Wireless Bridge

Web Operation Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the functions and operations of the Wireless Bridge (hereinafter referred to as "the Device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save your time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	February 2025

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Table of Contents

1 Product Overview

1.1 Introduction

With a stylish and elegant streamlined design, the Device adopts PoE technology, TDMA (Time Division Multiple Access) technology, and professional Wi-Fi configuration management.

The Device is intended to solve the problems of wiring difficulties, high cost, and serious interference in the traditional security projects. It can meet the needs of smooth wireless transmission in severe environments.

While maintaining high availability and performance, the Device optimizes the space layout and installation design, making the installation and deployment more flexible.

1.2 Network Diagram

Figure 1-1 Network diagram (point-to-point)

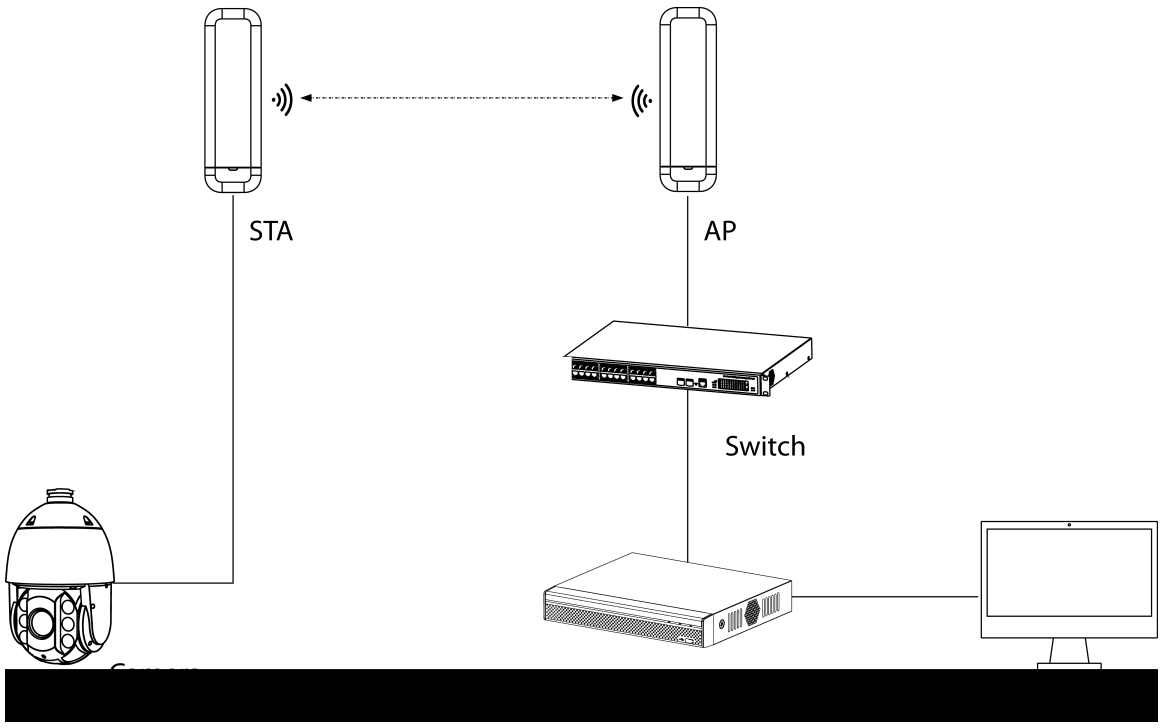


Figure 1-2 Network diagram (point-to-points)

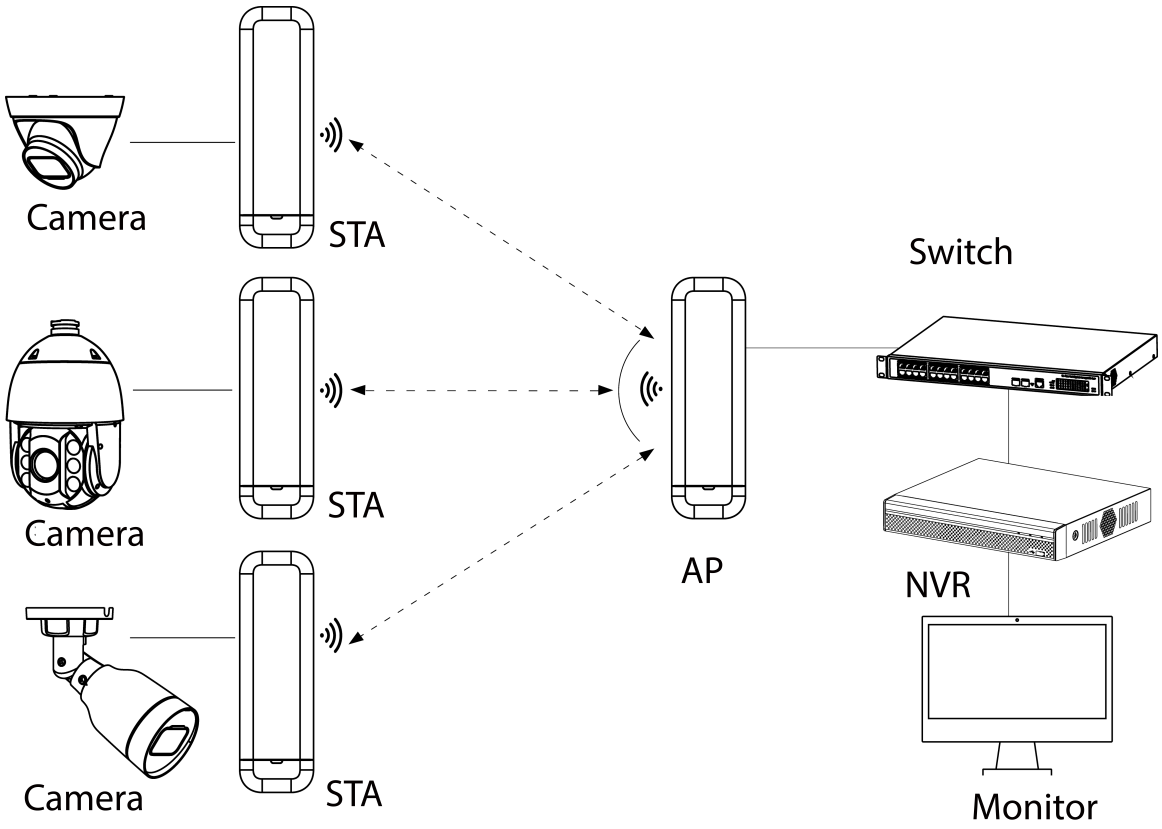
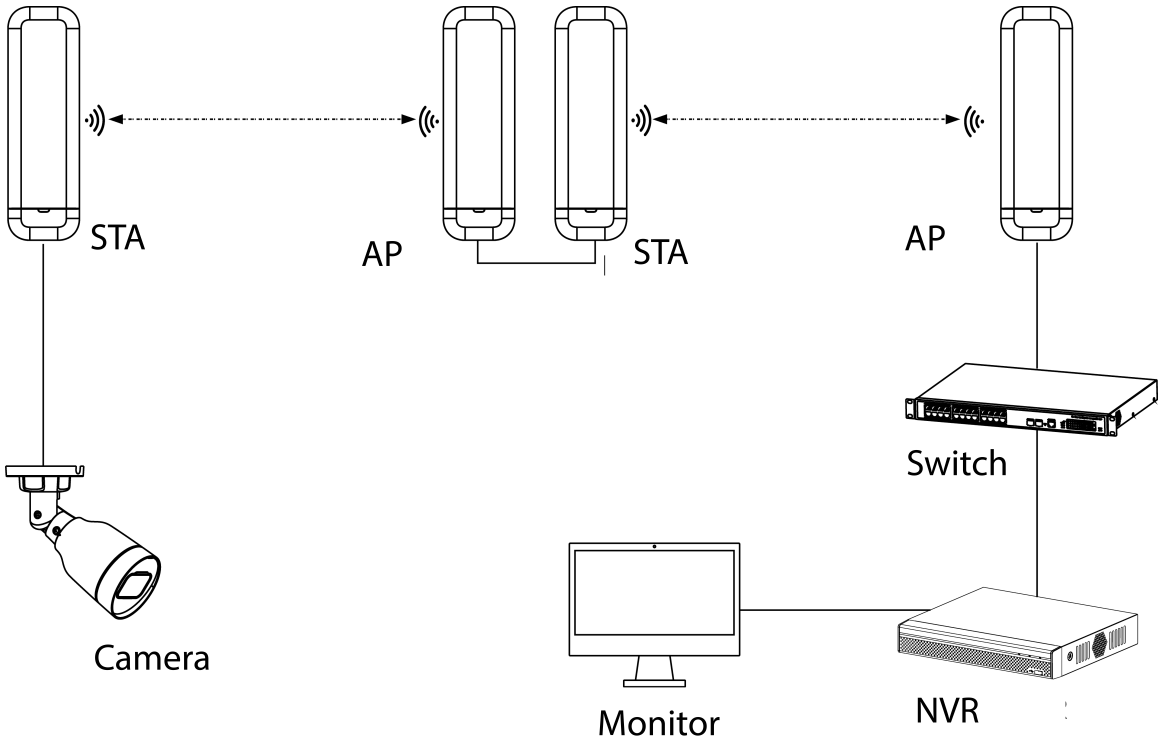


Figure 1-3 Network diagram (back-to-back)



2 Device Initialization

You need to initialize and configure the Device for the first time or after resetting it to factory settings

Background Information

- Ensure your computer is on the same network as the Device.
- Save the admin password after setup and change it regularly.

Procedure

Step 1 Open Internet Explorer (IE), enter the Device's IP address, and then press the Enter key.

When the Device is in the client mode, its default IP address is 192.168.1.36. When it is in the AP mode, its default address is 192.168.1.35.

DHCP is enabled by default. If there is DHCP server in the network, the IP addresses of the Device would be allocated by the server, and you need to log in to its web page with that IP address.

Step 2 Enter the default password, set the new one, enable the reserved Email address and enter yours, and then click **Next**.

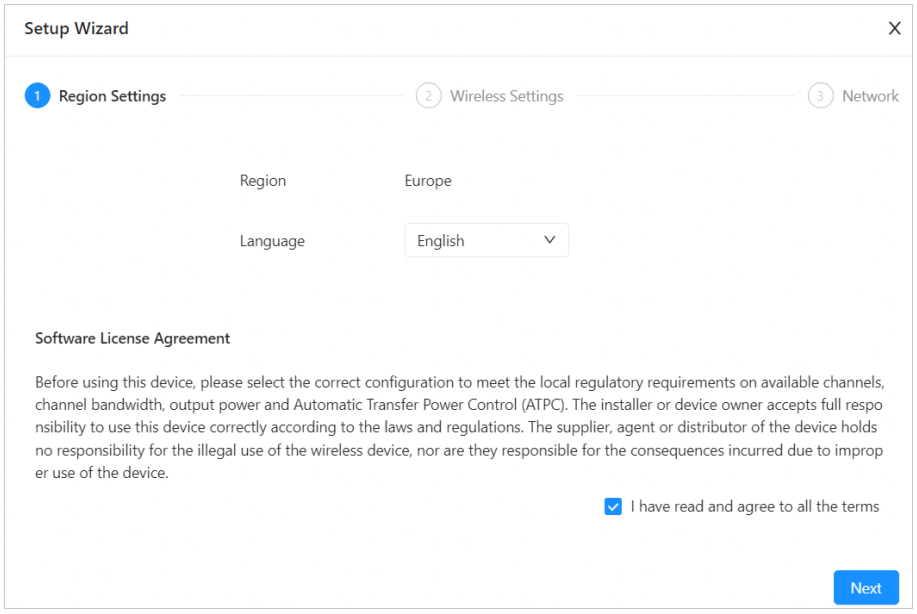
The default password is admin123. If you forget the password after you change it, you can reset the password with your reserved Email address.

The password length should be between 8 and 32 characters and must include at least two of the following: numbers, uppercase letters, lowercase letters, and special characters (excluding the following five characters: ' " ; : &).

Step 3 Enter the username and password, and then click **Login**.

Step 4 Select the language, read the software license agreement and click **I have read and agree to all the terms** , and then click **Next**.

Figure 2-1 Software license agreement



Step 5 Configure the parameters in wireless settings, and click **Next**.

When there are multiple access point devices in the same area, ensure that different channels are set for each device to avoid signal interference between them.

Figure 2-2 AP mode

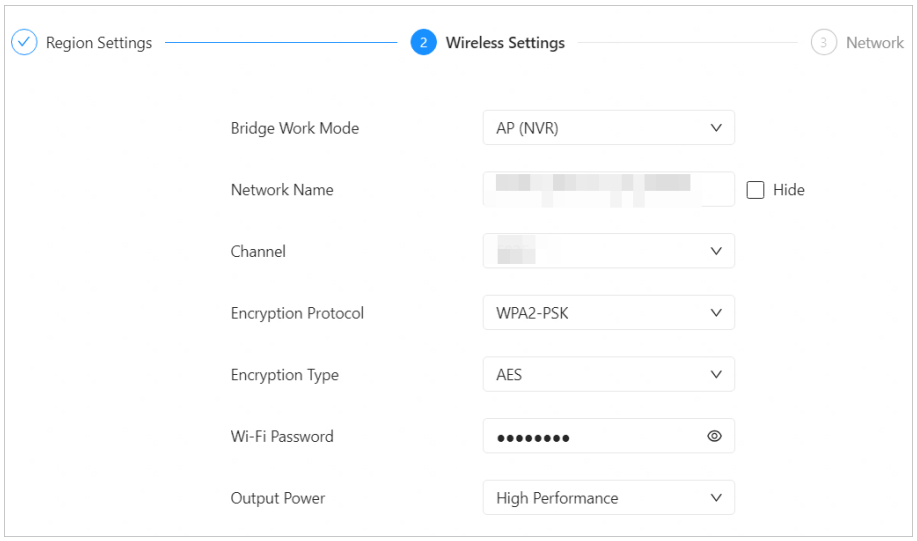


Figure 2-3 STA mode

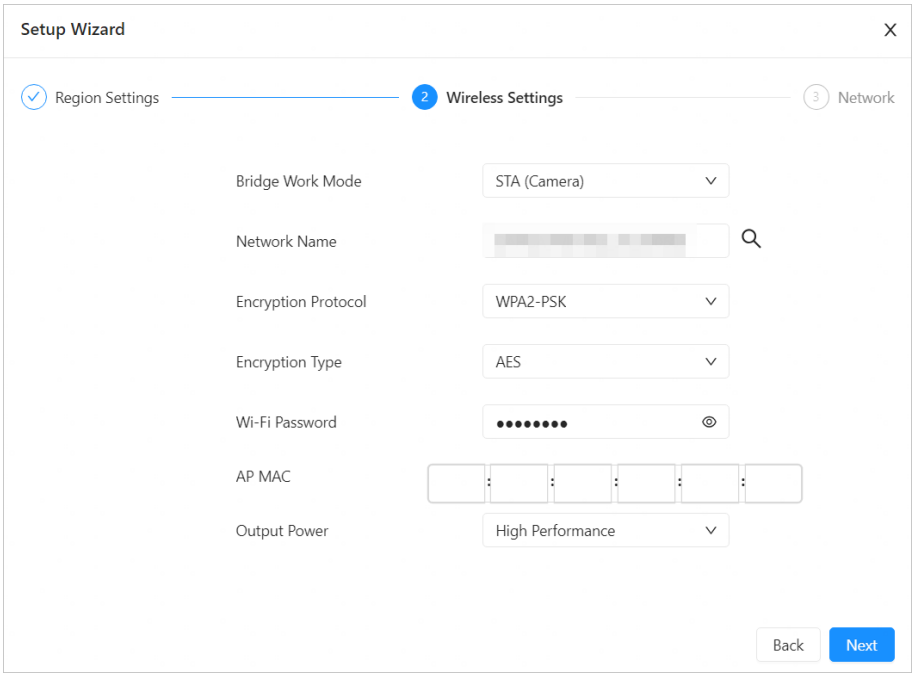


Table 2-1 Description of wireless setting parameters

Parameters	Description
Bridge Work Mode	It includes **AP (NVR)** and **STA (Camera)**. ● AP (NVR): Mainly configured on the side connected to storage devices. ● STA (Camera): Mainly configured on the side connected to cameras. Within the same local area network, ensure that the network name, encryption method, and wireless password of the configured access point and corresponding STA devices are consistent.
Network name	● Access Point: Set the network name, and other devices will connect to the network using this name. Enable **Hide** to support searching for peer bridges with a hidden SSID. ● STA: When this Device connects to other devices, communication is only possible if their network names are identical. Click on the right of the network name to search for surrounding wireless networks and connect to the desired wireless network as needed.

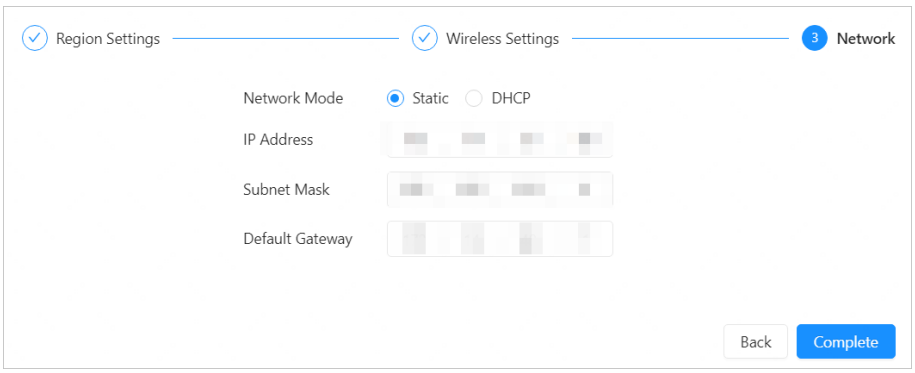
Parameters	Description
Channel	Select the channel used for data transmission, ensuring it does not overlap with the channels of adjacent wireless networks to minimize signal interference. Channel selection is only supported when the wireless bridge is operating in Access Point mode.
Encryption Protocol Encryption Type Wi-Fi Password	Select the encryption protocol and encryption type, and set a wireless password to encrypt the wireless connection. You can choose an appropriate encryption protocol based on the security requirements. • For devices that need to be paired with each other, the wireless encryption settings must be consistent; otherwise, the pairing connection cannot be established successfully. • If you select **No Encryption**, there is no need to set an encryption protocol or wireless password. In this case, other devices can access the Device without password verification. Please select with caution.
AP MAC	Display the MAC address of the access point. The MAC address of the access point is displayed only when the wireless bridge is operating in STA mode.
Output Power	Support eco mode, standard mode and high performance mode.

Step 6 Modify the Device's IP address according to the network plan, and then click **Complete**.

- Static: Manually enter the IP address, subnet mask, and default gateway.
- DHCP: IP addresses are dynamically assigned by the DHCP server.

Ensure that there are no IP address conflicts within the same local area network.

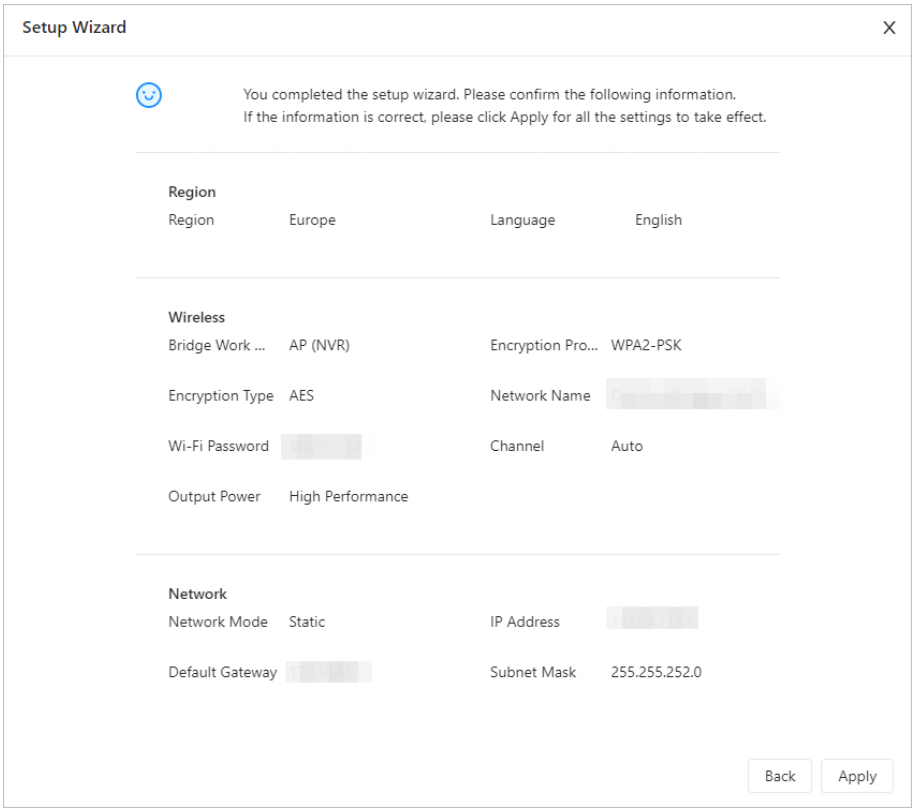
Figure 2-4 Network settings



Step 7 After confirming that the current configuration information is correct, click **Apply**.

If you need to modify the configuration, click **Back** to return to the configuration page.

Figure 2-5 Configuration information



3 Homepage overview

This topic describes how to log on to the WEB interface of a device through a browser.

Prerequisites

- Initialize the device before logging on to the device WEB page.
- When logging on to the device, make sure that the IP address of the PC and the IP address of the device are in the same network.

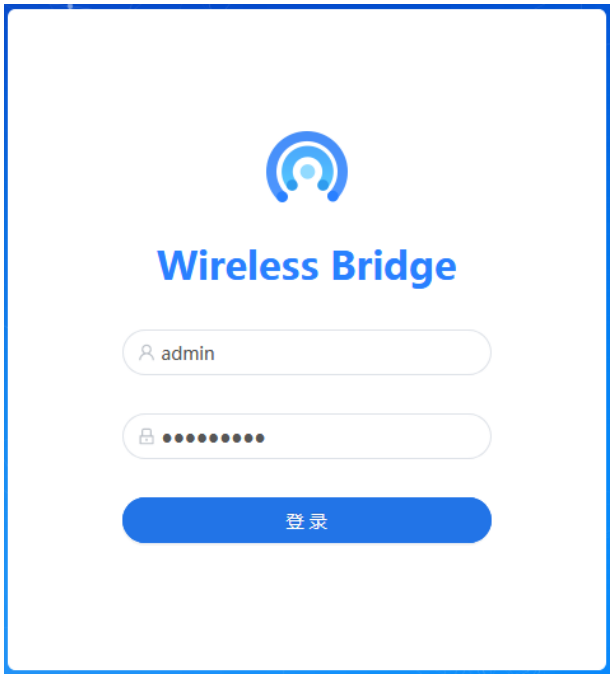
Procedure

Step 1 Open the browser, Enter the Device IP address in the address bar (the default IP address is 192.168.1.36), and press [Enter].

Step 2 Enter the username and password.

The default username is admin, and the password is the logon password of the admin user set in device initialization.

Figure 3-1 Log on to the WEB



Step 3 Click **Login**.

Figure 3-2 WEB main interface

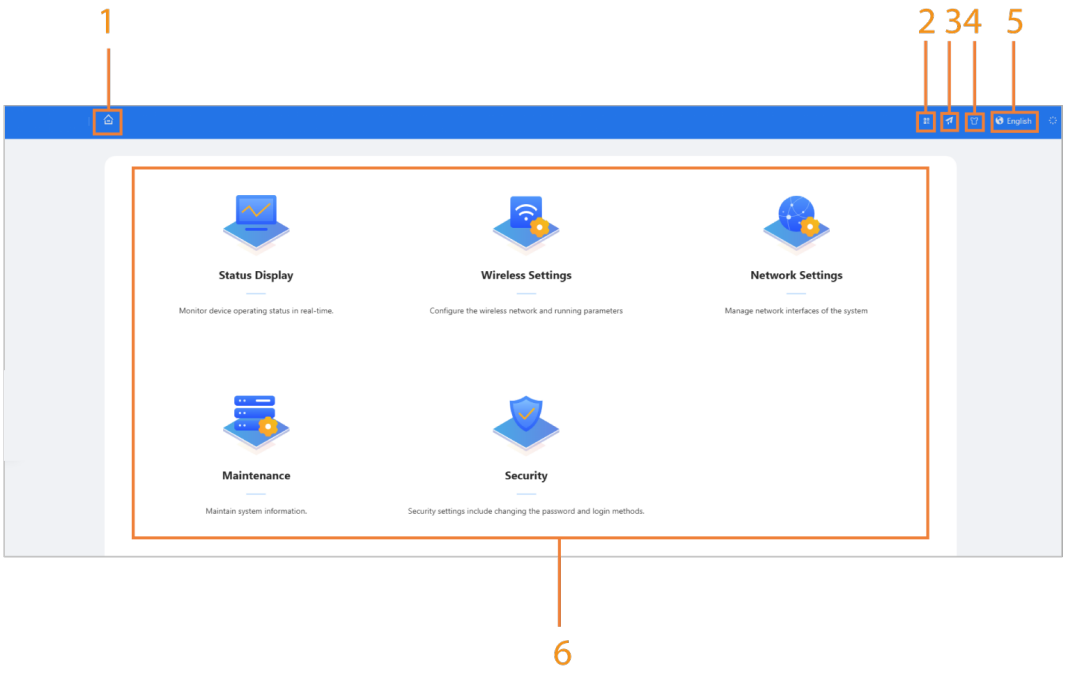


Table 3-1 WEB main interface layout description

No.	Function	Description
1	Main interface	Click this icon to go to the main WEB interface.
2	Product material QR code	Scan the code to obtain the user manual of the device.
3	Setup Wizard	Click this icon to go to the Setting Wizard interface.
4	Webpage theme	Click this icon to switch the webpage theme.
5	Language	Click this icon to change the language.
6	Configuration modules	Click different configuration modules to configure the device.

4 Status Display

The chapter introduces how to view device information, status monitoring and wireless network.

4.1 Viewing the Device Information

You can view device information, including basic information, wireless connection information, wired information, and network interface statistics.

On the home page, select **Status Display** > **Device Info**. You can view device information, including basic information, wireless connection information, wired information, and network page statistics.

4.2 Monitoring the Device Status

You can view device status, including device running duration, CPU usage, memory usage, throughput rate of different ports, and signal strength/noise level.

On the home page, select **Status Display** > **Status Monitor**.

Figure 4-1 Status monitoring

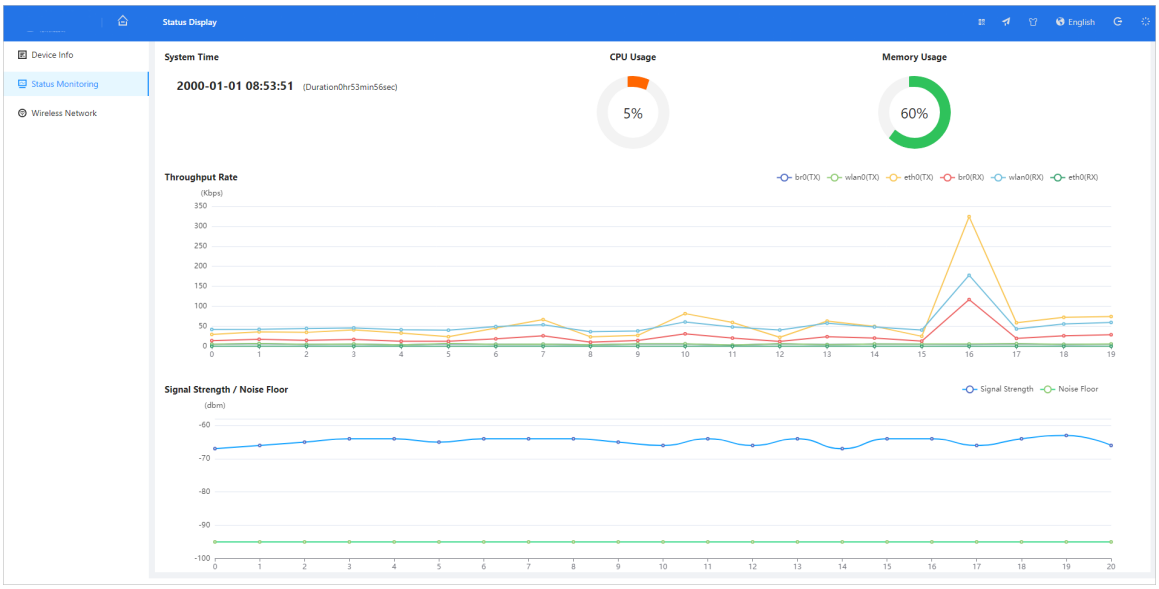


Table 4-1 Description of status monitoring

Parameter	Description
System Time	Displays the system time and the running duration of the Device.
CPU Usage	Displays the CPU usage of the Device.
Memory Usage	Displays the memory usage of the Device.

Parameter	Description
Throughput Rate	It refers to the amount of data transmitted over the network within a unit of time, used to measure network performance. You can monitor the speed of data transmission in real-time through the throughput rate. ● The system refreshes data every 5 seconds and displays the results of the latest 30 refreshes. ● Click on the interface type in the upper right corner of the chart (e.g., br0(TX)) to hide the data for the corresponding interface. ● Hover the mouse over the chart to display detailed data for the corresponding moment.
Signal Strength/Noise Floor	● Signal Strength: The signal strength of the current device. ● Noise Floor: The intensity of interference from the surrounding environment. ● The system refreshes data every 5 seconds and displays the results of the latest 30 refreshes. ● Click the type in the upper right corner of the chart (e.g., Signal Strength) to hide the data for the corresponding type. ● Hover the mouse over the chart to display detailed data for the corresponding moment.

4.3 Viewing Connection Information

You can view the connection information of access point and client.

Procedure

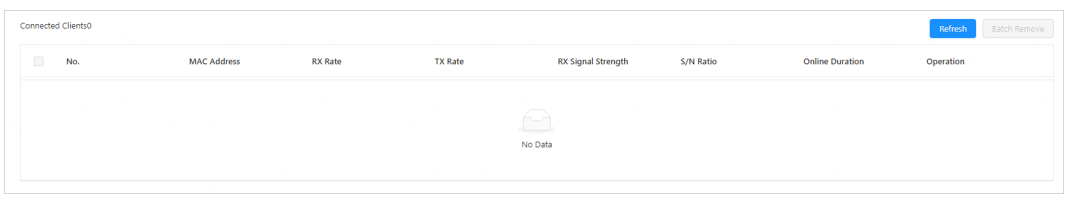
Step 1 On the main interface, select **Status Display** > **Wireless Network**.

Step 2 View the connection information of access point and client.

- Access point: View the number of connected clients and related information of clients in real time, including MAC address, RX rate, TX rate, RX signal strength, S/N Ratio, online duration and operation.

  You can click to delete the connected client. Click **Batch Remove** to remove the corresponding client devices.

Figure 4-2 Wireless network (1)



- Client: View related information of connected access point.

Figure 4-3 Wireless network (2)

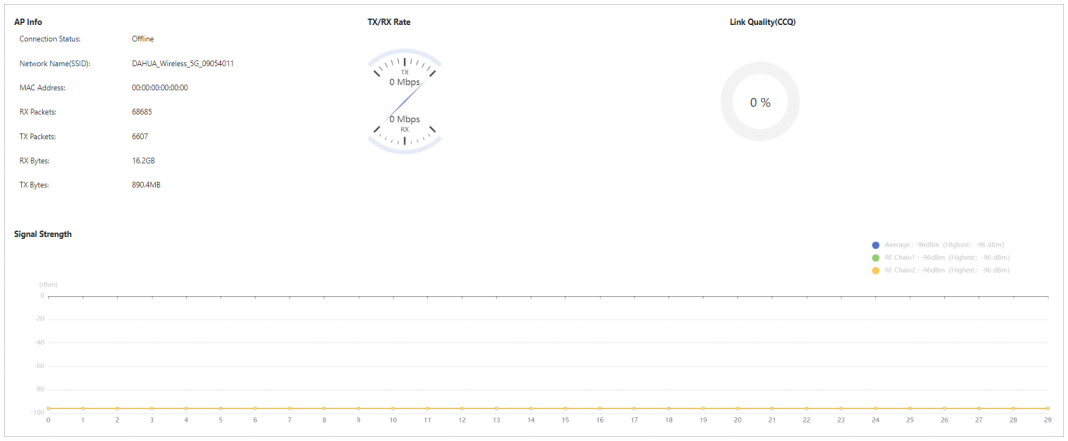


Table 4-2 Description of client information

Parameter	Description
AP Info	Displays information about the connected access point devices on the client, such as connection status, network name, MAC address, etc.
TX/RX Rate	Displays instantaneous rate when device sends or receives data.
Link Quality (CCQ)	Displays the quality of the connected channel.
Signal Strength	Displays total signal strength of the client and the signal strength received by different links on the client. The system refreshes the data every five seconds and displays the results of the latest thirty refreshes.

5 Wireless Settings

This chapter introduces basic wireless settings, advanced wireless settings and management settings.

5.1 Basic Wireless Settings

Procedure

Step 1 On the main webpage, select **Wireless Setting** > **Basic Setting**.

Step 2 Set basic wireless parameters of the Device.

Figure 5-1 Basic wireless settings of access point

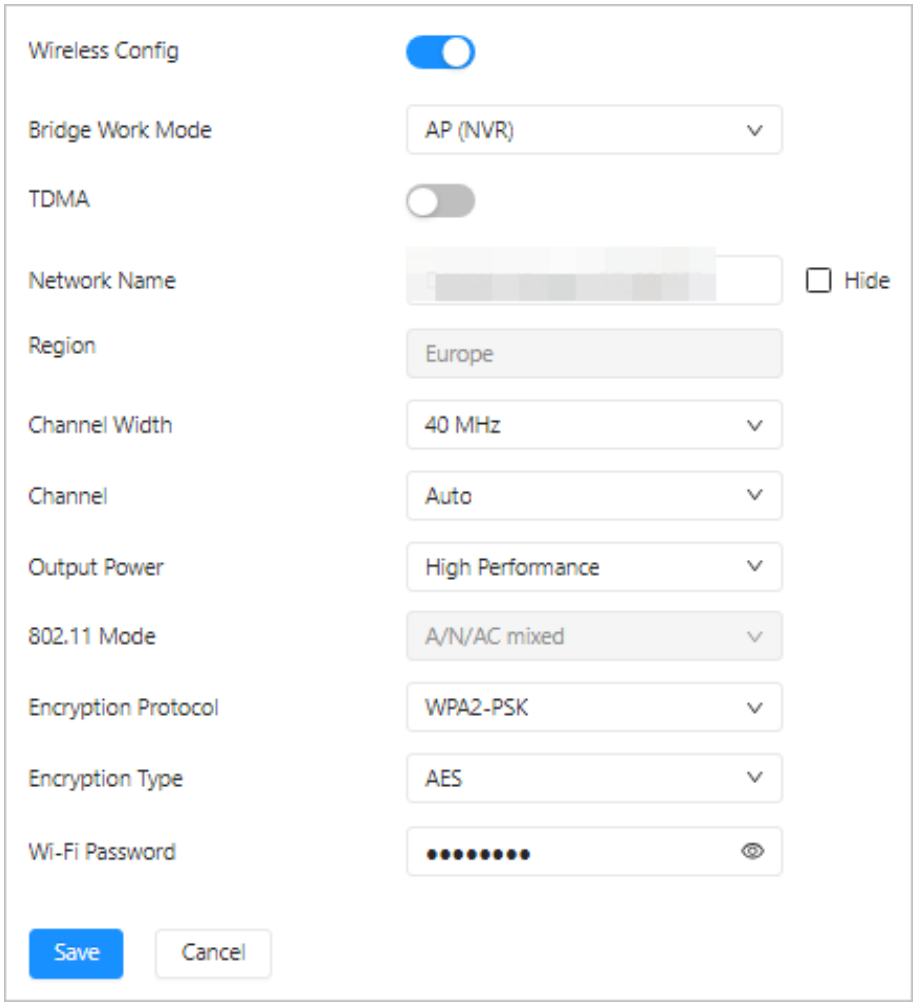


Figure 5-2 Basic wireless settings of client

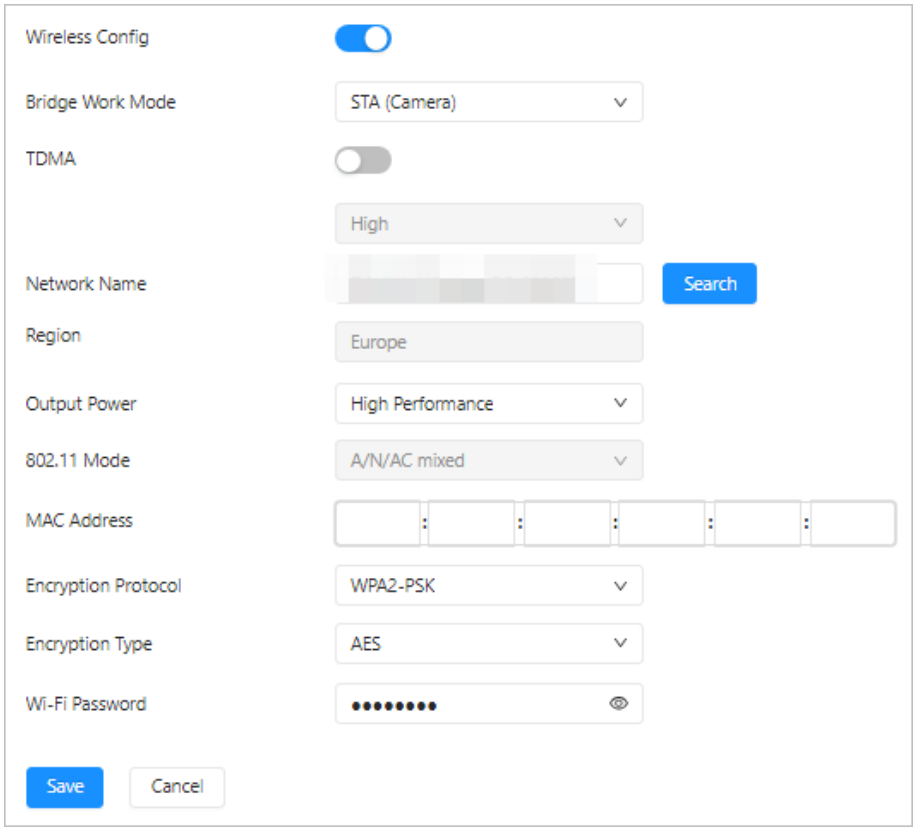


Table 5-1 Description of wireless basic settings

Parameter	Description
Wireless Config	Enabled by default.
Bridge Working Mode	• Access point: Wireless access node. It can be connected to a device such as a NVR. An access point can be connected to multiple clients. • Client: Works with the access point. It can be connected to a device as a camera. A client can only be connected to one access point.
TDMA	Enable the TDMA (Time Division Multiple Access) function, which reduces data interference between devices by assigning independent time slots to each user, ensuring that each device can transmit or receive data without interference within a specific time period.

Parameter	Description
Network Name	Access point: Set the network name, and other devices will connect to the network based on this name. Enable **Hide** to support searching for peer bridges with hidden SSIDs Client: When this device connects to other devices, communication is only possible if the same network name is set. Click on the network name to search for surrounding wireless networks and connect to the desired wireless network as needed.
Region	Displays the region that the Device's frequency matches.
Channel Width	The passing frequency range of the signal frequency. It defines the upper and lower limits of the signal frequency allowed to pass through the channel.
Channel	We recommend selecting an unoccupied channel in the current environment or the one where the weak signal in the scanning list is located, to ensure more stable wireless transmission.
Output Power	The output power of wireless signal. You can configure the output power of the device according to the actual working conditions and local regulations. The higher the output power, the longer the wireless transmission distance.
802.11 Mode	Currently follows the 802.11 protocol. **A/N/AC mixed** is set by default.
MAC Address	By specifying the MAC address of the pairing access point, the client can only be connected to the specific access point. The MAC address is displayed only when the bridge is operating in Client mode.
Encryption Protocol	Select the encryption type, encryption protocol, and set a Wi-Fi password to encrypt the wireless connection. Users can choose an appropriate encryption protocol based on their security requirements. The devices to be paired must have the same encryption type, otherwise they will not be paired.
Encryption Type	
Wi-Fi Password	

Step 3 Click **Save**.

5.2 Advanced Wireless Settings

Procedure

Step 1 Select **Wireless Setting** > **Wireless Advanced Setting**.

Step 2 Set wireless advanced parameters of the Device.

Figure 5-3 Advanced wireless settings of access point

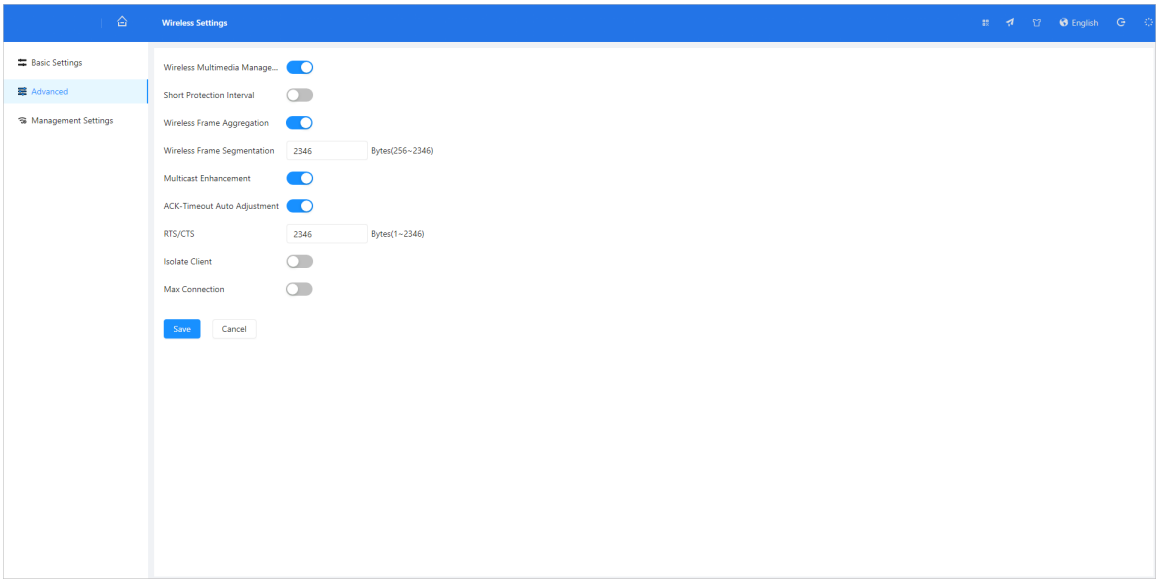


Figure 5-4 Advanced wireless settings of client

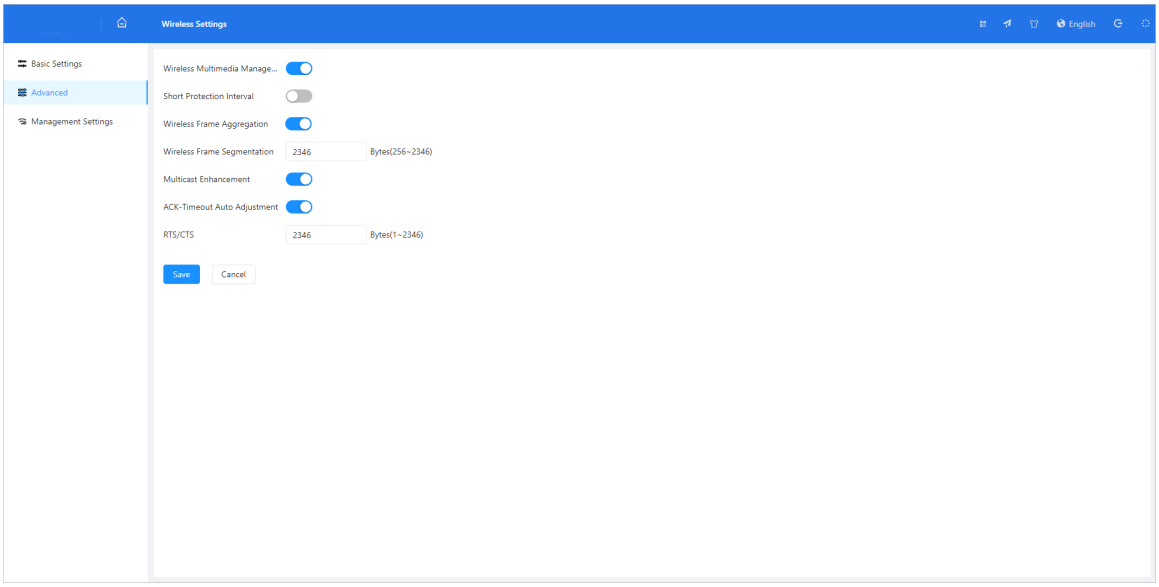


Table 5-2 Description of advanced wireless settings

Parameter	Description
Wireless Multimedia Management	Enabled by default to realize wireless Quality of Service (QoS).
Short Protection Interval	Contribute to more efficient use of the wireless spectrum and can increase the data throughput of the connection. But if you experience issues such as dropped connections or poor signal quality, you might need to disable it for more stability. It is disabled by default.

Parameter	Description
Wireless Frame Aggregation	Enable different frames to be combined together and then sent out. Enabling this function can improve the throughput to a certain extent. It is enabled by default.
Wireless Frame Segmentation	If the length of the packet exceeds the defined value, the packet is divided into multiple data segments, and the number of data segments can only be even. According to the network environment, configuring different wireless frame segmentation values can reduce the network transmission error rate and improve the frame transmission efficiency.
Multicast Enhancement	With the function enabled, multicast packets are allowed to pass through. It is enabled by default.
ACK-Timeout Auto Adjustment	Automatically tests the distance between 2 devices, and sets parameters according to this distance to achieve the best wireless connection quality. Enabled by default.
RTS/CTS	Set the byte count for RTS/CTS (Request To Send/Clear To Send). When the length of the data packet that this device is about to send to the access point is greater than or equal to the preset value, the RTS/CTS mechanism will be activated. RTS/CTS Mechanism: 1. This device sends an RTS packet to the access point, notifying it that this device is about to start sending data. 2. Upon receiving the RTS packet, the access point notifies all other devices within its coverage area to defer their transmissions via a CTS packet. 3. At the same time, the access point informs this device that it can begin sending data. 4. This device starts transmitting the data packet.
Isolate Client	Enabling this function to prevent devices connected to the same access point from communicating with each other. Disabled by default.
Max Connection	Enabling this function to set the maximum number of clients connected to the access point, and the number is 8 by default.

Step 3 Click **Save**.

5.3 Management Settings

Procedure

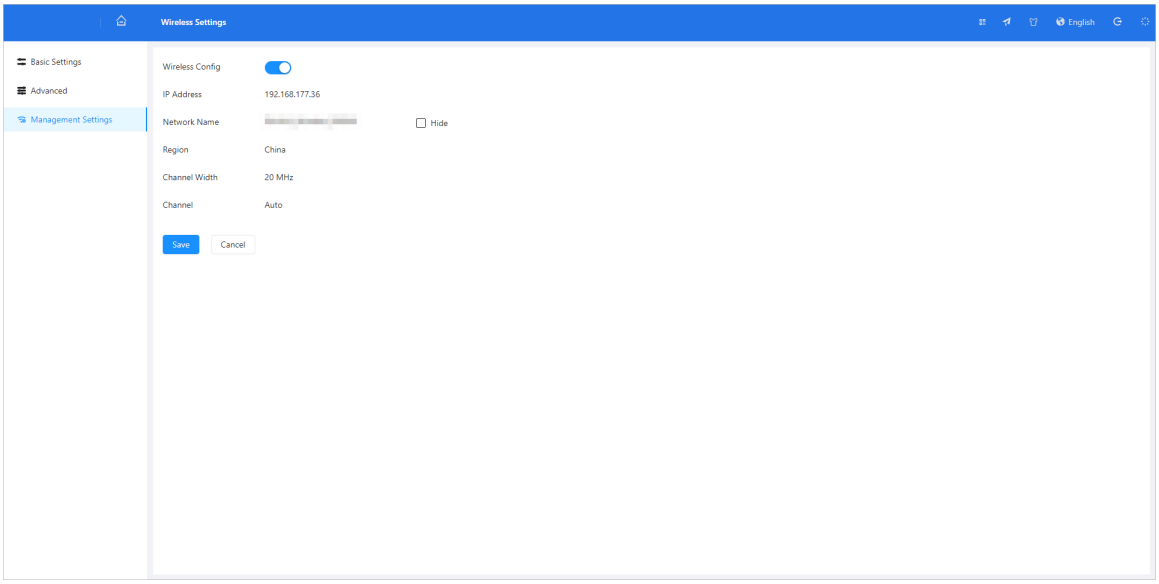
Step 1 Select **Management Settings**.

Step 2 Click **Wireless Config** to configure the AP. It is enabled by default.

Step 3 (Optional) Select **Hide** to hide the AP from being searched by other clients.

Step 4 Click **Save**.

Figure 5-5 Management Settings



6 Network Settings

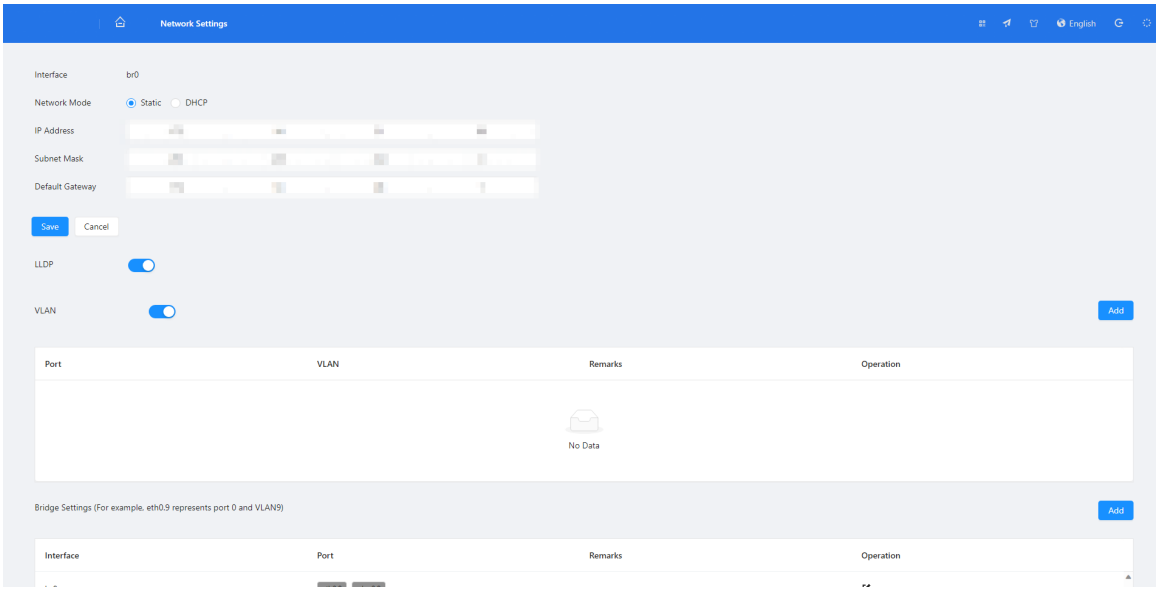
This chapter introduces how to set interface, VLAN, and bridge.

Procedure

Step 1 Select **Network Settings**.

Step 2 Set network parameters of the Device.

Figure 6-1 Network settings



- Port settings

  1. Set relevant parameters.
  2. Click **Save**.

Table 6-1 Description of interface parameters

Parameter	Description
Network Mode	◇ Static: Manually set the IP address, subnet mask, and default gateway. ◇ DHCP: IP addresses are assigned by the DHCP server.
IP Address	
Subnet Mask	
Default Gateway	

Step 3 Enable LLDP.

After you enable it, the bridge could detect other devices (such as switches or routers) in the network. Moreover, it can obtain their identity and attributes to help the admin to check the communication quality.

7 Maintenance

This chapter introduces how to set the system time and general configuration, backup and restore the configuration, update the system, diagnose and restart the Device, set the iperf test, query logs and legal information and enable cloud management.

7.1 Setting System Time

Set the time zone, NTP sever and the port.

Procedure

Step 1 On the homepage, select **Maintenance** > **System Time**.

Step 2 Configure the system time.

- Manual setting: Disable the NTP function, select the system time and time zone, and click **Save**.

  Click **Synchronized with the current end device time**, and then the Device will adjust the system time according to the current computer time.

Figure 7-1 Manually set the system time

- NTP: Enable NTP to automatically obtain NTP server information, and click **Save**.

  The Device will synchronize its time with the NTP server.

  You can also manually set the NTP server's domain name/IP address and port number, and click **Manual Update** to apply the changes.

Figure 7-2 Enable NTP

7.2 General Configuration

The section introduces general configuration, including basic information and LED settings.

7.2.1 Basic Information

Procedure

Step 1 On the main interface, select **Maintenance** > **General Config** > **Basic Info**.

Step 2 Configure related parameters.

Figure 7-3 Basic Info

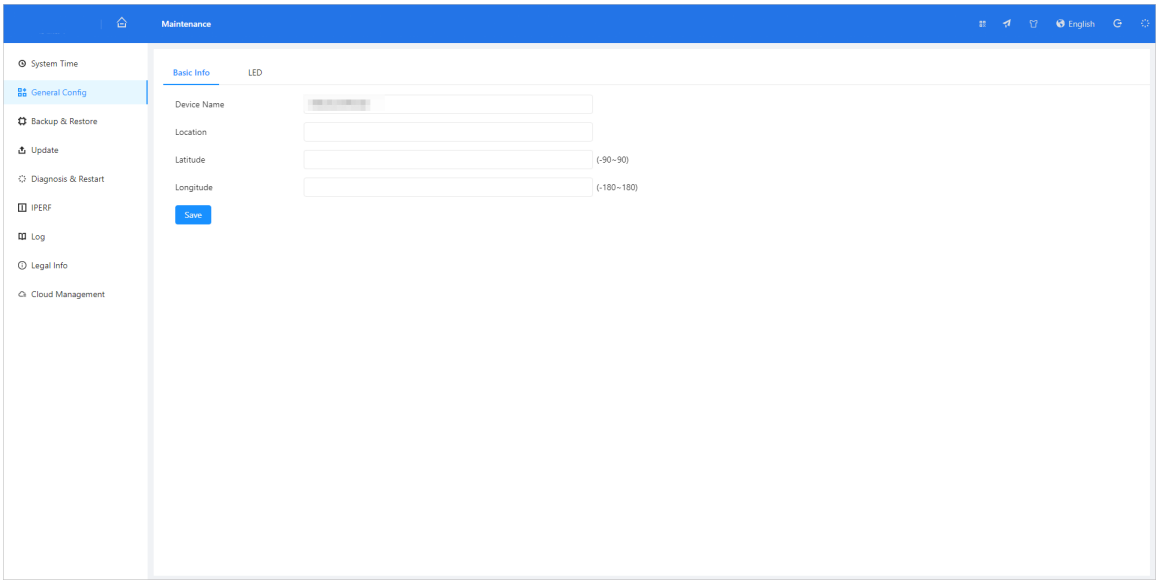


Table 7-1 Description of basic info

Parameter	Description
Device Name	Name of the current device.
Location	Geographical location of the current device.
Latitude	Latitude of the current device, ranging from –90° to 90°.
Longitude	Longitude of the current device, ranging from –180° to 180°.

Step 3 Click **Save**.

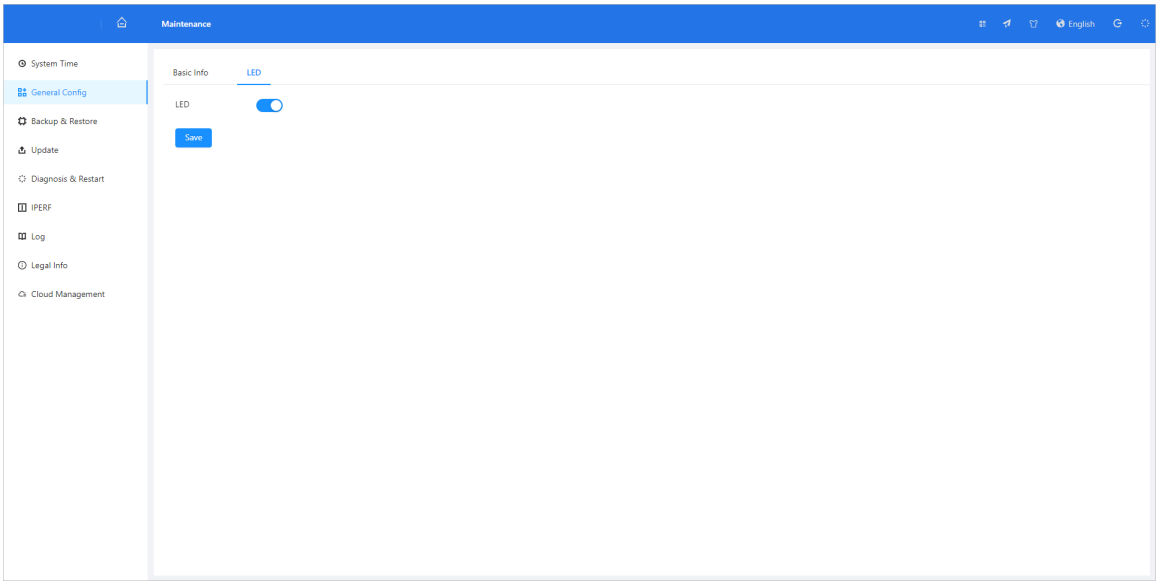
7.2.2 LED

Procedure

Step 1 On the home page, select **Maintenance** > **General Config** > **LED**.

Step 2 Enable **LED**.

Figure 7-4 LED

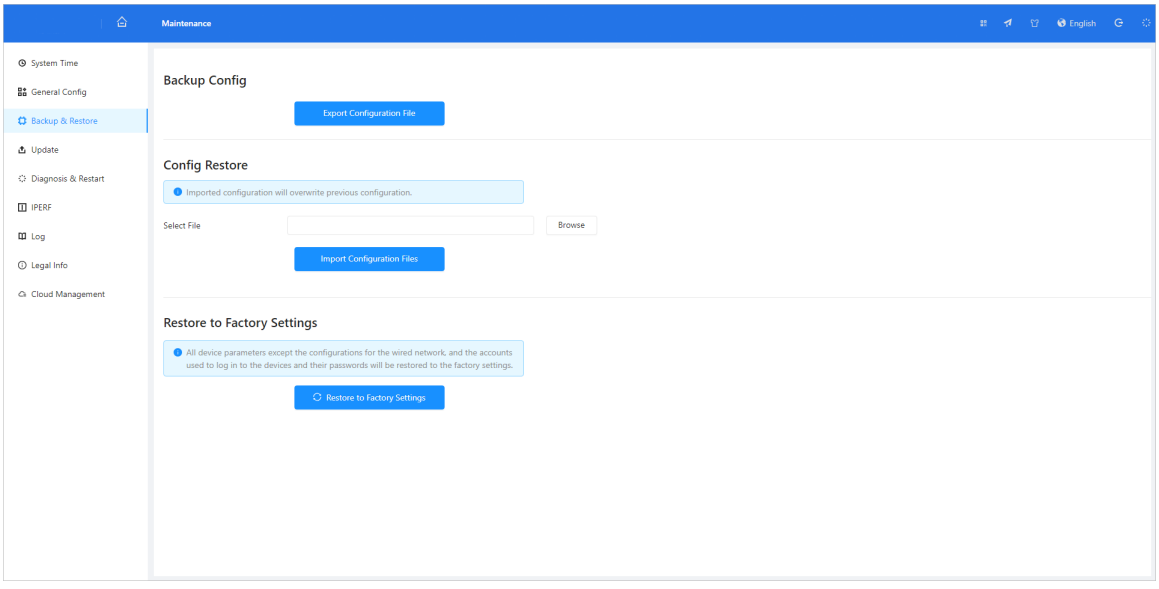


Step 3 Click **Save**.

7.3 Backup & Restore

On the home page, select **Maintenance** > **Backup & Restore**. It introduces how to export and import configuration files, and restore the Device to factory settings.

Figure 7-5 Backup & restore



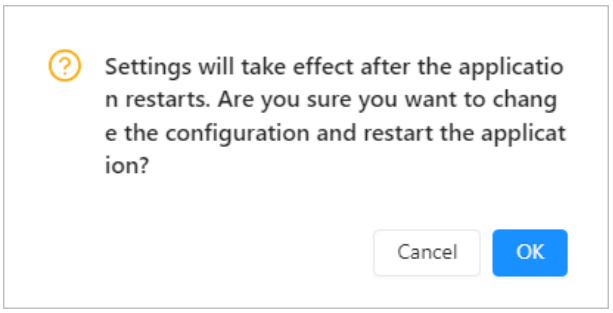
Backup Config

Click **Export Configuration File** to download the current device configuration.

Config Restoration

- Click **Browse** to choose the file to be imported.
- Click **Import Configuration Files** to upload the file and replace the current configuration. After that, there would be a pop-up window for confirmation, and then click **OK**.

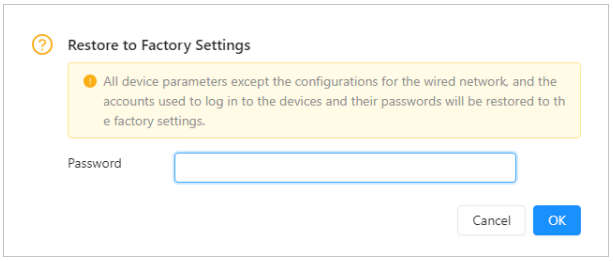
Figure 7-6 Confirmation



Restore to Factory Settings

Click **Restore to Factory Settings** , a pop-up window will appear, prompting you to enter the password for the account used to log in to the Device. Enter the password and click **OK**.

Figure 7-7 Enter the password



7.4 Diagnosis & Restart

On the **Diagnosis & Restart** interface of the client or access point, you can set destination IP or domain name, packet size, and ping times, and restart the device.

7.4.1 Diagnosing the Device

Procedure

Step 1 On the main interface, select **Maintenance** > **Diagnosis & Restart**.

Step 2 Set relevant parameters.

Figure 7-8 Diagnosis settings

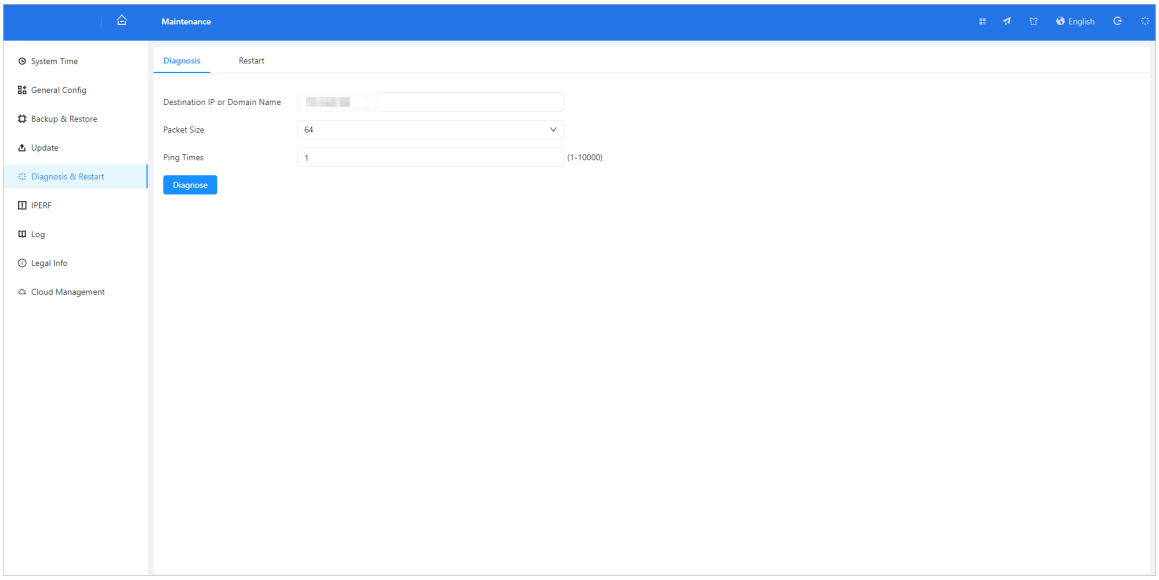


Table 7-2 Description of diagnosis parameters

Parameter	Description
Destination IP or Domain Name	Enter the IP address or domain name of the target host.
Package Size	Select the packet size.
Ping Times	Set ping times.

Step 3 Click **Diagnose**. The system automatically starts the diagnosis and displays the results.

7.4.2 Restarting the Device

On the home page, select **Maintenance** > **Diagnostics & Restart** > **Restart**, click **Restart Now** , and then click **OK** in the pop-up window to begin restarting the Device.

7.5 IPERF

When access point and client are connected, you can test network performance by setting the IP address of the access point (client), iperf test duration, iperf thread number, and iperf interval in the client (access point).

Procedure

Step 1 On the home page, select **Maintenance** > **IPERF**.

Step 2 Select the IPERF type, and then configure related parameters.

Figure 7-9 IPERF settings

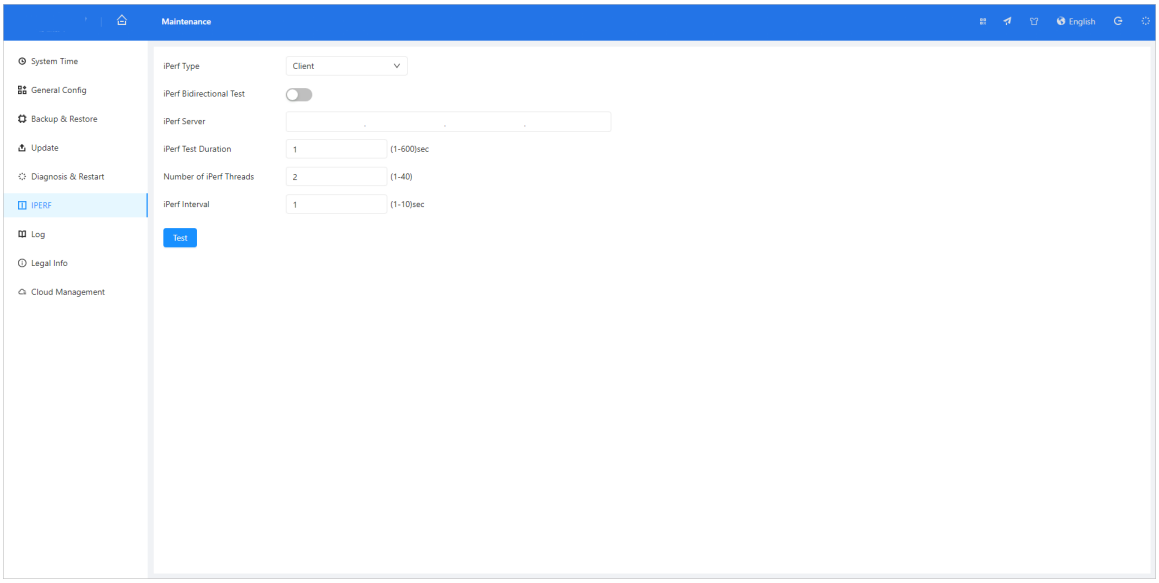


Table 7-3 Description of IPERF parameters

Parameter	Description
IPERF Type	Select the bridge working mode of the peer device. ● Client: When this device is an access point, select **Client** for the IPERF type. ● Server: When this device is a client, select **Access Point** for the IPERF type.
IPERF Bidirectional Testing	Enable this function to test the network speed in two directions. It is disabled by default.
IPERF Server	Enter the IP address of the device to be tested.
IPERF Test Duration	Set throughput test duration, ranging from 1 second to 600 seconds.
Number of IPERF Threads	Set the number of throughput threads, ranging from 1 to 40.
IPERF Interval	Set the feedback printing interval of throughput test results, ranging from 1 second to 10 seconds.

Step 3 Click **Test**.

7.6 Log

You can view device logs by time and keywords, connect to log the server and save the device log information to the server to ensure the security of log information.

On the main interface, select **Maintenance** > **Log**.

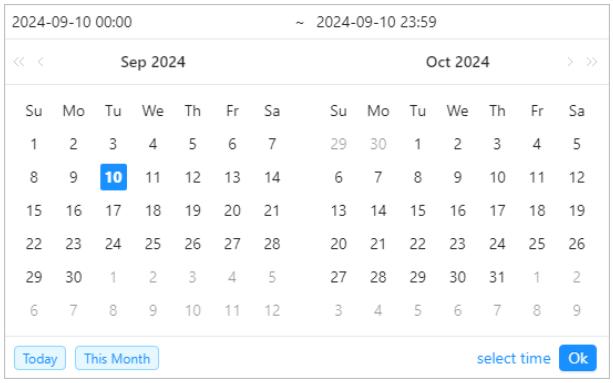
7.6.1 Viewing Device Log

Procedure

Step 1 On the home page, select **Maintenance** > **Log** > **Device Log**.

Step 2 On the time setting column, select the start date and end date, choose the needed filter type and then enter the related keywords. Click **Search**.

Figure 7-10 Select the date



Step 3 Click **Backup** to download the log information to your local device.

7.6.2 Configuring System Log Remote Storage

Procedure

Step 1 Enable the remote storage of system log, and then set parameters.

Step 2 Click **Save**.

Figure 7-11 System log remote storage

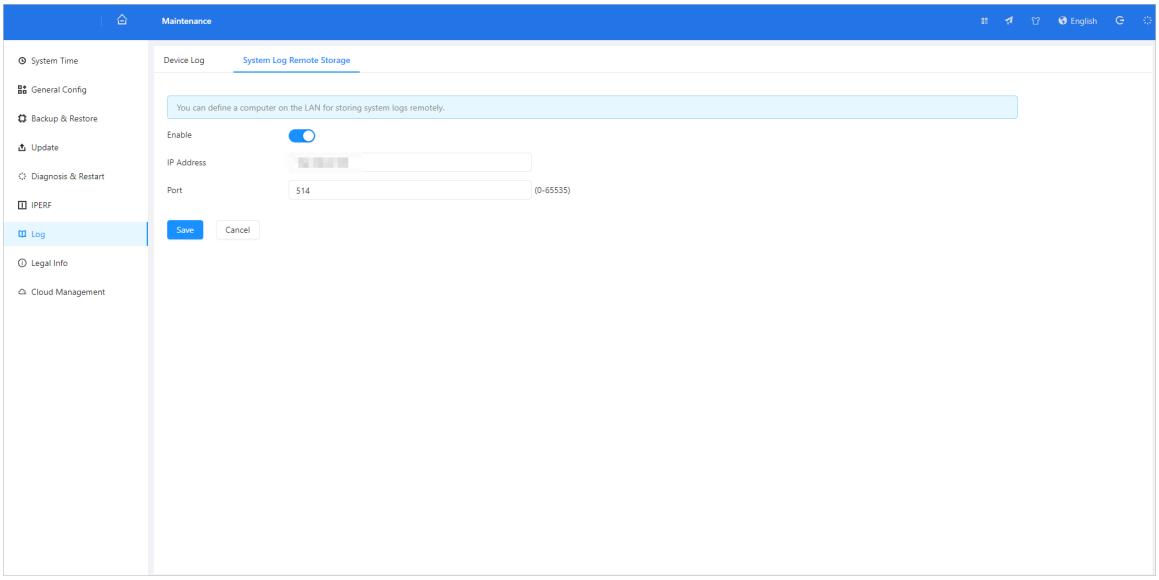


Table 7-4 Parameter description of system log remote storage

Parameter	Description
IP Address	Enter the IP address of the log server.
Port	Enter the port value, ranging from 1 to 65535.

7.7 Legal Information

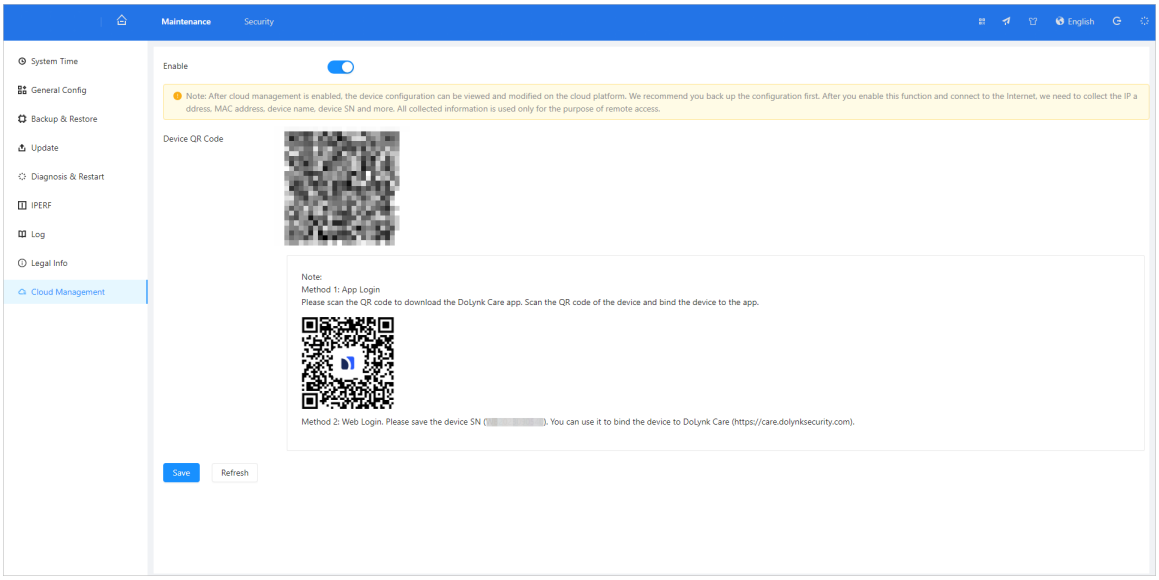
On the home page, select **Maintenance** > **Legal Info**. You can view software license agreement, privacy policy and open source software notice.

7.8 Cloud Management

You can manage the device through DoLynk Care app or DoLynk Care webpage.

1. Enable the function of cloud management. The device QR code, device SN and a login note would be displayed below.
2. Click **Save** to save your operation. Click **Refresh** to refresh the latest configuration in case that it was changed in other clients.
3. Select the login method as needed according to the instructions of the note.

Figure 7-12 Cloud management



8 Security

This chapter introduces how to change password and set contact mode, basic services, HTTPS, CA certificates, attack defense and security authentication.

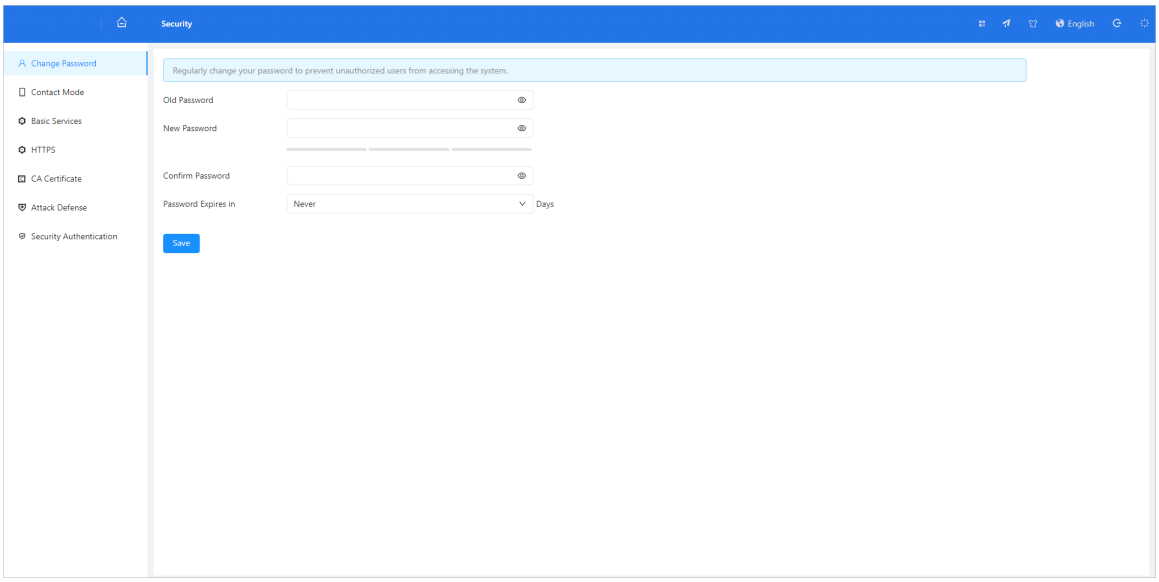
8.1 Changing Password

This section introduces the method to change your password.

Procedure

Step 1 On the main interface, select **Security** > **Change Password**.

Figure 8-1 Change password



Step 2 Enter your current password and the new one, and then re-enter the new password in the text box below for confirmation.

Step 3 Set an expiration period for the new password by choosing one duration in the drop-down list.

When the expiration period reaches the preset password update cycle, the system will prompt the user to update the password in a timely manner.

Step 4 Click **Save**.

8.2 Contact Mode

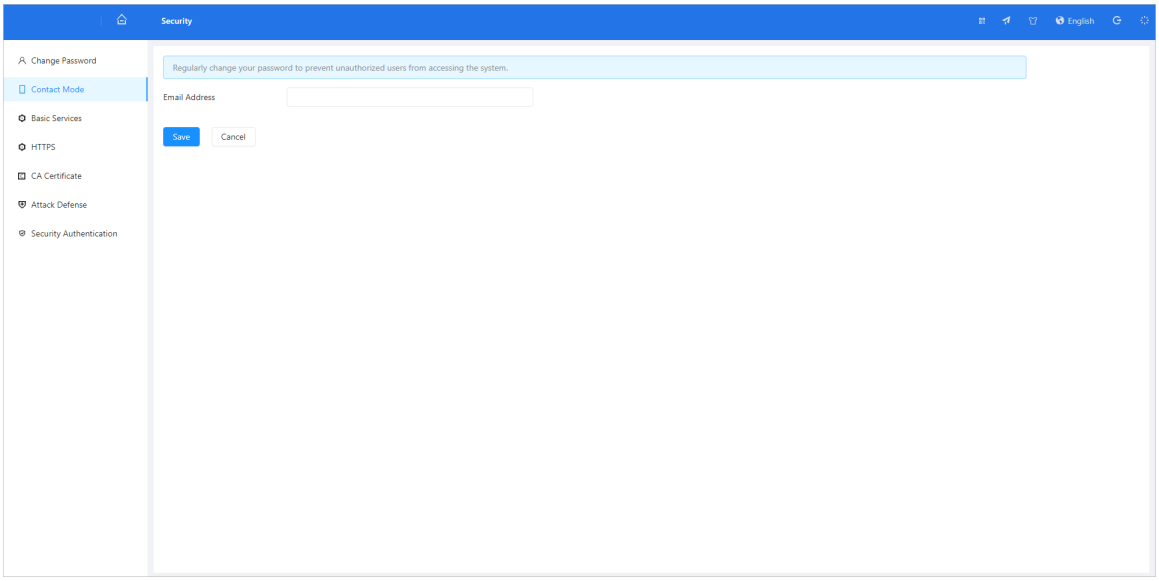
Reserve your email address for the convenient communication on any possible issue.

Procedure

Step 1 On the main interface, select **Security** > **Contact Mode**.

Step 2 Enter your email address in the text box.

Figure 8-2 Contact mode



Step 3 Click **Save**.

8.3 Basic Services

Set SSH (Secure Shell), TLS1.1 (Transport Layer Security) and Private Protocol.

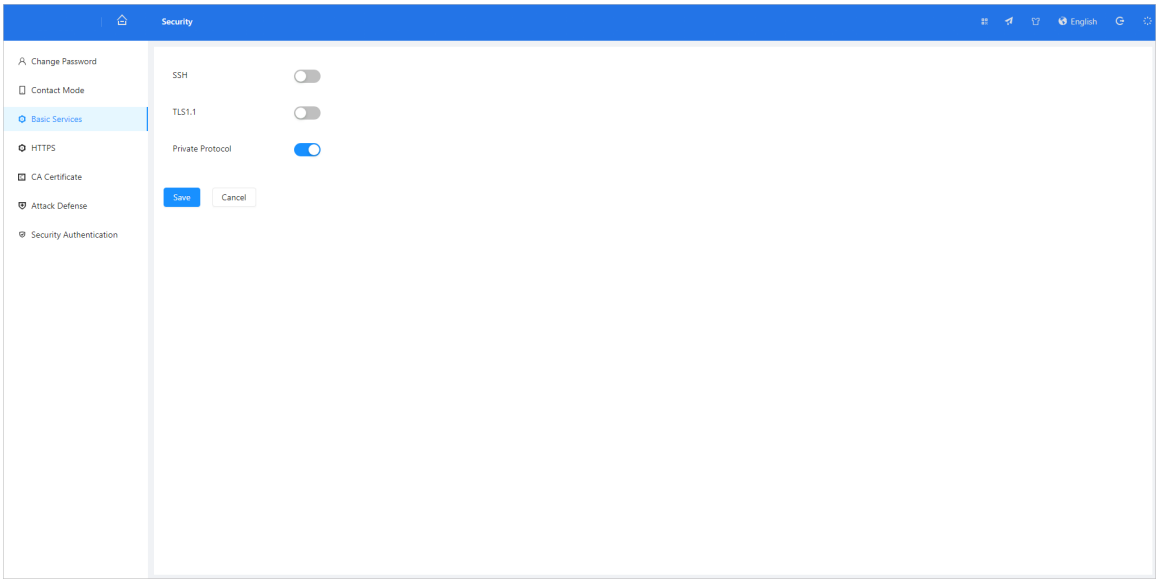
Procedure

Step 1 On the main interface, select **Security** > **Basic Services**.

Step 2 Enable **SSH** or **TLS1.1** as needed. **Private Protocol** is enabled by default.

- SSH: SSH is a security protocol that provides secure remote access and command execution by encrypting the communication. By enabling SSH on the wireless bridge, you can securely connect to the bridge using an SSH client and perform management operations and configuration changes.
- TLS: TLS is a security protocol used for providing secure communication over computer networks. By enabling TLS 1.1, you can extend the encryption method used for transmission. But enabling it may have risks since it is outdated.

Figure 8-3 Basic services



Step 3 Click **Save**.

8.4 HTTPS

Set HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer). Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) is a protocol used for secure communication over a computer network. It is essentially an extension of the standard Hyper Text Transfer Protocol (HTTP), enhanced by incorporating the Secure Socket Layer (SSL) or its successor, Transport Layer Security (TLS).

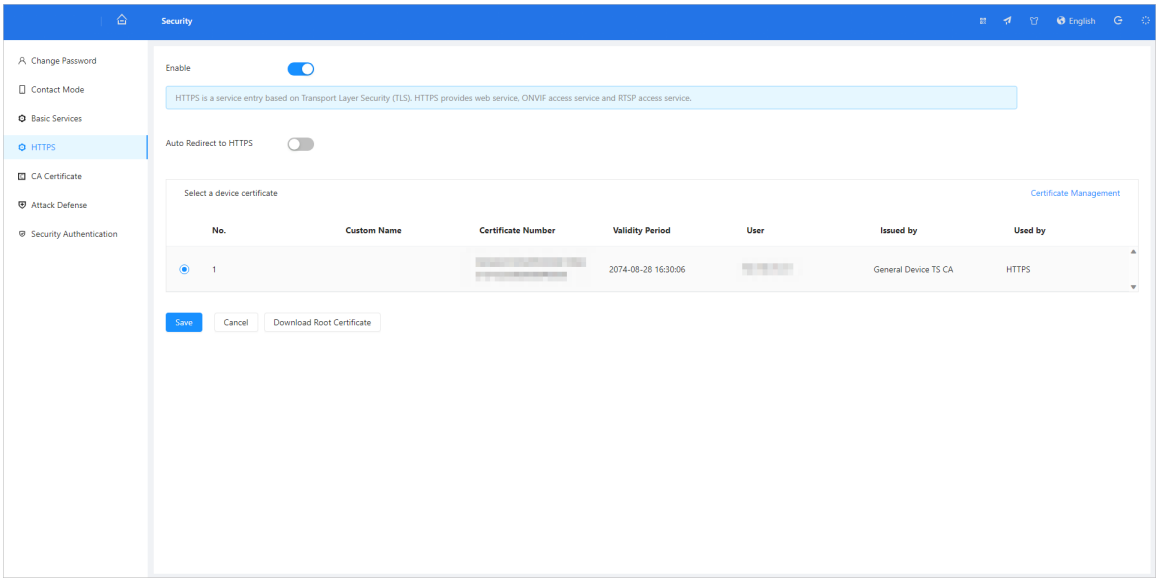
Procedure

Step 1 On the main interface, select **Security** > **HTTPS**.

Step 2 HTTPS is enabled by default. You can enable **Auto Redirect to HTTPS** for entering this webpage automatically in HTTPS mode next time, and then click **Save**.

Step 3 (Optional) You are supported to download root certificate to your local device by selecting a device certificate in the certificate list above and clicking **Download Root Certificate** . And by clicking **Certificate Management** on the upper right corner of the list, you can manage the certificates after the webpage goes to CA Certificate module.

Figure 8-4 Setting HTTPS



8.5 CA Certificate

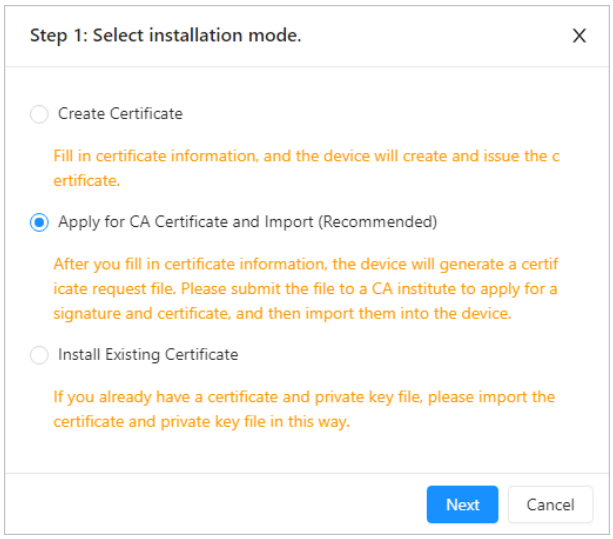
8.5.1 Device Certificates

Procedure

Step 1 On the main interface, select **Security** > **CA Certificate**.

Step 2 Click **Install Device Certificate** to add device certificates.

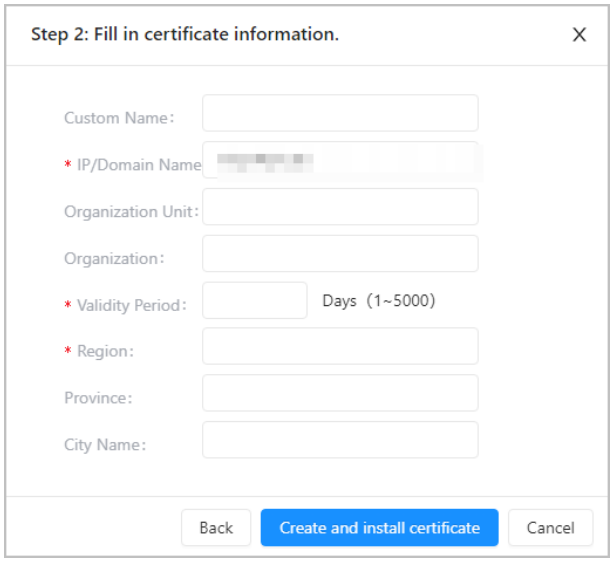
Figure 8-5 Select installation mode



- Create certificate: Enter related information, and then click **Create and install certificate**.

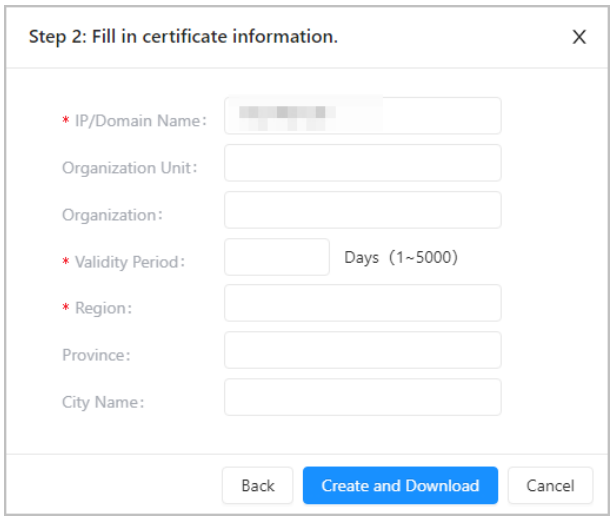
IP/Domain Name would be automatically set with the IP or domain name of the device.

Figure 8-6 Fill in certificate information (1)



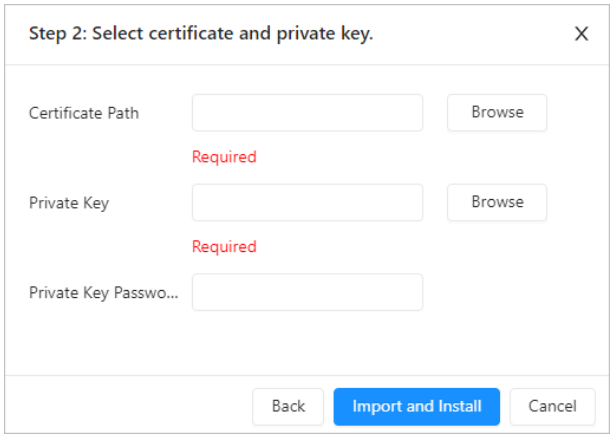
- Apply for CA certificate and import: Enter related information, and then click **Create and Download**.

Figure 8-7 Fill in certificate information (2)



- Install existing certificate: Import the certificate and private key files, enter the private key password, and then click **Import and Install**.

Figure 8-8 Select certificate and private key



Step 3 You can define names of current device certificates, download the certificate files or delete the certificates from the device.

- Define names of device certificates by clicking **Enter Edit Mode** on the upper right corner of the list, entering the desired name in the text box of each device certificate and click **Save Config**.
- Download the certificate files by clicking in each device certificate column.
- You can delete the certificates from the device by clicking in each device certificate column.

8.5.2 Trusted CA Certificates

Procedure

Step 1 On the main interface, select **Security** > **CA Certificate**.

Step 2 Click **Install Trusted Certificate** , import local certificate files and click **OK**.

Figure 8-9 Trusted CA certificate

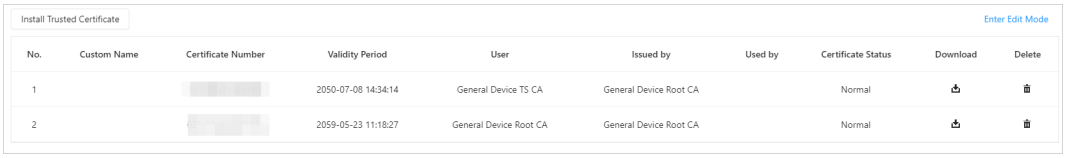


Figure 8-10 Install trusted certificate

Step 3 (Optional) You can define names of current device certificates, download the certificate files or delete the certificates from the device.

- Define names of device certificates by clicking **Enter Edit Mode** on the upper right corner of the list, entering the desired name in the text box of each device certificate and click **Save Config**.
- Download the certificate files by clicking  in each device certificate column.
- Delete the certificates from the device by clicking  in each device certificate column.

8.6 Attack Defense

8.6.1 Firewall

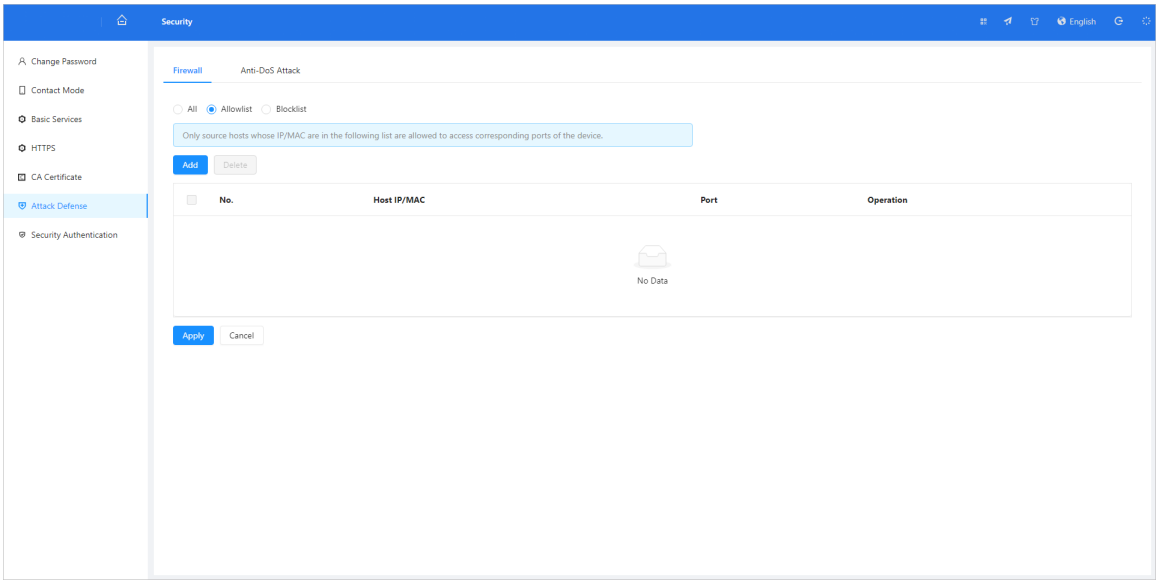
Set firewall, including adding allowlist and blocklist.

Procedure

Step 1 On the main interface, select **Security** > **Attack Defense** > **Firewall**.

Step 2 Select **All** , **Allowlist** or **Blocklist** as needed.

Figure 8-11 Firewall configuration



- If you select **All** , click **Apply**.
- If you select **Allowlist** or **Blocklist**, click **Add Mode** to configure related parameters in the **Add** interface and then click **Apply**.

Figure 8-12 Add IP mode

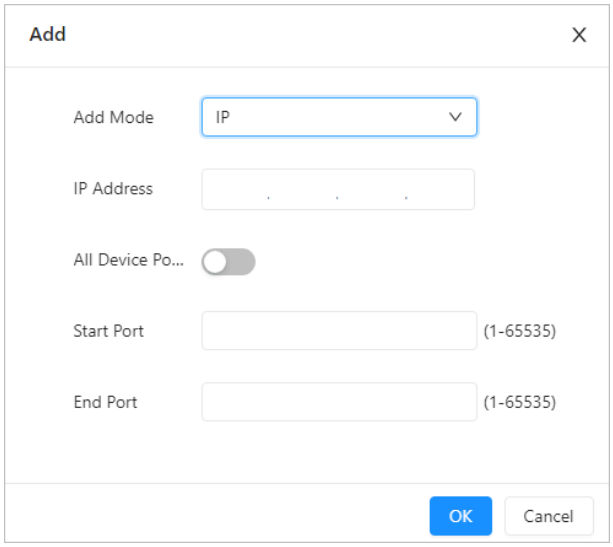


Table 8-1 Description of adding mode

Parameter	Description
IP Address	Enter the IP address of a device to be added.
Start Address	
End Address	
All Device Ports	Enabled by default. You can set the port range after it is disabled.
Start Port	Enter the start port number.
End Port	Enter the end port number.
MAC Address	Enter the MAC address of the device to be added.

8.6.2 Anti-DoS Attack

Set anti-DoS (Denial of Service) attack, including SYN flood attack defense, and ICMP flood attack defense.

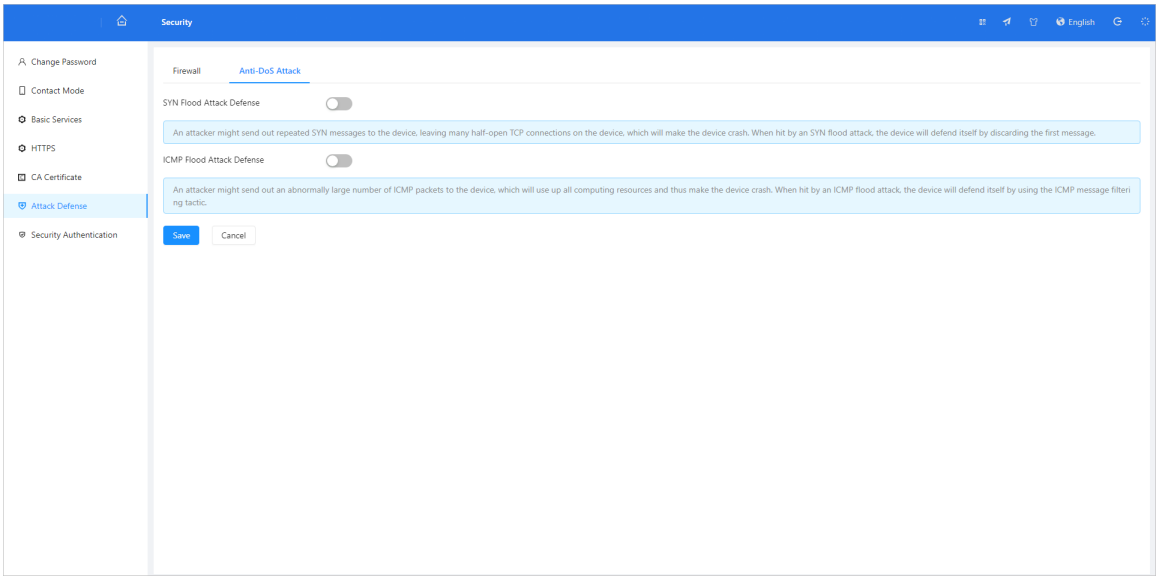
Procedure

Step 1 On the main interface, select **Security** > **Attack Defense** > **Anti-DoS Attack**.

Step 2 Enable or disable **SYN flood attack defense** and **ICMP flood attack defense** as needed.

- SYN flood attack defense: By sending SYN (Synchronize Sequence Numbers) message, the attacker causes a large number of TCP (transmission control protocol) semi-connections and resource exhaustion. The device uses the first-packet discard strategy to defend.
- ICMP flood attack defense: The attacker takes advantage of the asymmetry of computing resources of both sides, and sends a large number of ICMP (Internet Control Message Protocol) message to cause the device computing resources to run out. The device uses ICMP packet filtering strategy to defend.

Figure 8-13 Anti-DoS attack



Step 3 Click **Save**.

8.7 Security Authentication

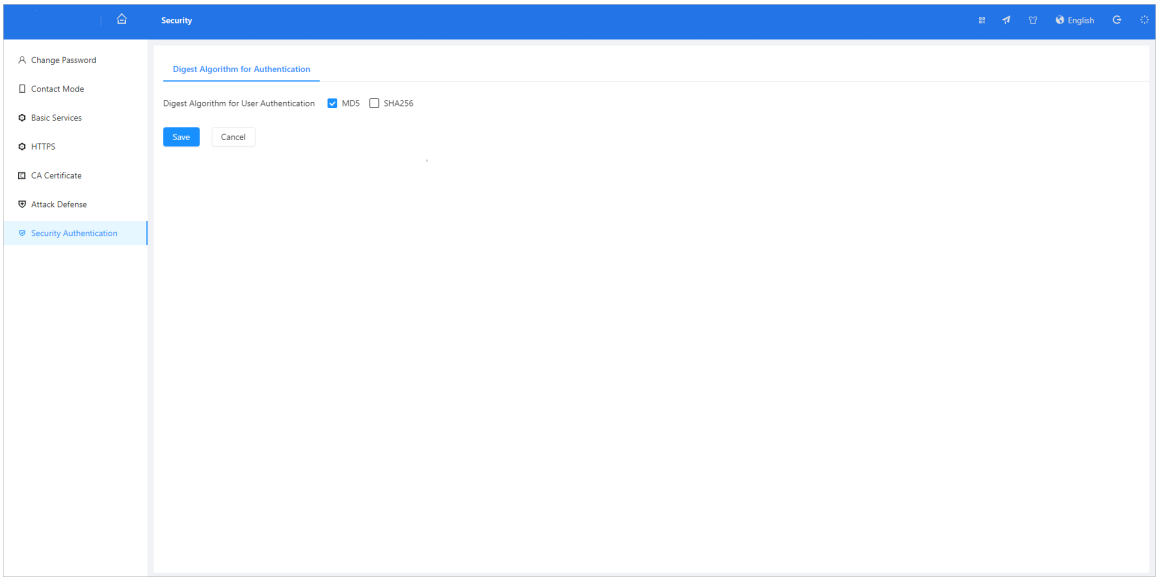
Set digest algorithm for user authentication.

Procedure

Step 1 On the main interface, select **Security** > **Security Authentication**.

Step 2 MD5 is enabled by default. You can choose to tick **SHA256** as needed.

Figure 8-14 Digest algorithm for user authentication



Step 3 Click **Save**.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access Web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

   We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188