optional, so click **Exit Configuration Wizard** if you wish to do this configuration later.

2.1 Network Configuration

In this section, you can configure the Internet access mode, enable/disable Hik-Connect, or enable/disable cloud fault collection.

The screenshot shows the 'Configuration Guide' interface with 'Network Configuration' selected. The 'Internet Access Method' is set to 'Dynamic IP Address'. Below this, there are two toggle switches: 'Hik-Connect Configuration' and 'Cloud Fault Collection Authoriz...', both of which are turned on. A red 'Next' button is at the bottom.

Figure 2-1 Dynamic IP Address

The screenshot shows the 'Configuration Guide' interface with 'Network Configuration' selected. The 'Internet Access Method' is set to 'Static IP Address'. Below this, there are five input fields: '* IP Address' (10), '* Subnet Mask' (255), '* Gateway Address' (10), '* DNS Server' (10), and 'Preferred DNS Server' (10). There are also two toggle switches: 'Hik-Connect Configuration' and 'Cloud Fault Collection Authoriz...', both of which are turned on. A red 'Next' button is at the bottom.

Figure 2-2 Static IP Address

See [6.1 Uplink Port Configuration](#) for details.

2.2 Wireless Network Settings

In this section, you can customize your wireless network name, encryption type, and password for accessing the network.

The screenshot shows a web-based configuration interface for a wireless access point. At the top, a 'Configuration Guide' bar indicates the current step is 'Wireless Network Settings' (step 2), with 'Network Configuration' (step 1) completed. An 'Exit Configuration Wizard' button is in the top right. The main form contains the following fields:

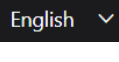
- *Wi-Fi Name:** A text input field containing 'HIKVISION_3674'.
- Encryption Type:** A group of radio buttons with the following options:
 - ☐ No Encryption (OPEN)
 - ☒ Strong Encryption (WPA2)
 - ☐ Strong Encryption (WPA3)
 - ☐ Mixed Encryption (WPA/WPA2)
 - ☐ Hybrid Strong (WPA2/WPA3)
- *Wi-Fi Password:** A text input field with a toggle icon on the right.
- *Country/Region:** A dropdown menu currently showing 'Albania'.

At the bottom of the form are two buttons: 'Back' and 'Completed'.

Figure 2-3 Wireless Network Setup

Chapter 3 General Toolbar

After you log in to the platform, the general toolbar will be displayed in the upper-right corner of the interface. The functions are described as follows:

- Click  to enter the configuration wizard page, where you can configure the Internet access mode, cloud platform switch, and Wi-Fi parameters.
- Click  to enter the fault alarm page and view alarm information.
- Click  to enter the network self-test page. When the device has network issues, you can perform quick network test and configure the device according to the test result.
- Click  to enter the page for changing login password, and then enter the old and new passwords to complete the password change.
- Click  to switch the platform language.
- Click  to log out.

Chapter 4 Overview Information

Upon logging into the platform, you will be automatically directed to the **Overview** page, where you can quickly browse the major device information sections.

Table 4-1 Device Information Sections

Section	Description
Connection Status	● Click  to view the information about the user terminal. ● Hover the mouse between Gateway and AP to click Network Self-Test to go through a network test. ● Hover the mouse over  to select AP location to help you locate device quickly.
Device Information	Click AP Mode / Routing Mode /  to go to the Basic Information page in System Configuration to view and edit AP information such as device name and working mode.
Port Information	Check the connection status and speed of the AP port.
Wireless Information	View the status of the wireless network. Click  to go to the wireless network configuration page.
RF Information	View the RF information of the wireless network. Click  to go to the RF configuration page.
Gateway Information	View the gateway information in the lower-right corner.

Chapter 5 User Terminal Management

Click **User Terminal** to enter the page for terminal management.

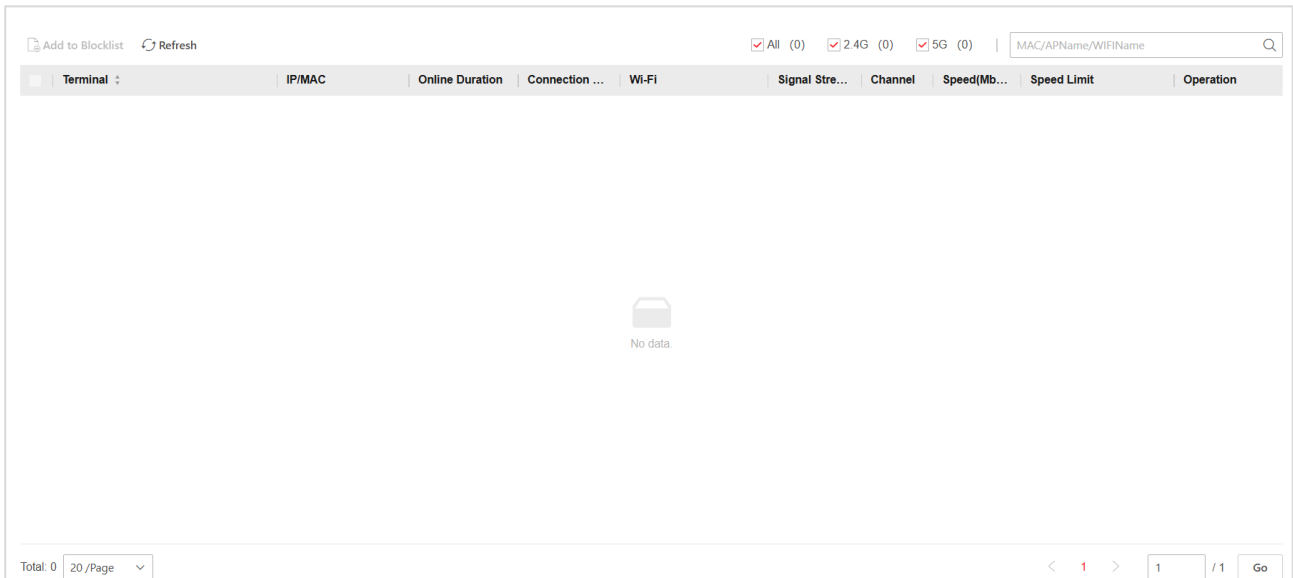


Figure 5-1 User Terminal

In this page, you can perform the following operations:

- Click  on the right of the terminal name to edit the user terminal name.
- Click  in the **Operation** column of the terminal to add the user terminal to the blocklist and disable its network access.
- Click  in the **Operation** column to limit the terminal's downstream and upstream rate.
- Select the terminals you want to block in batch, and click **Add to Blocklist** in the upper-left corner of the device list to block the selected terminals from accessing the network.

Note

To withdraw the operation, go to **Wireless Network Management** -> **Wireless Access Control** -> **Blocklist** to delete the device from the list.

- Click **Refresh** in the upper-left corner of the device list to refresh the current device statuses.
- Enter MAC address / AP Name / Wi-Fi Name in the search box to filter device(s) as per your needs.

Chapter 6 Network Management

Click **Network Management** to configure uplink port, LAN, and port VLAN.

6.1 Uplink Port Configuration

Steps

Step 1 Click **Uplink Port Configuration** to enter the page for uplink port basic and advanced configuration.

The screenshot displays the 'Uplink Port Configuration' interface. It is divided into two main sections: 'Basic Configuration' and 'Advanced Configuration'.

Basic Configuration:

- Internet Access Method:** Two radio buttons are present. 'Static IP Address' is unselected, and 'Dynamic IP Address' is selected (indicated by a red dot). Below this, a note states: 'Automatically obtain IP address and subnet mask to access the Internet.'
- IP Address:** A text input field containing '10.' followed by a blurred area.
- Subnet Mask:** A text input field containing '255.' followed by a blurred area.
- Gateway Address:** A text input field containing '10.' followed by a blurred area.
- DNS Server:** A text input field containing '10.' followed by a blurred area.
- Preferred DNS Server:** A text input field containing '10.' followed by a blurred area.

Advanced Configuration: This section is expanded, indicated by a downward arrow icon.

- *MAC Address:** A text input field containing '84' followed by a blurred area.
- Enable VLAN:** A green toggle switch is turned on.
- *VLAN ID:** An empty text input field.

At the bottom of the configuration area, there is a red button labeled 'Save'.

Figure 6-1 Uplink Port Configuration

Step 2 Select **Internet Access Method**.

- **Dynamic IP Address (Recommended):** In this mode, a dynamic IP address will be automatically assigned and no additional configuration is required.
- **Static IP Address:** In this mode, you should enter the IP address, subnet mask, gateway address, and DNS information provided by your broadband service provider manually.

Step 3 Manually enter **MAC Address** in **Advanced Configuration**.

**Note**

The default mac address is the factory MAC address of the interface. When you access the WAN via the public IP address assigned by your carrier, enter the MAC address bound to your carrier here.

Step 4 (Optional) Enable VLAN and set VLAN ID for the uplink port.

Step 5 Click **Save**.

6.2 LAN Settings

Click **LAN Settings** to enter the page for LAN configuration.

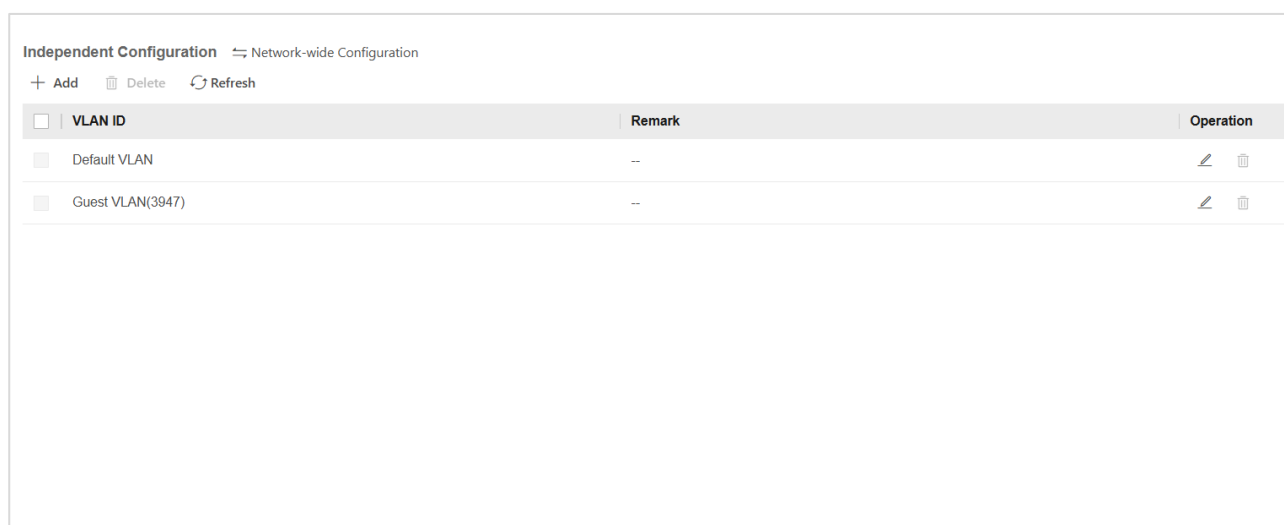


Figure 6-2 LAN Settings

Two major configuration methods are supported. You can select the one you need.

- **Network-wide Configuration:** Select this mode to directly sync the AP wired port parameters set by AC router. You cannot perform independent operations such as adding, deleting, or editing configurations.
- **Independent Configuration:** Select this mode to independently add or delete LAN(s) and configure port VLAN(s). The subsequent AP wired port parameter configuration set by AC router will not be synced to this device.

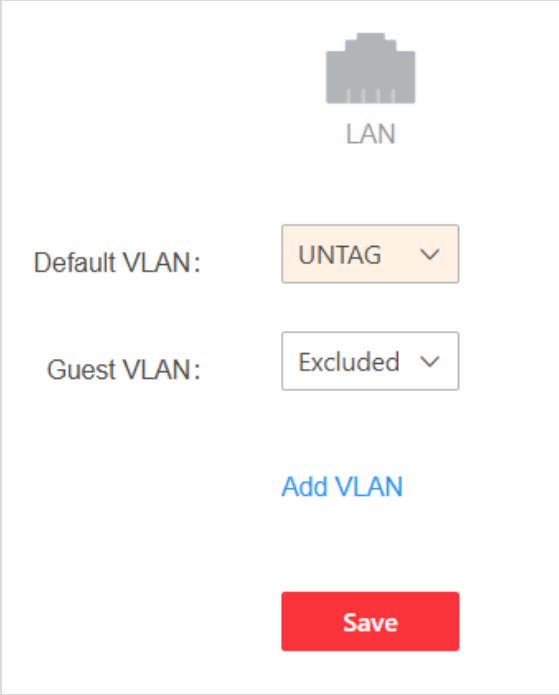
6.3 Port VLAN

Prerequisite

You have added VLAN(s).

Steps

Step 1 Click **Port VLAN** to enter the page for port VLAN configuration.



LAN

Default VLAN: UNTAG ▾

Guest VLAN: Excluded ▾

Add VLAN

Save

Figure 6-3 Port VLAN

Step 2 Configure default VLAN and guest VLAN for the target LAN port.

- **UNTAG:** Set the VLAN as the only PVID of this LAN port.
- **TAG:** The VLAN is assigned to LAN port.
- **Excluded:** The LAN port is excluded from the VLAN.

Step 3 (Optional) Click **Add VLAN** to add a new VLAN.

Step 4 Click **Save**.

Chapter 7 Wireless Network Management

Click **Wireless Network Management** to configure wireless network, access control, speed limit and others.

7.1 Wireless Network Settings

Click **Wireless Network Settings** to view the current information of the wireless network.

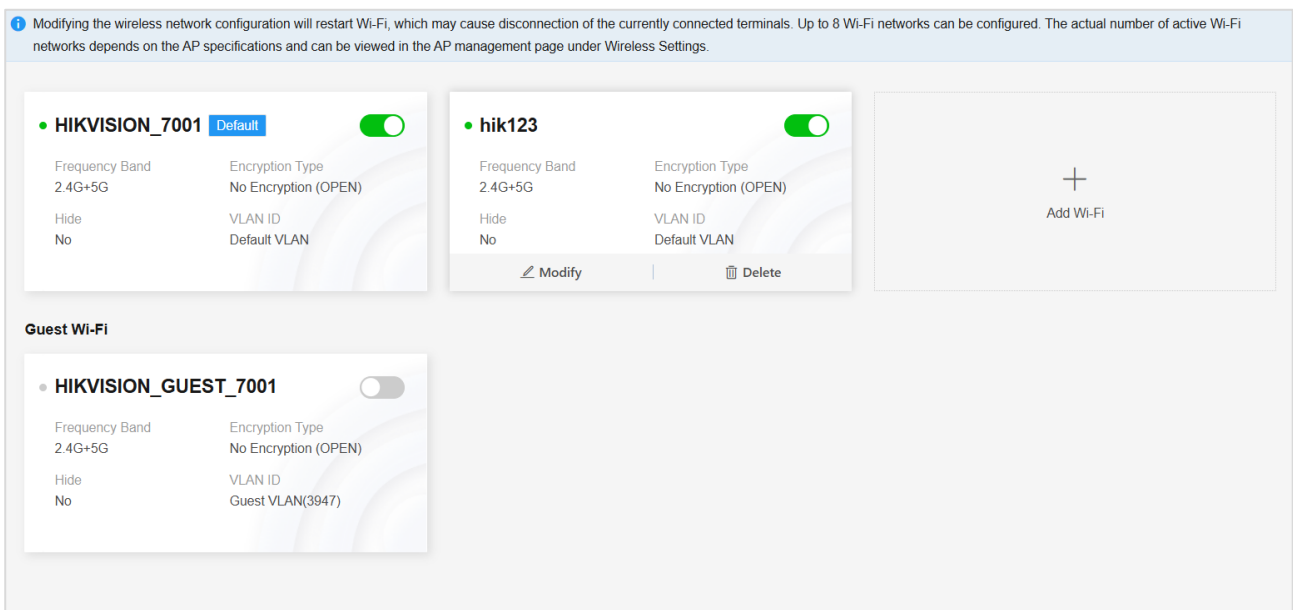


Figure 7-1 Wireless Network Settings

If your cloud service is enabled (see [10.2 Hik-Connect Configuration](#) for details), you also can add, modify, or delete the Wi-Fi network as desired.

- Add Wi-Fi: Click **+** to fill in network parameters such as Wi-Fi name, Wi-Fi password, encryption type, and frequency band, to add a Wi-Fi network.

Wi-Fi Name *

test

Encryption Type

☐ No Encryption (OPEN)

☒ Strong Encryption (WPA2)

☐ Strong Encryption (WPA3)

☐ Mixed Encryption (WPA/WPA2)

☐ Hybrid Strong (WPA2/WPA3)

Frequency Band

☒ 2.4G+5G

☐ 2.4G

☐ 5G

Wi-Fi Password *

Advanced Settings ▾

Add Cancel

Figure 7-2 Add Wi-Fi

- Enable/Disable Wi-Fi: Click the toggle switch on the upper-right corner of the network card to enable/disable the functioning of the network.
- Modify/Delete Wi-Fi: Hover the mouse over a Wi-Fi network card and click **Modify/Delete** to modify or delete the target network.

Note

The default Wi-Fi and the guest Wi-Fi cannot be deleted.

7.2 Wireless Optimization

Click **Wireless Optimization** -> **Quick Optimize** / **Scheduled Optimization** to choose an appropriate method for wireless network optimization.

7.2.1 Quick Optimization

Click **Quick Optimize** to perform one-click optimization of your network.

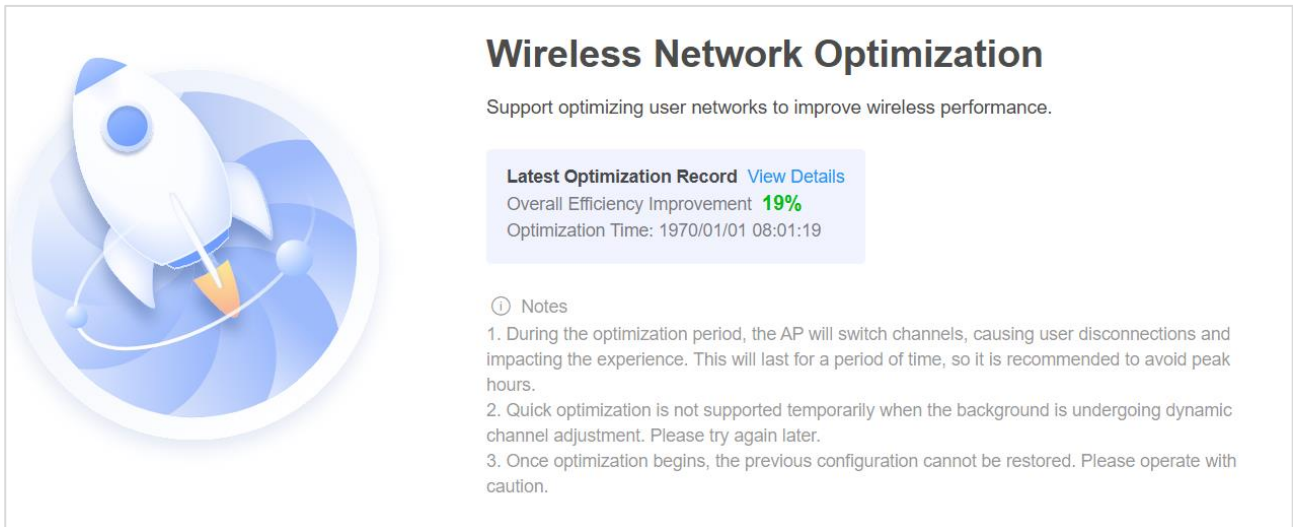


Figure 7-3 Quick Optimize

Note

- During the optimization period, the AP will go through channel switch, which may cause user network disconnections. This process will last for a period of time, so it is recommended to avoid peak hours.
- When dynamic channel adjustment is in progress, this function may not be supported temporarily. In this condition, please try again later.
- Once the optimization begins, the previous configuration cannot be restored. Please operate with caution.

7.2.2 Scheduled Optimization

Automatic Optimization

Enable ☐

After automatic optimization is enabled, the device will detect the running load and environment status, and adjust the RF parameters automatically.

Scheduled Optimization

Enable ☐

Enable and configure scheduled optimization, the device will perform optimization operations at the specified time and automatically adjust RF parameters.

Save

Figure 7-4 Scheduled Optimization

- **Automatic Optimization**

After you enable this function, the device will detect the running load and environment status, and adjust the RF parameters automatically.

- **Scheduled Optimization**

After enabling this function, you have to set the time schedule for the optimization. The device will perform optimization operations and automatically adjust RF parameters at the set time.

7.2.3 Optimization Record

After completing the optimization, you can go to **Optimization Record** to see historical records.

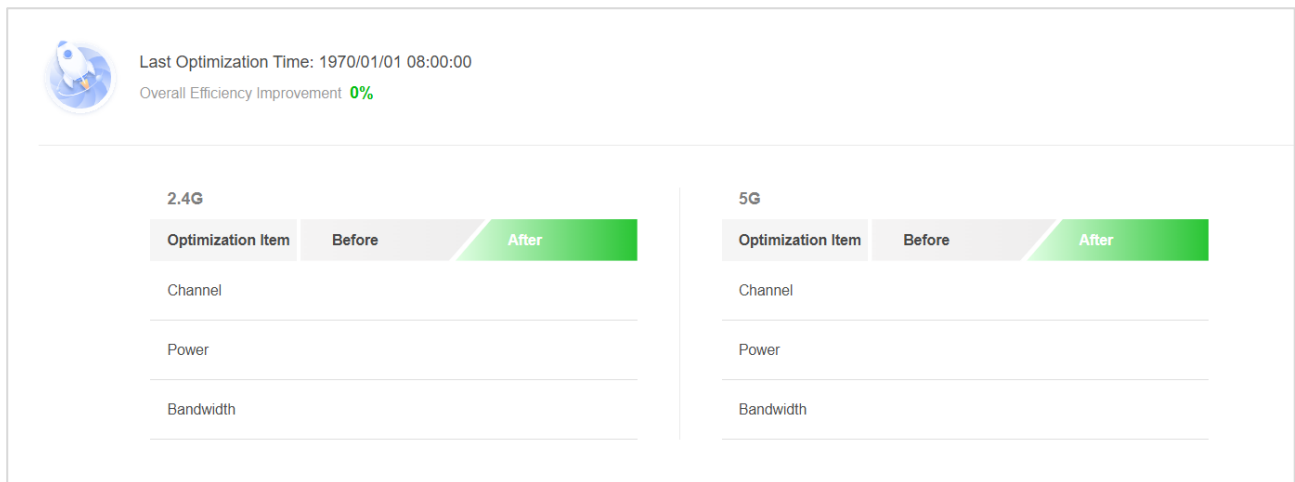


Figure 7-5 Optimization Record

7.3 Wireless Access Control

Click **Wireless Access Control** to manage your blocklist and allowlist.

7.3.1 Blocklist

Steps

Step 1 Click to choose **Blocklist** as the function to be configured.

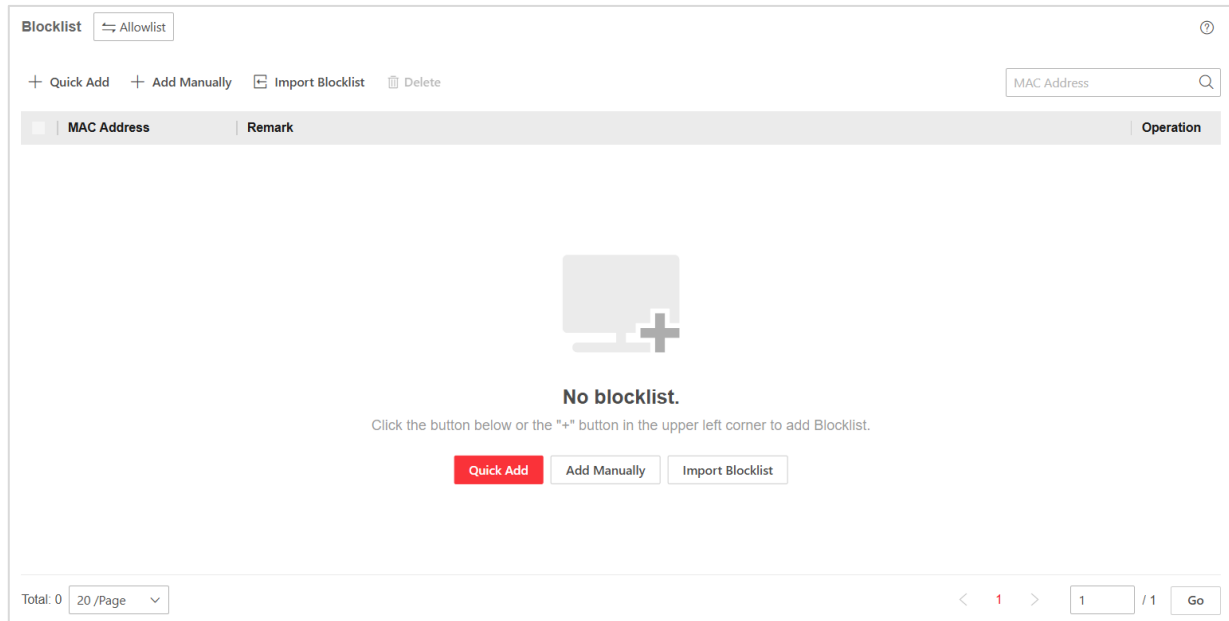


Figure 7-6 Blocklist

Step 2 Add or import blocklist.

- Click **Add Manually** to enter the mac address to be blocked for access.
- Click **Import Blocklist** to download template and then click  to choose the file to be imported. If you want to automatically replace the terminal list of the repeated MAC address, enable the corresponding function.
- Click **Quick Add** to add all online terminals detected.

Step 3 Click **Import/Add**.

Step 4 (Optional) Click  to delete the selected terminal MAC address or click **Delete** after checking the addresses in batch.

7.3.2 Allowlist

Steps

Step 1 Click to choose **Allowlist** as the function to be configured.

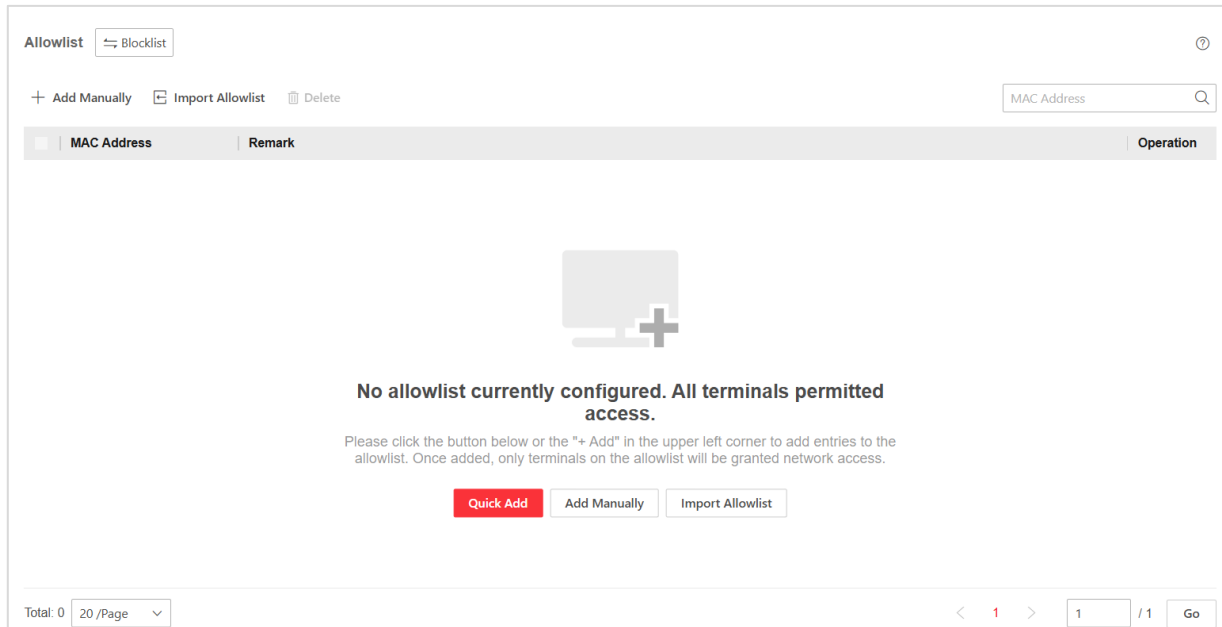


Figure 7-7 Allowlist

Step 2 Add or import allowlist.

- Click **Add Manually** to enter the mac address to be allowed for access.
- Click **Import Allowlist** to download template and then click  to choose the file to be imported. If you want to automatically replace the terminal list of the repeated MAC address, enable the corresponding function.
- Click **Quick Add** to add all online terminals detected.

Step 3 Click **Import/Add**.

Step 4 (Optional) Click  to delete the selected terminal MAC address or click **Delete** after checking the addresses in batch.

7.4 Wireless Speed Limit

Click **Wireless Speed Limit** to set speed limit for your network. You can choose from the following four speed limit options to suit your needs.

Note

When multiple speed limit rules of different types exist simultaneously, the following order defines the priority: terminal speed limit > Wi-Fi speed limit > RF speed limit > intelligent speed limit.

- **Intelligent Speed Limit**

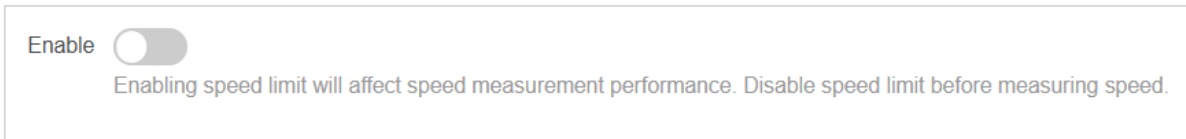


Figure 7-8 Intelligent Speed Limit

In this section, you can click the switch to enable intelligent speed limit. Enabling speed limit will affect speed measurement performance, so please disable this function in conditions of speed limit.

● Terminal Speed Limit

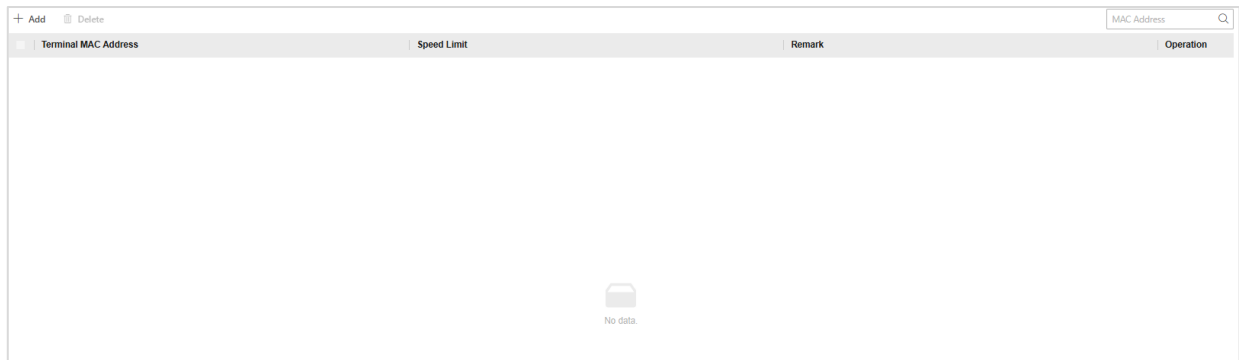


Figure 7-9 Terminal Speed Limit

In this section, you can select terminals from the user terminal list or manually add terminal MAC addresses, and set uplink and downlink speed limits.

● Wi-Fi Speed Limit

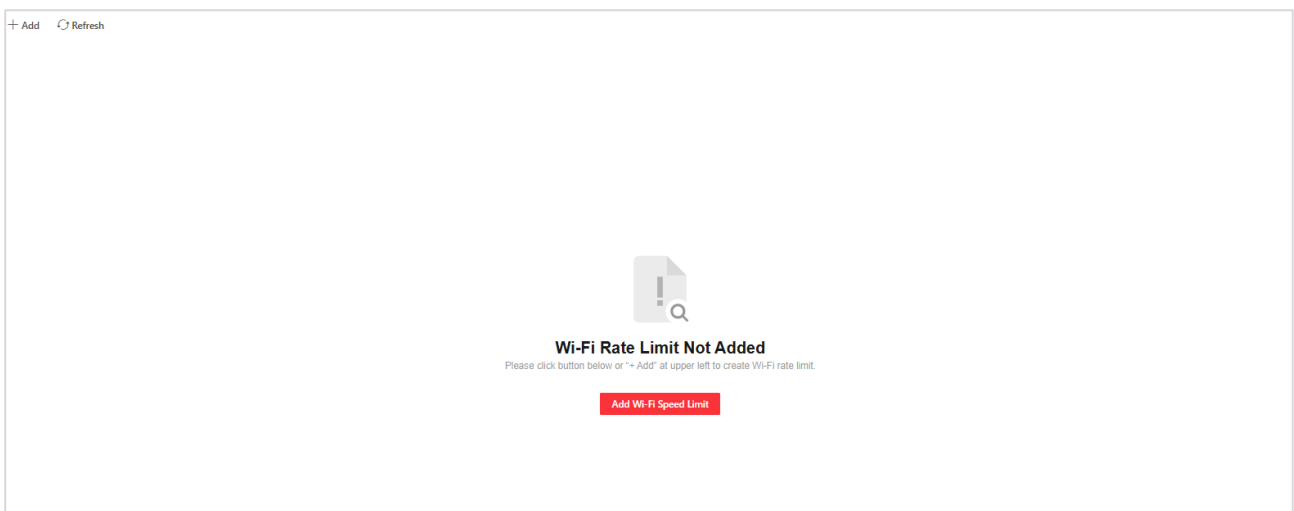


Figure 7-10 Wi-Fi Speed Limit

In this section, you can select a target wireless network, select uplink and downlink speed limit methods respectively, and set uplink and downlink speed limits.

● RF Speed Limit

2.4G RF Speed Limit

Enable ☒

Uplink Speed Limit Method ☒ Per-user Rate Limiting ☐ Share Equal Limit ☐ No Limit

* Uplink Speed Limit Mbps

Downlink Speed Limit Method ☒ Per-user Rate Limiting ☐ Share Equal Limit ☐ No Limit

* Downlink Speed Limit Mbps

5G RF Rate Limit

Enable ☒

Uplink Speed Limit Method ☒ Per-user Rate Limiting ☐ Share Equal Limit ☐ No Limit

* Uplink Speed Limit Mbps

Downlink Speed Limit Method ☒ Per-user Rate Limiting ☐ Share Equal Limit ☐ No Limit

* Downlink Speed Limit Mbps

Save

Figure 7-11 RF Speed Limit

In this section, you can set the uplink and downlink speed limit methods and rates for 2.4G and 5G separately.

7.5 RF Configuration

Click **RF Configuration** to enter the page for RF configuration for 2.4G and 5G network.

Note

- The bandwidth and max. number of connections of some devices are configured by the AC device in the network, which cannot be edited on the AP. Please refer to actual interface for details.
- If the device is in the health mode now, it will run with lower power settings by default. You need to disable the health mode on the AC router to make the power settings take effect.
- The supported parameters vary for different device models and firmware versions. The following picture and parameters are examples only. The actual parameters may differ.

Some parameters are centrally configured by the the AC device and cannot be modified on the AP. If in health mode, the device defaults to low-power settings; close health mode on AC to make the current page settings effective.

Country/Region: Hong Kong, China

① Enable Directional Antenna: ☐

2.4G

Enable: ☒

Bandwidth: Auto(20MHz)

Max. Connections: 256

Channel: Auto(6)

Power: ☒ High ☐ Medium ☐ Low ☐ Lower

Enable Weak Signal Access Control: ☐

① Offline Threshold:
 -99(Close) -85(Recommended) -72(High)
 Recommend -85dBm, and exceeding this threshold may affect normal Internet access.

① Roaming Sensitivity:
 Low 20% 40% 60% 80% High
 Excessive sensitivity may lead to frequent switching of terminal Wi-Fi connection and further affect your Internet surfing experience.

① Roaming guidance threshold:
 Low -72(Recommended) High
 It is recommended to be below -72 dBm. Exceeding this threshold may affect normal terminal internet access.

5G

Enable: ☒

Save

Figure 7-12 RF Configuration

- **Enable Directional Antenna:** After this function is enabled, the wireless signal will be transmitted in a specific direction, which may contribute to concentrated and further signal transmission. It is suitable for long-distance transmission scenes such as corridors and outdoor areas.
- **Bandwidth:** Bandwidth is the width of the frequency band occupied by the wireless signal in the frequency domain. The larger the bandwidth, the faster the signal transmission speed.
- **Max. Connections:** The maximum number of devices that an AP can manage simultaneously.
- **Channel:** A channel is a data transmission path that uses wireless signals as the transmission medium. If you select **Auto**, the AP will select an optimal channel based on its surrounding environment.

- **Power:** The power affects the wireless signal strength. For large area or areas with more partitions, it is recommended to set power as **High**.
- **Enable Weak Signal Access Control:** By enabling the access threshold and setting rejection times, you can prevent AP devices with weak signals from accessing the network and occupying the wireless channel, and thus improve the overall performance and user experience of the wireless network.
- **Offline Threshold:** Terminal users with wireless signal strength below the set threshold will be forcibly disconnected.
- **Roaming Sensitivity:** This determines how aggressively a device switches between different APs to maintain connectivity. A high sensitivity leads to frequent device roaming to seek the best available signal, optimizing performance but potentially increasing network overload.
- **Roaming Guidance Threshold:** This determines when the network should actively advise or steer a client device to roam from its current AP to a better one.

Chapter 8 Behavior Management

Click **Behavior Management** to configure the data flow control policy. By configuring QoS (Quality of Service) and DSCP (Differentiated Services Code Point), you can categorize data packets by priority and differentiate their handling strategies to achieve effective network data flow control.



Note

Only some device models support this function. The actual device interface prevails.

8.1 QoS

Steps

Step 1 Click **QoS**.

Step 2 Click the switch below **Enable** to enable the QoS global configuration.

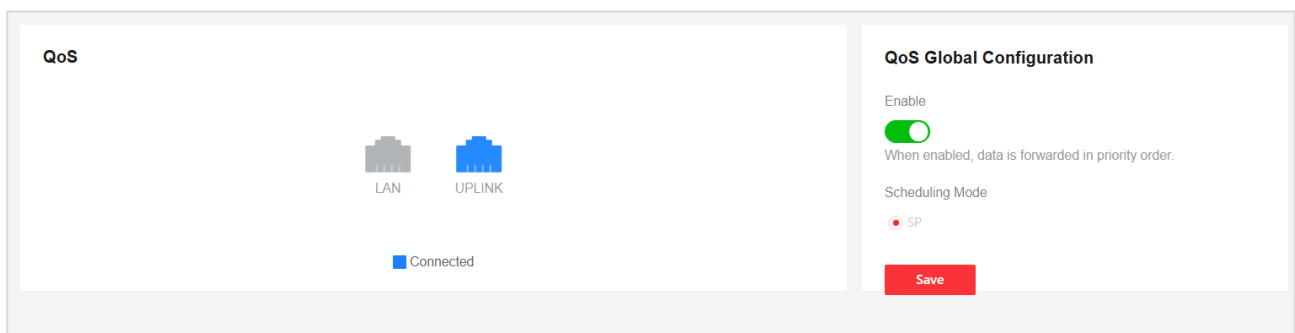


Figure 8-1 QoS



Note

The default QoS scheduling mode is SP (Strict Priority).

Step 3 Click **Save**.

8.2 DSCP

Prerequisite

You have enabled QoS.

Steps

Step 1 Click **DSCP**.

Step 2 Click the switch below **Enable** to enable the DSCP-based priority forwarding.

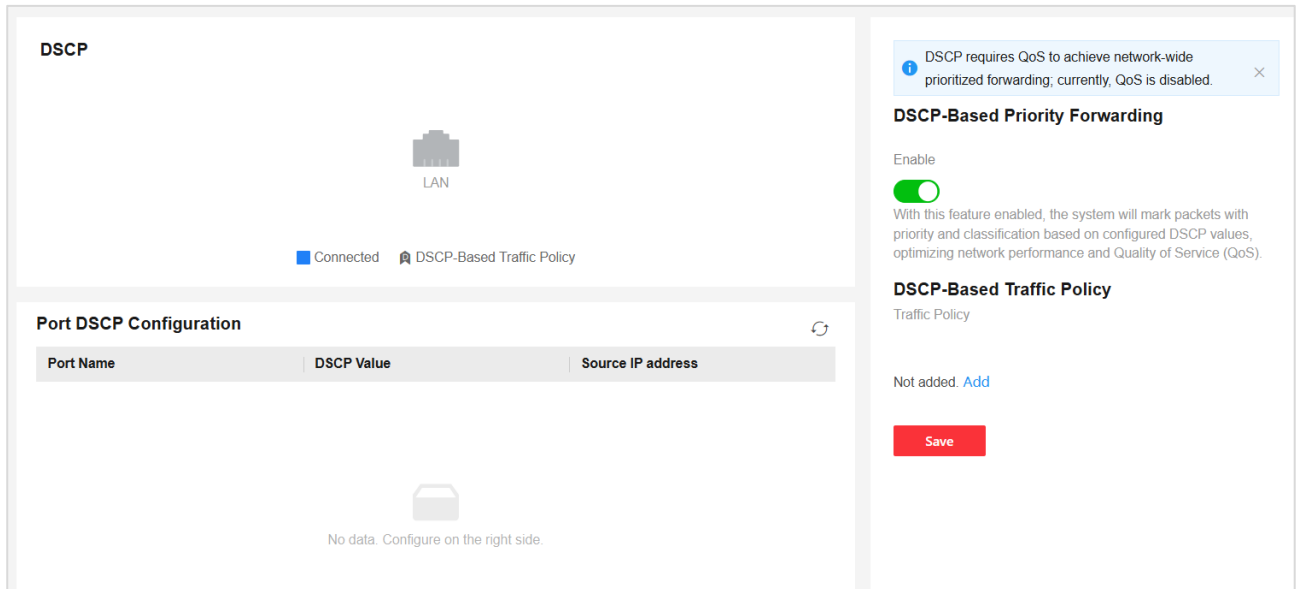


Figure 8-2 DSCP

Step 3 Click **Add** to add a DSCP-based traffic policy.

The form for adding a DSCP-based traffic policy contains the following fields and buttons:

- Port No. ***: A dropdown menu with the text 'Select' and a downward arrow.
- DSCP Value ***: A text input field.
- Source IP address**: A text input field.
- Add**: A red button.
- Cancel**: A white button with a gray border.

Figure 8-3 Add DSCP-Based Traffic Policy

Step 4 Select a port and enter the corresponding DSCP value.

Note

The default mapping relations between DSCP values and QoS priorities are as follows:

DSCP Value	QoS Priority
0~7	1
8~15	2
16~23	3
... (Arranged in sets of 8 values in ascending numerical order)	... (Arranged in ascending numerical order)

Step 5 (Optional) Enter the source IP address of the port.

Step 6 Click **Add**.

Step 7 (Optional) Click **Edit** to edit or delete the existing DSCP flow control policy, or create a new one.

Chapter 9 Fault Diagnosis

Click **Fault Diagnosis** to perform tests, collect faults, check alarms, and finish other trouble-shooting activities.

9.1 Network Self-Test

Click **Network Self-Test** to enter the page for network test.

When network issues occurred, click **Start Detection** to check your network status.

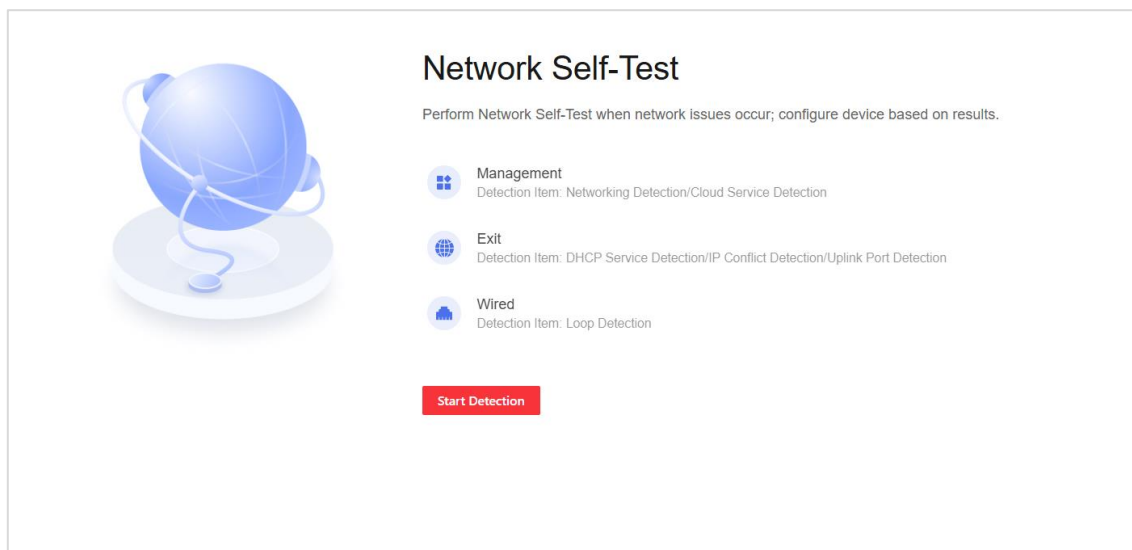


Figure 9-1 Network Self-Test

9.2 Fault Alarm

Click **Fault Alarm** to view existing alarms and handle them appropriately.

Confirm					
☐	Alarm Time	Alarm Category	Alarm Details	Suggestion	Operation
☐	2025-11-21 17:11:33	Networking Detection	Networking status is exception.	Check AC/AP Networking Status	
☐	2025-11-21 17:11:57	DHCP Service Detection	There are multiple DHCP Server conflicts in the network.	Disable DHCP server for (MAC:) or (MAC:)	

Figure 9-2 Fault Alarm

- For alarms that need to be handled, see **Suggestion** for handling methods.

- For alarms that can be ignored or have been handled already, click  to confirm the alarms and delete the records.

9.3 Network Tool

Click **Network Tool** to resort to network tools to diagnose your network problems.

9.3.1 PING

When you need to detect the connectivity of a node in the network, choose **PING**.

Steps

Step 1 Select **PING** as the diagnosis mode.

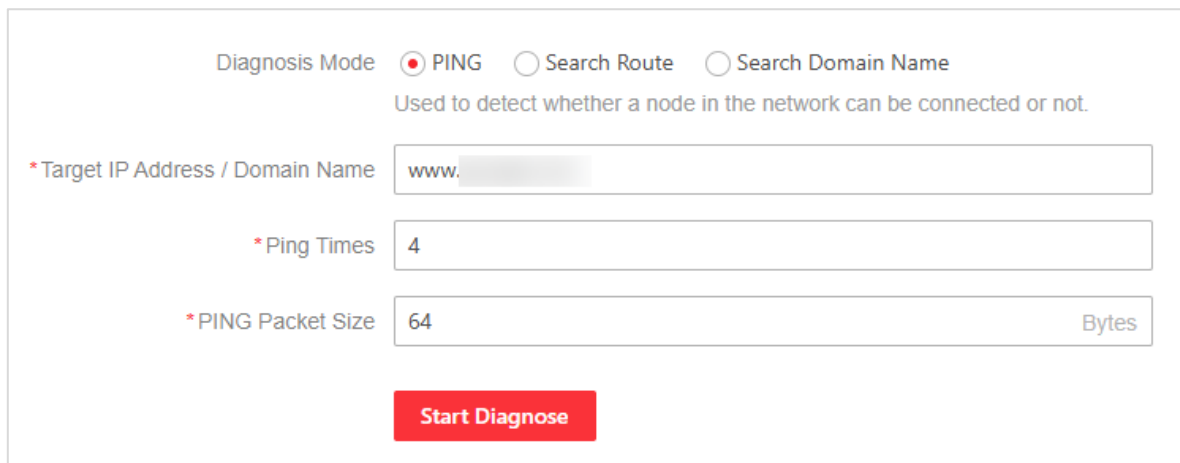


Figure 9-3 PING

Step 2 Set **Target IP Address / Domain Name**, **Ping Times**, and **PING Packet Size**.

Step 3 Click **Start Diagnose**.

Step Result

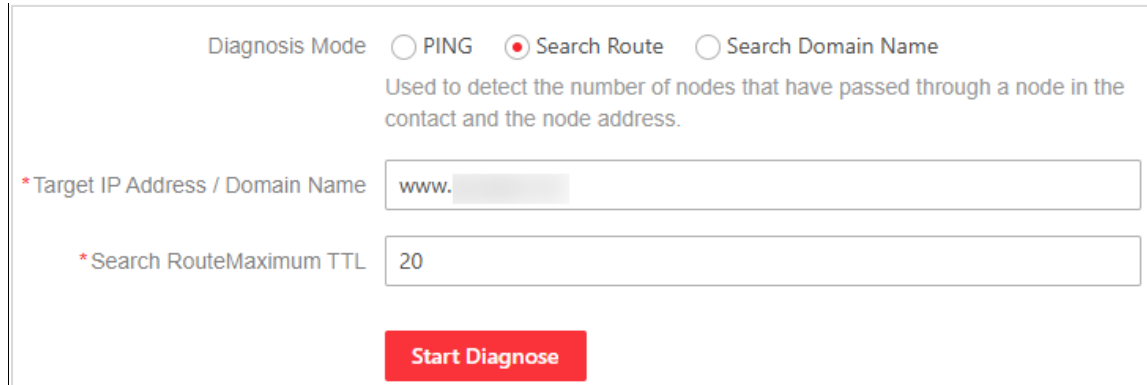
If the ping communication fails, it indicates that the device is not connected to this IP address or domain name.

9.3.2 Search Route

When you need to search the number and addresses of nodes that need to be passed through to reach a node, choose **Search Route**.

Steps

Step 1 Select **Search Route** as the diagnosis mode.



Diagnosis Mode ☐ PING ☒ Search Route ☐ Search Domain Name

Used to detect the number of nodes that have passed through a node in the contact and the node address.

*Target IP Address / Domain Name

* Search RouteMaximum TTL

Start Diagnose

Figure 9-4 Search Route

Step 2 Set **Target IP Address / Domain Name**, and **Maximum TTL**.

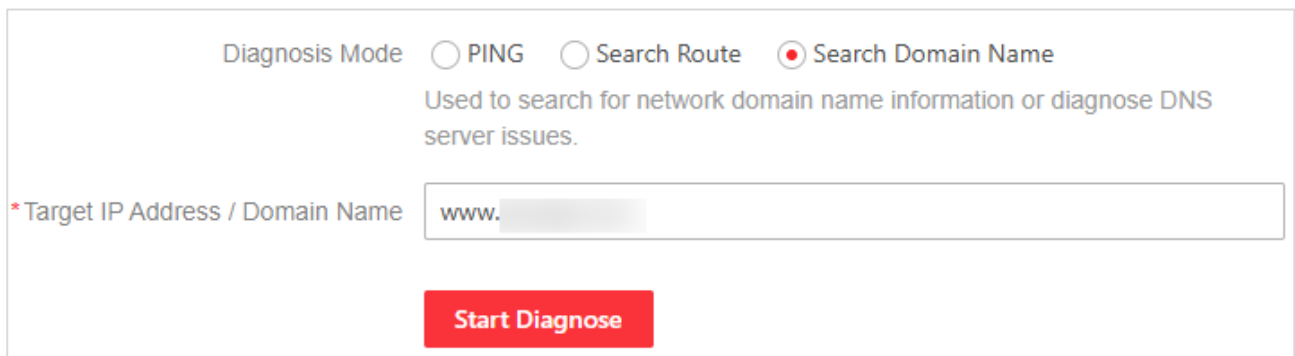
Step 3 Click **Start Diagnose**.

9.3.3 Search Domain Name

When you need to search for network domain name information or diagnose DNS server issues, choose **Search Domain Name**.

Steps

Step 1 Select **Search Domain Name** as the diagnosis mode.



Diagnosis Mode ☐ PING ☐ Search Route ☒ Search Domain Name

Used to search for network domain name information or diagnose DNS server issues.

*Target IP Address / Domain Name

Start Diagnose

Figure 9-5 Search Domain Name

Step 2 Set **Target IP Address / Domain Name**.

Step 3 Click **Start Diagnose**.

9.4 Faults Collection

Click **Faults Collection** -> **Quick Collect** to collect the existing device faults.

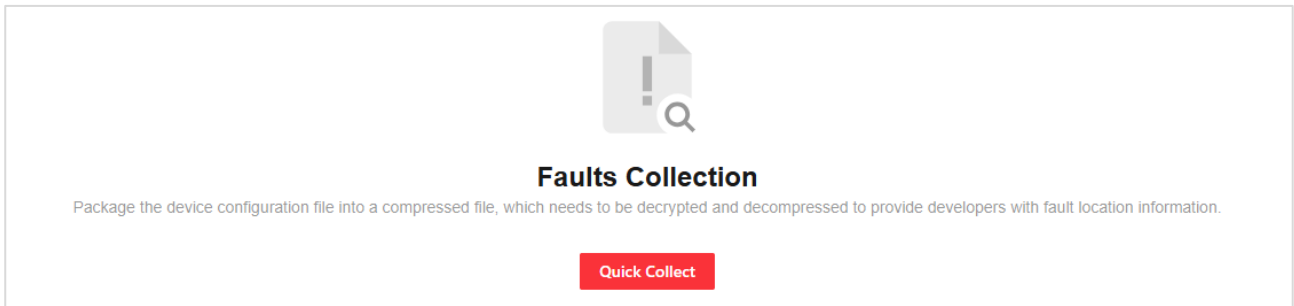


Figure 9-6 Faults Collection

9.5 SSH

Click **SSH** to enable/disable secure remote login. For network security, you may keep the SSH disabled by default. It is usually reserved for professional personnel debugging.

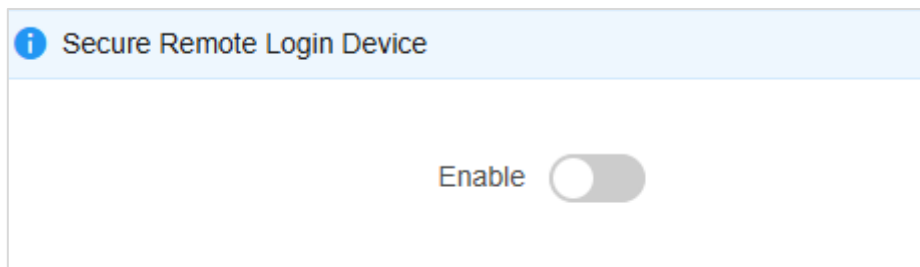


Figure 9-7 SSH

Chapter 10 System Configuration

10.1 System Configuration

10.1.1 Basic Information

Click **System Configuration** -> **System Configuration** -> **Basic Information** to view device name, model, serial No., working mode, and other basic device information. For customized purpose, you can edit the device name or switch the working mode.

**Note**

- **AP Mode:** In this mode, the device acts as a central hub for wireless devices to connect to a wired network. This mode allows networking with an AC router and independent device-to-cloud connection.
- **Routing Mode:** In this mode, the device combines the features of a wireless AP and a router. This mode does not allow networking with an AC router but allows independent device-to-cloud connection.

*Name DS

Model DS

Serial No. GF

Working Mode ☒ AP Mode ☐ Routing Mode

After mode switching, device IP may change. Management address in AP mode is the uplink port address; in router mode, default is 192.168.19.1. Mode switch retains activation status, login password, device name, login timeout, wireless settings, radio config, access control, speed limit, terminal names, and cloud platform status

Software Version V1.5.400 build 251113

MAC Address 84

CPU Usage 1%

Memory Usage 71%

Save

Figure 10-1 Basic Information

10.1.2 Time Settings

Click **System Configuration** -> **System Configuration** -> **Time Settings** to view or edit time configuration.

Figure 10-2 Time Settings

- **NTP Time Sync:** To synchronize device time with that of a NTP server. This time synchronization mode requires configuration of server address and time sync interval. Click **Test** for connectivity test.
- **Manual Time Sync:** To set device time manually or synchronize device time with that of your computer.

10.2 Hik-Connect Configuration

Steps

Step 1 Click **System Configuration** -> **Hik-Connect Configuration**.

Figure 10-3 Hik-Connect Configuration

Step 2 Enable the cloud platform function.

Step 3 (Optional) Enable **Cloud Fault Collection Authorization** to allow the manufacturer to collect device fault logs via cloud service for troubleshooting and improving your Internet experience.

Step 4 (Optional) Scan the QR code of the device to link it with your Hik-Connect account.

Note

- The device should be online to link with the cloud account.
- After binding the device to a cloud account, if you want to unlink it, please go to the APP for unbinding. Restoring the device to factory settings will automatically unlink the device from any account it has been bound to.

10.3 AP Status Indicator

Click **System Configuration** -> **AP Status Indicator** to enable/disable the device status indicator by clicking the toggle switch.

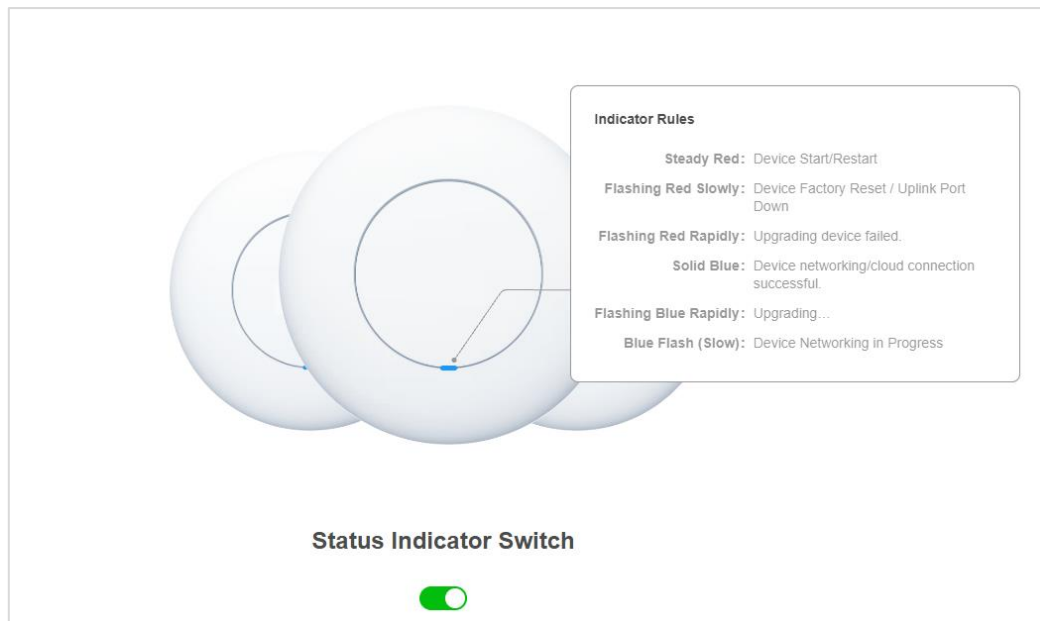


Figure 10-4 AP Status Indicator

Note

The indicator rules of different models may vary. Please refer to the Quick Start Guide in the package for details.

Chapter 11 Maintenance and Security

11.1 System Maintenance

11.1.1 Restart

Click **Maintenance and Security** -> **System Maintenance**-> **Restart**. Click **Restart**.

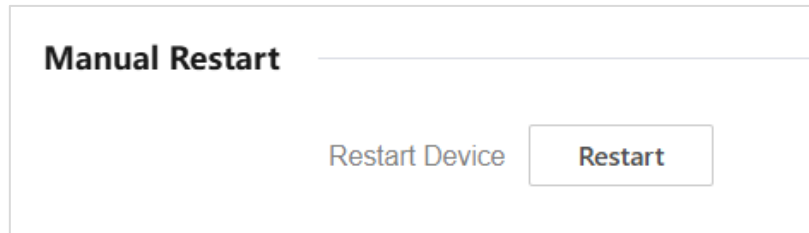


Figure 11-1 Restart



Caution

Please keep the device powered during the restart.

11.1.2 Upgrade

Click **Maintenance and Security** -> **System Maintenance**-> **Upgrade**.

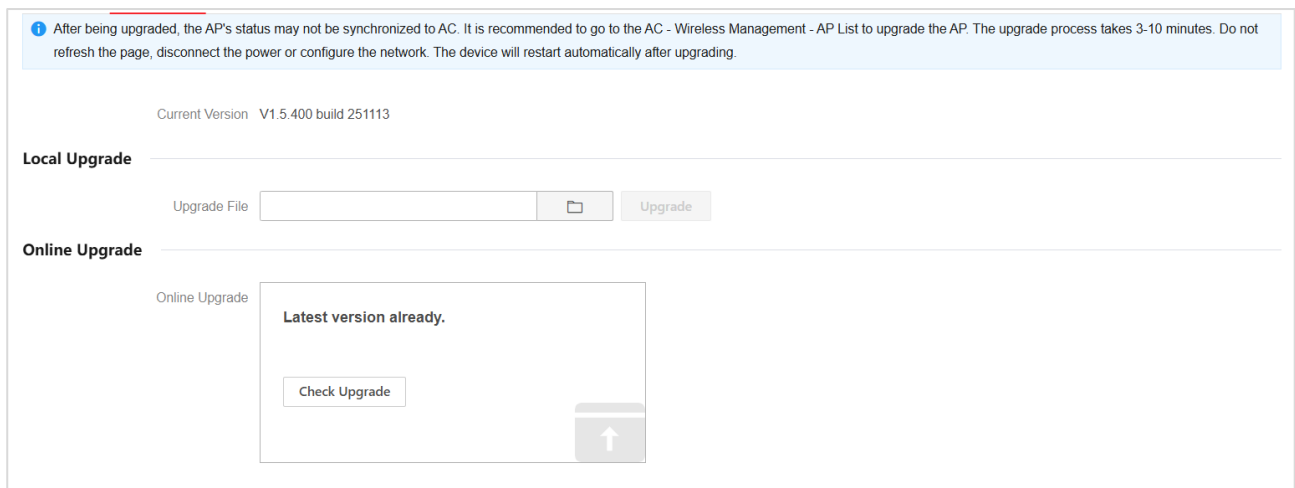


Figure 11-2 Upgrade

Choose from the following methods for device upgrade:

- **Local Upgrade:** Click  to select a local upgrade file and click **Upgrade**.

- **Online Upgrade:** In conditions of networking with the AC router, you may click **Check Upgrade** to check the version status of your device and trigger device upgrade automatically after the latest version has been detected. The device will restart automatically after the upgrade.

11.1.3 Restore

Click **Maintenance and Security** -> **System Maintenance**-> **Restore**. Click **Restore** to restore the device to factory settings.

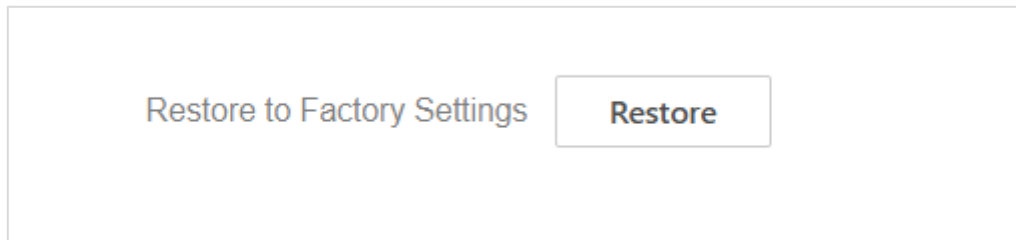


Figure 11-3 Restore



Caution

Please keep the device powered during the restoration.

11.1.4 Security Audit Log

Click **Maintenance and Security** -> **System Maintenance**-> **Security Audit Log**.

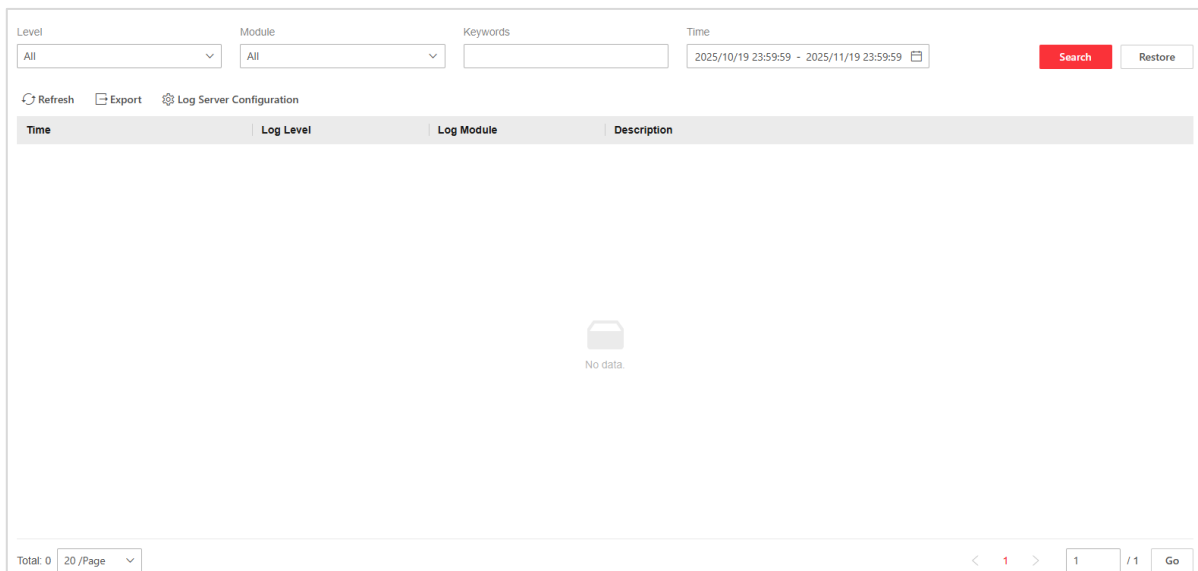


Figure 11-4 Security Audit Log

- For security audit log search, set search conditions such as level and module first and then click **Search**.
- For security audit log export, click **Export** after the searching.

- For log server configuration, click **Log Server Configuration** and set related parameters as desired.

11.2 Login Management

Click **Maintenance and Security** -> **Login Management**. You can modify or restore the timeout duration for login.



The default timeout duration is 10 minutes.

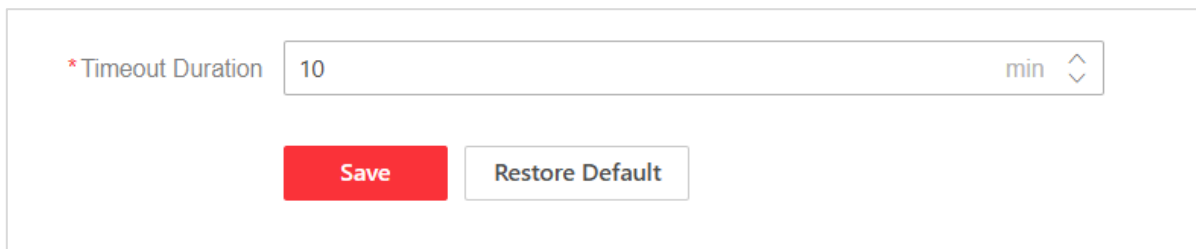
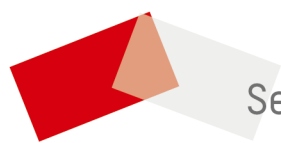


Figure 11-5 Timeout Duration



See Far, Go Further