



# Wireless Router

## User's Manual






# Foreword

## General

This manual introduces the functions and operations of the Wireless Router (hereinafter referred to as "the Device"). Read carefully before using the Device, and keep the manual safe for future reference.

## Safety Instructions

The following signal words 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, reductions in performance, or unpredictable result.
 NOTE	Provides additional information as a supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December 2024

## Privacy Protection Notice

As the Device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

## About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the Device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Table of Contents

Foreword .....	I
1 Overview .....	1
1.1 Introduction .....	1
1.2 Network Connection .....	1
2 Login to the WEB .....	2
2.1 Initializing and Login to the Device .....	2
2.2 Home Screen .....	5
3 Device Status .....	6
3.1 Network Status .....	6
3.2 Device Info .....	7
3.3 End Device Info .....	8
4 WLAN Config .....	10
4.1 General Settings .....	10
4.1.1 Host Wi-Fi .....	10
4.1.2 Guest Wi-Fi .....	11
4.2 Global Config .....	12
4.3 MAC Filter .....	13
4.3 Wi-Fi Relay .....	14
5 End Device Management .....	16
6 Advanced Config .....	17
6.1 Network Settings .....	17
6.1.1 LAN Config .....	17
6.1.2 Static Routing .....	19
6.1.3 IPv6 .....	20
6.2 Security .....	21
6.2.1 MAC Filter .....	21
6.2.2 DMZ .....	21
6.2.3 Port Mapping .....	21
6.2.4 Legal Info .....	23
6.2.5 HTTPS .....	23
6.3 System Settings .....	24
6.3.1 Device Info .....	24
6.3.2 Modify Password .....	25
6.3.3 System Time .....	26
6.4 Maintenance .....	27

---

6.4.1 Log.....	27
6.4.2 LED Indicator.....	29
6.4.3 Diagnosis & Restart.....	29
6.4.4 Backup & Restore.....	31
6.4.5 Updating .....	32
6.5 Parental Control.....	33
Appendix 1 Security Commitment and Recommendation .....	1

# 1 Overview

## 1.1 Introduction

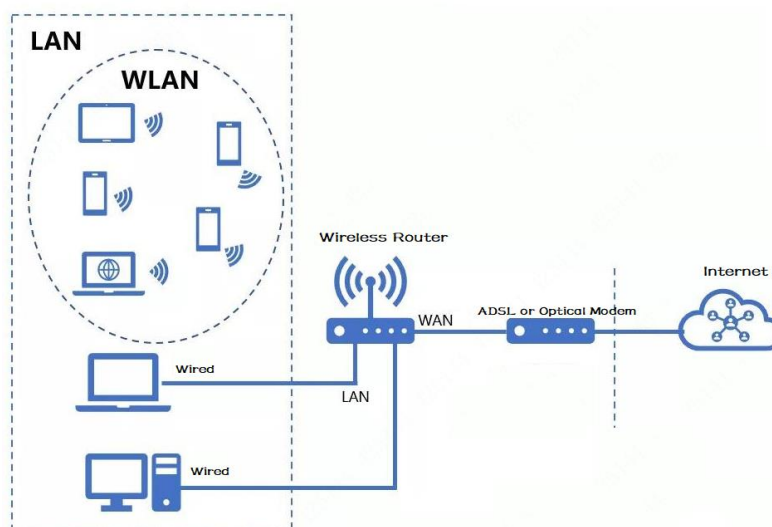
Wireless Router is a router with wireless coverage function. It can forward broadband network signals to nearby wireless network device, such as notebook computers and mobile phones supporting Wi-Fi, through the antenna, so as to meet the needs of users to access the Internet anytime and anywhere. The wireless router not only has all the functions of the traditional router, such as network address translation (NAT), dynamic host configuration protocol (DHCP), and the wireless function is also added. So that the mobile device can also be connected to the wireless network.

According to different wireless protocols and wireless rates, Wireless Router can be divided into various specifications, but the function configuration mode is basically the same.

## 1.2 Network Connection

The Wireless Router is connected to the Internet network through ADSL or Optical Modem. It can not only provide wireless services for the user, but also provide wired services.

Figure 1-1 Wireless Network



## 2 Login to the WEB

### 2.1 Initializing and Login to the Device

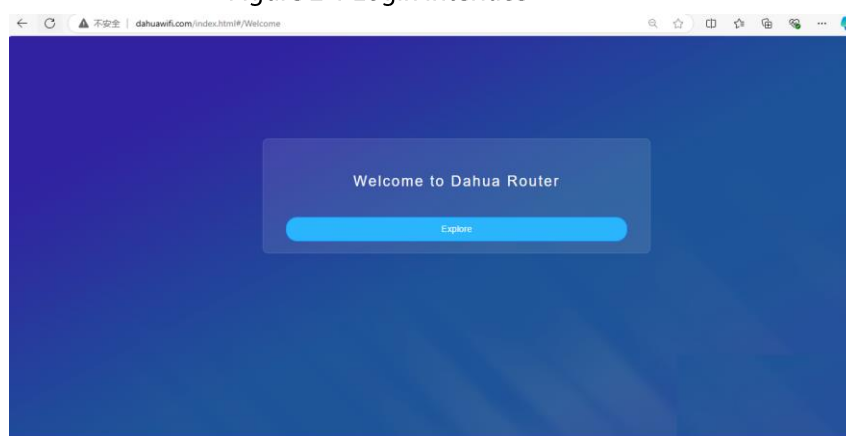
#### Prerequisites

Ensure the PC IP and device IP in the same network.

#### Procedure

- Step 1** The end device connects to the router through wired and wireless connection. Enter the device domain name (**dahuawifi.com**) or device IP (**default IP 192.168.10.110**) to log in to the device to configure settings.
- Step 2** Click **Explore**.

Figure 2-1 Login interface



- Step 3** Select the **I have read and agree to the terms of the Software License Agreement** and **Privacy Policy** checkbox, and then Click **OK**.
- Step 4** For the first-time login, you need to set the **Time Zone Settings** and **login password**, and then click **Next**.

Figure 2-2 Time Zone settings

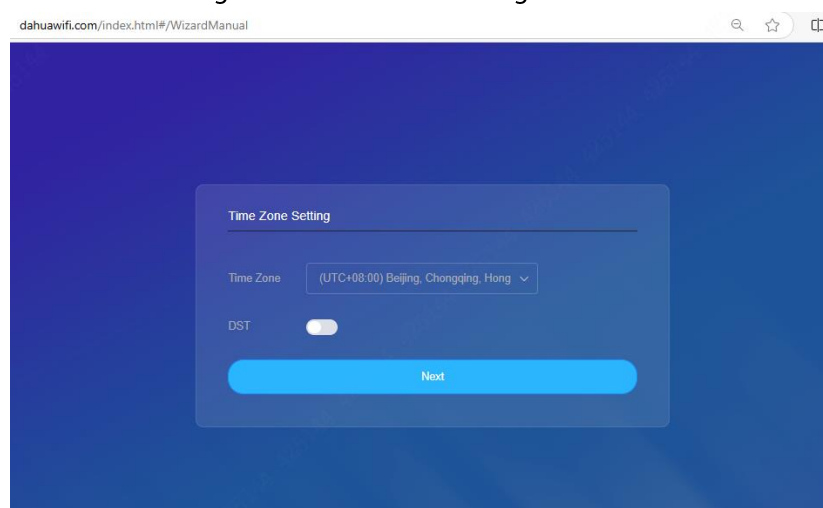
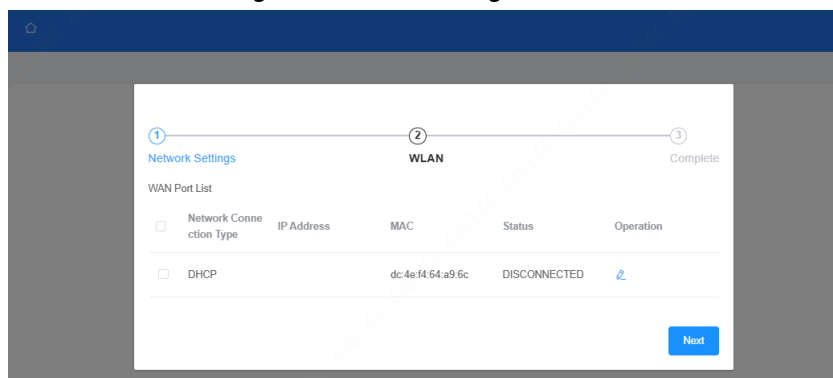


Figure 2-3 Login password settings

Step 5 Enter the login password, and then enter the web page.

Step 6 For the first-time login, the device will pop up a setup wizard. You can change the **networking method** (default DHCP), click the **Operation** icon to change, and then click **Next**.

Figure 2-4 WAN settings

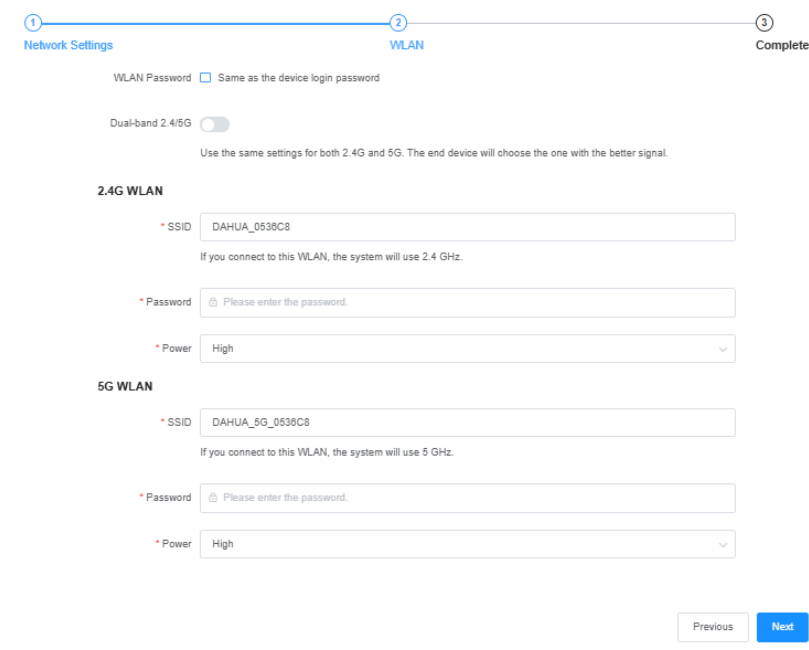


Network Connection Type	IP Address	MAC	Status	Operation
DHCP		dc:4e:f4:64:a9:6c	DISCONNECTED	<a href="#">⚙️</a>

Step 7 Set up **Dual-band 2.4G/5G, SSID Password** and **Power** for 2.4G and 5G, and then click **Next**.



Figure 2-5 WLAN settings



1 Network Settings 2 WLAN 3 Complete

WLAN Password ☐ Same as the device login password

Dual-band 2.4/5G ☐

Use the same settings for both 2.4G and 5G. The end device will choose the one with the better signal.

**2.4G WLAN**

\* SSID DAHUA\_0536C8  
If you connect to this WLAN, the system will use 2.4 GHz.

\* Password  Please enter the password.

\* Power High

**5G WLAN**

\* SSID DAHUA\_5G\_0536C8  
If you connect to this WLAN, the system will use 5 GHz.

\* Password  Please enter the password.

\* Power High

Previous Next



Setting a wireless password will enhance the security of the wireless network.

**Step 8** Click **Complete** to finish configuration wizard.

Figure 2-6 Complete configuration wizard



1 Network Settings 2 WLAN 3 Complete

Configuration is complete. Please manually reconnect to WLAN.

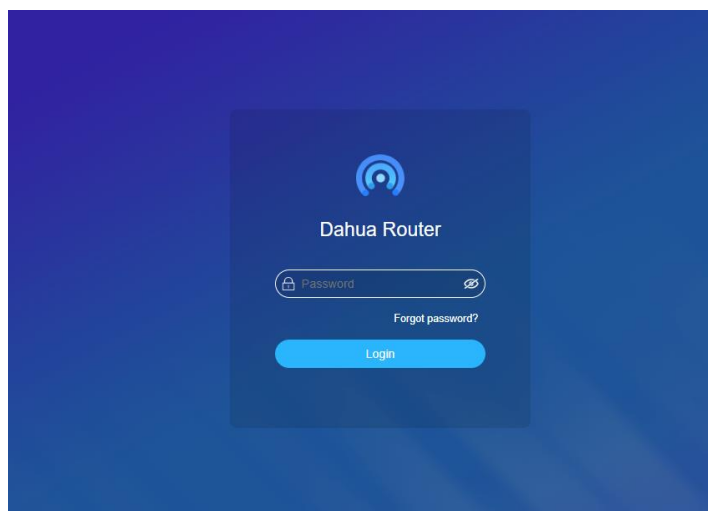
New SSID

- DAHUA\_0536C8
- DAHUA\_5G\_0536C8

Previous Complete

**Step 9** After the configuration wizard is completed, use the new password to log in again.

Figure 2-7 Login interface



## 2.2 Home Screen

After Logging in, you will be directed to the home page.

Figure 2-8 Home Screen

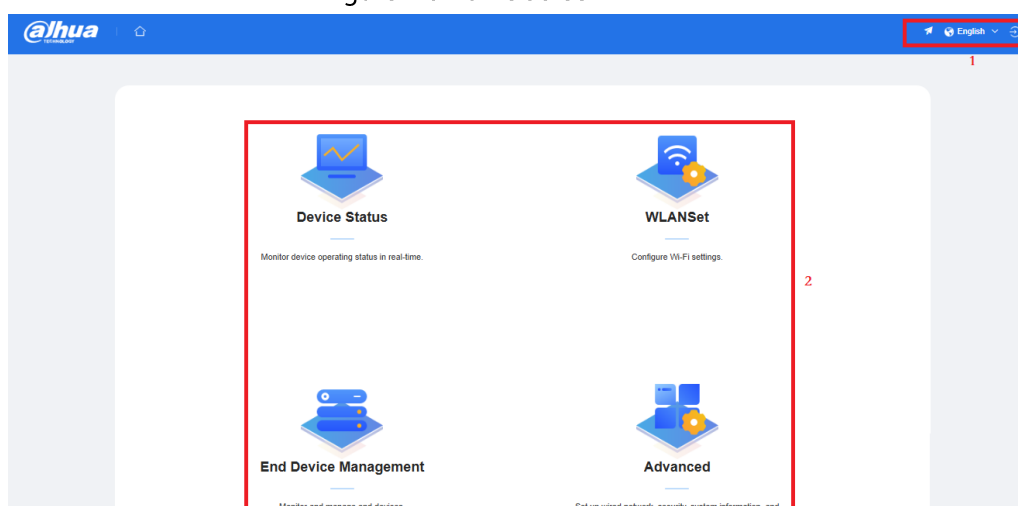


Table 2-1 Descriptions of the home screen

No.	Module	Description
1	Configuration Wizard	Complete the preliminary settings
	Language settings	Change the language displayed on interface
	Log Out	Return to the login screen
	Restart	Reboot the device
2	Device Status	Monitor device operating status in real-time
	WLANSet	Configure Wi-Fi settings
	End Device Management	Monitor and manage end devices
	Advanced	Set up wired network, security, system information and device maintenance

## 3 Device Status

Monitor device operating status in real-time. It includes network status, device information and end device information.

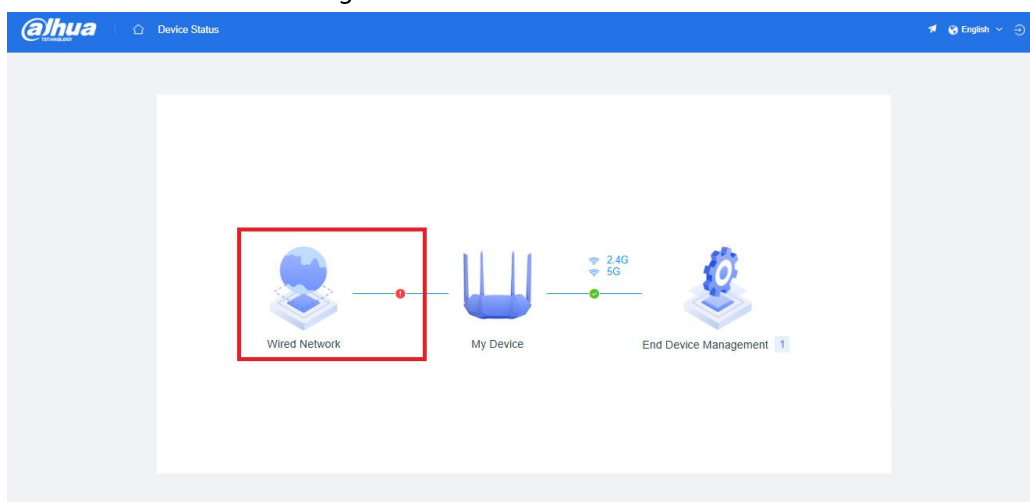
### 3.1 Network Status

Displays the connectivity of the device network. If an exclamation mark is displayed, it indicates in that part the network is not working; If a check mark is displayed, it indicates in that part the network is functioning properly.

#### Procedure

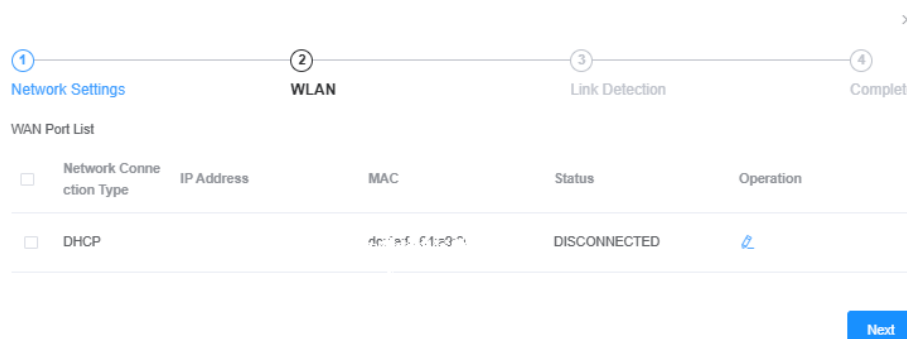
**Step 1** Click **Device Status** to enter the device networking diagram.

Figure 3-1 Network Status



**Step 2** Click **Wired Network** icon to enter the configuration wizard, set the Internet access mode for the WAN port, Wi-Fi configuration, Link Detection, and Click **Complete** to finish configuration wizard.

Figure 3-2 Configuration Wizard



Network Connection Type	IP Address	MAC	Status	Operation
<input type="checkbox"/> DHCP		68:0a:35:01:23:00	DISCONNECTED	<a href="#">?</a>

Next

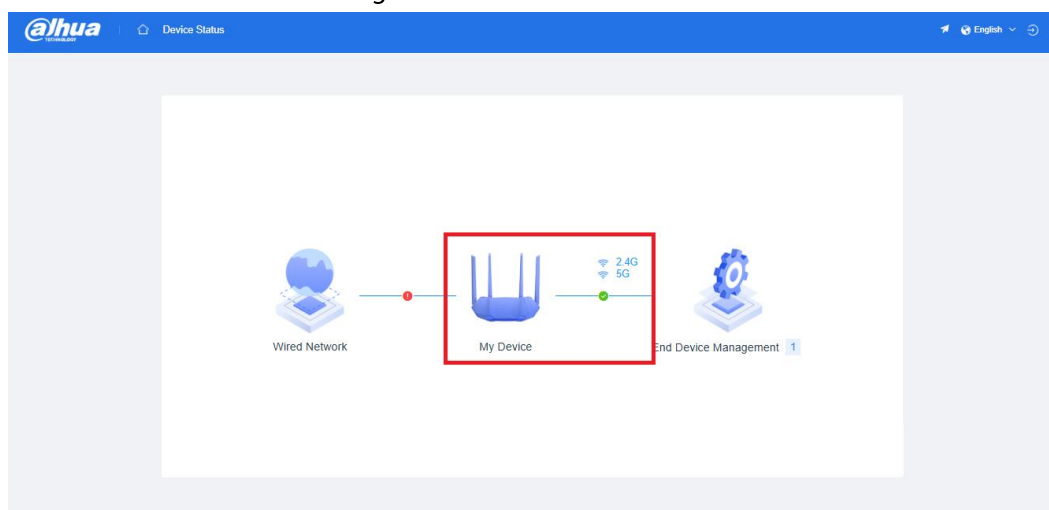
## 3.2 Device Info

Displays device information, including network status and Wi-Fi status. If both 2.4G and 5G Wi-Fi are turned off, Wi-Fi information will not be displayed; If one of the Wi-Fi is turned off, only the Wi-Fi that is turned on will be displayed.

### Procedure

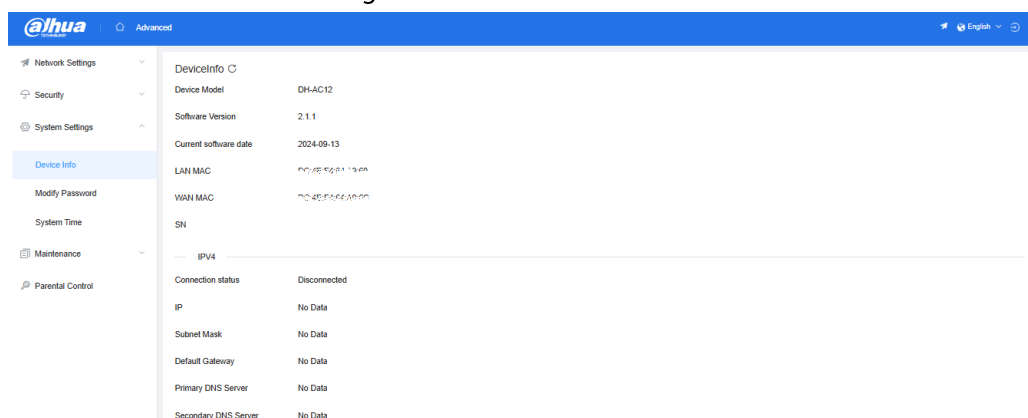
**Step 1** Click **My Device** to enter the detailed information about the device.

Figure 3-3 Device Info



This page displays detailed device information, including device model, software version, LAN MAC, WAN MAC, SN, IPv4 information, and IPv6 information.

Figure 3-4 Device Info



**Step 2** Click **2.4G and 5G Wi-Fi** icon to enter the Host Wi-Fi settings. After setting up the Wi-Fi configuration for 2.4G and 5G, and then click **Save**.

Figure 3-5 Host Wi-Fi



If 5G is not supported, 5G does not need to be configured.

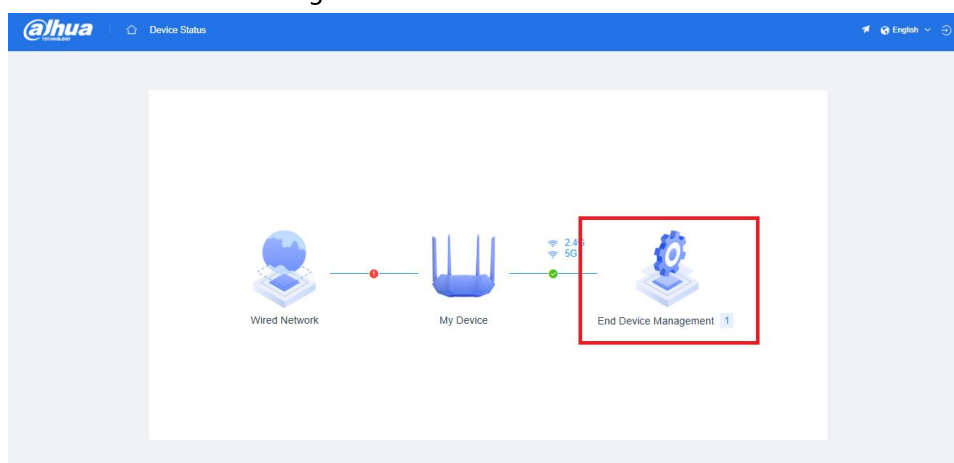
## 3.3 End Device Info

Displays the connection status of wired and wireless terminals.

### Procedure

**Step 1** Click **End Device Management** icon to enter the End Device Management page.

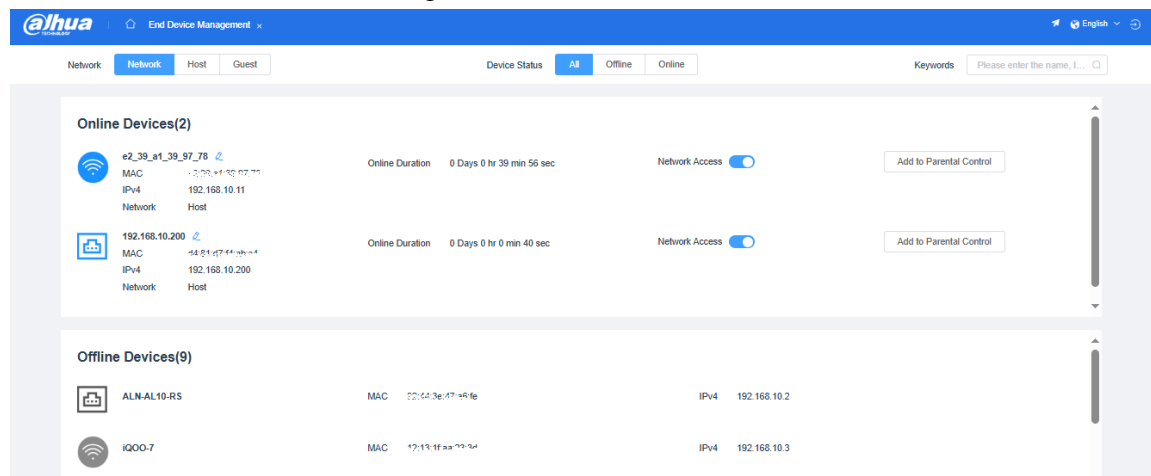
Figure 3-6 Terminals Info



You can view information for all terminals, including online and offline terminals, and set whether

the terminal can access the network.

Figure 3-7 Terminal List



## 4 WLAN Config

Set Wi-Fi configurations, mainly including Host Wi-Fi, Guest Wi-Fi, Wi-Fi Schedule, Wi-Fi Global Configuration, Wireless MAC Filtering, and Wireless Repeater.

### 4.1 General Settings

Configure Host Wi-Fi and Guest Wi-Fi.

#### 4.1.1 Host Wi-Fi

##### Wi-Fi Config Procedure

- Step 1** Select **WLANSet > General Settings > Host Wi-Fi > Setting**.
- Step 2** Fill in the Host Wi-Fi information of 2.4G and 5G, and then click **Save**.

Figure 4-1 Host Wi-Fi Config

The screenshot shows the 'Host Wi-Fi' configuration page in the Dahua WLANSet interface. The page is divided into two main sections: '2.4G WLAN' and '5G WLAN'. Both sections have a 'Dual-band 2.4/5G' toggle at the top, which is currently turned off. Below this, there are fields for 'Name', 'Security Mode', 'Encryption Type', and 'Password'. The '2.4G WLAN' section has a '2.4G WLAN' toggle that is turned on. The '5G WLAN' section has a '5G WLAN' toggle that is also turned on. Both sections have a 'Name' field with the value 'DAHUA\_0536C8', a 'Security Mode' dropdown set to 'WPA2-PSK', and an 'Encryption Type' dropdown set to 'AES'. The 'Password' field is masked with asterisks. There are 'Save' and 'Cancel' buttons at the bottom of the page.



If 5G is not supported, 5G does not need to be configured.

Table 4-1 Description of parameters

Parameter	Description
Dual-band 2.4/5G	Use the same settings for both 2.4G and 5G.
2.4G WLAN	
2.4G WLAN	Enable or disable Wi-Fi on 2.4GHz.
Name	2.4G Wi-Fi name.
Security Mode	2.4G Wi-Fi encryption method, mainly including OPEN、WPA-PSK、WPA2-PSK 、WPA3-SAE、WPAORWPA2-PSK、WPA2-PSKORWPA3-SAE.

Parameter	Description
Encryption Type	2.4G Wi Fi encryption protocol, only supports AES protocol.
Password	2.4G Wi-Fi password.
5G WLAN	
5G WLAN	Enable or disable Wi-Fi on 5GHz.
Name	5G Wi-Fi name.
Security Mode	5G Wi-Fi encryption method, mainly including OPEN、 WPA-PSK、 WPA2-PSK 、 WPA3-SAE、 WPAORWPA2-PSK、 WPA2-PSKORWPA3-SAE.
Encryption Type	5G Wi Fi encryption protocol, only supports AES protocol.
Password	5G Wi-Fi password.

## Wi-Fi Schedule Plan Procedure

**Step 1** Select **WLANSet > General Settings > Host Wi-Fi > Schedule Plan**.

**Step 2** Fill in the time information, and then click **Save**.

Figure 4-2 Host Wi-Fi Schedule config

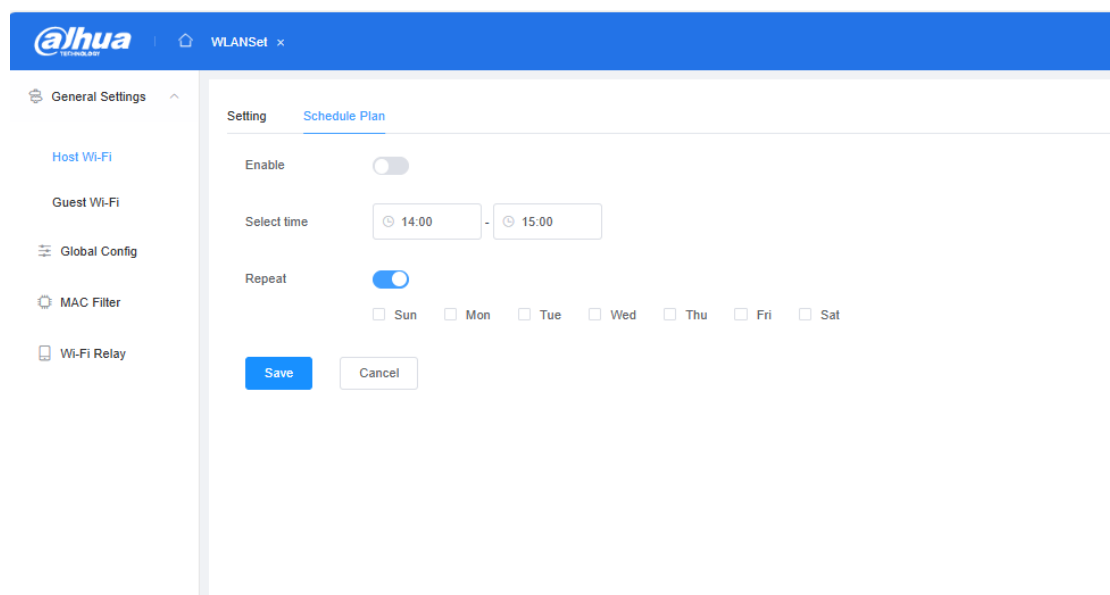


Table 4-2 Description of parameters

Parameter	Description
Enable	Enable Wi-Fi timer.
Select time	Wi-Fi timer on and off time.
Repeat	The dates of Wi-Fi periodically turned on and off.

### 4.1.2 Guest Wi-Fi

The configuration of this part is the same as that of the Host Wi-Fi. Please refer to 4.1.1 Host Wi-Fi.



## 4.2 Global Config

Configure the Global configurations of 2.4G and 5G.



If 5G is not supported, 5G does not need to be configured.

### Procedure

**Step 1** Select **WLANSet** > **Global Config**.

**Step 2** Set the RF configuration for 2.4G and 5G, and then click **Save**.

Figure 4-3 Global config

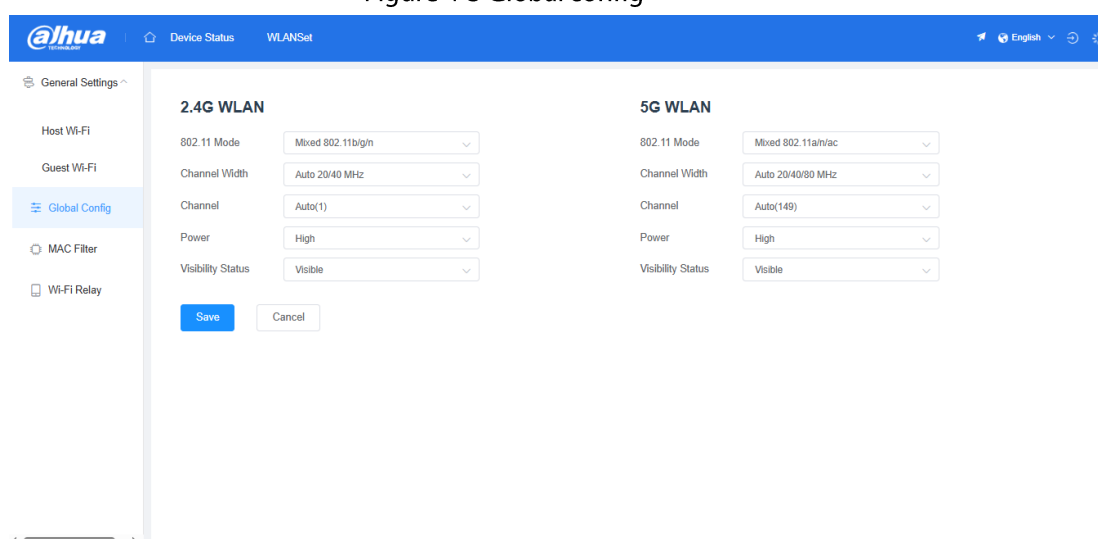


Table 4-3 Description of parameters

Parameter	Description
802.11 Mode	<p>Wireless mode settings:</p> <ul style="list-style-type: none"> <li>2.4G wireless mode mainly includes 802.11b only, 802.11g only, 802.11n only, Mixed 802.11b/g, Mixed 802.11b/g/n, Mixed 802.11b/g/n/ax.</li> <li>5G wireless mode mainly include 802.11a/n, Mixed 802.11a/n/ac, Mixed 802.11a/n/ac/ax.</li> </ul>
Channel Width	<p>Channel bandwidth settings:</p> <ul style="list-style-type: none"> <li>2.4G mainly includes 20MHz, 40MHz, and Auto 20/40MHz.</li> <li>5G mainly includes 20MHz, 40MHz, 80MHz, Auto 20/40/80MHz, and Auto 20/40/80/160MHz.</li> </ul>
Channel	<p>The working channel settings for 2.4G and 5G:</p> <ul style="list-style-type: none"> <li>2.4G channels mainly include AUTO, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11.</li> <li>5G channels mainly include AUTO, 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, and 165.</li> </ul>
Power	<p>The transmission power settings for 2.4G and 5G can be set to High, Middle, and Low.</p>

Parameter	Description
Visibility Status	Set whether the host network signals for 2.4G and 5G are visible: <ul style="list-style-type: none"> <li>● If set to Visible, the wireless terminal can search to found the wireless signal.</li> <li>● If set to Invisible, the wireless terminal cannot search to found the wireless signal.</li> </ul>

## 4.3 MAC Filter

Mainly used to control whether wireless terminals can connect to Wi-Fi. Wireless terminals added to the WLAN MAC List are unable to connect to 2.4G and 5G Wi-Fi.

### Procedure

Step 1 Select **WLANSet** > **MAC Filter**.

Figure 4-4 WLAN MAC List

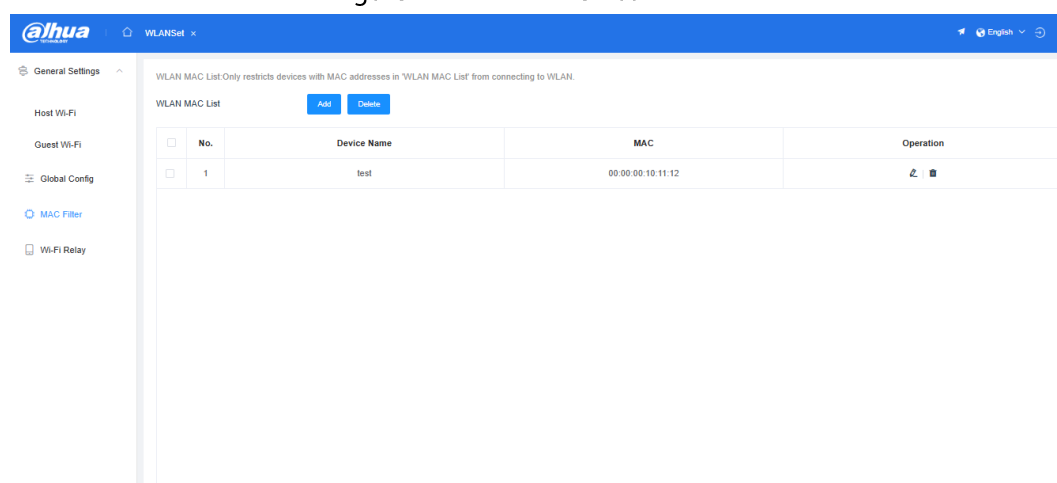


Table 4-4 Description of parameters

Parameter	Description
Device Name	Terminal name.
MAC	MAC address of the terminal.
Operation	Edit or delete terminals in the list.

Step 2 Click the **Add** to add terminal information.

Figure 4-5 MAC Config

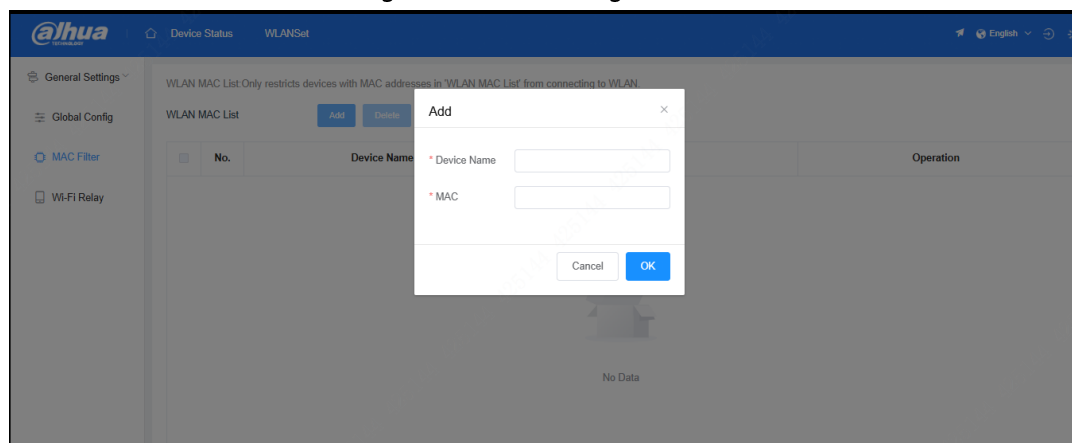


Table 4-5 Description of parameters

Parameter	Description
Device Name	The name of terminal.
MAC	The MAC address of terminal.

## 4.3 Wi-Fi Relay

The wireless relay function is used to expand the coverage of wireless networks and is turned off by default. After successful relay, the device will operate in AP mode. If you choose wireless signal encryption for relay, you need to enter a password before you can proceed with the relay.

### Procedure

- Step 1** Select **WLANSet > Wi-Fi Relay**.
- Step 2** Enable the **Wi-Fi Relay** to select the Wireless information that requires relay.

Figure 4-6 Wi-Fi Repeater Config



Table 4-6 Description of parameters

Parameter	Description
Wi-Fi Relay	Enable Wi-Fi relay function.
Network List	Scanned wireless network list.

Parameter	Description
Wi-Fi Password	Password of relay Wi-Fi.

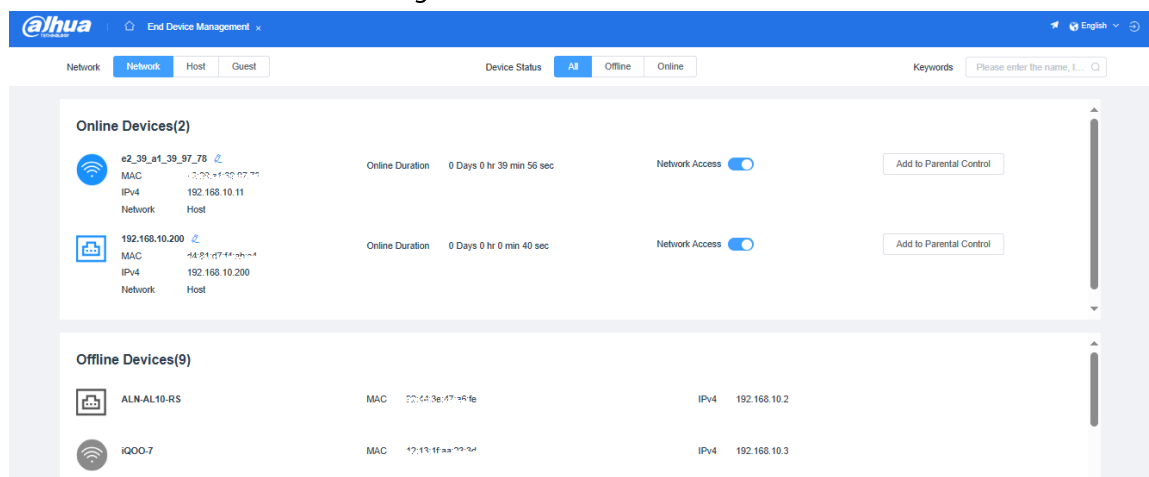
## 5 End Device Management

Displays all online and offline terminals for easy viewing and management.

### Procedure

**Step 1** Select **End Device Management**.

Figure 5-1 Terminal List



Displays detailed information about online and offline terminals, including name, MAC, IP, network affiliation, and online duration; Click  to edit the name of the terminal.

Additionally, by clicking on the Network Access and Add to Parental Control icon, you can configure whether online terminals can access the network and join parental control.

## 6 Advanced Config

You can set up wired network, security, system information, device maintenance and parental control.

### 6.1 Network Settings

Configure LAN, Static Routing, and IPv6.

#### 6.1.1 LAN Config

Configure the IP address, mask, DHCP service, and IP/MAC binding of the local area network.

##### LAN Configuration Procedure

**Step 1** Select **Advanced** > **Network Settings** > **LAN**.

**Step 2** Fill in LAN information, and then click **Save**.

Figure 6-1 LAN Config

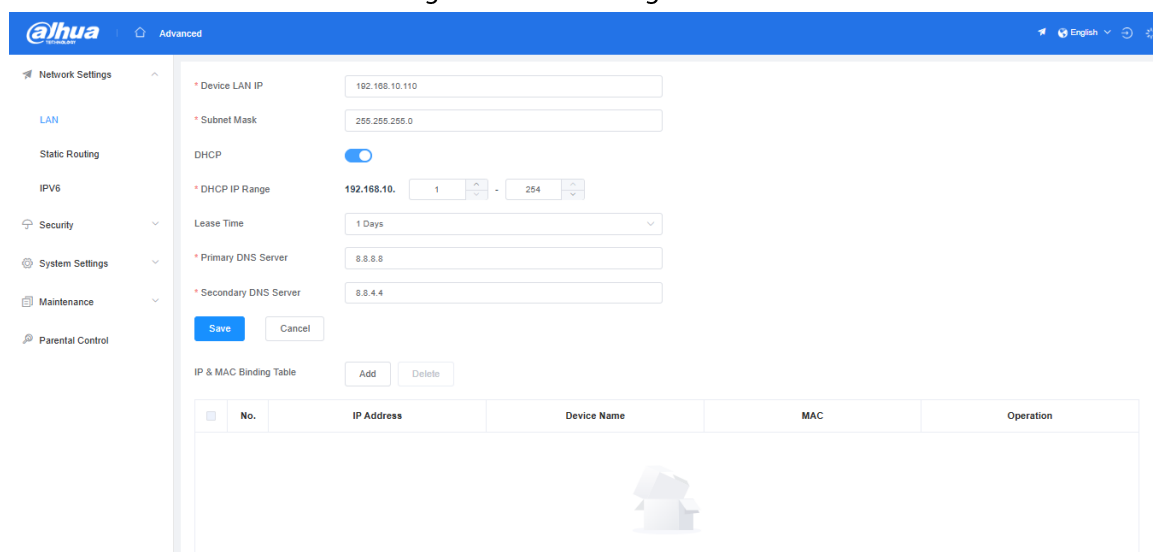


Table 6-1 Description of parameters

Parameter	Description
Device LAN IP	LAN management address.
Subnet Mask	LAN management address mask.
DHCP	Enable DHCP service.
DHCP IP Range	The address pool range of DHCP service.
Lease Time	DHCP address lease duration.
Primary DNS Server	Preferred DNS Server address.
Secondary DNS Server	Secondary DNS Server address.

## IP&MAC Binding Procedure

**Step 1** Select **Advanced** > **Network Settings** > **LAN**.

Figure 6-2 IP/MAC Binding Table

No.	IP Address	Device Name	MAC	Operation
1	192.168.10.2	pad	00:00:00:00:00:01	

Table 6-2 Description of parameters

Parameter	Description
IP Address	The IP address of terminal.
Device Name	The name of terminal.
MAC	The MAC address of terminal.
Operation	The operations of IP/MAC binding, including editing and deleting.

**Step 2** Fill in **IP address**, **Device name**, and **MAC**, and then click **OK**.

Figure 6-3 IP/MAC Binding Config

IP Address

Device Name

MAC

Cancel

OK

Table 6-3 Description of parameters

Parameter	Description
IP Address	The IP address of terminal.
Device Name	The name of terminal.
MAC	The MAC address of terminal.

## 6.1.2 Static Routing

Manually configure the static routing table to determine the packet forwarding path based on the pre-specified destination network and the address of the next hop router.

### Procedure

**Step 1** Select **Advanced** > **Network Settings** > **Static Routing**.

Figure 6-4 Static Routing Table

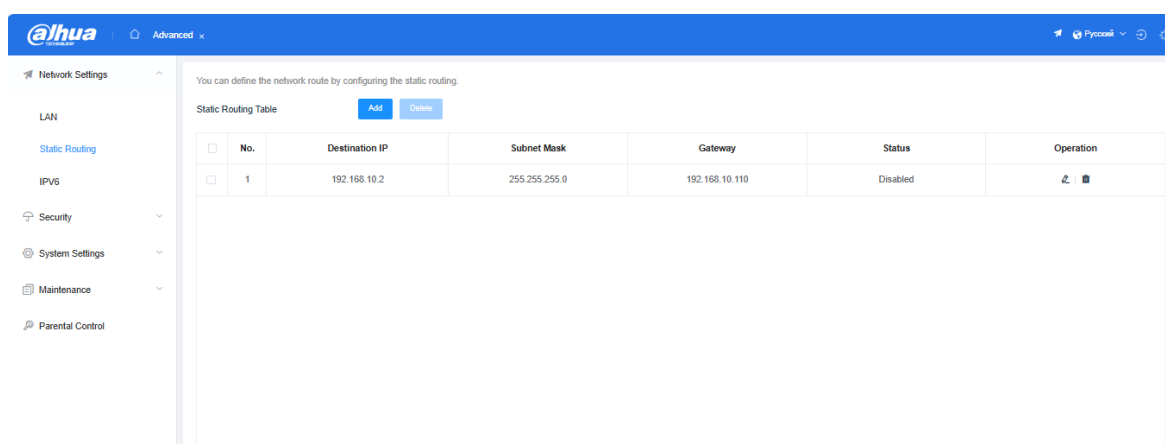


Table 6-4 Description of parameters

Parameter	Description
Destination IP	Destination IP address.
Subnet Mask	Mask of destination IP address.
Gateway	Next hop gateway address.
Status	The status of static routing table entries, enabled or disabled.
Operation	Edit or delete terminals in the list.

**Step 2** Fill in routing information, and then click **OK**.

Figure 6-5 Static Routing Config

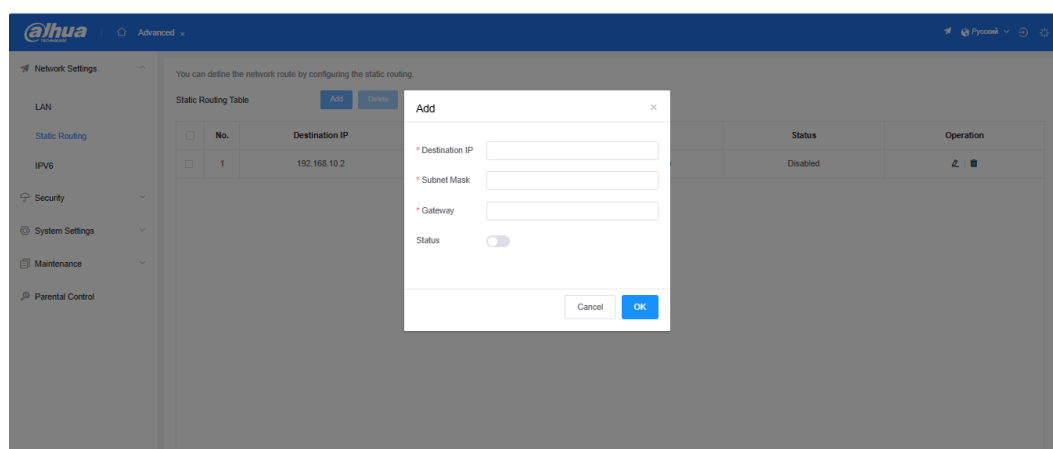


Table 6-5 Description of parameters

Parameter	Description
Destination IP	Destination IP address.



Parameter	Description
Subnet Mask	Mask of destination IP address.
Gateway	Next hop gateway address.
Status	The status of static routing table entries, enabled or disabled.

### 6.1.3 IPv6

Enable IPv6 function, both WAN and LAN terminals can obtain IPv6 addresses and use them to access the internet.

#### Procedure

**Step 1** Select **Advanced** > **Network Settings** > **IPv6**.

**Step 2** Fill in IPv6 information, and then click **Save**.

Figure 6-6 IPv6 Config

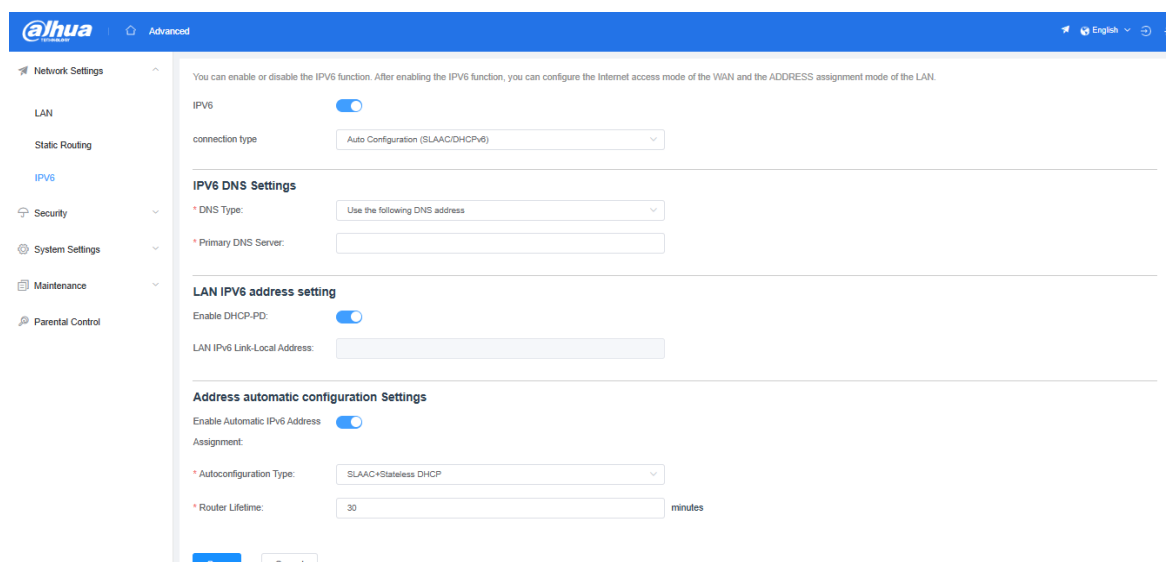


Table 6-6 Description of parameters

Parameter	Description
Connection type	The type for WAN to obtain IPv6 addresses including Static IPv6, Auto Configuration (SLAAC/DHCPv6), and PPPoE.
DNS Type	DNS settings include Obtain a DNS server address automatically, and use the following DNS address.
Primary DNS Server	Preferred DNS Server.
LAN IPv6 Link-Local Address	Local IPv6 link address of LAN port.
Auto configuration Type	The type for LAN terminals to obtain IPv6 addresses include SLAAC+RDNSS, SLAAC+stateless DHCP, and Stateful DHCPv6.
Router Lifetime	The effective time of IPv6 routing.

## 6.2 Security

Supports the settings of MAC Filter, DMZ, Port Mapping, Legal Info, and HTTPS.

### 6.2.1 MAC Filter

This feature is the same as "4.3 MAC Filter" in Chapter 4.

### 6.2.2 DMZ

DMZ can redirect the access of **all service port** on the WAN port to the corresponding port of a designated server within the local area network.

#### Procedure

- Step 1** Select **Advanced > Security > DMZ**.
- Step 2** Enable DMZ, select Device, fill in DMZ Host IP, and then click **Save**.

Figure 6-7 DMZ Config

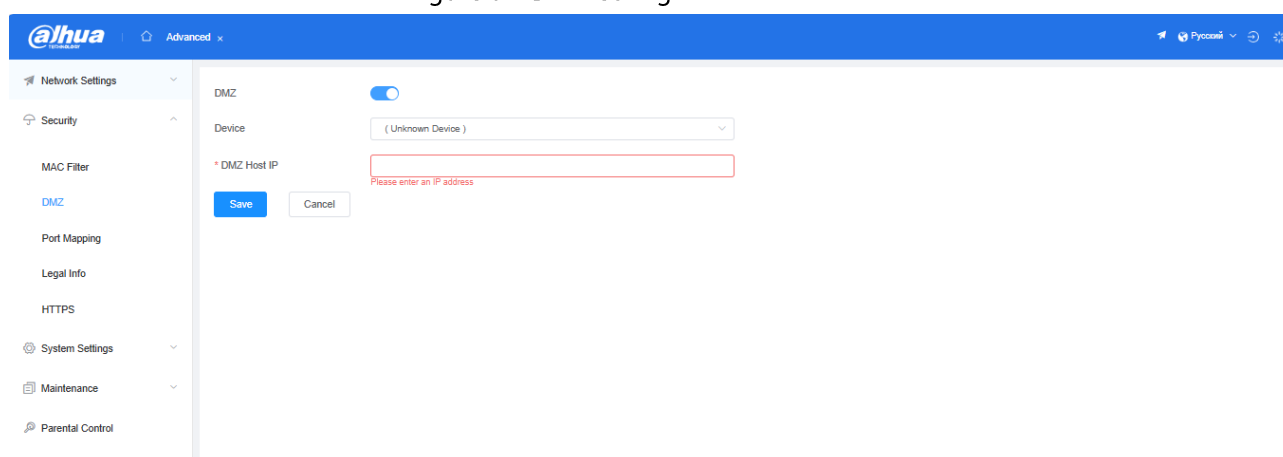


Table 6-7 Description of parameters

Parameter	Description
DMZ	Enable DMZ function.
Device	Internal servers can choose connected network devices or unknown devices; Select the connected device, and the DMZ Host IP will be automatically brought out. If you select an unknown device, you need to manually enter the DMZ Host IP.
DMZ Host IP	Internal server IP address, can be manually set or selected from terminals that have already been connected to the network.

### 6.2.3 Port Mapping

Port mapping can establish a mapping relationship between WAN port IP address, external port number, and LAN server IP address and internal port number, redirecting all access to a service port

of the WAN port to the corresponding port of the designated LAN server.

## Procedure

**Step 1** Select **Advanced** > **Security** > **Port Mapping**.

Figure 6-8 Port Mapping List

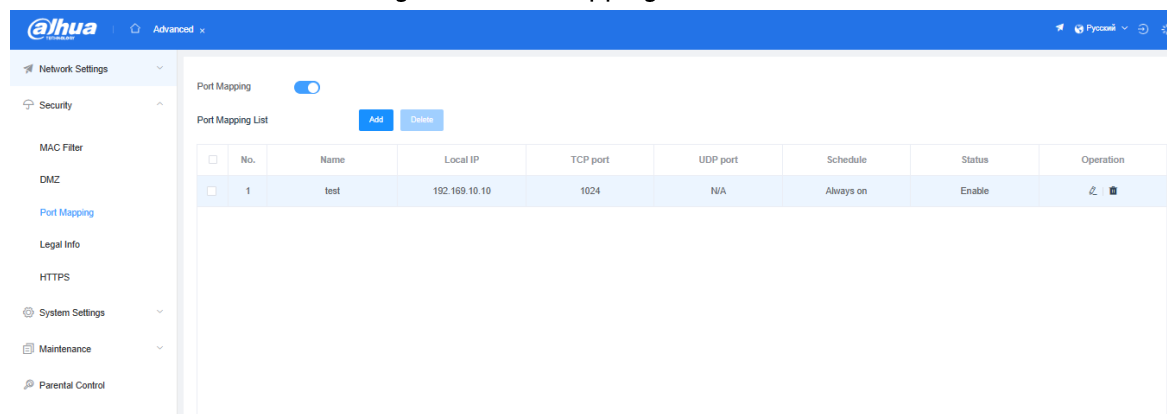


Table 6-8 Description of parameters

Parameter	Description
Name	The name of Port mapping rule..
Local IP	Internal server IP address
TCP port	TCP port number.
UDP port	UDP port number.
Schedule	The effective time of the rule is assumed to be continuous and cannot be configured.
Status	Rule enabled state.
Operation	Edit or delete rules in the list.

**Step 2** Click **Add**, fill in the information, and then click **OK**.

Figure 6-9 Port Mapping Config

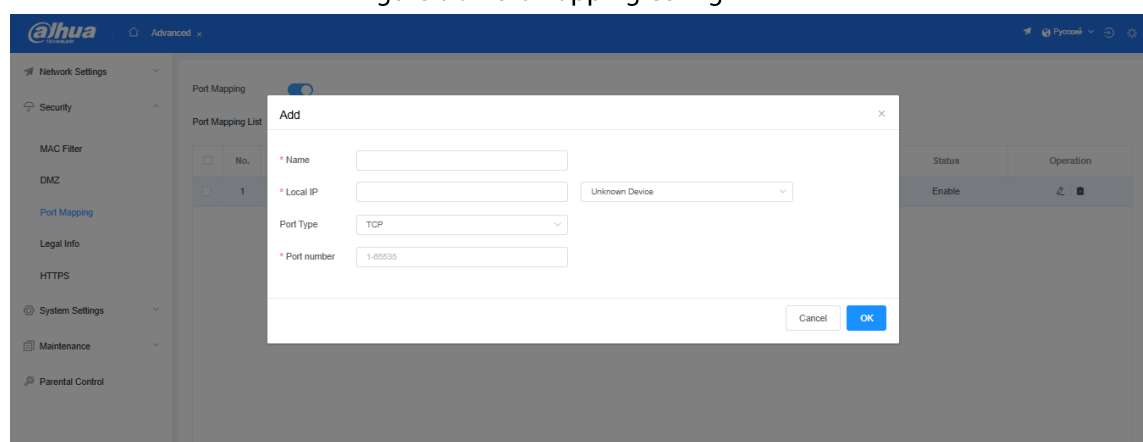


Table 6-9 Description of parameters

Parameter	Description
Name	The name of Port mapping rule.

Parameter	Description
Local IP	Internal server IP address, can be manually set or selected from terminals that have already been connected to the network.
Port Type	Port types, including TCP, UDP, or TCP&UDP.
Port number	The external and internal ports of the port mapping are set to the same port number, ranging from 1 to 65535.

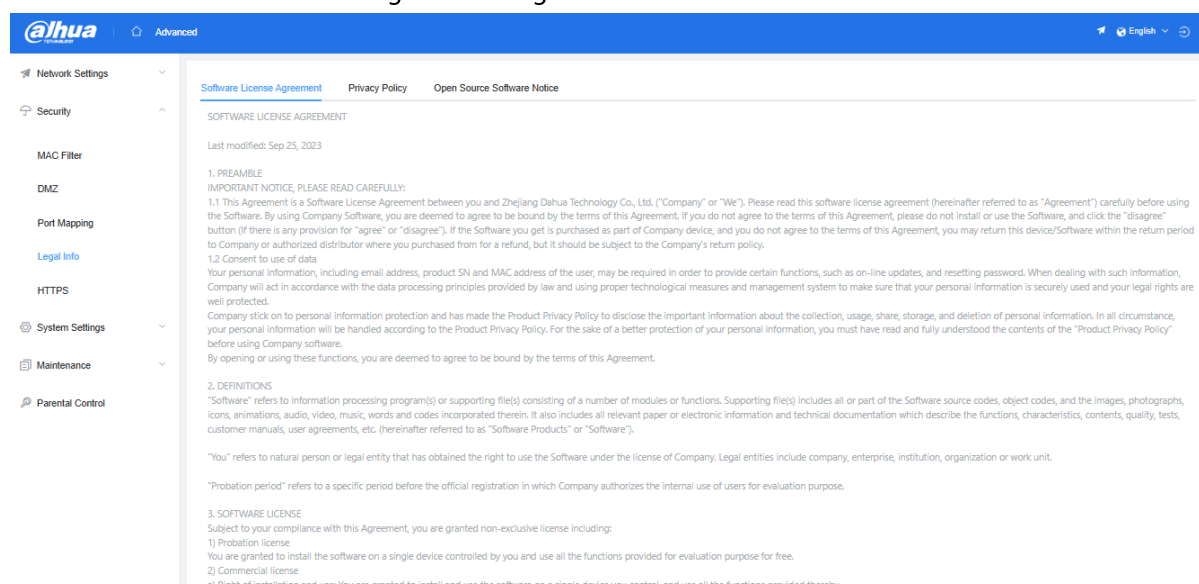
## 6.2.4 Legal Info

Displays the Software License Agreement, Privacy Policy, and Open Source Software Notice.

### Procedure

**Step 1** Select **Advanced > Security > Legal Info**.

Figure 6-10 Legal Information



## 6.2.5 HTTPS

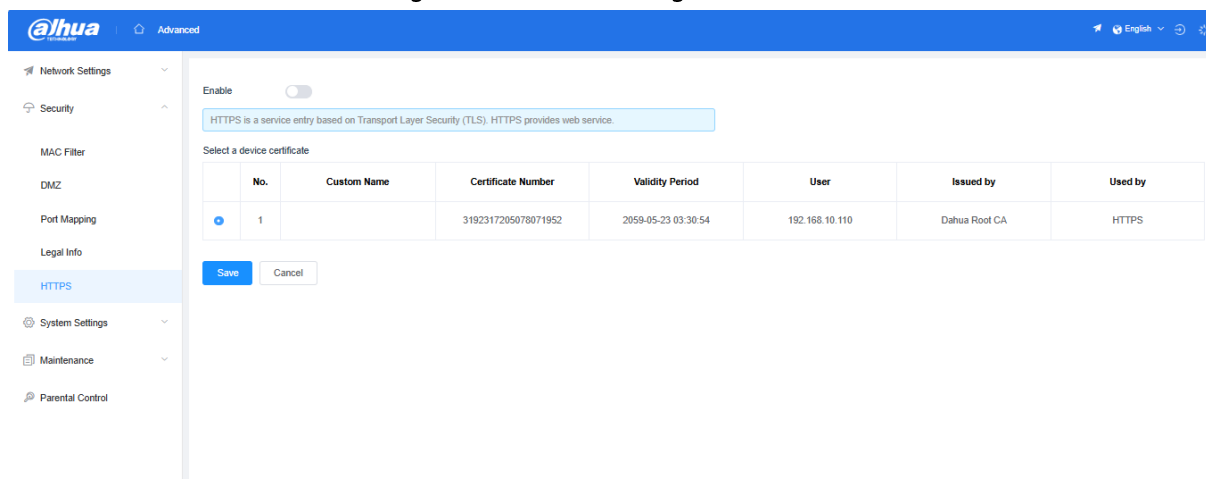
Web management supports both HTTP and HTTPS access methods. HTTPS has enhanced security compared to HTTP. It combines HTTP and TLS, verifies client identity and server through TLS, encrypts transmitted data, and achieves secure management of devices. The HTTPS service is turned off by default.

### Procedure

**Step 1** Select **Advanced > Security > HTTPS**.

**Step 1** Open the **Enable** button, and click **Save**.

Figure 6-10 HTTPS Config



## 6.3 System Settings

Displays the device information, set device management passwords, and system time.

### 6.3.1 Device Info

Displays detailed information about the device, including device information, WAN port information, and IPv6 information.

Figure 6-11 Device Info

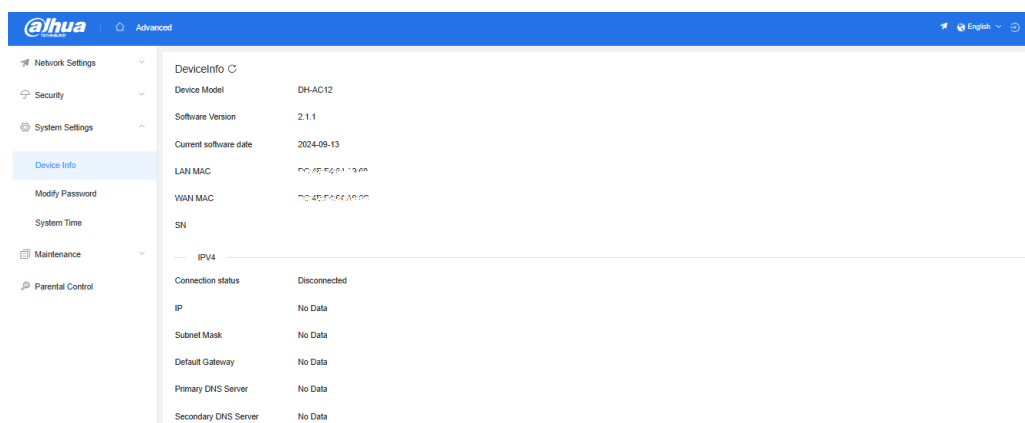


Table 6-11 Description of parameters

Parameter	Description
Device Info	
Device Model	Model information of the device.
Software Version	Software version of the device.
Current software date	Software version time of the device.
LAN MAC	The LAN MAC address of the device.
WAN MAC	The WAN MAC address of the device.

Parameter	Description
SN	The serial number of the device.
IPv4	
Connection status	WAN port connection status.
IP	IP address of WAN port.
Subnet Mask	Subnet mask for the IP address of the WAN port.
Default Gateway	Default gateway for IP address of WAN port.
Primary DNS Server	The primary DNS used for WAN port.
Secondary DNS Server	The secondary DNS used for WAN port.
IPv6	
IPv6Address	IPv6 address of WAN port.
WAN IPv6 Link Local Address	Local IPv6 address of WAN port link.
Default Gateway	Default gateway for IPv6 address on WAN port.
Primary DNS Server	The primary DNS used for WAN port.
Secondary DNS Server	The secondary DNS used for WAN port.

## 6.3.2 Modify Password

Set the management password for the device.

### Procedure

- Step 1    Select **Advanced > System Settings > Modify Password**.
- Step 2    Enter the original password, then enter the new password, and click **Save**.

Figure 6-12 Password Config

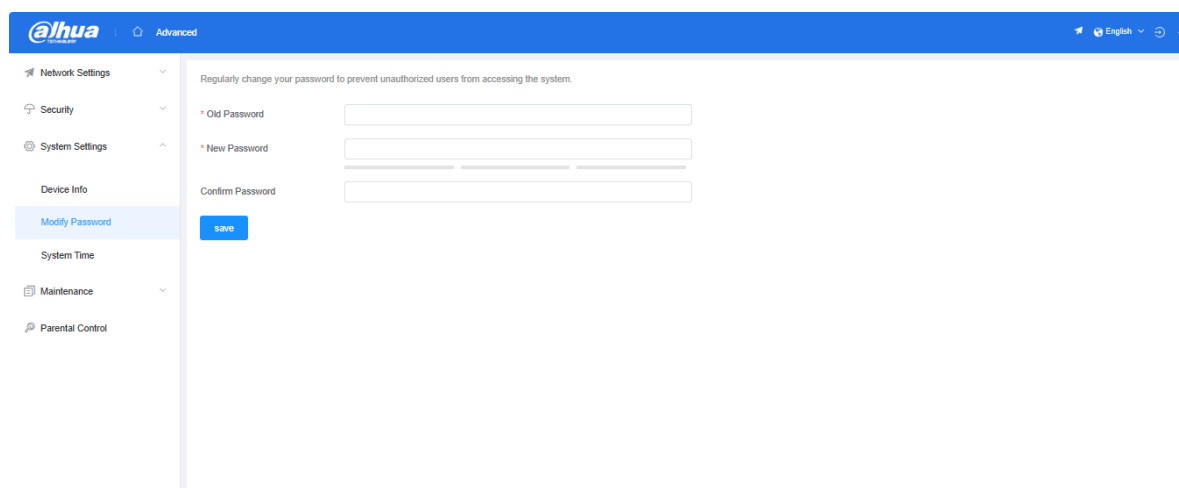


Table 6-12 Description of parameters

Parameter	Description
Old Password	The original password of device.
New Password	The new password of device.
Confirm Password	Confirm the new password of device.

### 6.3.3 System Time

Configure the Time Zone, NTP Server, and Summer Time for the Device.

#### Procedure

- Step 1 Select **Advanced > System Settings > System Time**.
- Step 2 Select the **Time Zone, Update time using NTP Server**. If you choose the NTP mode, you need to enter the **NTP Server address** manually.
- Step 3 If Summer Time needs to be configured, enable **DST** for configuration.
- Step 4 Click **Save**.

Figure 6-13 System Time Config

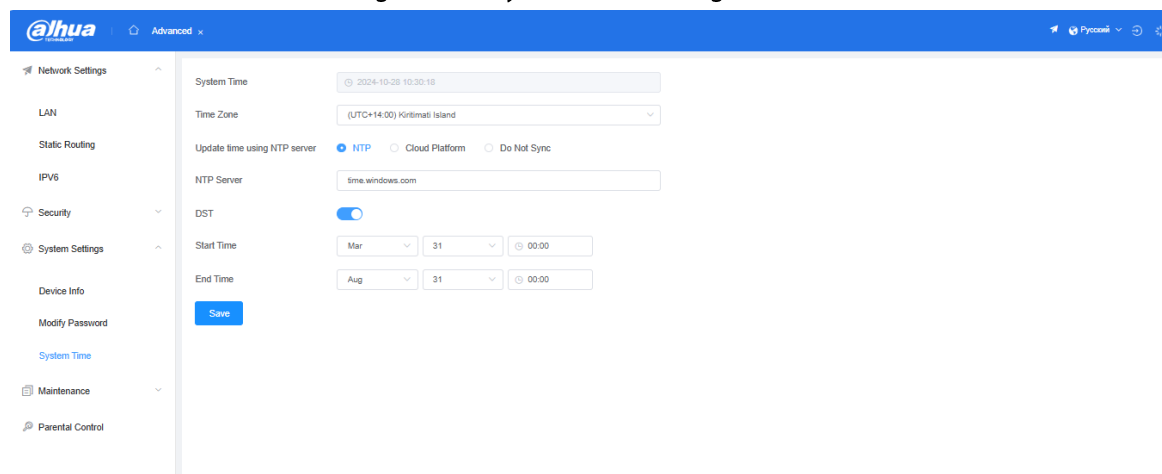


Table 6-13 Description of parameters

Parameter	Description
System Time	The system time of the device.
Time Zone	the working time zone of the device.
Update time using NTP server	The method of device time synchronization.
NTP Server	Set up NTP Server.
DST	Summer Time Enabled.
Start Time	Start time of summer time.
End Time	End time of summer time.

## 6.4 Maintenance

Displays the device information, set device management passwords, and system time.

### 6.4.1 Log

The device's log can be exported locally or sent to a remote server.

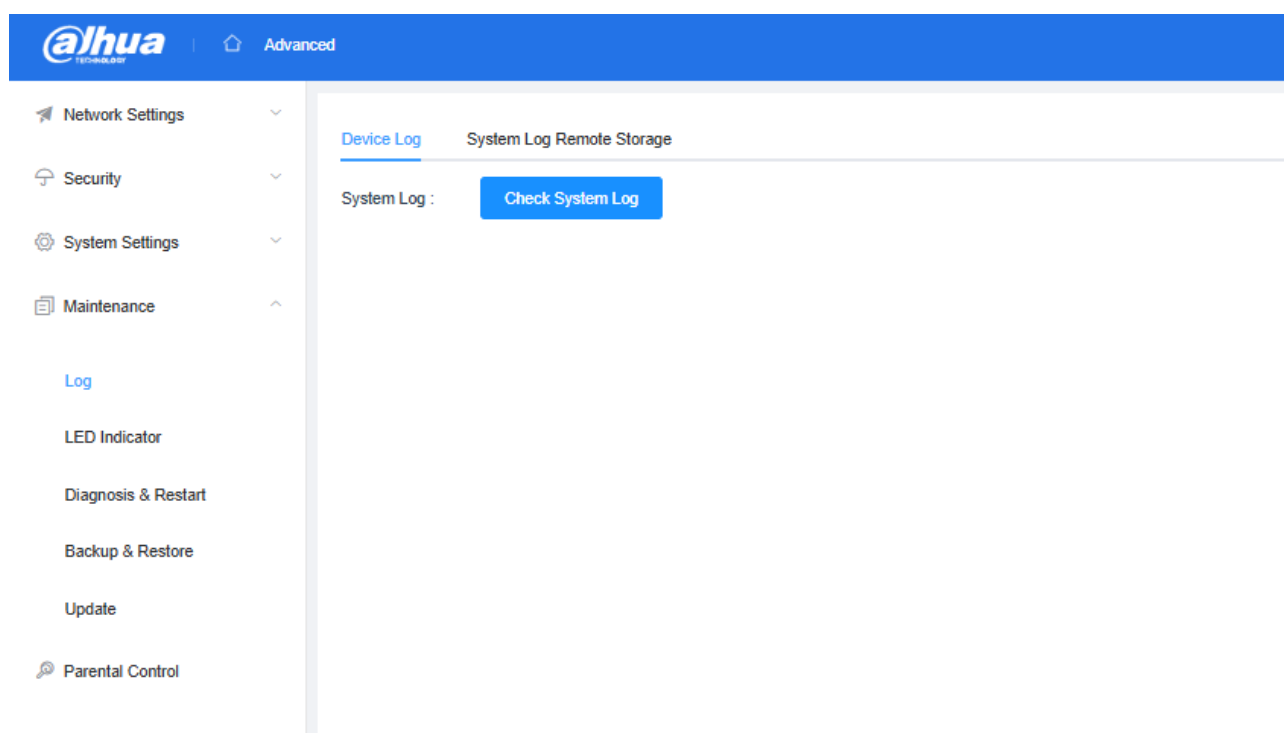
#### Device Log Procedure

**Step 1** Select **Advanced > Maintenance > Log > Device Log**.

**Step 2** Click **Check System Log**, and then export logs to local.

Figure 6-14 Log Config





## System Log Remote Storage Procedure

**Step 1** Select **Advanced** > **Maintenance** > **Log** > **System Log Remote Storage**.

**Step 2** Enable Remote Log, select Device, fill in IP Address, and then click **Save**.

Figure 6-15 Log Config

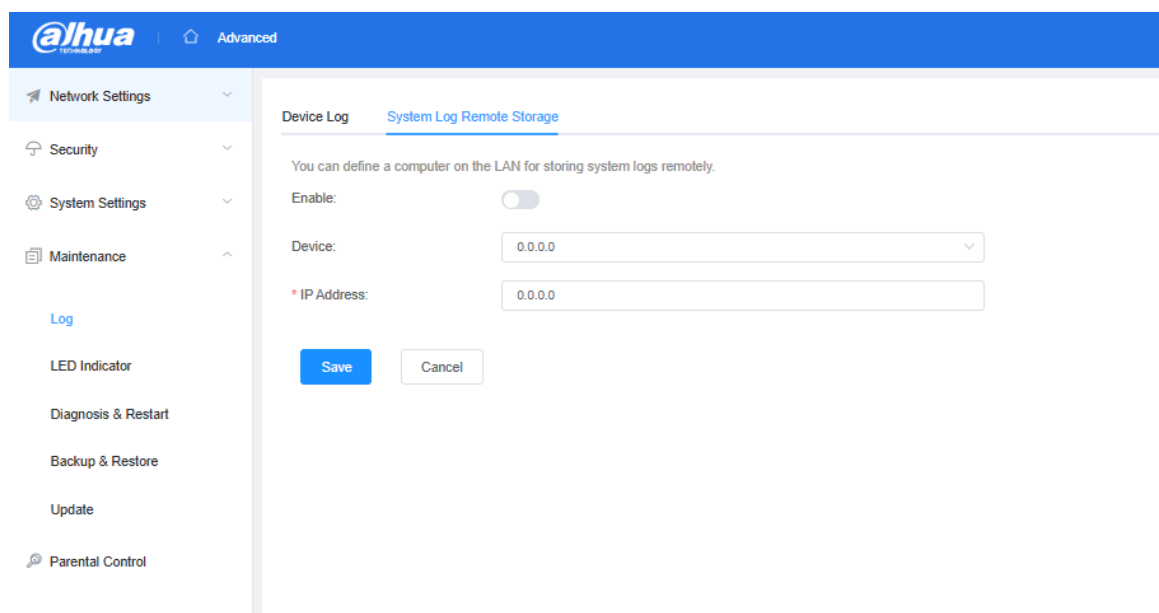


Table 6-14 Description of parameters

Parameter	Description
Enable	Enable Remote Log function.
Device	Choose a remote log server, which can be connected to a network terminal or manually configured.
IP Address	The server IP address can be manually set or selected from terminals that have already been connected to the network.

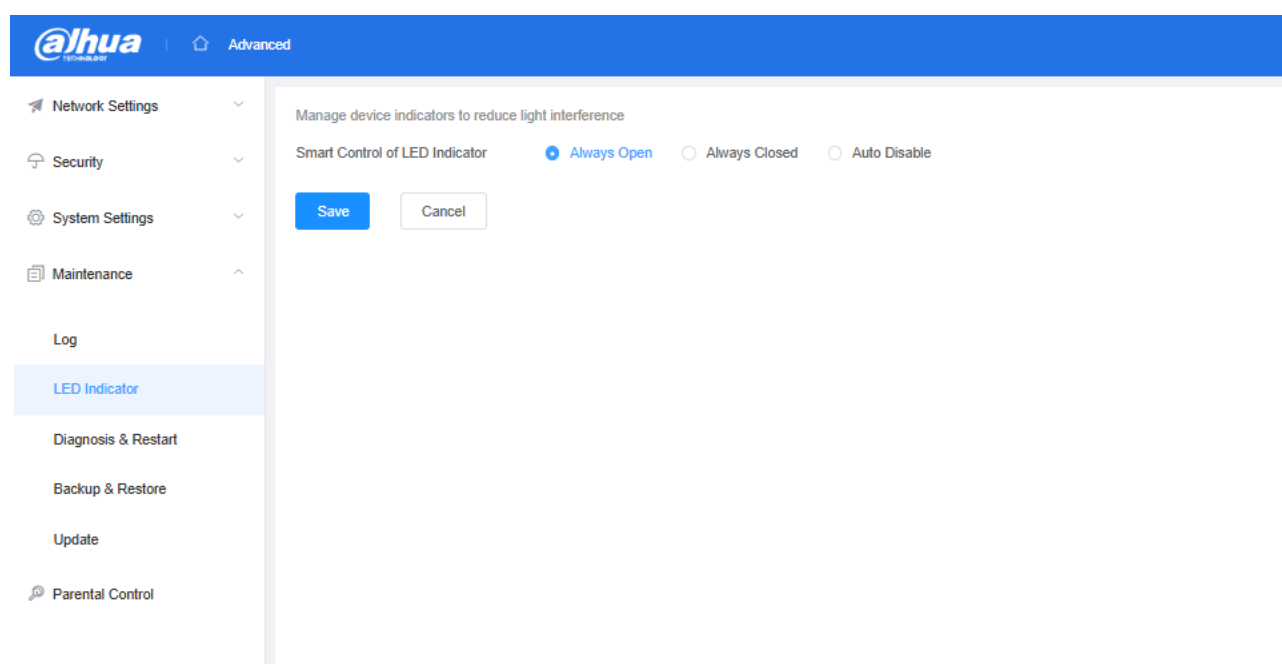
## 6.4.2 LED Indicator

Intelligent control the LED Indicator light on or off.

### Procedure

- Step 1 Select **Advanced** > **Maintenance** > **LED Indicator**.
- Step 2 Select the strategy of turning on or off the LED indicator, and click **Save**.

Figure 6-16 LED Indicator Config



## 6.4.3 Diagnosis & Restart

Diagnose the network condition of the device and perform a restart operation on the device.

### Diagnosis Procedure

- Step 1 Select **Advanced** > **Maintenance** > **Diagnosis & Restart** > **Diagnosis**.
- Step 2 Fill in **Destination IP or Domain Name, Packet Size, Ping Times**.
- Step 3 Click **Diagnosis**.

Figure 6-17 Network Diagnosis

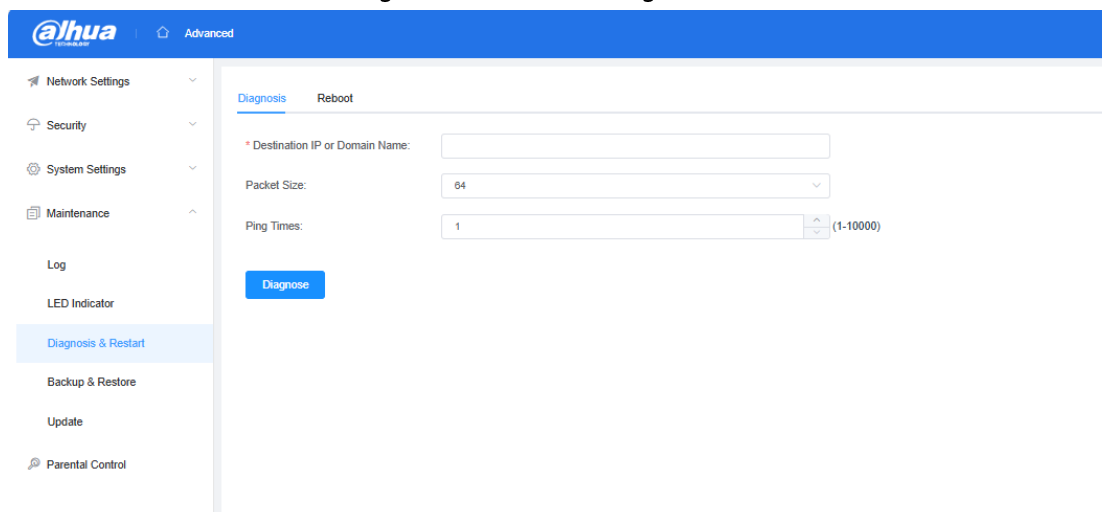


Table 6-15 Description of parameters

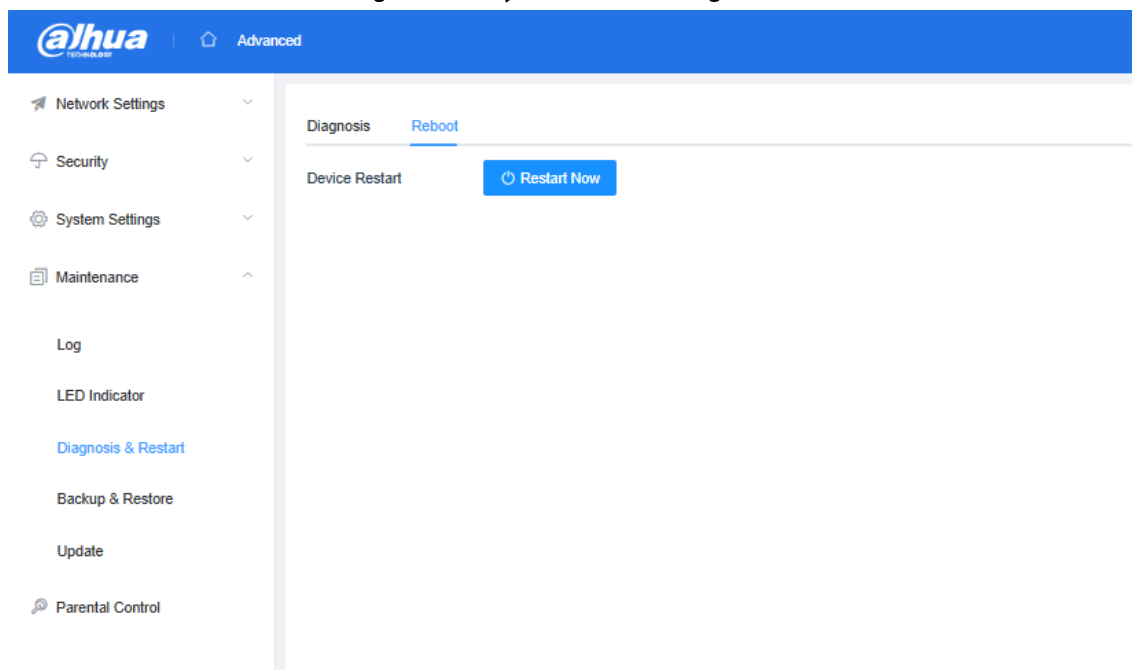
Parameter	Description
Destination IP or Domain Name	The destination IP or domain name for PING detection.
Packet Size	The packet size for PING detection, default is 64 bytes.
Ping Times	The number of PING detections, default is 1.

## Restart Procedure

Step 1 Select **Advanced** > **Maintenance** > **Diagnosis & Restart** > **Reboot**.

Step 2 Click the **Restart Now** button to restart the device.

Figure 6-18 System Time Config



## 6.4.4 Backup & Restore

Operate on device configuration, mainly including configuration backup, configuration import, and configuration recovery from factory.

Figure 6-19 Backup &amp; Restore

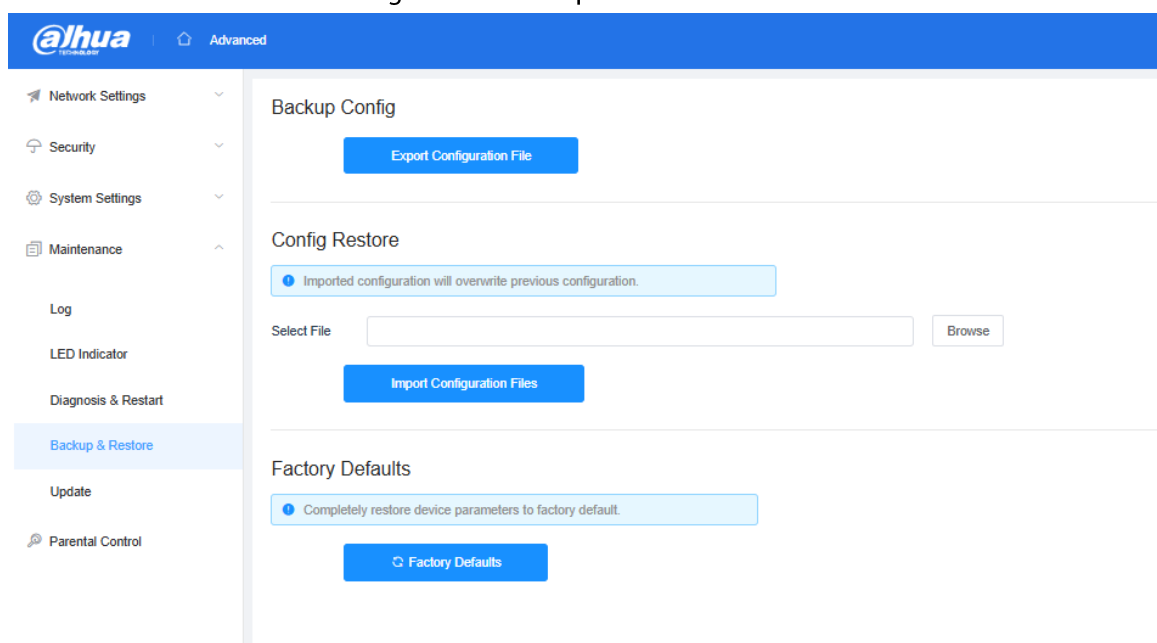


Table 6-16 Description of parameters

Parameter	Description
Backup Config	Backup the current configuration of the device locally.
Config Restore	Select the backup configuration file and import it to restore the device to its previous configuration.

Parameter	Description
Factory Defaults	Restore the device to factory settings.

## 6.4.5 Updating

The upgrade mainly includes online upgrade and local upgrade. When the Internet is connected, online upgrade only requires users to manually click on the version detection and upgrade buttons. Local upgrade does not require Internet connectivity, but users need to get the version first and manually select the version to upgrade.



**During the upgrade process, please do not power off or restart the device.**

### Online Upgrade Procedure

- Step 1** Select **Advanced > Maintenance > Upgrade > Upgrade Online**.
- Step 2** Click the **Check For New Firmware** button to upgrade the latest version.

Figure 6-20 Online Upgrade

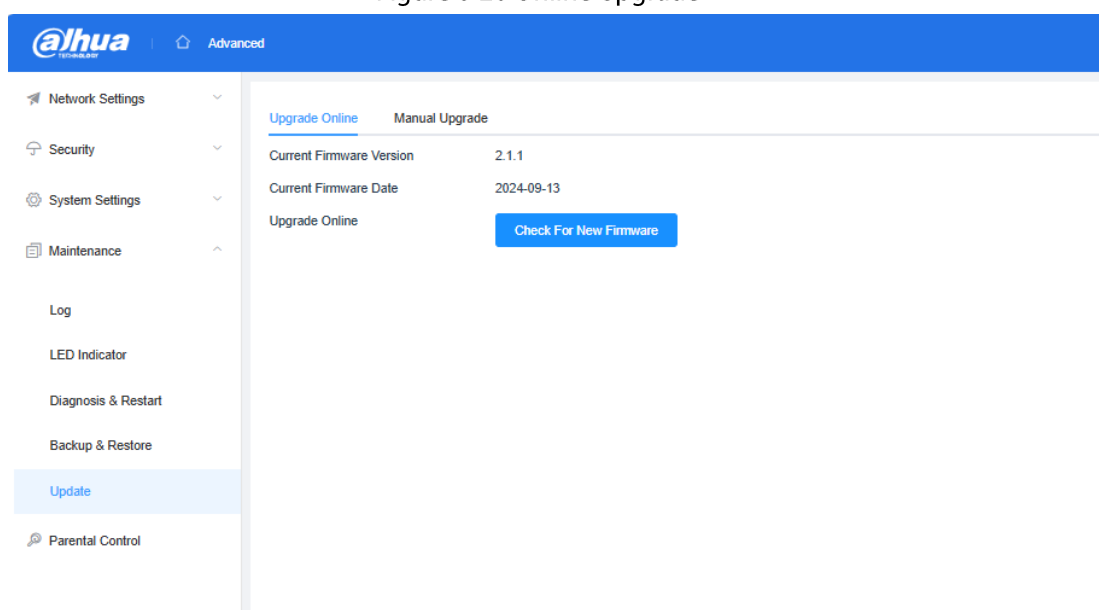


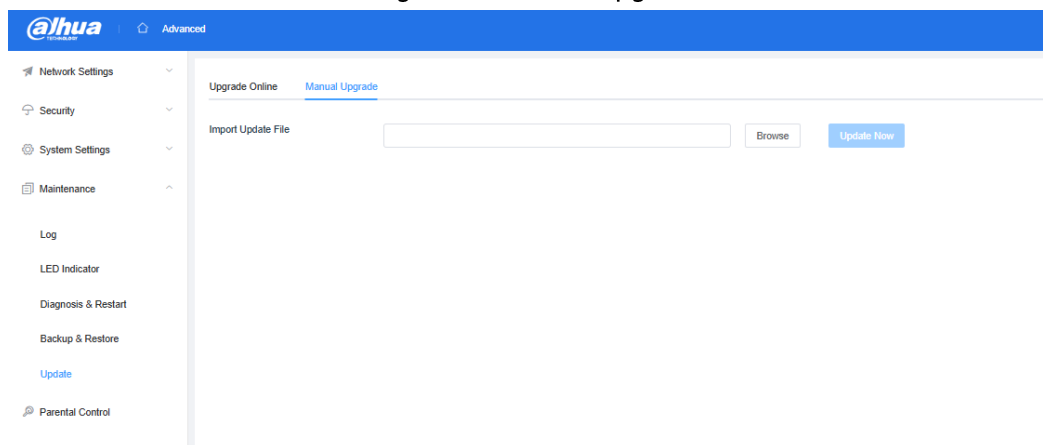
Table 6-17 Description of parameters

Parameter	Description
Current Firmware Version	The current firmware version of the device.
Current Firmware Date	The current firmware version date of the device.
Upgrade Online	Online upgrade for device.

### Manual Upgrade Procedure

- Step 1** Select **Advanced > Maintenance > Upgrade > Manual Upgrade**.
- Step 2** Click the **Browse** button to select the firmware, and then Click the **Update Now** button to upgrade.

Figure 6-21 Online Upgrade



## 6.5 Parental Control

Control the internet time of terminals added to the list, multiple roles can be created to control the internet time periods of different terminals.

### Procedure

- Step 1** Select **Advanced > Parental Control**.
- Step 2** Click the **Enable** button to enable parental control.

Figure 6-22 Parental control list

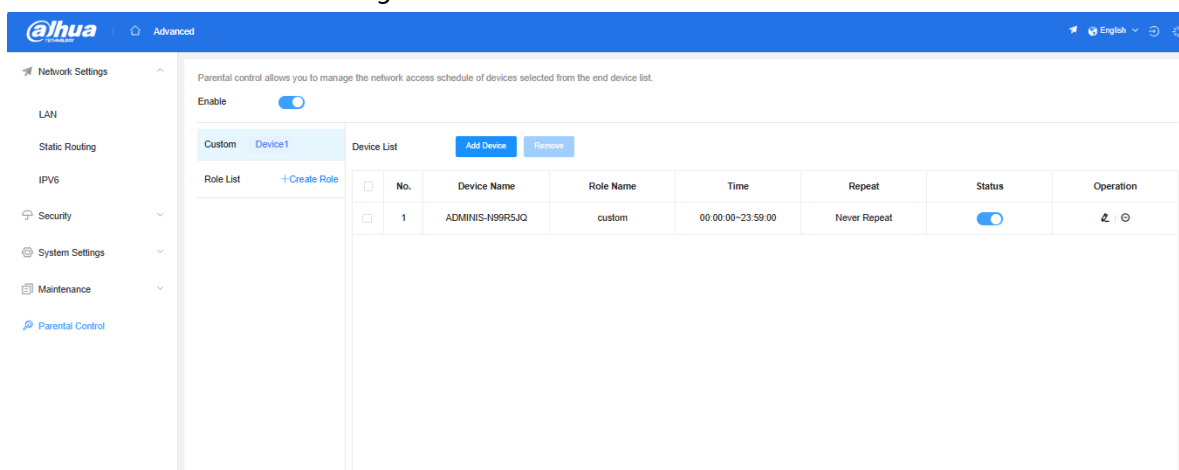


Table 6-18 Description of parameters

Parameter	Description
Device Name	Terminal name.
Role Name	Role Name.
Time	The time when the terminal cannot access the internet.
Repeat	The period during which the terminal cannot access the internet.
Status	The status of the rule, on or off.
Operation	The operation of rules, editing or deleting.

**Step 3** Click the **Add Device** button to set network period, select device, and then Click **OK**.

Figure 6-23 Add Device

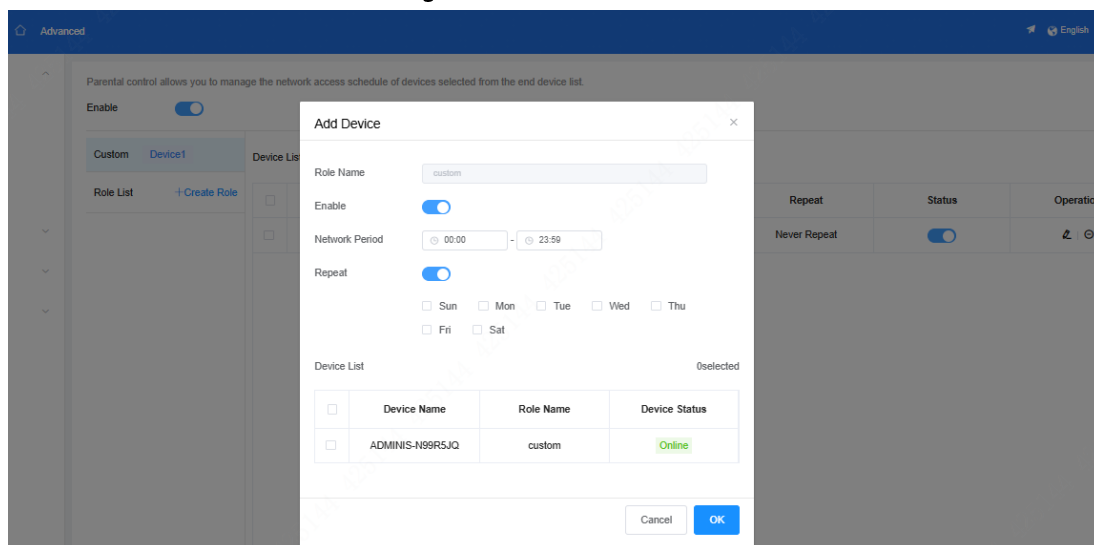


Table 6-19 Description of parameters

Parameter	Description
Role Name	Role name, default is Custom; Users can also manually create roles
Enable	The enabled state of the rule, default is disabled
Network Period	The time period when the terminal cannot access the internet
Repeat	The time period during which the terminal cannot access the internet repeat, and default is it turned off
Device List	List of selectable terminals



If you do not want to use the default Role Custom, they can also create a role through Create Role.

# 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;
- Establish 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](http://www.dahuasecurity.com) | Postcode: 310053

Email: [dhoverseas@dhvisiontech.com](mailto:dhoverseas@dhvisiontech.com) | Tel: +86-571-87688888 28933188