Network Alarm Box

User Manual



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.1.0

Foreword

General

This user manual introduces the installation, functions and operations of the Network Alarm Box (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
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
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 results.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.1.0	Updated the event linkage.	April 2026
V1.0.0	First release.	February 2026

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 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.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, and comply with the guidelines when using it.

Transportation Requirements



Transport the Device under allowed humidity and temperature conditions.

Storage Requirements



Store the Device under allowed humidity and temperature conditions.

Installation Requirements



Stability Hazard

Possible result: The rack might fall down and cause serious personal injury.

Preventive measures (including but not limited to):

- Before extending the rack to the installation position, read the installation instructions.
- When the Device is installed on the slide rail, do not place any load on it.
- Do not retract the slide rail while the Device is installed on it.



-  Rotating Fan Blades Hazard

  Avoid touching the fan blades, especially when they are moving.
-  Before installation, disconnect all the power cords.
- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Use the power adapter and cables provided with the Device. We assume no responsibility for injuries or damage caused by using the incorrect power adapter and cables.



-  Reliably ground the grounding terminal of the Device to improve safety. The grounding terminal differs depending on the device, and some devices do not have grounding terminals. Process the situation according to the device model.

- The Device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- The Device must be reliably grounded by professionals. They must install the grounding conductor in the building floor and verify the grounding connection of the output receptacle.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements, and are rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the Device, make sure that the power plug can be easily reached to cut off the power.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- Affix the controller securely to the building before use.

Operation Requirements

DANGER

- The Device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

  Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

  Preventive measures (including but not limited to):

  - Keep new and used batteries out of reach of children.
  - If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
  - Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

  Preventive measures (including but not limited to):

  - Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
  - Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
  - Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
  - Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

WARNING

Place the Device in a location that children cannot easily access.

- This is a class 1 laser device. You can only insert modules that meet the requirements of class 1 lasers.

- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- Operate the Device within the rated range of power input and output.
- Do not disassemble the Device without professional instruction.
- Transport, use and store the Device under allowed humidity and temperature conditions.

Maintenance Requirements

DANGER

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.

The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Product Introduction 1
1.1 Overview 1
1.2 Features 1
1.3 Structure 4
2 Initialization 5
2.1 Initializing the Device 5
2.2 Login 7
3 Events 8
3.1 Alarm Settings 8
3.1.1 Alarm-in Port 8
3.1.2 Alarm-out Port 9
3.1.3 Exception 10
3.1.4 One-Click Disarm 11
3.2 Event Linkage 12
4 Network Settings 18
4.1 TCP/IP 18
4.2 Port 20
4.3 Email 21
4.4 Alarm Center 22
5 System Settings 24
5.1 Basic Settings 24
5.2 Time 24
5.2.1 Date and Time 24
5.2.2 Holiday 26
5.3 Account 27
5.3.1 User 27
5.3.2 Group 30
5.3.3 Password Reset 31
5.4 Security 32
5.4.1 Security Status 32
5.4.2 System Service 32
5.4.3 Attack Defense 36
5.4.4 CA Certificate 38
5.4.5 Security Warning 40
5.4.6 Security Authentication 41

6 Searching Events and the History 42
6.1 Searching Real-Time Events 42
6.2 Searching Event History 42
7 Maintenance 44
7.1 Log 44
7.2 System Information 44
7.2.1 Version 44
7.2.2 Legal Information 45
7.2.3 Online User 45
7.3 Maintenance Management 45
7.3.1 Update 45
7.3.2 Device Maintenance 45
7.3.3 Import/Export 46
7.3.4 Default 46
7.3.5 Advanced Maintenance 47
Appendix 1 Security Commitment and Recommendation 48

1 Product Introduction

1.1 Overview

The Network Alarm Box is a standalone IP-based device that extends alarm signal integration. It provides scalable alarm I/O ports for devices, features an intuitive webpage for direct configuration, and operates with dual-mode—executing actions locally for instant response or seamlessly working with NVR (Network Video Recorder) for advanced alarm linkage. By moving beyond physical port limits, it enables flexible, network-based deployment and scalable security solutions.

1.2 Features

Real-Time Surveillance

- Connects the NVR to a monitor through the VGA or HDMI port. Some series support TV/VGA/HDMI output at the same time.
- Shortcut menu for preview.
- Supports multiple popular PTZ decoder control protocols. Supports preset, tour and pattern.

Playback

- Supports independent real-time recording for each channel. At the same time, it supports functions such as smart search, forward play, network monitor, record search and download.
- Supports various playback modes: slow play, fast play, backward play and frame-by-frame play.
- Supports time title overlay so that you can view the event accurate occurred time.
- Supports specified zone enlargement.

Smart Playback

This function is available on select models.

- IVS playback. It can screen out and replay the records meeting the set rules.
- Face detection playback. It can screen out and replay the records with human faces.
- Face recognition playback. It can compare the face information in the video with the information in the database and replay the corresponding records.
- ANPR playback. It can screen out the record with a specific car plate number or all the records with car plate numbers.
- Human body detection playback. It can screen out and replay the records with specific human bodies.
- Smart search. It includes smart functions such as searching by attribute and searching by image to enable users to get target records quickly.

AI Functions

AI functions are available on select models and vary with models.

- Face detection. The system can detect the faces are on the video image.
- Face recognition. The system can compare the detected faces with the images in the face database in real time.
- Human body detection. The system activates alarm actions once human body is detected.
- People counting. The system can effectively count the number of people and flow direction.
- Heat map. The system can monitor the active objects in a specific area.
- Automatic number plate recognition (ANPR). The system can effectively monitor the passing vehicles.

Cloud Upgrade

For the NVR connected to the Internet, it supports application online upgrade.

User Management

Users can be added to user groups for management. Each group has a set of permissions that can be individually edited.

Storage

- With corresponding settings (such as alarm settings and schedule settings), you can back up related audio/video data in the network video recorder.
- You can take records via the web and the record files are saved on the PC in which the client locates.

Network Surveillance

- Sends audio/video data compressed by IPC or NVS to client-ends through the network, and then the data will be decompressed and displayed.
- Supports max 128 connections at the same time.
- Transmits audio/video data by protocols such as HTTP, TCP, UDP, MULTICAST and RTP/RTCP.
- Transmits some alarm data or alarm info by SNMP.
- Supports web access in WAN/LAN.

Window Split

Adopts video compression and digital processing to display several windows in one monitor. Supports 1/4/8/9/16/25/36 window split in preview and 1/4/9/16 window split in playback.

Record

Supports regular record, motion record, alarm record and smart record. Saves the recorded files in the HDD, USB device, client-end PC or network storage server and you can search or playback the saved files at the local-end or via the Web/USB devices.

Backup

Supports network backup and USB record backup. You can back up the record files in devices such as network storage server, peripheral USB 2.0 device and burner.

Network Management

- Supervises NVR configuration and control power via Ethernet.
- Supports web management.

Peripheral Equipment Management

- Supports peripheral device control and you can freely set the control protocol and connection port.
- Supports transparent data transmission such as RS-232 and RS-485.

Auxiliary

- Supports switch between NTSC and PAL.
- Supports real-time display of system resources information and running status.
- Supports log record.
- Local GUI output. Shortcut menu operation with the mouse.
- IR control function (for some series only). Shortcut menu operation with remote control.
- Supports playing the video/audio files from remote IPC or NVS.

Alarm

- Responds to external alarm simultaneously (within 200 ms). Based on user's pre-defined relay settings, the system can process the alarm input correctly and sends user screen or voice prompts (supporting pre-recorded audio).
- Supports settings of the central alarm server, so that the system can automatically notify users of the alarm information. Alarm input can be derived from various connected peripheral devices.
- Alerts you of alarm information via email.

1.3 Structure

Figure 1-1 Ports

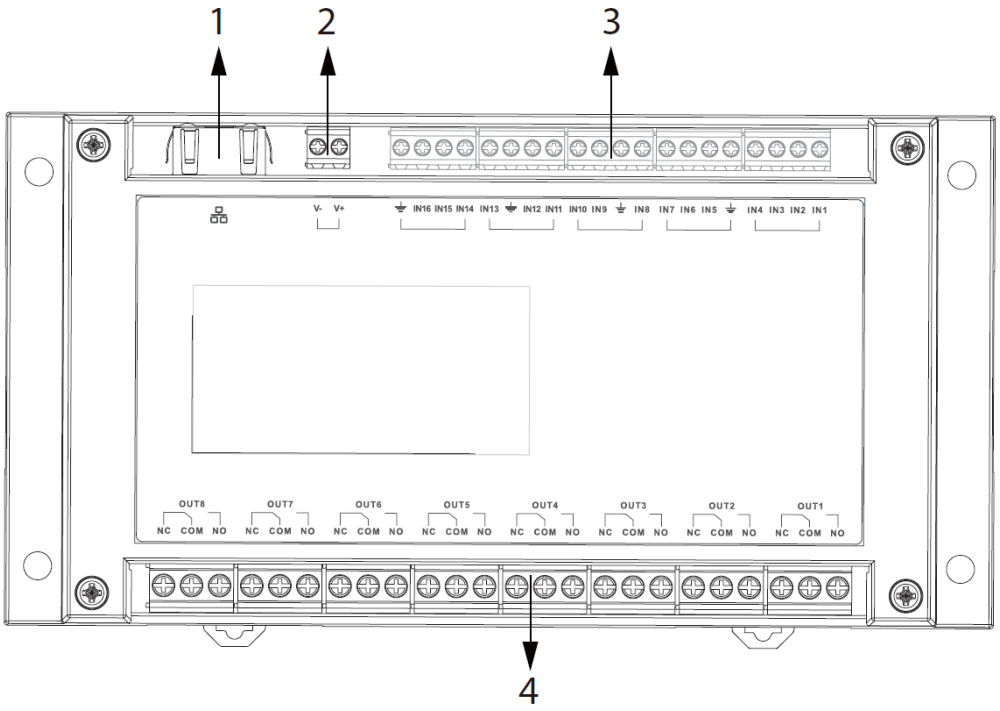


Table 1-1 Ports description

No.	Ports name	Description
1	Network port	Ethernet port, speed: 100 Mbps. It supports Power over Ethernet (PoE), functioning as a Powered Device (PD) to receive power from a Power Sourcing Equipment (PSE).
2	Power input	Electrical parameters: DC 12 V-24 V/1 A, supporting reverse polarity protection
3	Alarm input	In default configuration, a low level indicates an alarm event (IN connected to GND). Electrical parameters: high level 2.0-3.3 V, low level 0.0 V-1.0 V, drive current greater than 3 mA.
4	Alarm output	Each alarm interface group includes three terminals: NO, COM and NC. Electrical rating: 2 A/250 VAC or 2 A/30 VDC. Contact states are as follows: 1. When the device is powered off, COM is closed with NC and open with NO. 2. When the device is powered on and in the default configuration, COM is closed with NC and open with NO. 3. When the device is powered on and in the alarm output state, COM is closed with NO and open with NC.

2 Initialization

2.1 Initializing the Device

Background Information

For first-time use, set a login password for the admin account (default user).

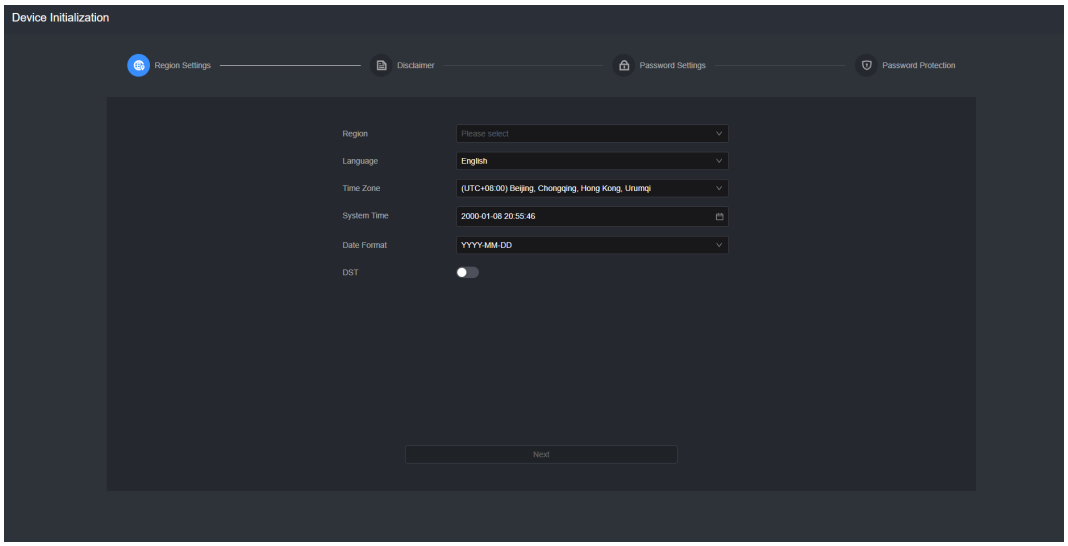
- For your device safety, keep your login password well, and change the password regularly.
- The IP address of the Device is 192.168.1.108 by default.
- If a DHCP service exists in the network environment, use a tool to locate the device IP (device category: ARC).

Procedure

Step 1 Start the alarm box.

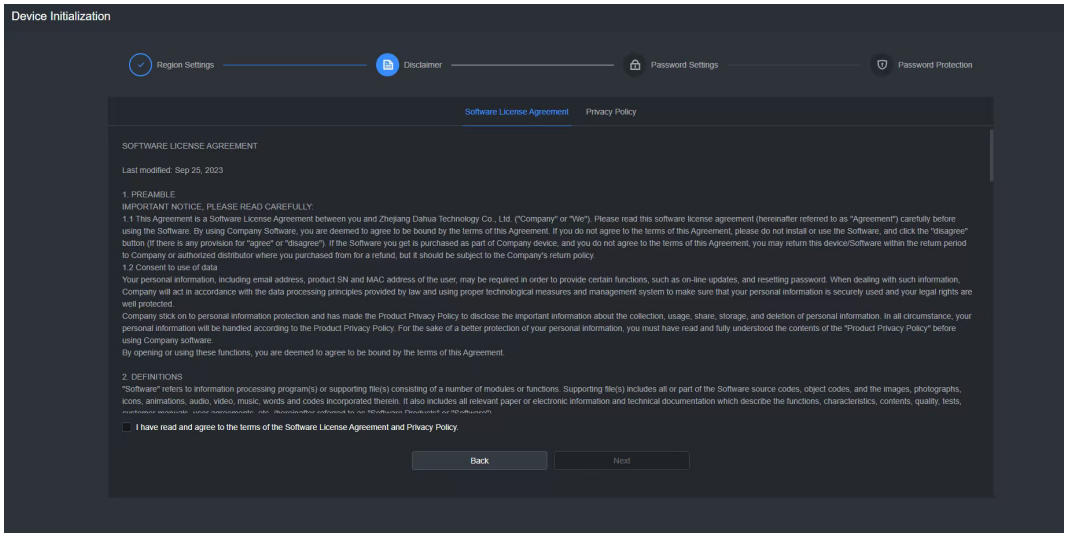
Step 2 Set region, time zone, and time according to the actual situation, and then click **Next**.

Figure 2-1 Region settings



Step 3 Read the disclaimer, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy** , and then click **Next**.

Figure 2-2 Disclaimer



Step 4 Set the login password for the admin account, set the login password for trying to log in the alarm box, and then click **Next**.

Figure 2-3 Password settings

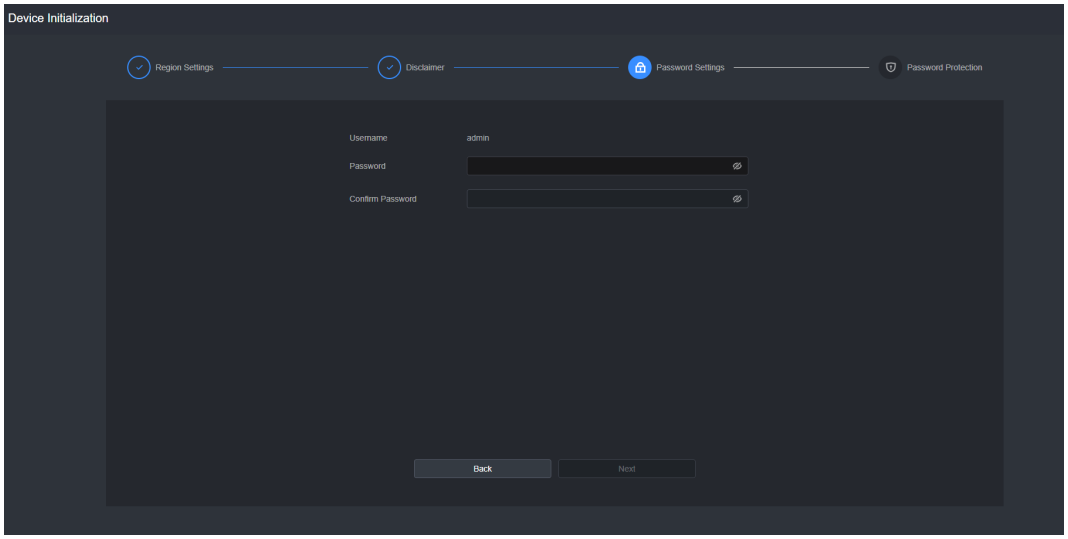
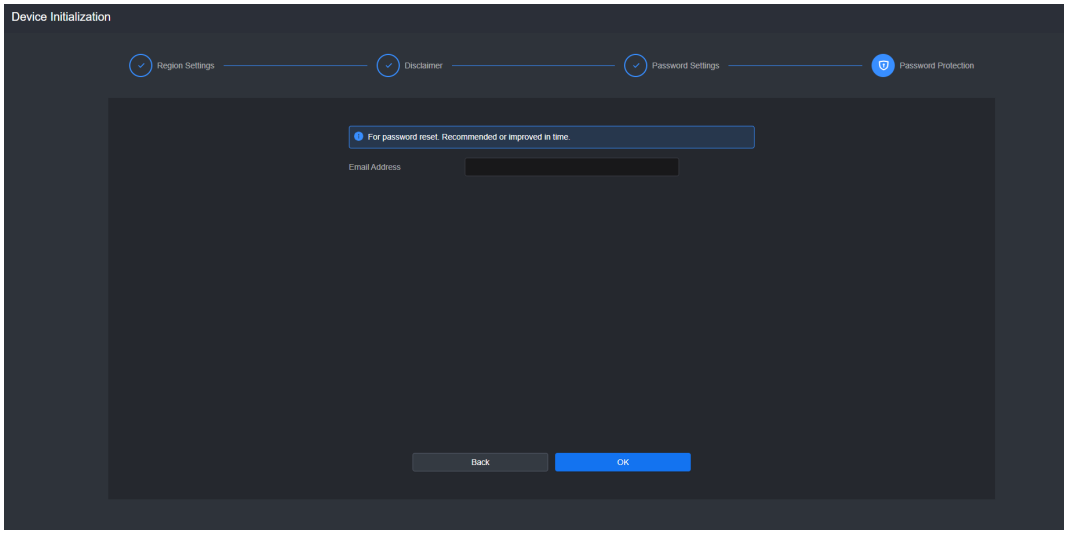


Table 2-1 Password parameters

Parameter	Description
Username	By default, the user is admin.
Password	Enter the password for admin and then confirm the password.
Confirm Password	

Step 5 Enter the email address for the password protection.

Figure 2-4 Password protection



Step 6 Click **OK**.

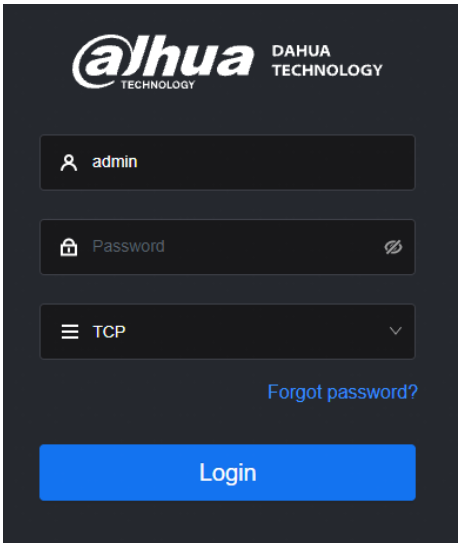
2.2 Login

Log in to the Device to perform local operations.

Procedure

Step 1 Enter the alarm box's IP address in the browser, and the password login window is displayed.

Figure 2-5 Password login



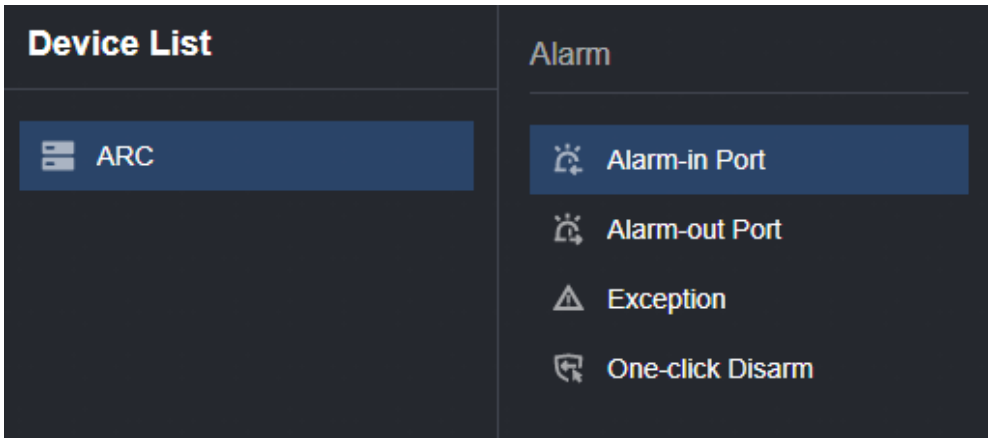
Step 2 Enter password, and then click **Login**.

3 Events

View and modify alarm functions of the device.

Log in to the main menu, select **SETTINGS** > **EVENT**. In **Device List** , click **ARC**.

Figure 3-1 Events



3.1 Alarm Settings

3.1.1 Alarm-in Port

Set up alarm input detection. When the configured alarm rules are triggered, the system will execute alarm linkage actions.

Background Information

Alarm input detection includes local alarm and network alarm.

- Local alarm: When the alarm-in port of the device is connected to an alarm device and local alarm settings are configured, the system will execute alarm linkage actions when the alarm signal is transmitted to the device through the alarm input port.
- Network alarm: When the device receives an alarm signal transmitted over the network, the system will execute the alarm linkage actions.

Procedure

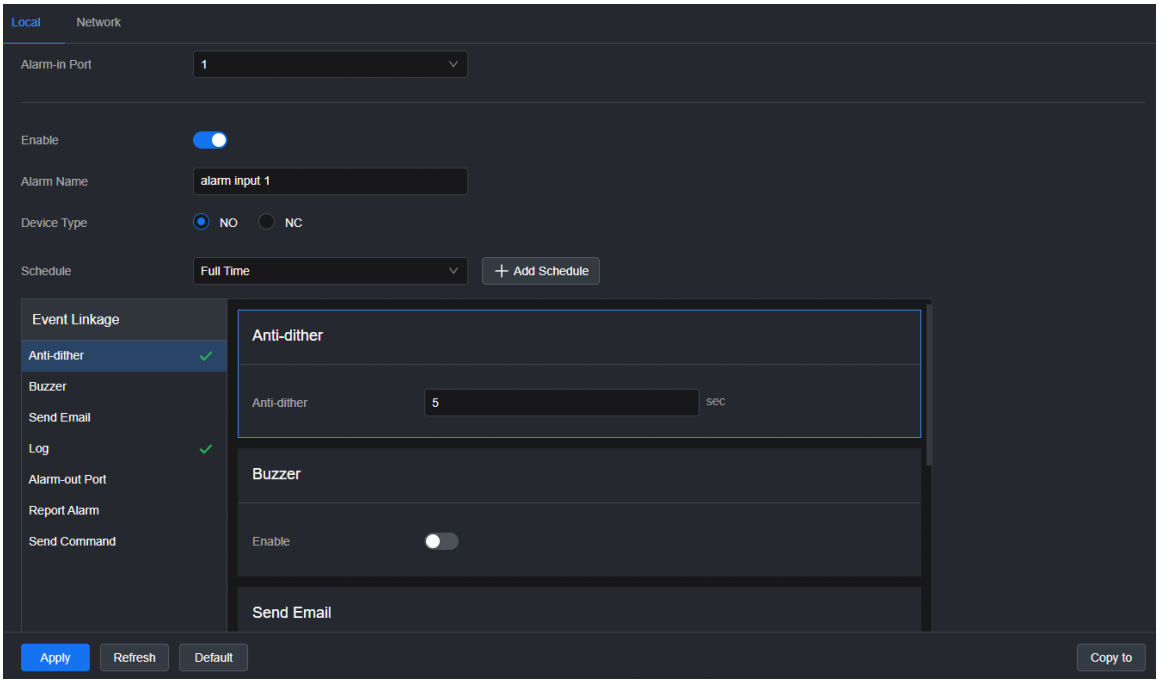
Step 1 Log in to the main menu, and then select **SETTINGS** > **EVENT**.

In **Device List**, select **ARC** > **Alarm** > **Alarm-in Port**.

Step 2 Select the alarm method tab and configure the alarm-in port.

Step 3 Enable the function and set up the alarm information.

Figure 3-2 Local alarm



Step 4 Click the schedule drop-down list to select an existing alarm schedule.

Click Add Schedule to add the alarm schedule and set the period.

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 5 Set up alarm linkage actions. For details, see "3.2 Event Linkage".

Step 6 Click **Apply**.

3.1.2 Alarm-out Port

Set the alarm output mode of the device to auto, manual, or off. When the alarm-out port is connected to an alarm device and the alarm linkage output function is enabled, the output mode must be set to **Auto** for the system to execute alarm linkage actions.

Procedure

Step 1 Log in to the main menu, and then select **SETTINGS** > **EVENT**.

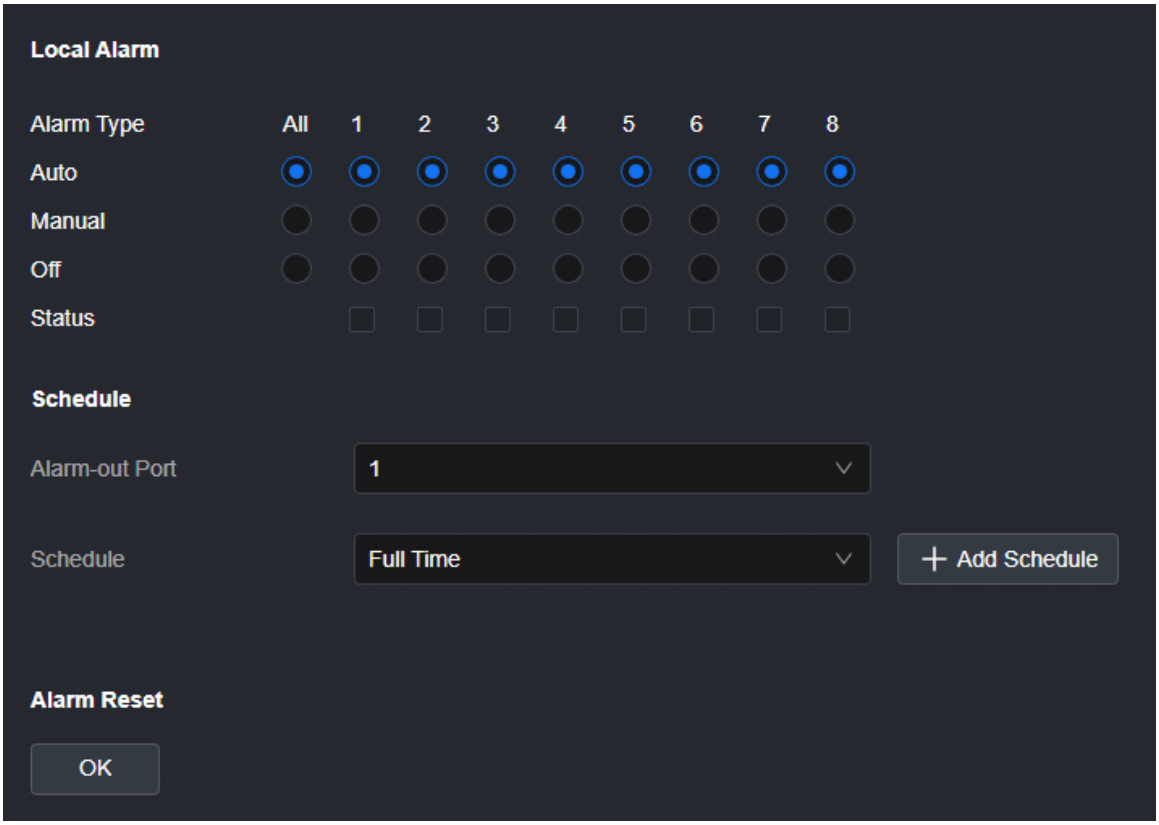
In **Device List**, click **ARC** > **Alarm** > **Alarm-out Port**.

Step 2 Set the local alarm output mode.

- **Auto** : Indicates that the alarm device only triggers the alarm when an event occurs.
- **Manual** : Indicates that the alarm device is in an alarm state continuously.
- **Off** : Indicates that the alarm output function is disabled.

In **All** list, you can simultaneously set the alarm mode for all alarm output channels.

Figure 3-3 Alarm mode



Step 3 Configure the extension alarm and select the alarm box.

- When the alarm device is in an alarm state, the status of the corresponding alarm output channel is displayed in green.
- In auto mode, when an alarm is triggered, clicking **OK** next to **Alarm Reset** will reset the alarm.

Step 4 Click the schedule drop-down list to select an existing alarm schedule.

Click Add Schedule to add the alarm schedule and set the period.

- After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.
- In auto mode, when an alarm is triggered, clicking **OK** next to **Alarm Reset** will reset the alarm.

Step 5 Click **Apply**.

3.1.3 Exception

Set up exception event alarm detection. When issues arise with network, or other components, the system will execute alarm linkage actions.

Procedure

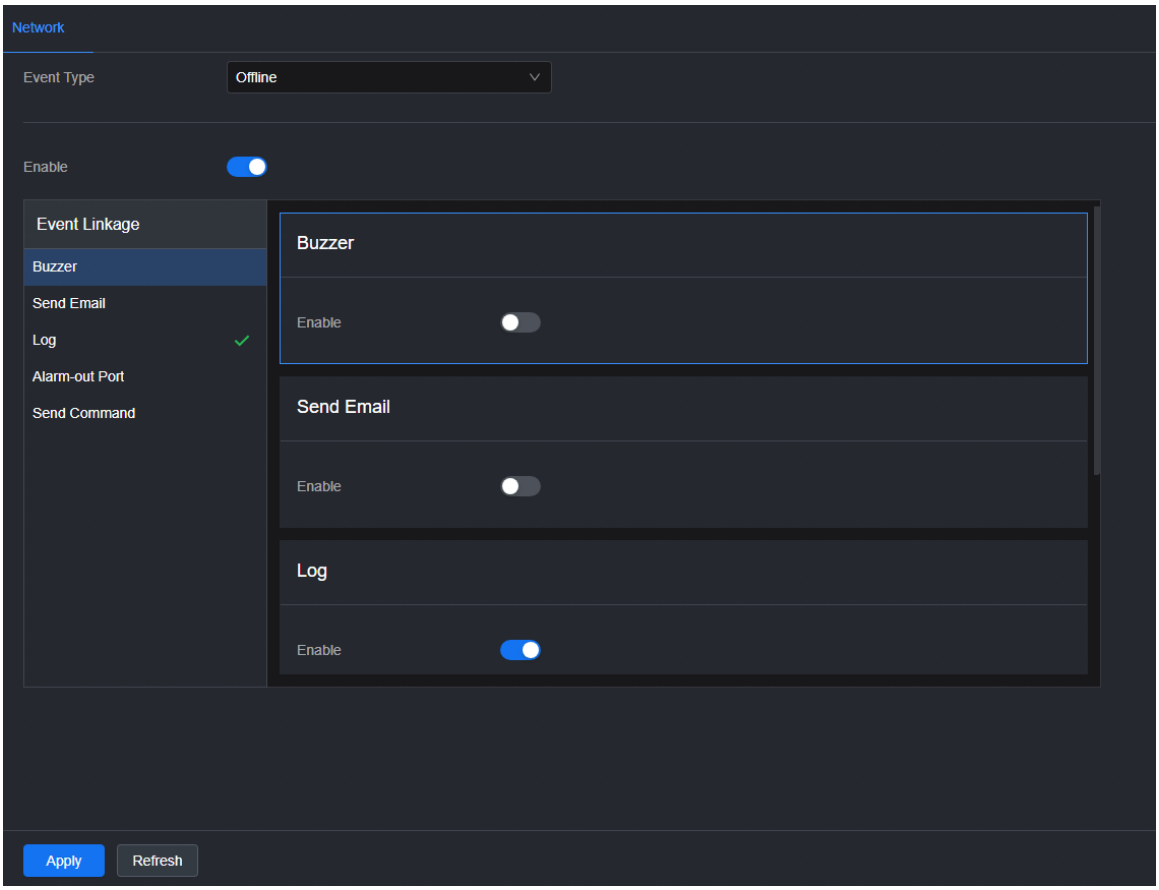
Step 1 Log in to the main menu, and then select **SETTINGS** > **EVENT**.

In **Device List**, click **ARC** > **Alarm** > **Exception**.

Step 2 Click different exception tab and select the event type.

Network : Set up alarm detection for network-related anomalies, including network disconnection, IP conflicts, and MAC address conflicts.

Figure 3-4 Exception



Step 3 Enable the exception alarm and configure the alarm parameters.

Step 4 Set up alarm linkage actions. For details, see "3.2 Event Linkage".

Step 5 Click **Apply**.

3.1.4 One-Click Disarm

Set up a one-click disarm function, allowing all linked alarm events to be turned off with one click based on actual needs.

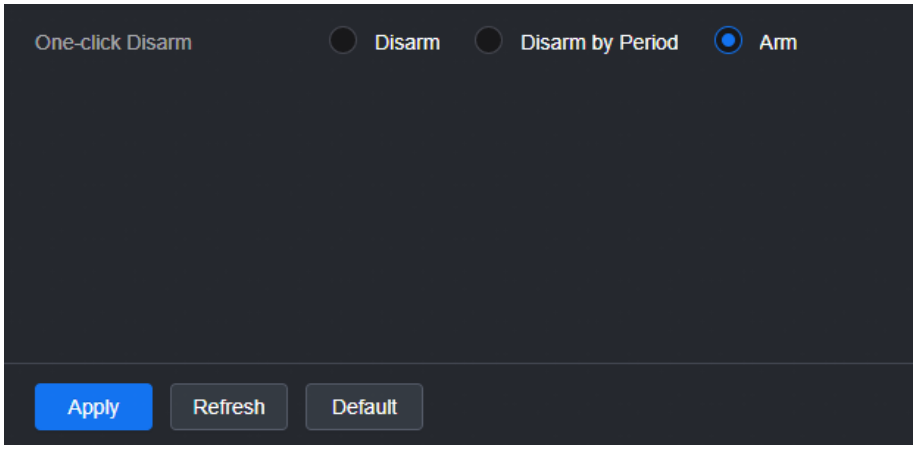
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click **ARC** > **Alarm** > **One-click Disarm**.

Step 2 Select arm and disarm plans.

Figure 3-5 Select the one-click disarm plan

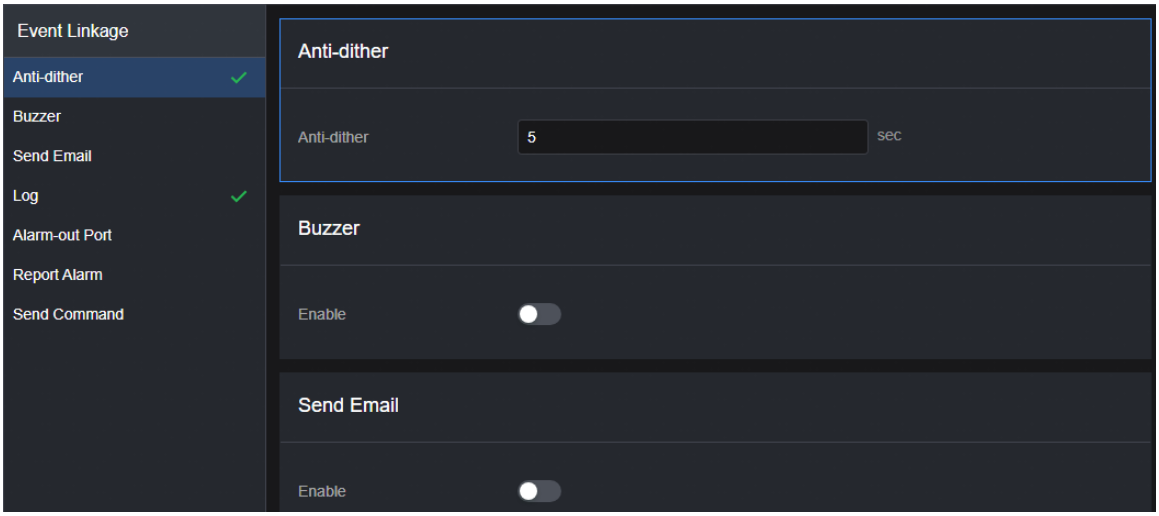


- Select **Disarm** to open the one-click disarm function.
- Select **Disarm by Period** to open the disarm by period function. Disable the alarm during the set time period and enable it outside of that period. Click to set the time range for disarm by period.
- Select **Arm** to open the one-click arm function.

3.2 Event Linkage

The event linkage can be configured in **Alarm** settings. After an alarm trigger or a smart event trigger, linked actions might be executed, including: **Anti-dither**, **Buzzer**, **Send Email**, **Log**, **Alarm-out Port**, **Report Alarm**, and **Send Command**.

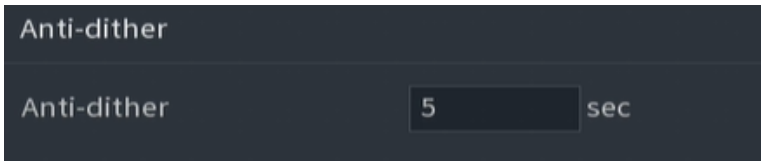
Figure 3-6 Event linkage



Anti-dither

Configure the anti-dither time and when it is triggered, the alarm will be processed for anti-dither.

Figure 3-7 Anti-dither



Buzzer

Enable the function and when linked actions are triggered, the device will trigger the buzzer.

Send Email

Enable the function and when an event is triggered, an email will be sent to the specified email address.

Log

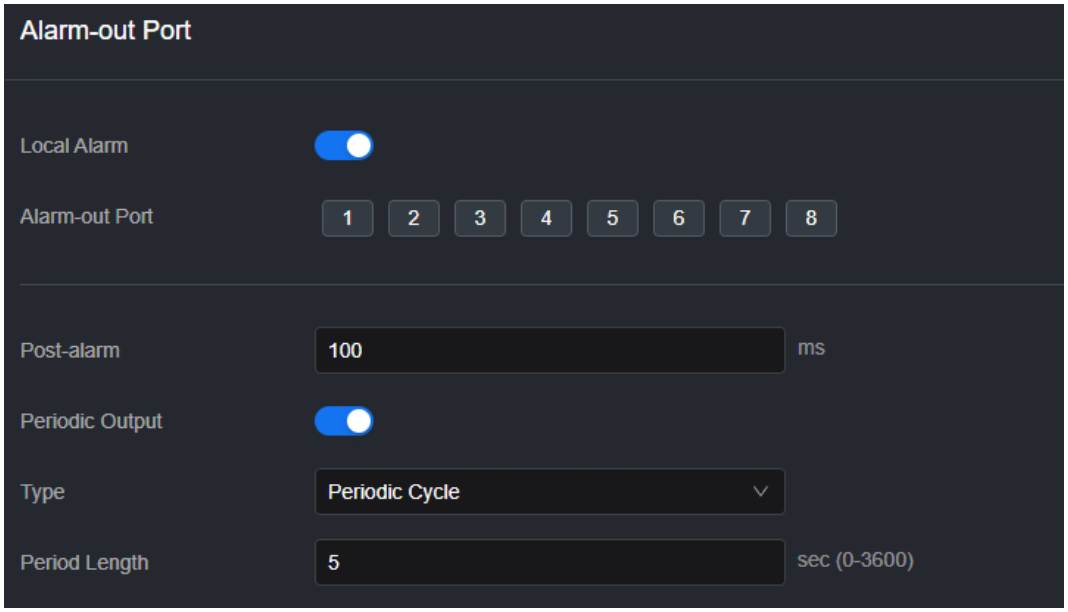
Enable the function and when a linkage is triggered, the system log will record the event information, which can be accessed from **APPLICATIONS** > **EVENT CENTER** > **Event History** > **Log**.

Alarm-out Port

To set the alarm output mode to auto, see "3.1.2 Alarm-out Port".

Enable this function, select the alarm output port, and then set the post-alarm period after triggering. When the linkage is activated, the alarm output device will trigger an alert, such as a siren or warning light.

Figure 3-8 Alarm-out port

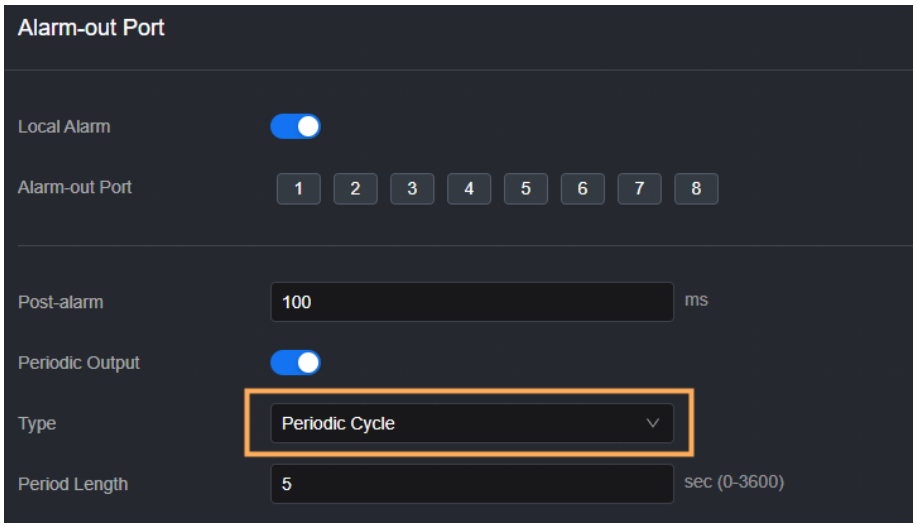


The post-alarm supports a minimum delay of 100 ms.

(Optional) Enable the periodic output and select the type.

- **Periodic Cycle** : After enabling the period, select the cycle period and configure the period duration. The alarm output can be cyclically enabled and disabled according to the configured time.

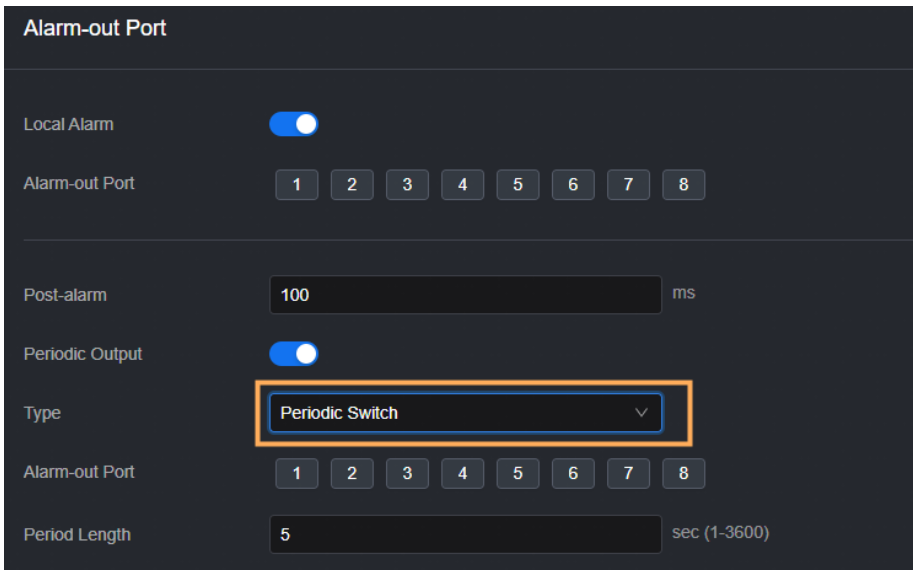
Figure 3-9 Periodic cycle



Once an alarm output interface is configured with a cycle period and enabled, it can no longer be triggered by other alarm inputs.

- **Periodic Switch** : After enabling **Periodic Output** and selecting **Periodic Switch** as the type, you can add a new alarm output port and set the period length in this section. The alarm output will then alternate cyclically—using the specified period length—between the newly configured alarm output port and the alarm output port defined in the periodic switch part.

Figure 3-10 Periodic switch



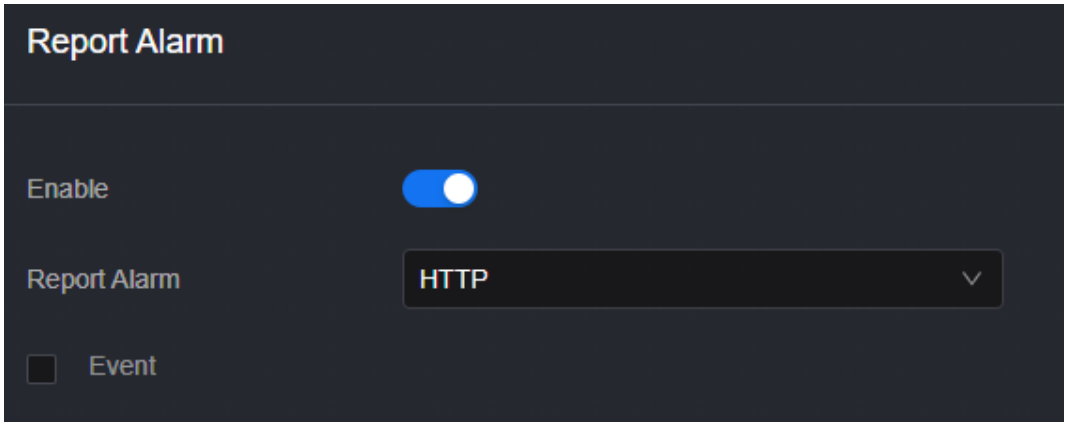
Once an alarm output interface is configured with a switching period and enabled, it can no longer be triggered by other alarm inputs.

Report Alarm

Enable and configure the alarm center in "4.4 Alarm Center".

Enable the function, click **Setting** to select the protocol type and event type, and then click **OK**. When the linkage is triggered, open the client on the alarm center. When the alarm is triggered, the client receives the alert.

Figure 3-11 Report alarm



Send command

After an alarm input is triggered and specific command actions are configured, the alarm box can use its HTTP command to link with or trigger other networked devices.

Click **Setting** to enter the command adding page, and then click **Add** to add the send command.

Figure 3-12 Send command

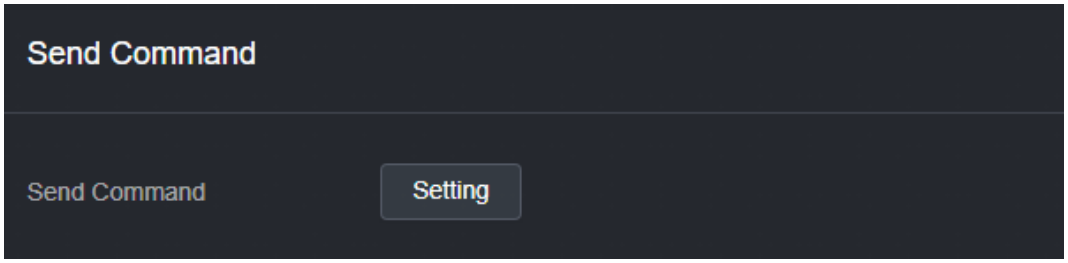
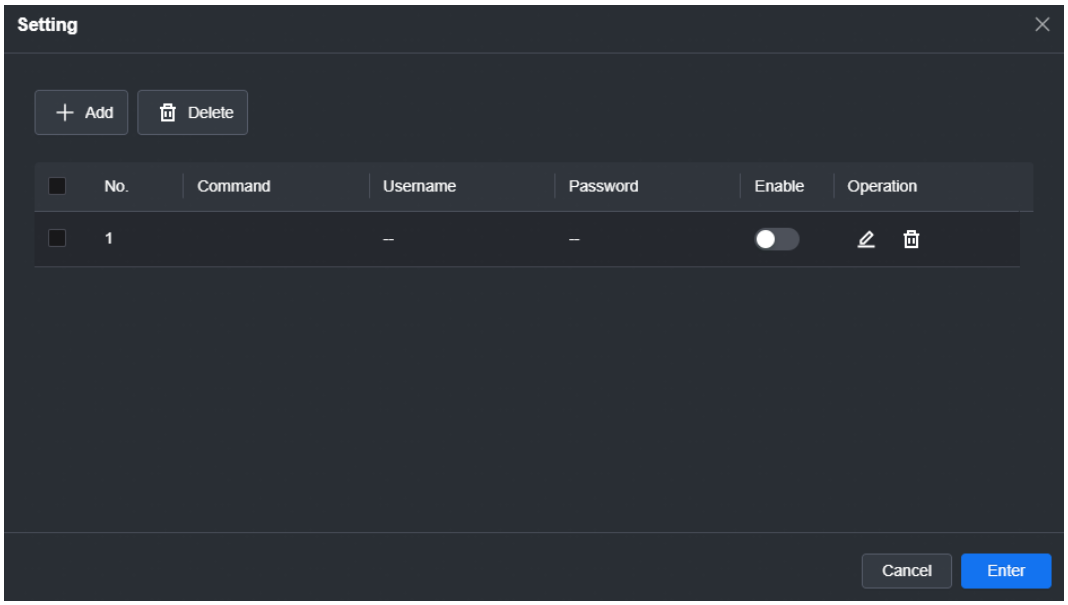
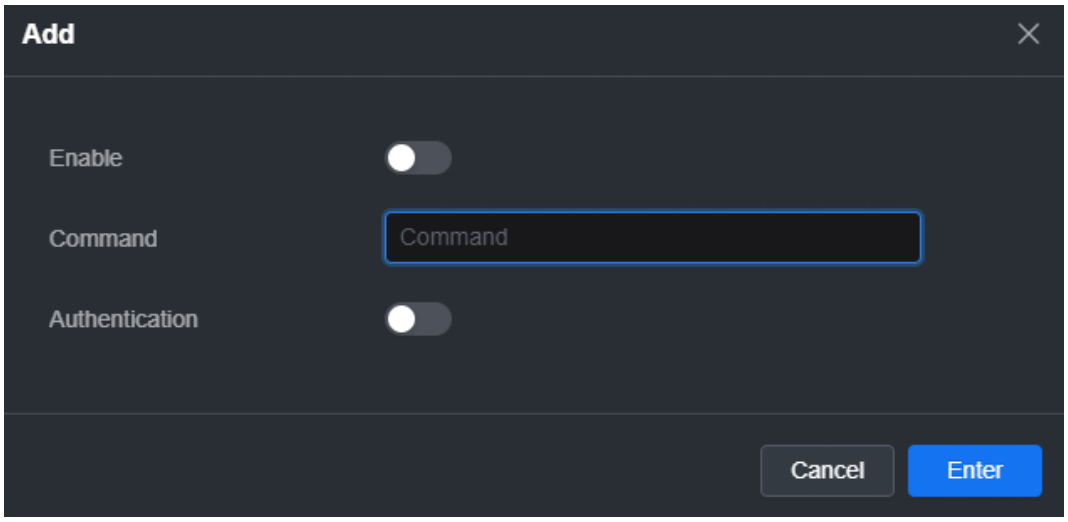


Figure 3-13 Send command settings



Enable the function, enter the command name. If the command requires authentication, you need to enter the username and password.

Figure 3-14 Add command



Supports configuring up to 50 commands; commands must follow the Dahua CGI format.

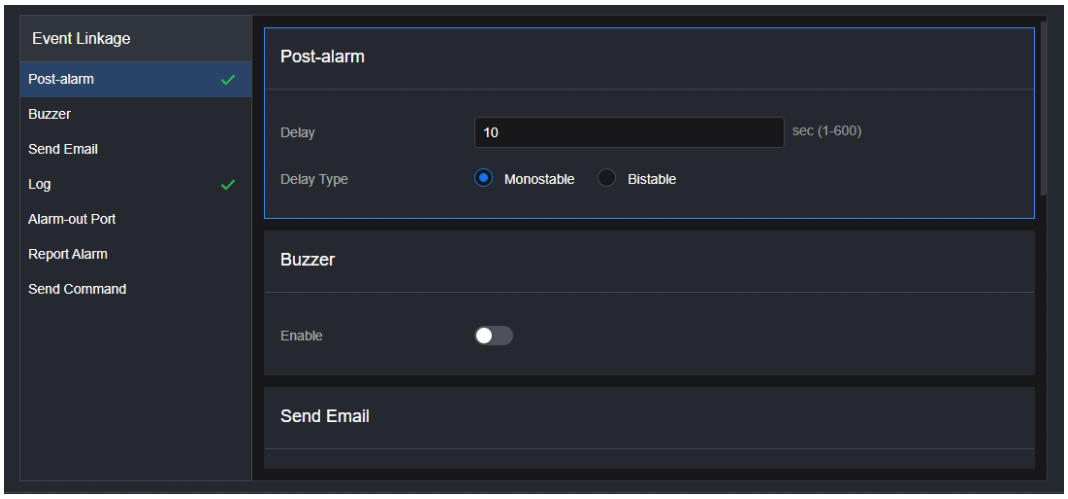
Post-alarm

In network alarms, you can configure two types of alarm trigger modes: **Monostable** and **Bistable**.

When you select **Monostable**, the alarm output will remain triggered upon receiving the trigger signal at the network alarm input and will automatically stop after the set the delay time.

When you select **Bistable**, the alarm output will remain triggered upon receiving the trigger signal at the network alarm input and will only stop after the set delay time once the network alarm input receives the stop signal.

Figure 3-15 Post-alarm



4 Network Settings

Set the basic network parameter information and network applications for the device.

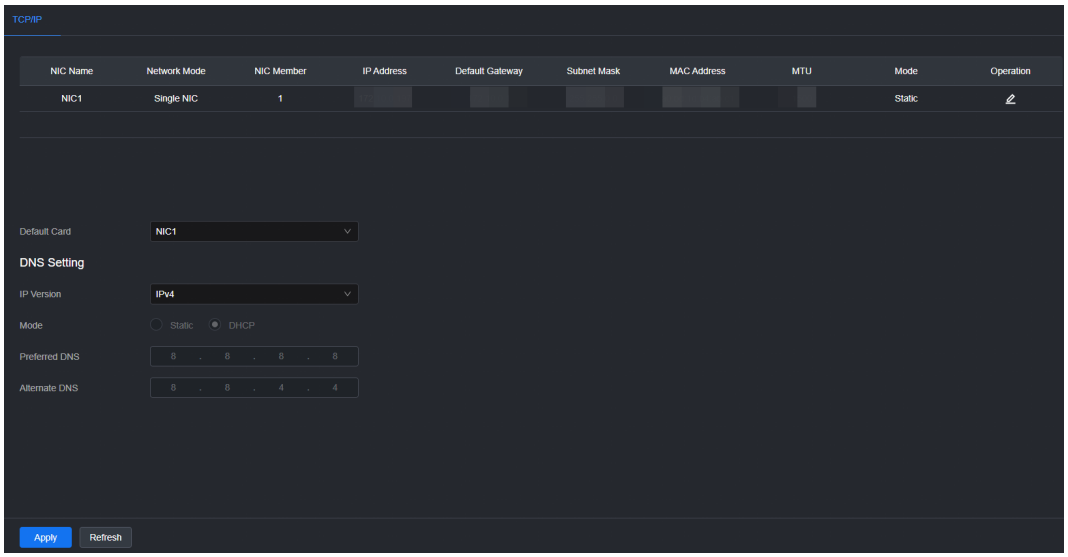
4.1 TCP/IP

You can configure the settings for the Device such as IP address, DNS according to the networking plan.

Procedure

Step 1 Log in to the webpage, select **SETTINGS** > **NETWORK** > **TCP/IP**.

Figure 4-1 TCP/IP



Step 2 Click  to configure the card, and then click **OK**.

Figure 4-2 TCP/IP

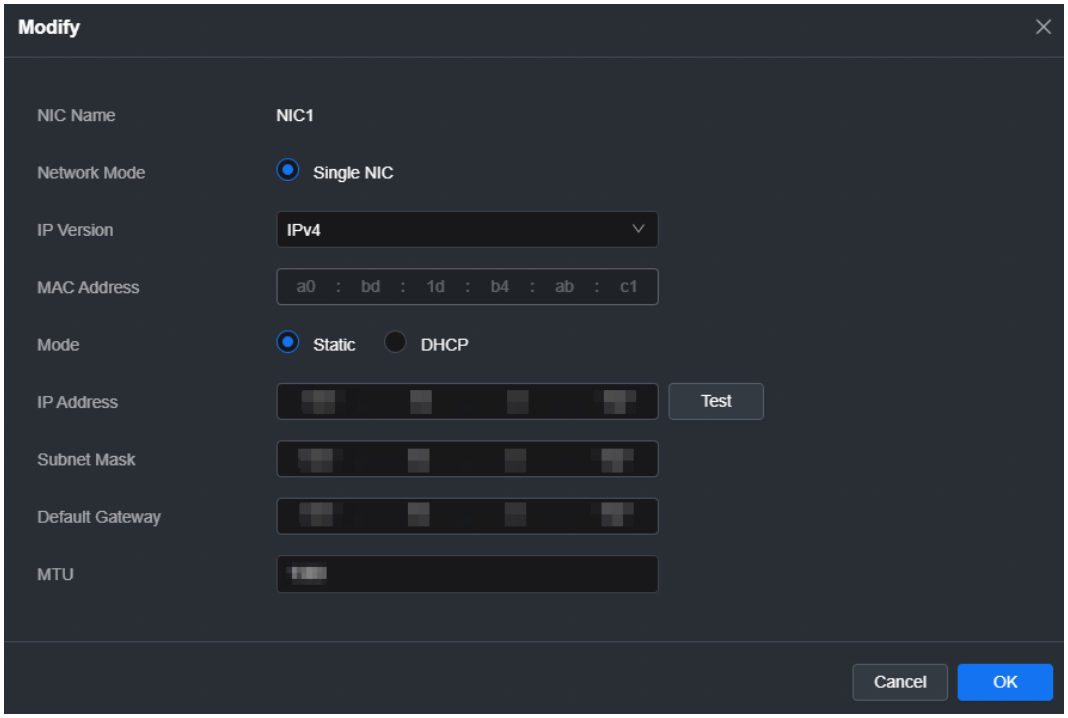


Table 4-1 TCP/IP parameters

Parameter	Description
Network Mode	**Single NIC** : The current NIC card works independently. If the current NIC card is disconnected, the Device becomes offline.
IP Version	Select IPv4 or IPv6. Both versions are supported for access.
MAC Address	Displays the MAC address of the Device.
DHCP	Enable the system to allocate a dynamic IP address to the Device. There is no need to set IP address manually. If you want to manually configure the IP information, disable the DHCP function first.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway. • The IP address and default gateway must be on the same network segment. • Click **Test** to check whether the IP address is available.
Subnet Mask	
Default Gateway	
MTU	Displays the MTU value of the NIC card.

Step 3 On the **TCP/IP** page, configure the DNS server.

- Obtain DNS server automatically.

When there is DHCP server on the network, you can enable **DHCP** so that the Device can automatically obtain a dynamic IP address.

- Configure DNS server manually.

  Select the IP version, and then enter the IP addresses of preferred and alternate DNS server.

Step 4 Click **Apply**.

4.2 Port

You can configure the maximum connection for accessing the device from webpage, platform, mobile phone or other clients at the same time, and then configure each port number.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **NETWORK** > **Port**.

Figure 4-3 Port



Step 2 Configure the parameters.

Table 4-2 Description of port parameters

Parameter	Description
Max Connection	The allowable maximum clients accessing the Device at the same time, such as web client and platform.
TCP Port	Transmission control protocol port. Enter the value according to your actual situation.
UDP Port	User datagram protocol port. Enter the value according to your actual situation.
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you change the HTTP port number to, for example, 70, then you need to enter 70 after the IP address when logging in to the Device through the browser.
HTTPS Port	HTTPS communication port. The default value is 443. You can enter the value according to your actual situation.

Parameter	Description
NTP Server Port	Network Time Protocol Server Port. The default value setting is 123. You can enter the value according to your actual situation.

Step 3 Click **Apply**.

4.3 Email

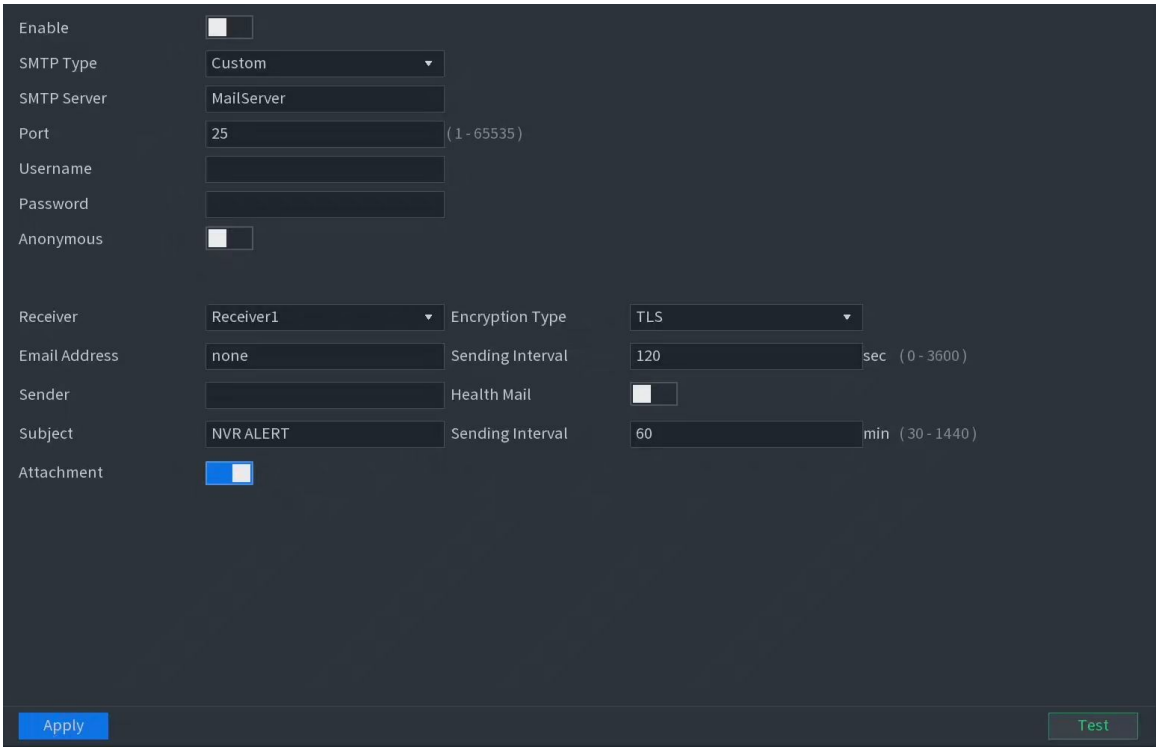
You can configure the email settings to enable the system to send the email as a notification when an alarm event occurs.

Procedure

Step 1 Log in to the main menu, and then select **SETTINGS** > **NETWORK** > **Email**.

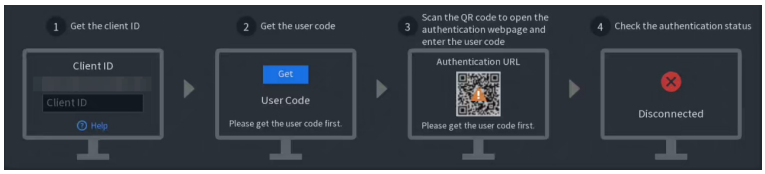
Step 2 Click  to enable the function.

Figure 4-4 Email settings



Step 3 Configure the Email parameters.

Table 4-3 Descriptions of Email parameters

Parameter	Description
SMTP Type	You can select **Custom** , **Gmail**, **Outlook**, and **Yahoo**. When configuring Outlook, follow the on-screen instructions to obtain the client ID and user code. 

Parameter	Description
SMTP Server	Enter the address of SMTP server of sender's email account.
Port	Enter the port of SMTP server. The default value is 25.
Username	Enter the username and password of sender's email account.
Password	
Anonymous	Enable anonymous login.
Receiver	Select the receiver to receive the notification. You can select up to three receivers.
Email Address	Enter the email address of mail receivers.
Sender	Enter the sender's email address. You can enter up to three senders separated by comma.
Subject	Enter the email subject. You can enter Chinese, English and numerals with the length limited to 64 characters.
Encryption Type	Select the encryption type from **NONE** , **SSL**, or **TLS**. For SMTP server, the default encryption type is **TLS**.
Sending Interval (Sec.)	Set the interval at which the system sends an email for the same type of alarm event to avoid excessive pileup of emails caused by frequent alarm events. The value ranges from 0 to 3600. 0 means that there is no interval.
Health Mail	Enable the health test function. The system can send a test email to check the connection.
Sending Interval	Set the interval at which the system sends a health test email. The value ranges from 30 to 1440. 0 means that there is no interval.
Attachment	After you enable **Attachment**, when an alarm occurs, the system can send alarm-triggered snapshots.
Test	Click **Test** to test the email sending function. If the configuration is correct, the receiver's email account will receive the email. Before testing, click **Apply** to save the settings.

Step 4 Click **Apply**.

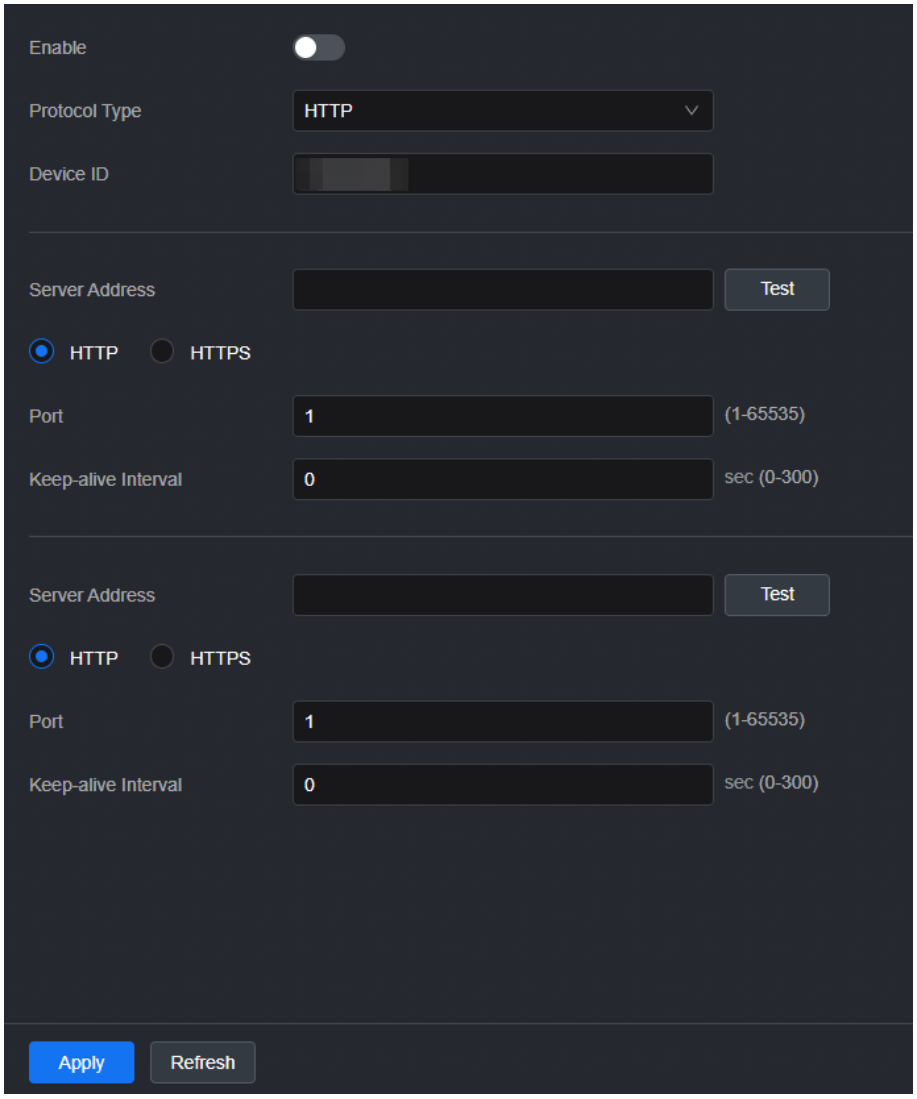
4.4 Alarm Center

You can configure the alarm center server to receive the uploaded alarm information.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **NETWORK** > **Alarm Center**.

Figure 4-5 Alarm center



Step 2 Enable the function, and then select a protocol type.

You can select **Private Protocol** or **HTTP**.

Step 3 Configure the parameters.

When selecting **HTTP** , you need to enter the server address, port, and then select **HTTP** or **HTTPS** as needed.

Table 4-4 Alarm center parameters

Parameter	Description
Server Address	The IP address and communication port of the computer installed with alarm client.
Port	
Keep-alive Interval	Enter the keep-alive interval maintaining connection between the Device and the server.

Step 4 Click **Apply**.

5 System Settings

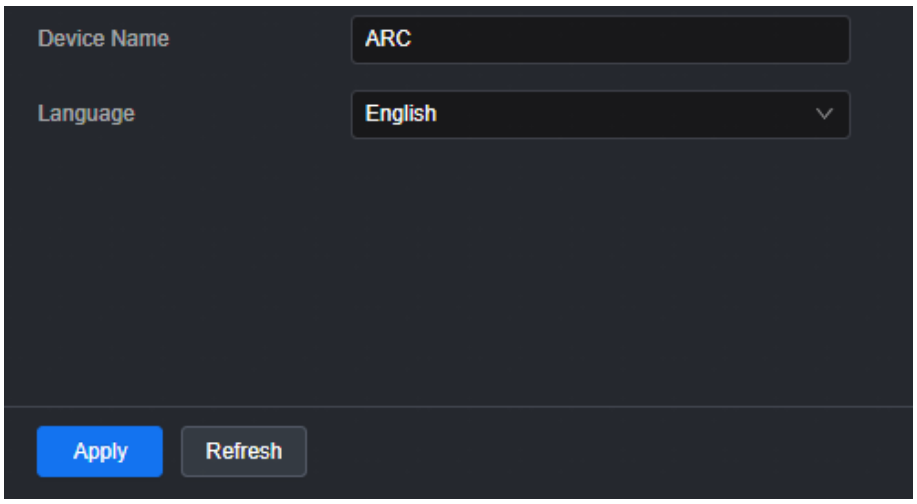
5.1 Basic Settings

You can set device basic information including the device name and language.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **General** > **Basic**.

Figure 5-1 Basic settings



Step 2 Configure parameters.

Table 5-1 Basic parameters

Parameter	Description
Device Name	Enter the Device name.
Language	Select a language for the Device system.

Step 3 Click **Apply** button to save settings.

5.2 Time

5.2.1 Date and Time

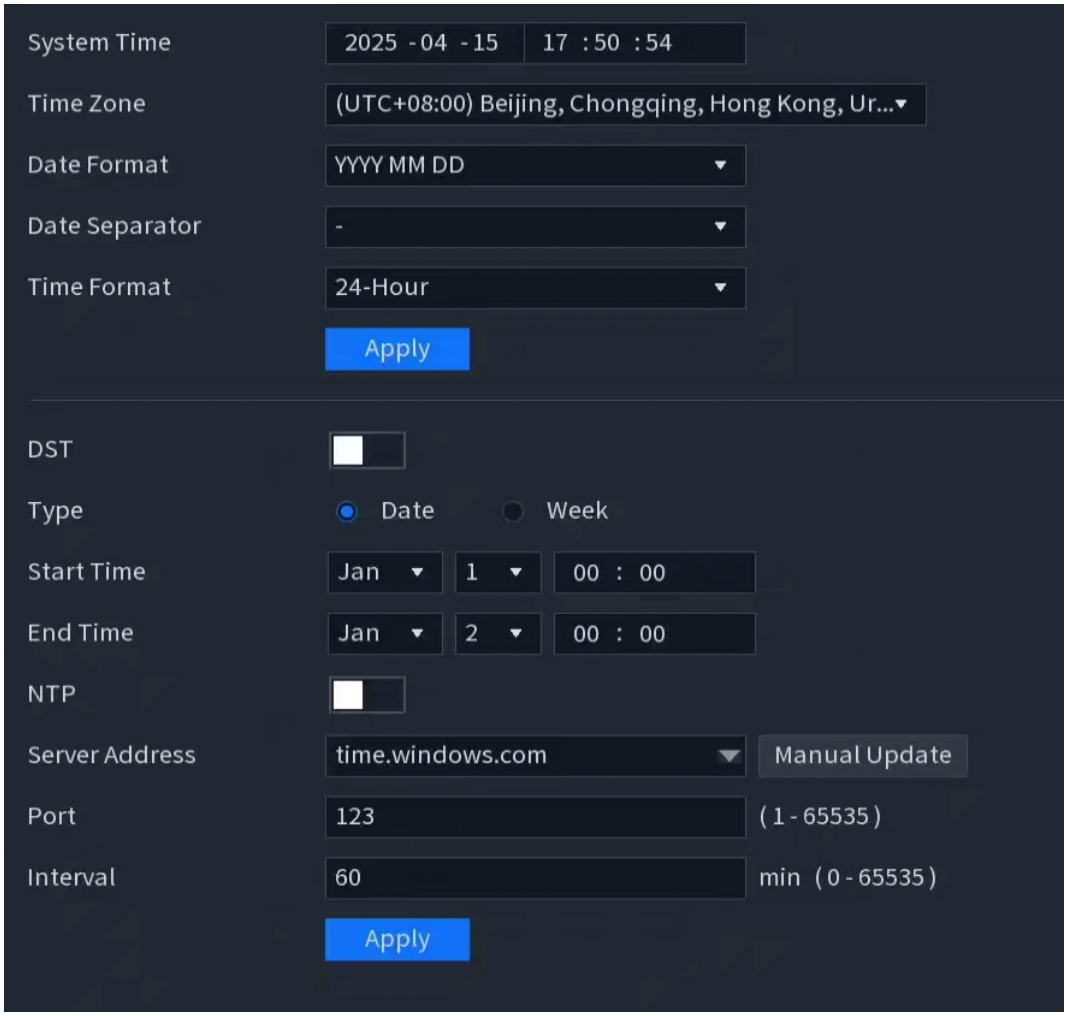
You can set device time. You can enable NTP (Network Time Protocol) function so that the device can sync time with the NTP server.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Time** > **Date&Time**.

Step 2 Click **Date&Time** tab.

Figure 5-2 Date and time



Step 3 Configure the settings for date and time parameters.

Table 5-2 Description of data and time parameters

Parameter	Description
System Time	In the **System Time** box, enter time for the system. After clicking the time zone list, you can select a time zone for the system, and the time will adjust automatically. ⚠ Do not change the system time randomly; otherwise the recorded video cannot be searched. It is recommended to avoid the recording period or stop recording first before you change the system time.
Time Zone	In the **Time Zone** list, select a time zone for the system.
Date Format	In the **Date Format** list, select a date format for the system.
Date Separator	In the **Date Separator** list, select a separator style for the date.
Time Format	In the **Time Format** list, select **12-HOUR** or **24-HOUR** for the time display style.

Parameter	Description
DST	Enable the Daylight Saving Time function. Click **Week** or **Date**.
Type	
Start Time	Configure the start time and end time for the DST.
End Time	
NTP	Enable the NTP function to sync the Device time with the NTP server. If NTP is enabled, device time will be automatically synchronized with server.
Server Address	In the **Server Address** box, enter the IP address or domain name of the corresponding NTP server. You can directly select **time.windows.com** or **time.google.com**. Click **Manual Update**, the Device starts syncing with the server immediately.
Port	The system supports TCP protocol only and the default setting is 123.
Interval	In the **Interval** box, enter the amount of time that you want the Device to sync time with the NTP server. The value ranges from 0 to 65535.

Step 4 Click **Apply** to save the settings.

5.2.2 Holiday

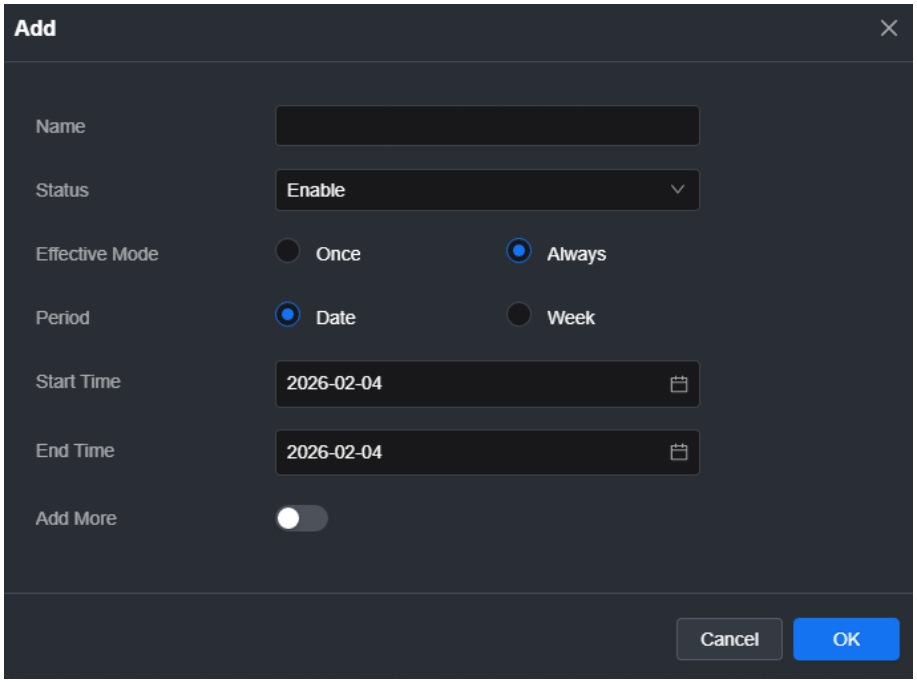
Here you can add, edit, and delete holiday. After you successfully set holiday information, you can view holiday item on the record and snapshot period.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Time** > **Holiday**.

Step 2 Click **Add** to add the holiday.

Figure 5-3 Add holiday



Step 3 Configure holiday name, status, effective mode, period, start time and end time.

Click **Add more** to add new holiday information.

Step 4 Click **OK**, you can add the current holiday to the list.

- Select **Enable** or **Close**, and you can enable or disable the holiday.
- Click to change the holiday information. Click to delete current date.

Step 5 Click **Next** to save settings.

5.3 Account

You can manage users, user group, and security email.

5.3.1 User

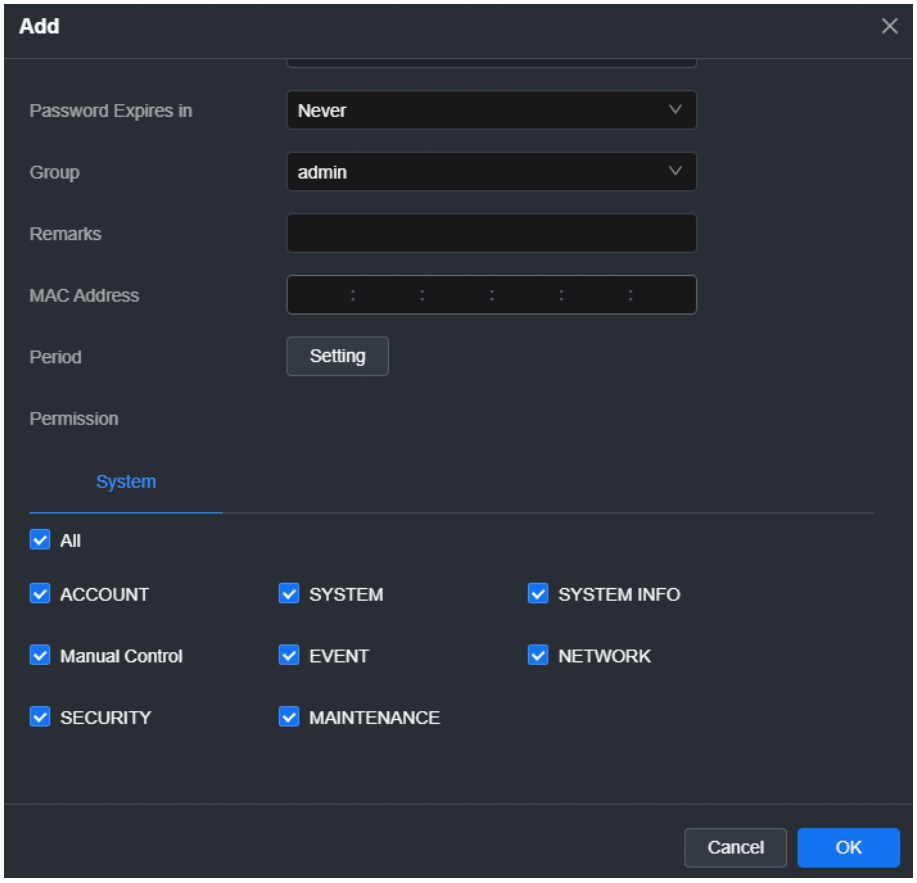
5.3.1.1 Adding User

Procedure

Step 1 Log in to the main menu, select **Main Menu** > **SETTINGS** > **SYSTEM** > **Account** > **User**.

Step 2 Click **Add**.

Figure 5-4 Add user



Step 3 Configure the parameters.

Table 5-3 Parameters of adding user

Parameter	Description
Username	Enter a username and password for the account.
Password	
Confirm Password	Enter the password again to confirm it.
Remarks	Optional. Enter a description of the account.
User MAC	Enter user MAC address.
Group	Select a group for the account. The user rights must be within the group permissions.
Period	Click **Setting** to define a period during which the new account can log in to the Device. The new account cannot access the device during other periods.
Password Expires in	Select a period that password expires and until that time, a new password is required.

Parameter	Description
Permission	Select the checkboxes to grant permissions to the user. To manage the user account easily, when defining the user account permission, do not give the authority to the common user account higher that the advanced user account.

Step 4 Click **OK**.

Click to modify the corresponding user information, click to delete the user.

5.3.1.2 Modifying Password

We recommend you change the password regularly to enhance device security.

Background Information

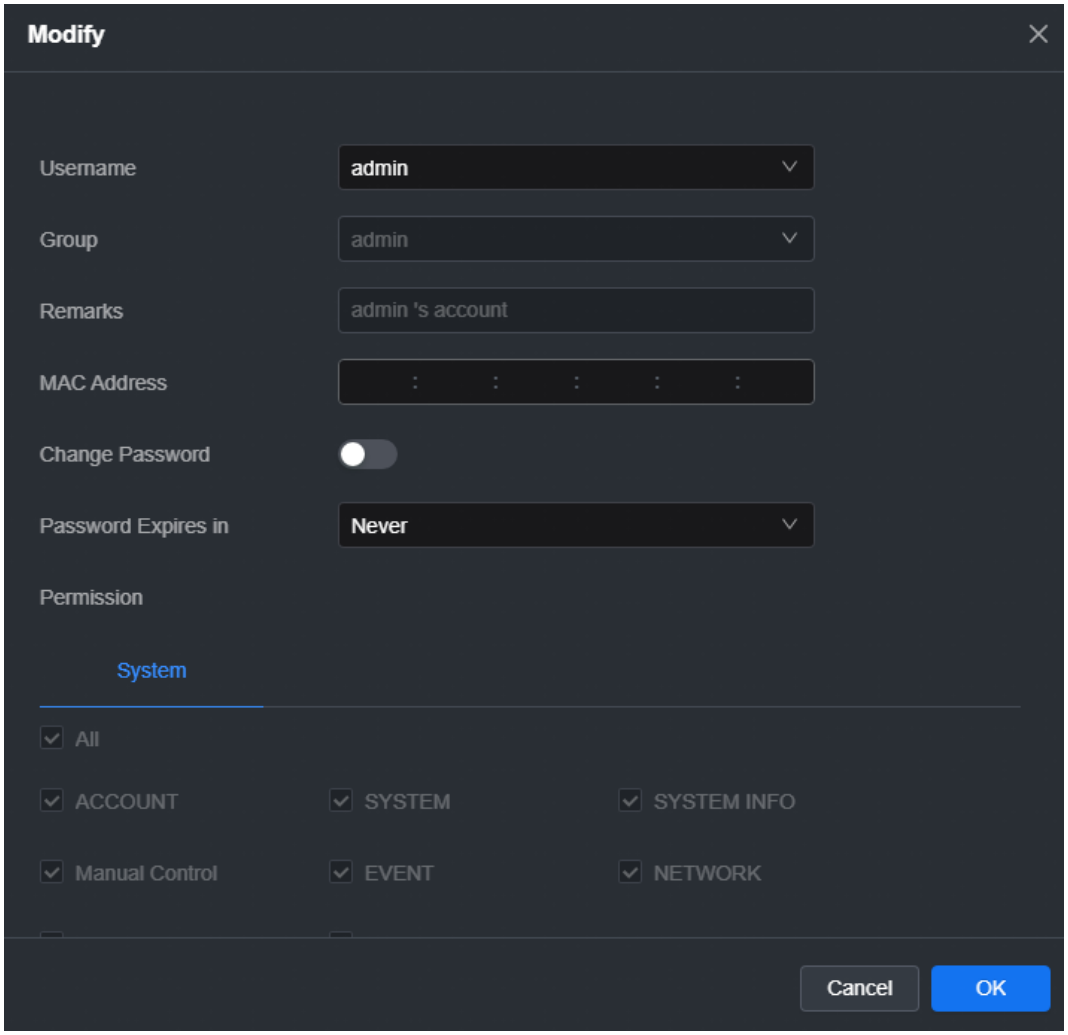
Users with account permissions can change the password of other users.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Account** > **User**.

Step 2 Click of the corresponding user.

Figure 5-5 Modify Password



Step 3 Click  to enable the modify password function.

Step 4 Enter old password and then enter new password twice.

- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).
- For your device security, create a strong password.

Step 5 Modify user's permission.

Select **System** to rearrange user's permissions.

Step 6 Click **OK**.

5.3.2 Group

The accounts of the Device adopt two-level management modes: user and user group. Every user must belong to one group, and only one group.

Background Information

The **admin** and **user** group are two default user groups that cannot be deleted. You can add more groups and define corresponding permissions.

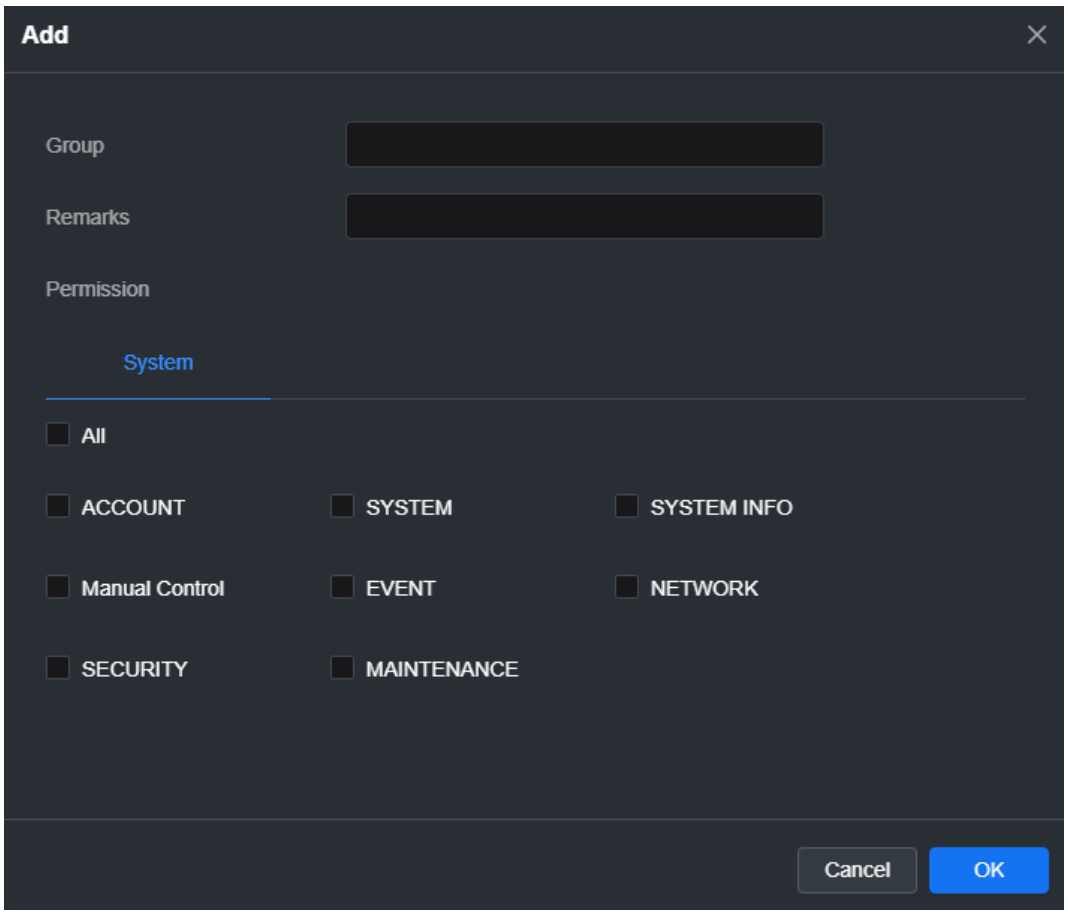
Procedure

Step 1 Log in to the main menu, select **Main Menu** > **SETTINGS** > **SYSTEM** > **Account** > **Group**.

Step 2 Click **Add**.

Step 3 Enter the group name, and then enter some remarks if necessary.

Figure 5-6 Add group



Step 4 Select the checkboxes to select permissions.

Step 5 Click **OK**.

Click  to modify the corresponding group information and click  to delete the group.

5.3.3 Password Reset

Enable the password reset function and configure the linked email address that is used to reset the password.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Account** > **Password Reset**.

Step 2 Enter an email address to receive the security code used to reset the password.

- The password reset function is enabled by default.

- The email address cannot be empty.

Step 3 Click **Apply**.

5.4 Security

5.4.1 Security Status

Security scanning helps get a whole picture of device security status. You can scan user, service and security module status for detailed information on the security status of the device.

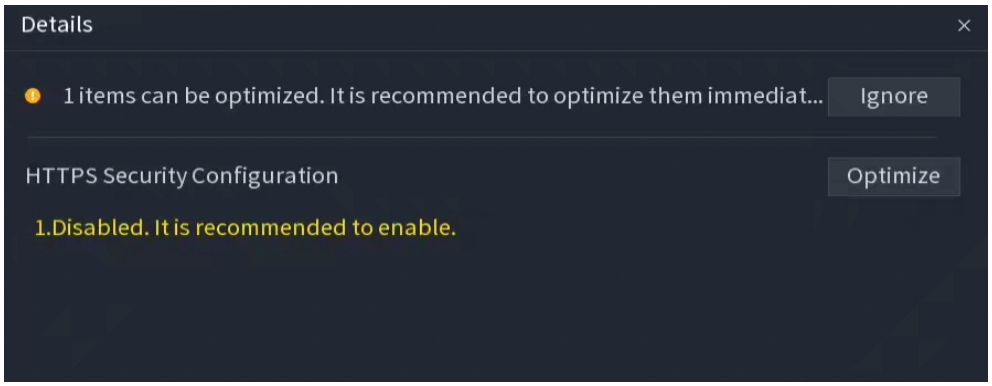
Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **System Service** > **System Status** to view the security status.

Detecting User and Service

The green icon represents a healthy status of the scanned item, and orange icon represents a risky status.

- Login authentication: When there is a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.
- Configuration Security: When there is a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.

Figure 5-7 Details



Scanning Security Modules

This area shows the running status of security modules. For details about the security modules, point to the icon to see the on-screen instructions.

Re-scanning Security Status

You can click **Rescan** to scan security status.

5.4.2 System Service

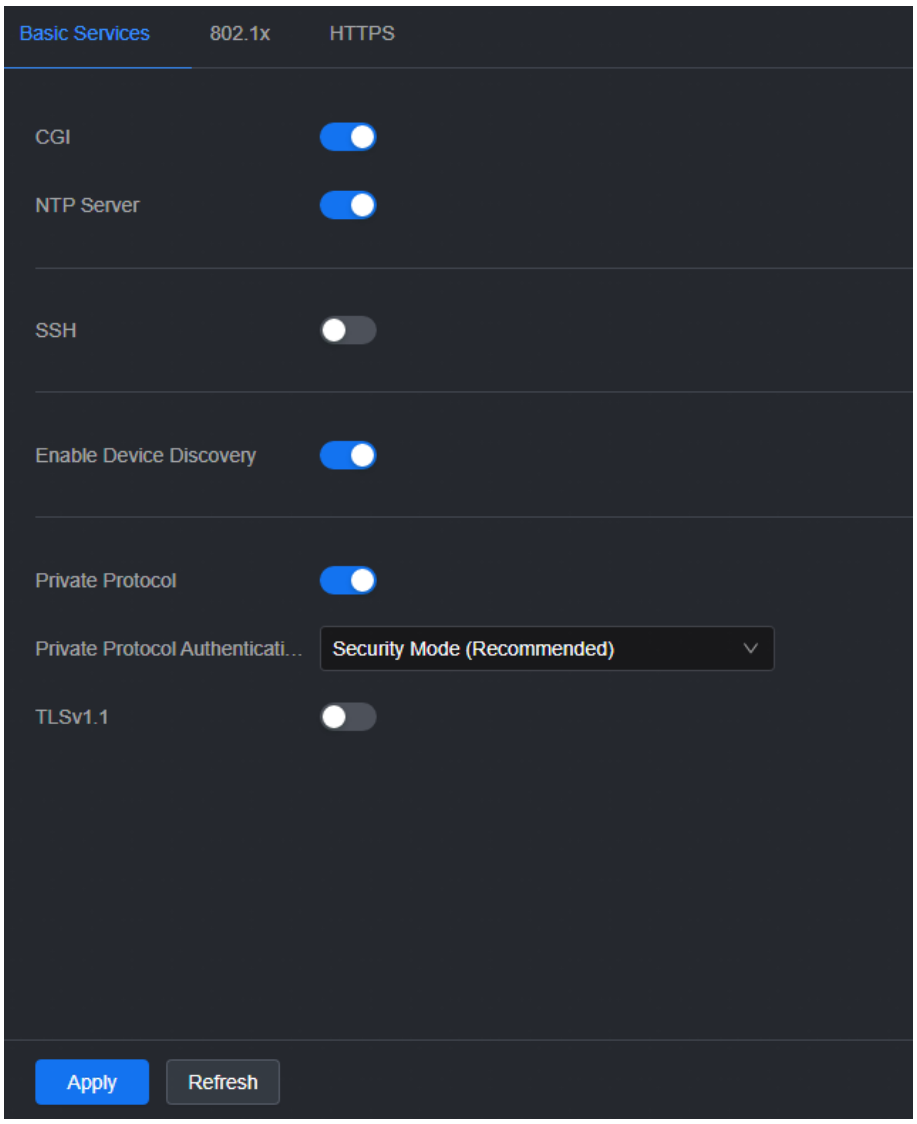
You can set the alarm box's basic information such as basic services, 802.1x and HTTPS.

5.4.2.1 Basic Services

Procedure

Step 1 Log in to the main menu, select **SYSTEM** > **Security** > **System Service** > **Basic Services**.

Figure 5-8 Basic services



Step 2 Enable the system services.

There might be safety risk when **CGI**, **SSH** and **NTP Server** is enabled. Disable these functions when they are not needed.

Table 5-4 Basic service parameters

Parameter	Description
CGI	If this function is enabled, the remote devices can be used to issue commands through the CGI protocol. This function is enabled by default.

Parameter	Description
NTP Server	After this function is enabled, a NTP server can be used for time synchronization. This function is enabled by default.
SSH	After this function is enabled, you can use SSH service. This function is disabled by default.
Enable Device Discovery	After this function is enabled, the alarm box can be found by other devices through searching.
Private Protocol Authentication Mode	• Security Mode (Recommended): Uses Digest access authentication when connecting to the alarm box. • Compatible Mode: Select this mode when the client does not support Digest access authentication.
TLSv1.1	Enable the TLSv1.1 encryption protocol.

Step 3 Click **Apply**.

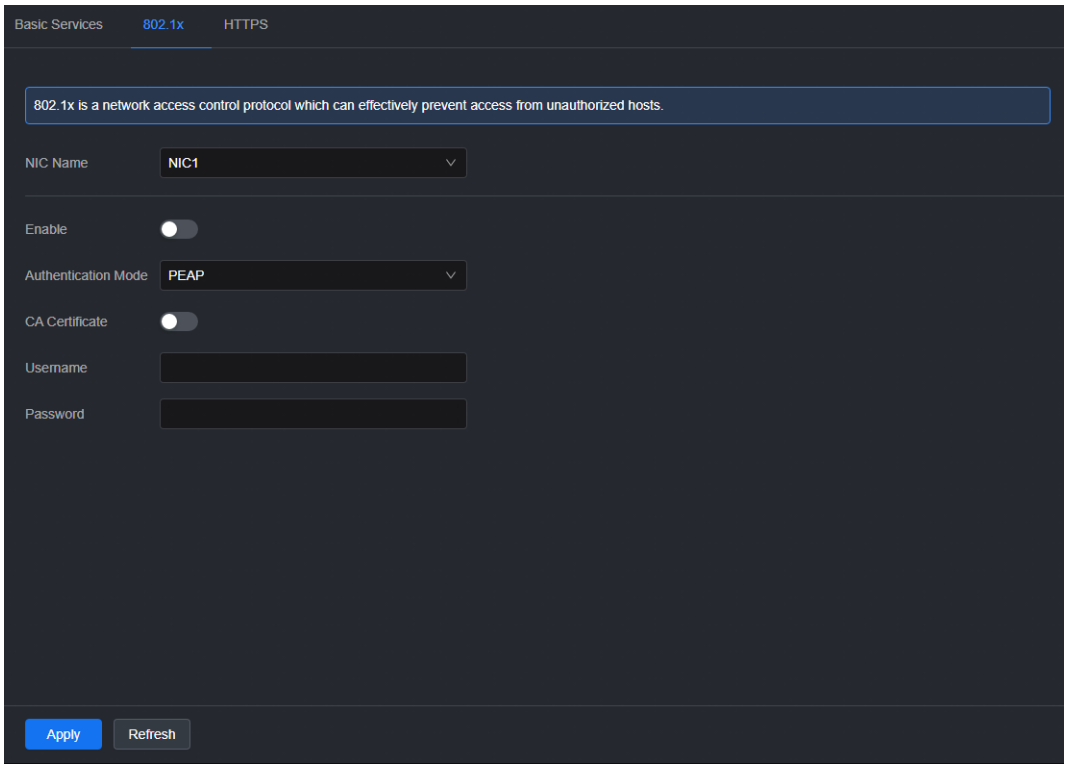
5.4.2.2 802.1x

The Device needs to pass 802.1x certification to enter the LAN.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **System Service** > **802.1x**.

Figure 5-9 802.1x



Step 2 Select the Ethernet card you want to certify.

Step 3 Select **Enable** and configure parameters.

Table 5-5 802.1x parameters

Parameter	Description
Authentication Mode	• PEAP: protected EAP protocol. • TLS: Transport Layer Security. Provide privacy and data integrity between two communications application programs.
CA Certificate	Enable it and click **Browse** to import CA certificate from flash drive. For details of creating certificates, see "5.4.4 CA Certificate".
Username	The username shall be authorized at server.
Password	Password of the corresponding username.

Step 4 Click **Apply**.

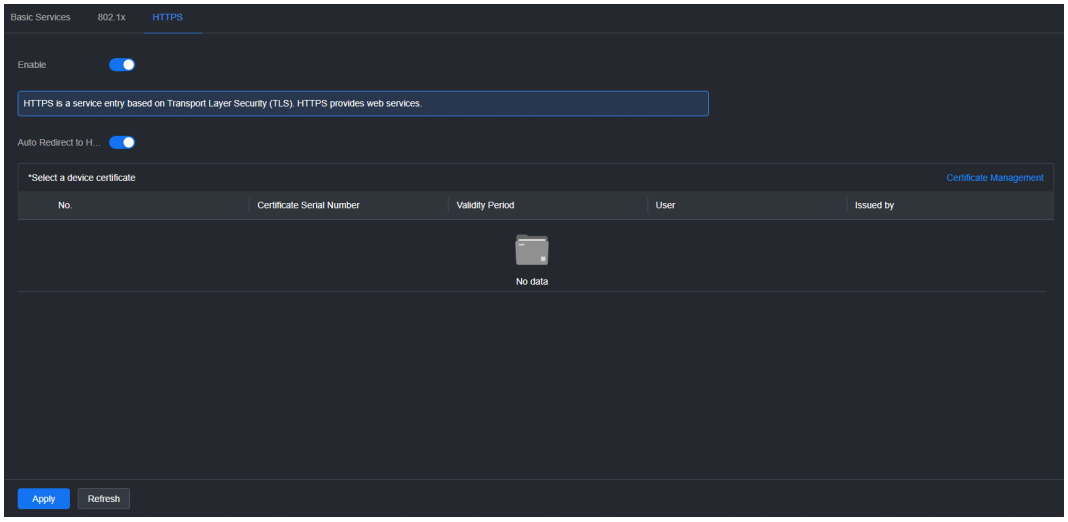
5.4.2.3 HTTPS

We recommend you enable HTTPS function to enhance system security.

Procedure

Step 1 Log in to the main menu, select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **System Service** > **HTTPS**.

Figure 5-10 HTTPS



Step 2 Enable HTTPS function.

Step 3 (Optional) Enable **Auto Redirect to HTTPS** to redirect to HTTPS automatically.

Step 4 Click **Certificate Management** to create or import a HTTPS certificate from the web. For details about importing or creating a CA certificate, see "5.4.4 CA Certificate".

Step 5 Select a HTTPS certificate.

Step 6 Click **Apply**.

5.4.3 Attack Defense

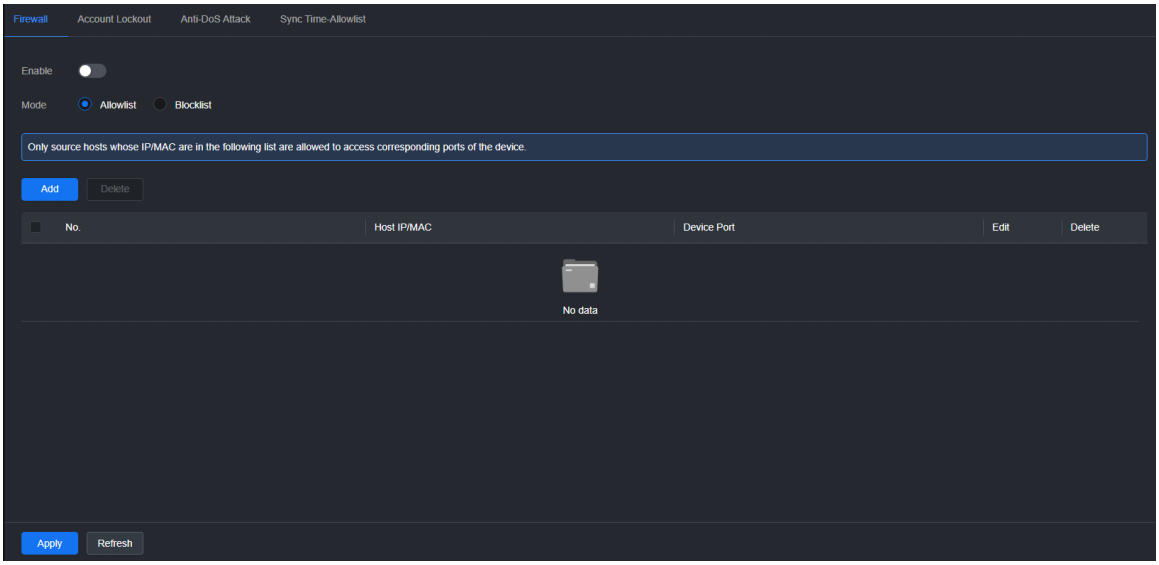
5.4.3.1 Firewall

You can configure the hosts that are allowed or prohibited to access the Device.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **Attack Defense** > **Firewall**.

Figure 5-11 Firewall



Step 2 Click  to enable the firewall.

Step 3 Select a firewall mode.

- **Allow List** : The hosts on the allowlist can access the Device.
- **Block List** : The hosts on the blocklist are prohibited to access the Device.

Step 4 Click **Add** and then select a type for the allowlist or blocklist.

You can allow or prohibit hosts through a specific IP address, a network segment, or a MAC address.

- IP address.

  Enter the IP address, start port and end port, and then click **OK**.
- IP segment.

  Enter the start address and end address, starting port and ending port, and then click **OK**.
- MAC address.

  Enter the MAC address, and then click **OK**.

Step 5 Click **Apply**.

5.4.3.2 Account Lockout

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **Attack Defense** > **Account Lockout**.

Figure 5-12 Account lockout



Step 2 Configure parameters.

Table 5-6 Account lockout parameters

Parameter	Description
Login Attempt(s)	Set the maximum number of allowable wrong password entries. The account will be locked after your entries exceed the maximum number.
Lock Time	Set how long the account is locked for.

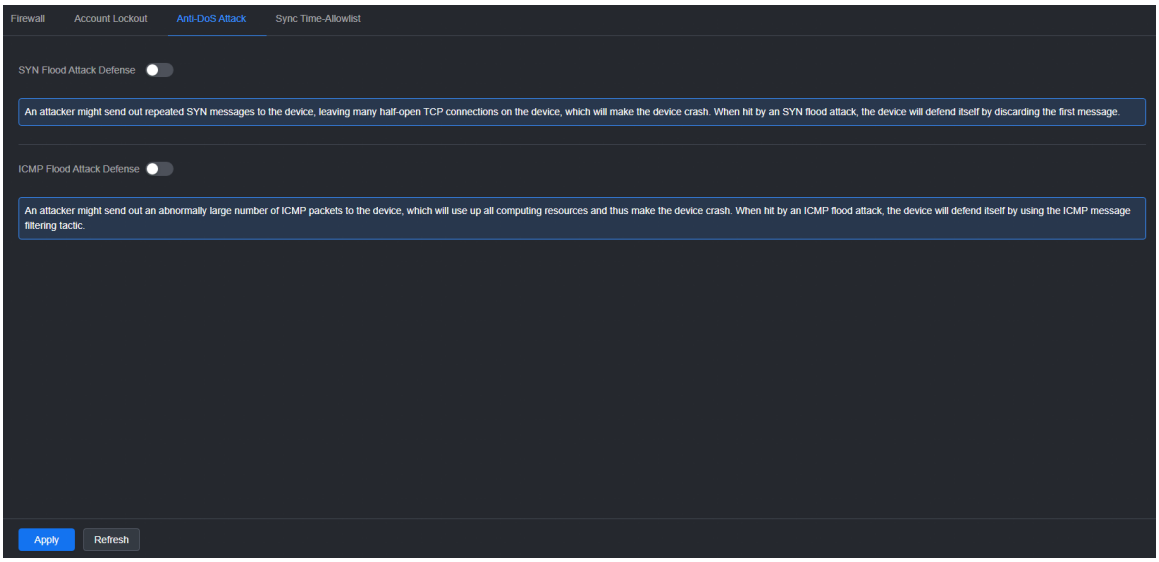
Step 3 Click **Apply**.

5.4.3.3 Anti-DoS Attack

Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **Attack Defense** > **Anti-DoS Attack**.

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attack.

Figure 5-13 Anti-Dos attack



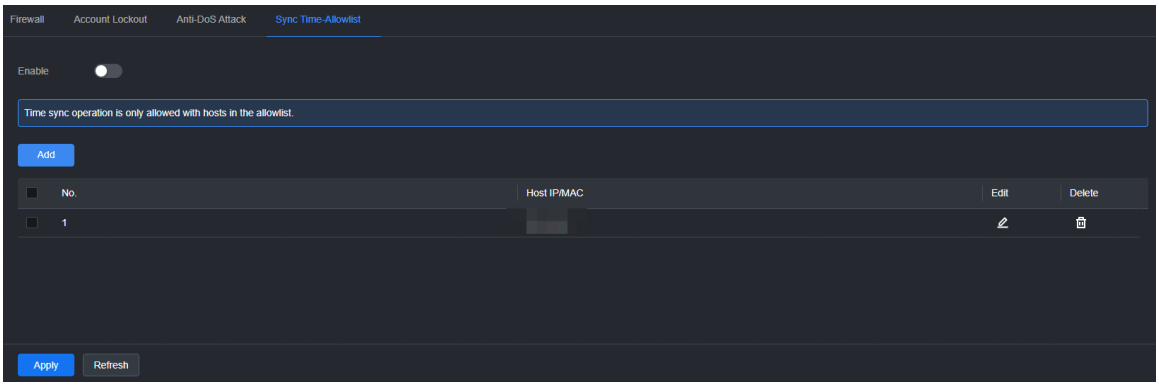
5.4.3.4 Sync Time-Allowlist

You can configure which hosts are allowed to synchronize time with the Device.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **Attack Defense** > **Sync Time-Allowlist**.

Figure 5-14 Sync time-allowlist



Step 2 Click  to enable the function.

Step 3 Click **Add** to add trusted hosts for time synchronization.

- If you set **Type** to **IP Address**, enter the IP address, and then click **OK**.
- If you set **Type** to **IP Segment**, enter the start address and end address, and then click **OK**.

Step 4 Click **Apply**.

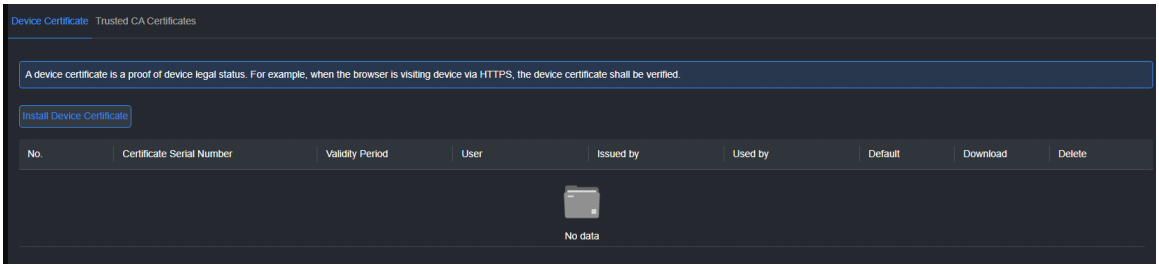
5.4.4 CA Certificate

5.4.4.1 Device Certificate

Procedure

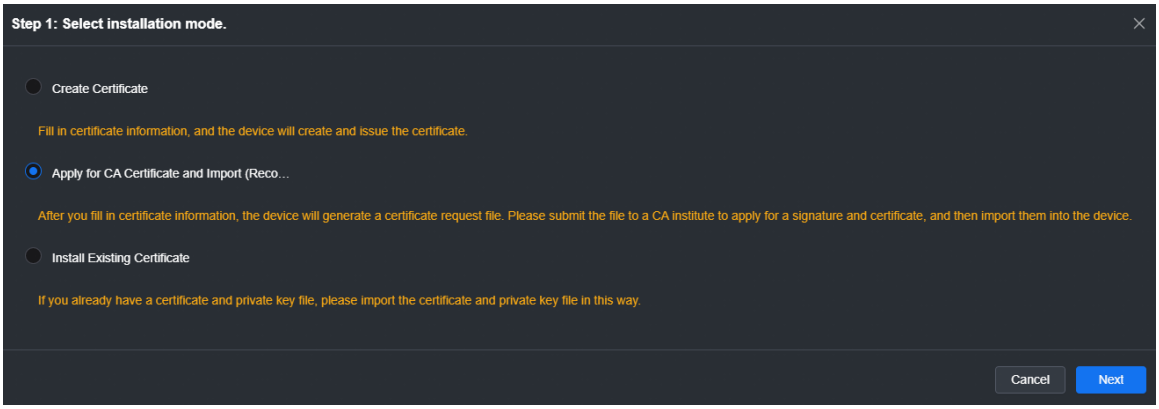
Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **CA Certificate** > **Device Certificate**.

Figure 5-15 Device certificate



Step 2 Click **Install Device Certificate** to select the installation mode.

Figure 5-16 Select installation mode



- Create certificate manually
  1. Select **Create certificate**.
  2. Fill in certificate information.
  3. Click **Create and install certificate**.
- Apply for a CA certificate and import it (recommended)
  1. Select **Apply for CA Certificate and Import (Recommended)**.
  2. Fill in certificate information.
  3. Click **Create** to save the certificate request file to the backup device.
  4. Use the request file to apply for a certificate from a third-party CA.
  5. Import the certificate.
- Install the existing certificate
  1. Select **Install Existing Certificate**.
  2. Select the file path and enter the private key and password.
  3. Click **Import**.

- Click to download the certificate.
- Click to delete the certificate.

Deleted certificates cannot be recovered, please proceed with caution when deleting.

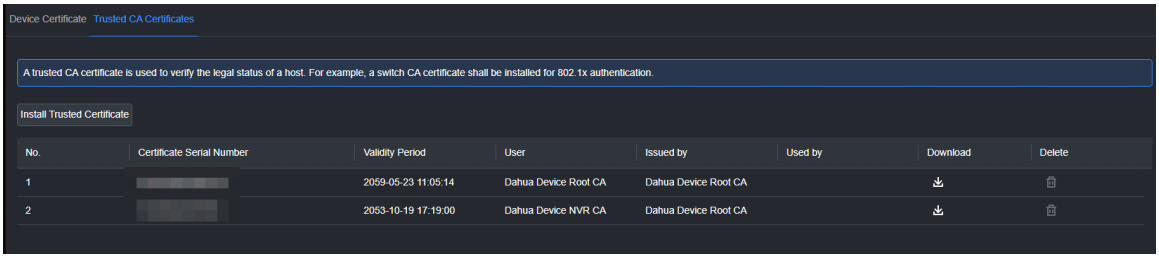
Once the certificate is created, you can view the created certificate in the **Device Certificate** page.

5.4.4.2 Trusted CA Certificates

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **CA Certificate** > **Trusted CA Certificates**

Figure 5-17 Trusted CA certificates



Step 2 Click **Install Trusted Certificate**.

Step 3 Click **Browse** to select the certificate that you want to install.

Step 4 Click **Import**.

5.4.5 Security Warning

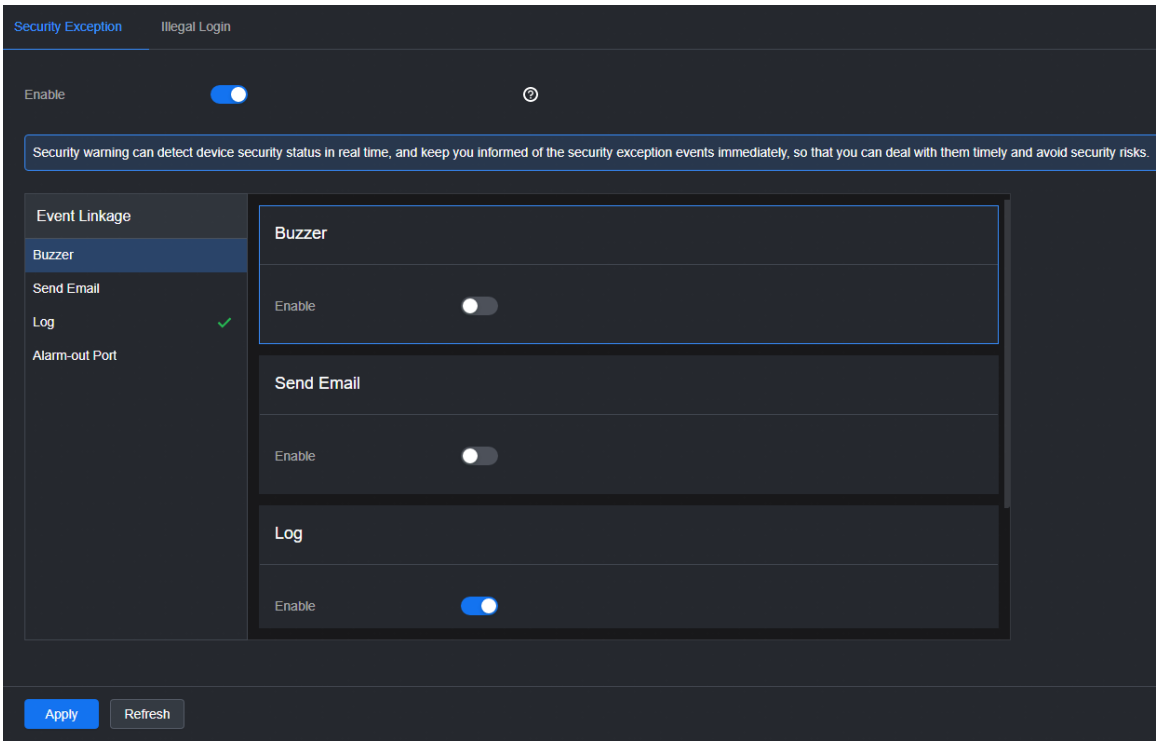
5.4.5.1 Security Exception

The device gives warnings to the user when a security exception occurs.

Procedure

Step 1 Log in to the main menu, select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Security Warning** > **Security Exception**.

Figure 5-18 Security exception



Step 2 Click  to enable the function.

Click  to view the list of security exception events.

Step 3 Configure alarm linkage. For details, see "3.2 Event Linkage".

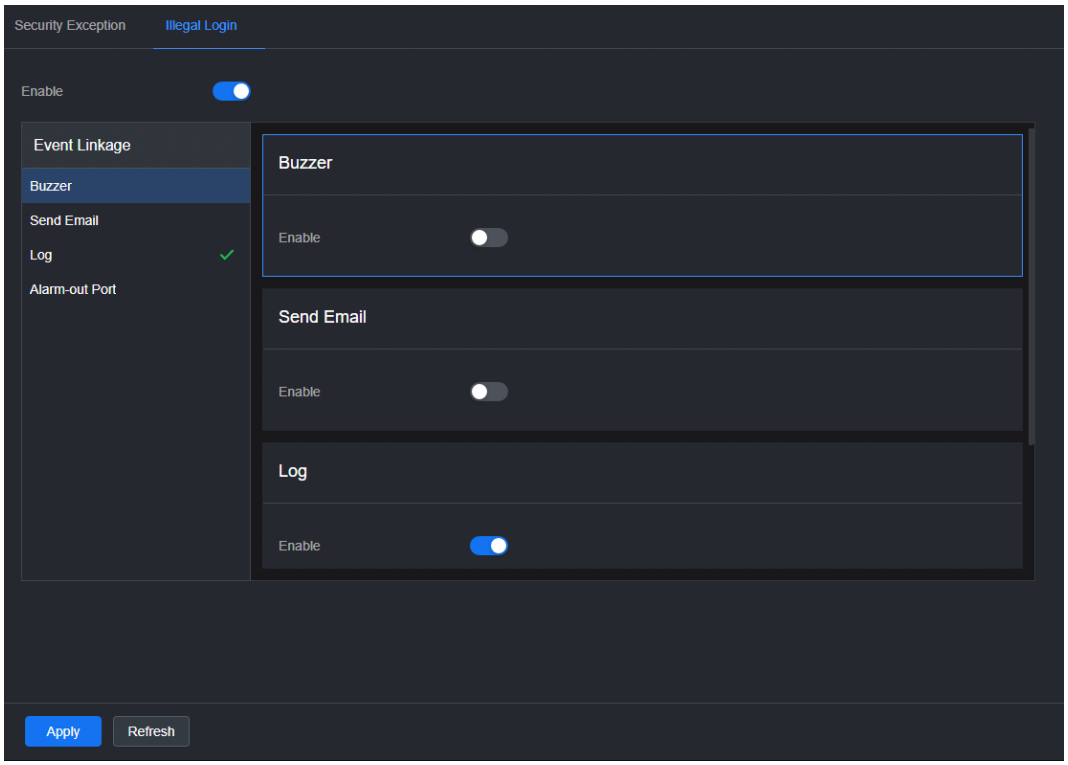
Step 4 Click **Apply**.

5.4.5.2 Illegal Login

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **SYSTEM** > **Security** > **Security Warning** > **Illegal Login**.

Figure 5-19 Illegal login



Step 2 Click  to enable the function.

Step 3 Configure alarm linkage. For details, see "3.2 Event Linkage".

Step 4 Click **Apply**.

5.4.6 Security Authentication

Select the digest algorithm for authentication you wish to use on the current page.

Procedure

Step 1 Log in to the main menu, select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Security Authentication** > **Digest Algorithm for Authentication**.

Step 2 Click **Apply**.

6 Searching Events and the History

6.1 Searching Real-Time Events

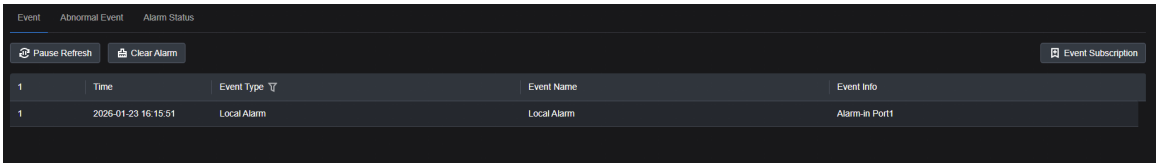
In the main menu, select **APPLICATIONS** > **EVENT CENTER** > **Real-Time Events**.

- **Refresh/Pause Refresh** : Enable real-time refresh or pause real-time refresh recording.
- **Clear Alarm** : Clear the alarm records of the current page.
- **Event Subscription** : Click to select the subscribed events; only the subscribed events will display records.

Event

1. Click **Event** to view the event history.
2. Click the event and view the event replay records on the right side.

Figure 6-1 View alarm events



Abnormal Event

Click **Abnormal Event** to view the event records.

Alarm Status

Click **Alarm Status** to view the event information.

6.2 Searching Event History

Procedure

Step 1 In the main menu, select **APPLICATIONS** > **EVENT CENTER** > **Event History**.

Step 2 Select the event type.

- **All** : Search all events of the Device.
- **Abnormal Event** : Search the Device's own abnormal events, such as network disconnection.
- **Alarm Event** : Search all alarms, local alarm events and network alarm events.

Step 3 Select the searching type. You can select **All** , **Local Alarm**, and **Network**.

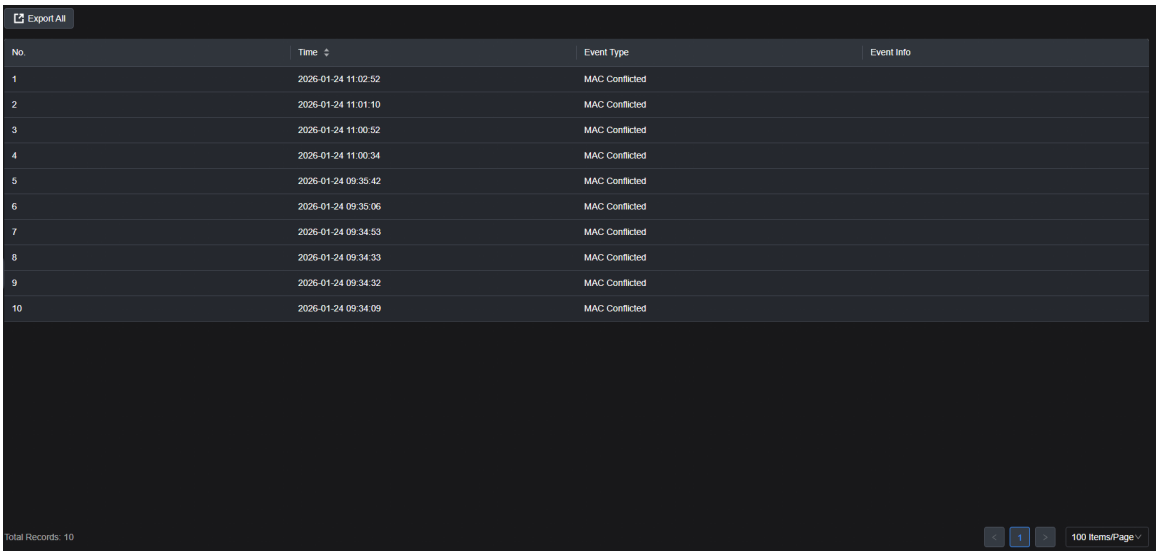
Step 4 Configure the searching period.

Quick search for today's, yesterday's, and the past 2, 3, or 7 days of data is supported.

Step 5 Click **Search**.

Click **Export All** to export the search results.

Figure 6-2 Search results



7 Maintenance

7.1 Log

You can view and search for the log information. By reviewing the logs, we can identify some abnormal access activities. To ensure the system operates normally, we recommend you regularly check the logs and promptly check any abnormal conditions.

Background Information

Data follows the principle of full coverage, and we recommend you back up regularly as needed.

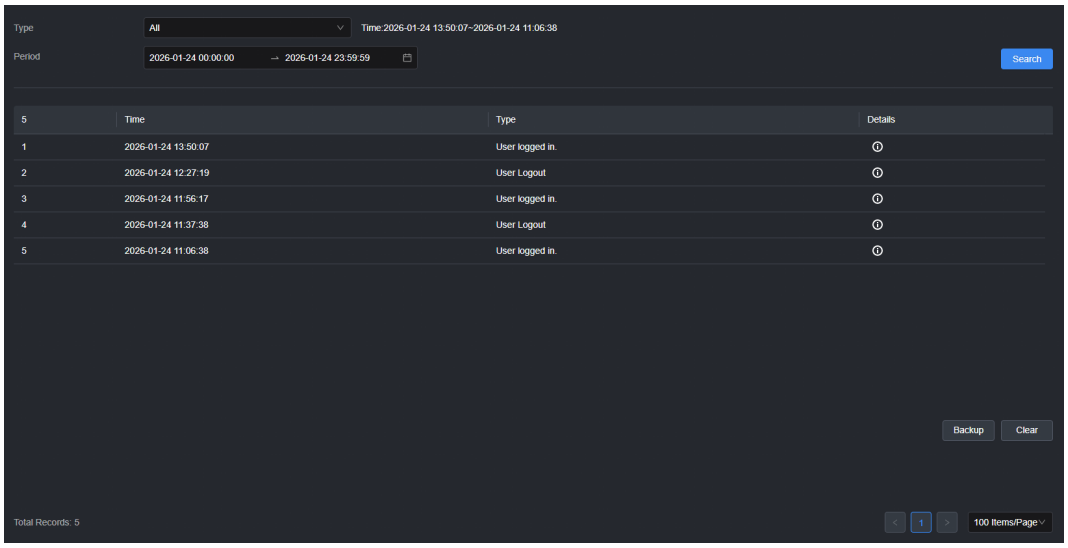
Procedure

Step 1 In the main menu, select **APPLICATIONS** > **MAINTENANCE** > **Log**.

Step 2 Configure the type and period, and then click **Search**.

- Click **Backup** to select the backup file path. You can back up the log information to the web end.
- Click **Details** to view the detailed log information.
- Click **Clear** to clear all logs.

Figure 7-1 Log



7.2 System Information

7.2.1 Version

Log in to the main menu, select **Main Menu** > **MAINTENANCE** > **System Info** > **Version**.

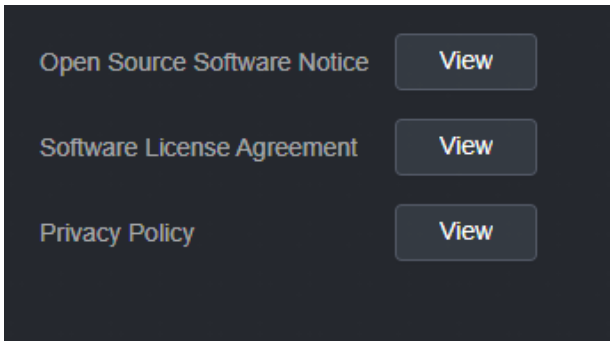
You can view the version information.

7.2.2 Legal Information

You can view the open source software notice, software license agreement and privacy policy.

Log in to the main menu, select **MAINTENANCE** > **System Info** > **Legal Info**.

Figure 7-2 Device status



7.2.3 Online User

The system detects every 5 seconds to check whether there is any user added or deleted, and update the user list timely.

Log in to the main menu, select **Main Menu** > **MAINTENANCE** > **System Info** > **Online User**.

7.3 Maintenance Management

7.3.1 Update

Procedure

Step 1 Download the upgrade files to the computer.

Step 2 Log in to the main menu, select **MAINTENANCE** > **Maintenance Management** > **Update**.

Step 3 Click **Update**.

Step 4 Click the file that you want to upgrade.

The selected file is displayed in the **Update File** box.

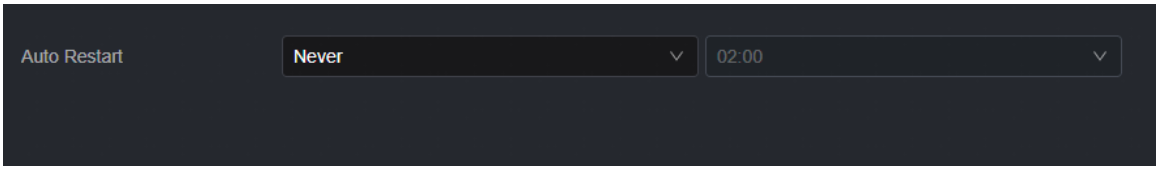
Step 5 Click **Start**.

7.3.2 Device Maintenance

When the Device has been running for a long time, you can enable the Device to restart automatically at the idle time.

Log in to the main menu, select **MAINTENANCE** > **Maintenance Management** > **Maintenance**.

Figure 7-3 Maintenance



7.3.3 Import/Export

You can export or import the device system settings if there are several devices that require the same setup.

Background Information

When you open the **Import/Export** page, the system refreshes the devices and sets the current directory as the first root directory.

Procedure

Step 1 Log in to the main menu, select **MAINTENANCE** > **Maintenance Management** > **Import/Export**.

Step 2 Click **Refresh** to refresh the page.

Step 3 Click **Export**.

There is a folder under the name style of "Config_xxxx". Double-click this folder to view the backup files.

7.3.4 Default

7.3.4.1 Restoring Defaults on the Webpage

You can restore the Device to default settings on the web page.

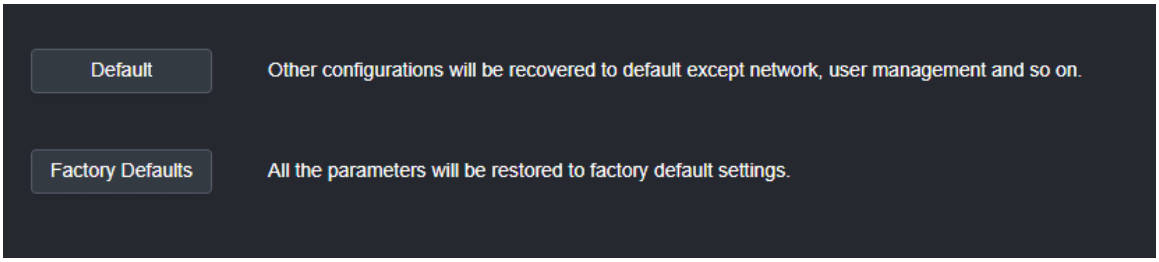
Background Information

This function is for admin account only.

Procedure

Step 1 Log in to the main menu, select **MAINTENANCE** > **Maintenance Management** > **Default**.

Figure 7-4 Default



Step 2 Restore the settings.

- **Default**: Restore all the configurations except network settings and user management to the default.
- **Factory Defaults**: Restore all the configurations to the factory default settings.

7.3.4.2 Resetting Device through the Reset Button

You can use the reset button on the mainboard to reset the Device to the factory default settings.

Background Information

After resetting, all the configurations will be lost.

Procedure

Step 1 Disconnect the Device from power source, and then remove the cover panel.

Step 2 Find the reset button on the mainboard, and then connect the Device to the power source again.

Step 3 Press and hold the reset button for 5 seconds to 10 seconds.

Figure 7-5 Reset button



Step 4 Restart the Device.

After the Device restarts, the settings have been restored to the factory default.

7.3.5 Advanced Maintenance

When exception occurs, export data to check details.

Log in to the main menu, select **MAINTENANCE** > **Maintenance Management** > **Advanced Maintenance**.

Appendix 1 Security Commitment and Recommendation

Zhejiang 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 Allowlist**

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