Alarm Control Panel

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V2.0.0

Foreword

General

This manual introduces the installation, functions and operations of the alarm control panel (hereinafter referred to as "the control panel"). 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, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V2.0.0	● Added 3 functions, including arming and disarming via SMS, bypassing and isolating zones via SMS, and voice prompt. ● Updated zone and subsystem configurations, and added public subsystem functions.	April 2022
V1.1.0	● Updated configuration guide, password resetting, audio function, fault handling, alarm receiving center configuration, 2G/4G modules, time settings, keypad initialization. ● Updated the descriptions of all the chapters. ● Updated images.	December 2021
V1.0.0	First release.	July 2021

Privacy Protection Notice

As the device user or data control panel, you might collect the personal data of others such as their face, 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.

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, comply with the guidelines when using it, and keep the manual safe for future reference.

Operation Requirements

⚠

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.

Installation Requirements

⚠ WARNING

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

⚠

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

1 Product Overview

1.1 Introduction

This high-performance alarm control panel is specially designed for alarm application scenarios based on embedded platform. The control panel adopts advanced control technology and has powerful data transmission capabilities. It runs stably as a whole.

With high security and reliability, the control panel can work independently, or connect to professional surveillance software (DSS Professional) to form a security network, displaying its powerful remote monitoring function.

The control panel is applicable for use with security and protection in areas such as schools, stores, factories, financial institutes, judiciary authorities and smart residential areas.

1.2 Features

- 8/16-channel (can be extended to 72/80/256) local alarm input and 4-channel (can be extended to 84/256) output are available.
- Connections with normally open or closed detectors and tamper, short circuit and masking alarms.
- Forcibly and automatically turn on or off the control panel and alarm linkage.
- Multiple zone types are available, such as real-time zone, time-delay zone and 24-hour silence zone.
- Provides protection for alarm input and output port circuit.
- Failure alarms include tamper alarm for the control panel and keypad, power failure alarm for the adapter and storage battery, storage battery undervoltage alarm, PSTN offline alarm, network disconnection alarm, IP or MAC address conflict alarm, and more.
- Open connection for 2 channels of RS-485, up to 32 channels for the keypad, printer and extension modules.
- Panic alarms such as fire, medical and duress alarms.
- PSTN and Contact ID protocols.
- SMS and network available on model G.
- Optional 4G module, TTS audio, network and SMS.
- Operate on the control panel by key commands (following audio instructions) on a phone call.
- Configure by keypad and web page. Supports quick configuration guide, remote configuration and search.
- arm and disarm single zone and subsystem (8 at most) by keypad, remote control, IC card, SMS (model G) and more.
- Data upload strategy for multiple alarm receiving centers.
- Massive log search.
- Remote update.
- Multiple methods of restoration.
- Dual network ports. Two wired alarm centers and two wireless alarm centers.

2 Unpack and Check

When you receive the control panel, check against the following checking list. If any of the items are missing or damaged, contact the local retailer or after-sale service staff immediately.

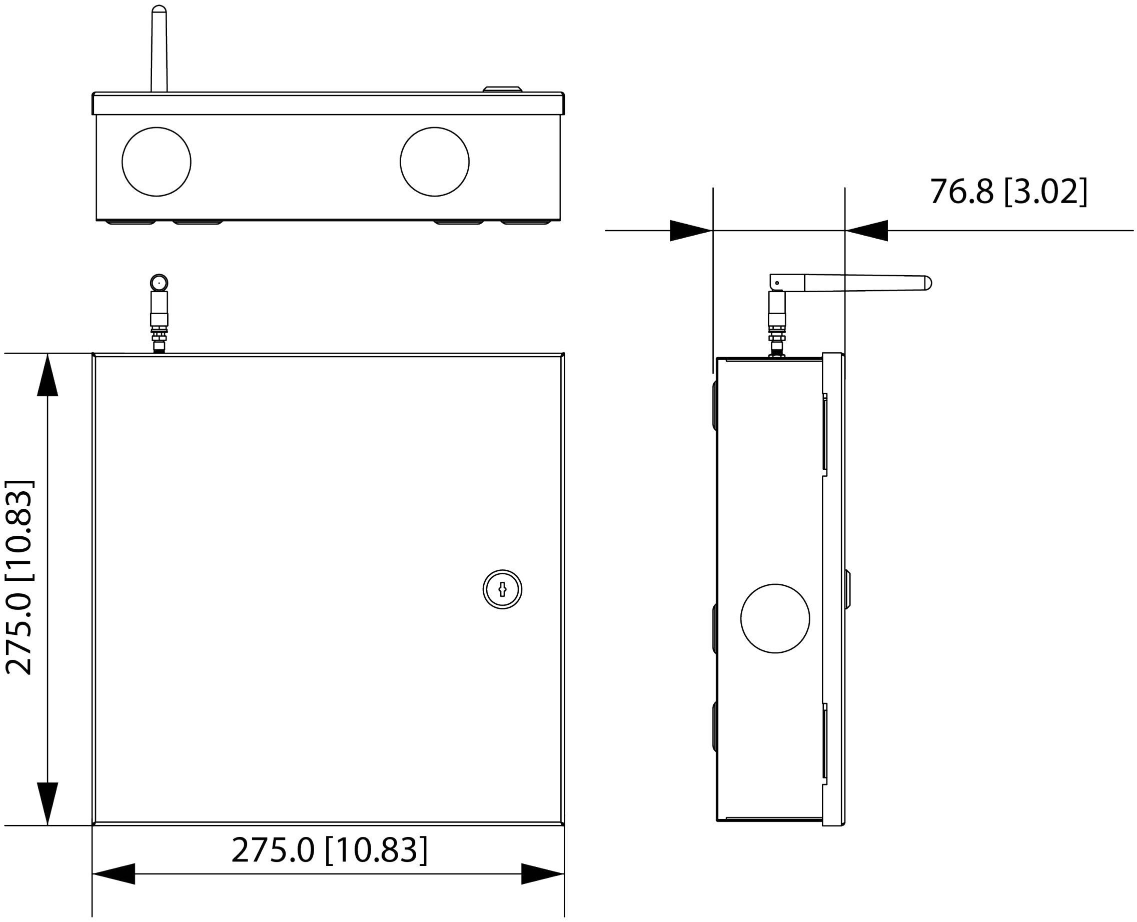
Table 2-1 Checklist

No.	Item		Content
1	Whole package	Appearance	No obvious damage.
		Package	Check whether there are signs of accidental impact.
		Accessory	Check whether the accessories are all present.
2	Casing	Appearance	No obvious damage.
		Data cables, power cables, fan cables, and main board	No loose connections. 📖 Contact after-sale service immediately if any of cables or lines are loose.
3	User's manual	—	Check whether there is 1 user's manual.
4	Resistance		Check whether there are 32 resistances.

3 Dimensions and Mainboard Ports

3.1 Dimensions

Figure 3-1 Dimensions (mm [inch])



3.2 Mainboard Ports

This section uses ARC9016C series' mainboard ports as an example.

Compared with ARC9016C series, ARC2016C series and ARC2008C series do not have MBUS module. ARC2008C series supports local 8-channel alarm input and 4-channel alarm output.

Figure 3-2 Mainboard Ports

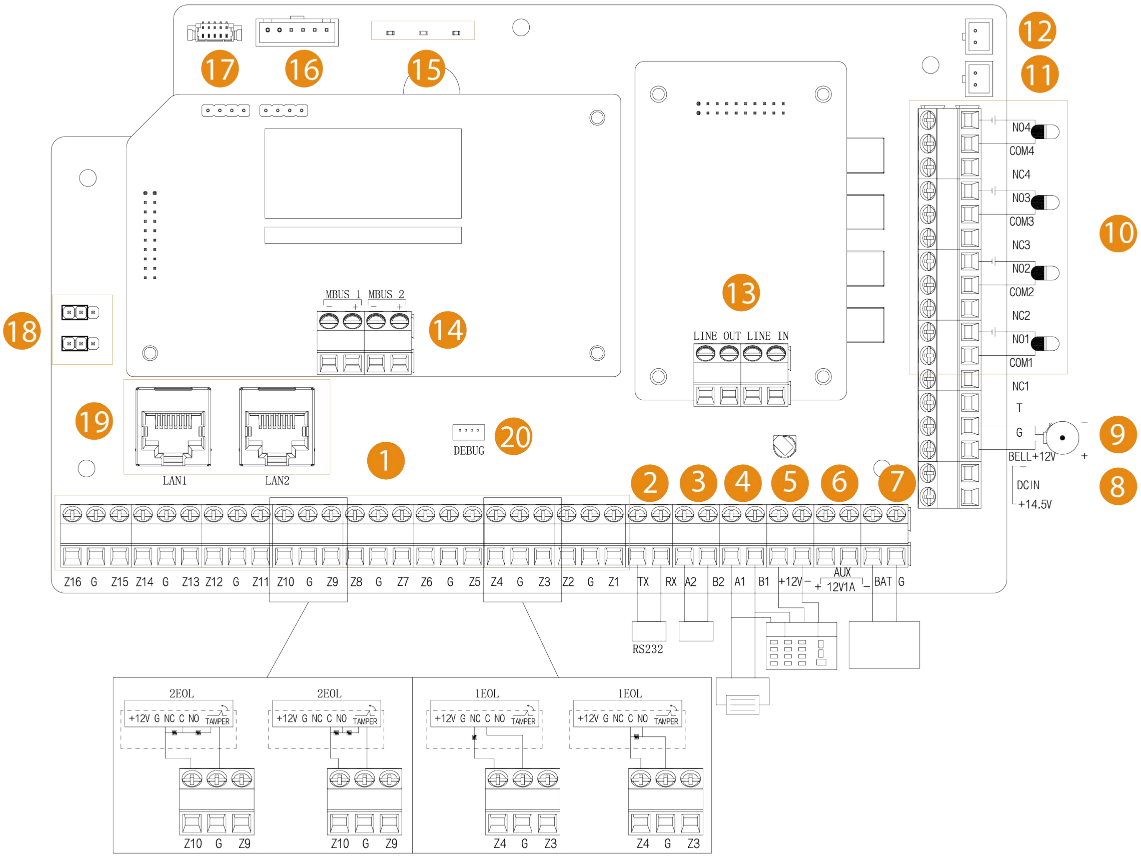


Table 3-1 Mainboard ports description

No.	Description
1	Local alarm input port. Supports 16-channel local alarm input. ARC2008C series supports 8-channel local alarm input.
2	RS-232.
3	A2, B2: Connects to RS-485 extension alarm input and output modules.
4	A1, B1: Connects to printer or keypad.
5	+12 VDC, –: Connects to alarm programming keypad power supply.
6	12 VDC auxiliary power supply, powering other device modules.
7	12 VDC lead-acid storage battery port.
8	14.5 VDC power port.
9	● BELL, G: Siren. ● T: Tamper siren.
10	Local alarm output port. Supports 4-channel alarm output.
11	Case tamper port.
12	Wall tamper port.
13	● LINE OUT: Telephone port. ● LINE IN: User line port.

No.	Description
14	M-BUS port. Supports 2-channel extension modules. 📖 ARC2016C series and ARC2008C series do not have M-BUS module.
15	Status indicator. Left: Battery in place or undervoltage. Middle: Battery discharge. Right: Power.
16	2G module port.
17	4G module port.
18	Restoring to factory settings and resetting password ports.
19	Network port. The default IP address of LAN1 is 192.168.1.108, and LAN2 is 192.168.2.108.
20	DEBUG port. Used for debugging.

4 Installation and Wiring

4.1 Wall Mount

Make sure that the distance between the wall and the control panel is no less than 15 mm for air circulation.

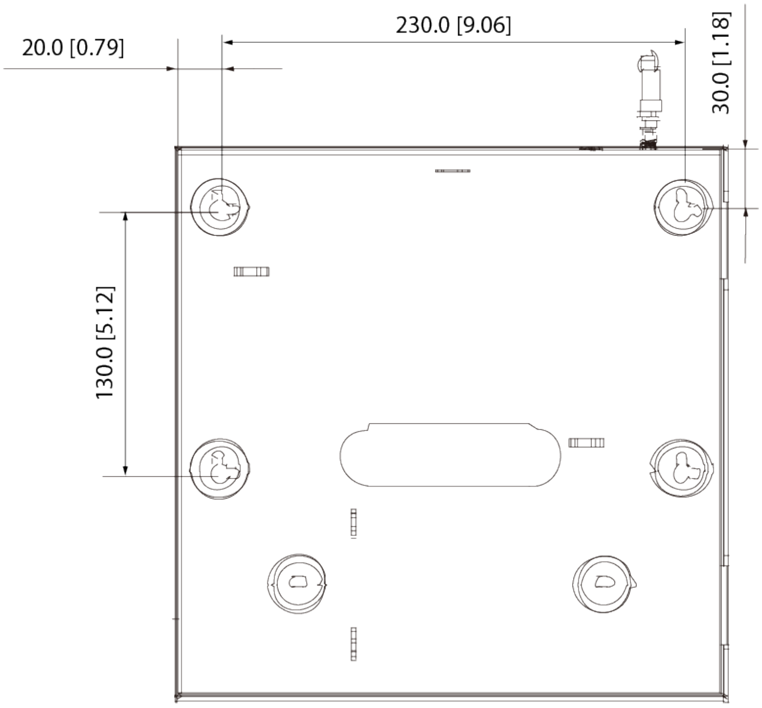
Step 1 Open the package box, take out the plastic expansion tube and self-tapping screws.

Step 2 Drill 4 holes into the wall.

Step 3 Insert the plastic expansion tube into the holes, and then insert the 4 self-tapping screws.

Step 4 Hang the control panel on the screws.

Figure 4-1 Installation (mm [inch])



4.2 Cable Connection

4.2.1 Cable Requirements

Table 4-1 Specifications for the recommended ARC alarm control panel cable

Device	Wire Materials	Section-area (mm²)	Recommended distance (m)
Wire	CAT-5	—	≤ 100 m
Detector	RVV	0.75	≤ 200 m
RS-485 signal line	RVS	1.0	≤ 1,000 m
Bell	RVV	0.75	≤ 200 m

Device	Wire Materials	Section-area (mm^2)	Recommended distance (m)
M-BUS signal line	RVVP	1.5	≤ 2,400 m

4.2.2 Local Alarm Input Cable Connection

This section uses 16-channel alarm input as an example, the corresponding ports are Z1 to Z16. 0 or 1 EOL, 2 EOL and 3 EOL are available for detectors that are normally open and closed. Set the control panel to 0 or 1 EOL when the detector tamper alarm is not required, 2 EOL for tamper alarm and 3 EOL for both tamper and mask alarms.

Figure 4-2 Detector wiring (normally open)

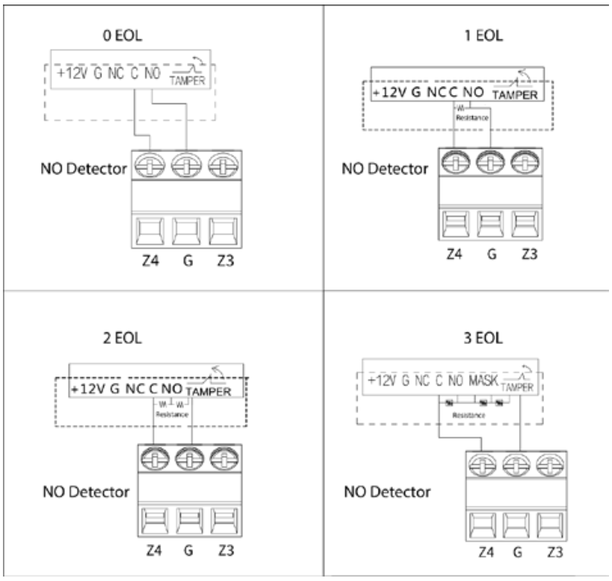
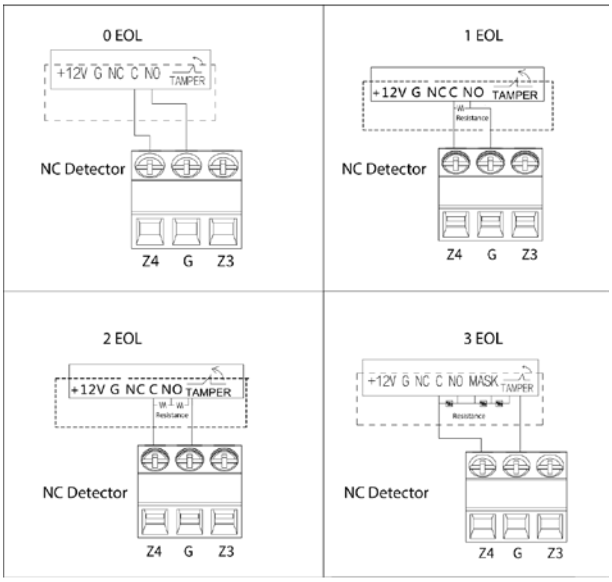


Figure 4-3 Detector wiring (normally closed)



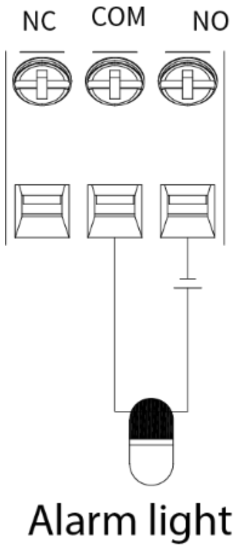
4.2.3 Local Alarm Output Cable Connection

To avoid relay damage from overcurrent, do not connect the alarm output port of the control panel where they can receive large power loads (no more than 1 VAC). If you need to use large power loads, use a contactor.

4-channel alarm outputs correspond to ports NC1–NC4, C1–C4 and NO1–NO4.

- NC: Normally closed port.
- C: Common port (COM).
- NO: Normally open port.

Figure 4-4 Local alarm output cable connection

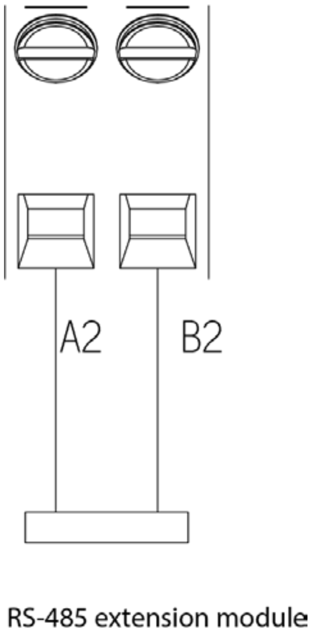


External devices need extra power supply. The load capacity of the alarm light is no more than 12 VDC and 1 VAC.

4.2.4 RS-485 Cable Connection

RS-485 port. Used to connect to RS-485 extension alarm input or output modules.

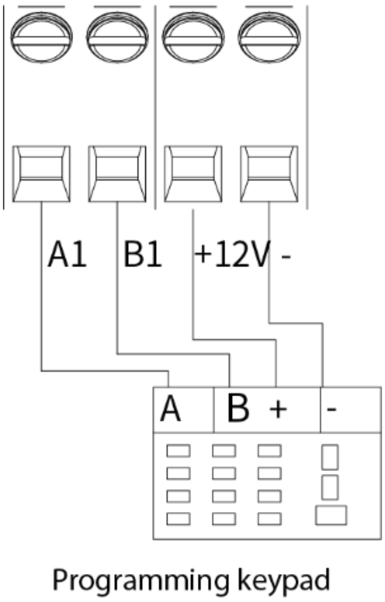
Figure 4-5 RS-485 Cable Connection



4.2.5 Keypad Cable Connection

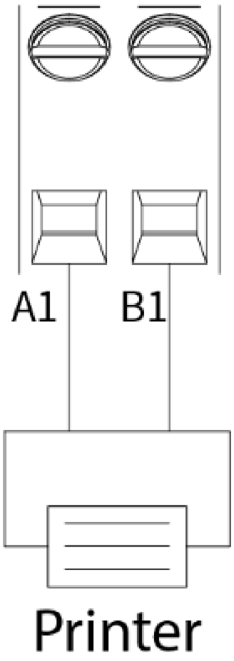
Connect port B and A of keypad to ports B and A on the control panel, port– and + to GND– and +12 VDC of the control panel.

Figure 4-6 Keypad cable connection



4.2.6 Printer Cable Connection

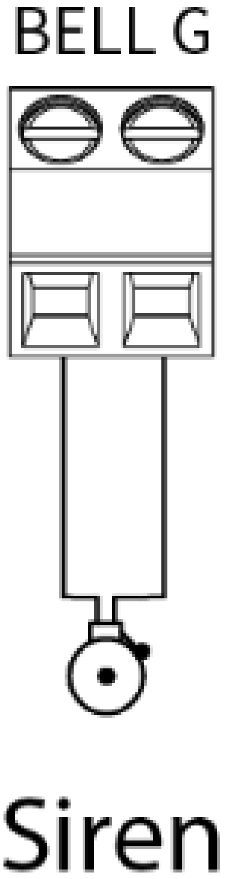
Figure 4-7 Printer cable connection



4.2.7 Siren Cable Connection

The load capacity of the siren port is 12 VDC and 1 VAC.

Figure 4-8 Siren cable connection

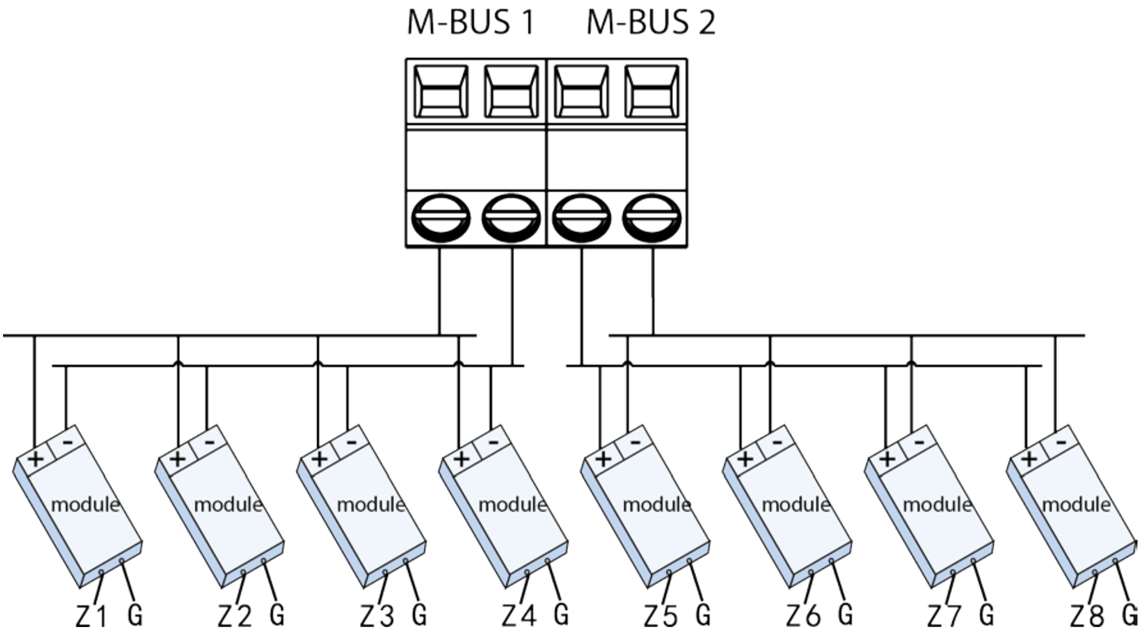


4.2.8 Expansion Module Cable Connection

Provides 2-channel M-BUS port.

- The end of the line resistor value of the extension module input is10 kΩ.
- The range of extension module address DIP code is 0–254. Based on the extension module (ARM801, ARM802, ARM911, ARM808), refer to 4.2.1Cable Requirements to see details on the cable connection requirements. Single channel M-BUS module supports a distance of 2.4 km for communication.
- The number of modules each M-BUS can connect to is as follows.
  - ◇ 801 module is a single zone input channel, which supports 120 modules.
  - ◇ 802 module is the input channel of 2 zones which supports 60 modules.
  - ◇ 911 module is a single zone input channel with one output, which supports 60 modules.
  - ◇ 808 module is the input channel of 8 zones with one output, which supports 15 modules.
- The address of the extension module cannot be repeated; otherwise the control panel might not be able to detect the extension module, or might not be able to recognize whether the extension module is online or offline.

Figure 4-9 Extension module cable connection



5 Web Operations

5.1 Starting the Device

5.1.1 Initializing the Control Panel

Background Information

When using control panel for the first time after installation or after restoring to factory settings, set the login password for the admin account. Also, set up an email address in case you need to reset the login password for the admin account.

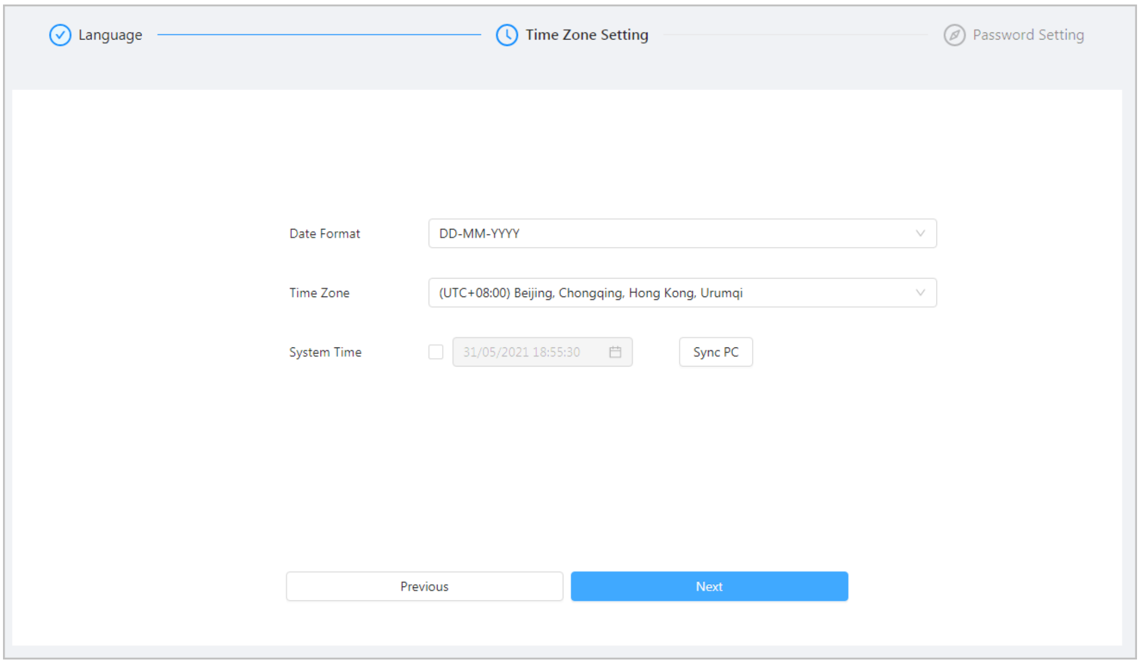
- To protect your device, keep your admin login password safe after completing the initialization steps, and change the password regularly.
- The default IP address of LAN1 is 192.168.1.108, and LAN2 is 192.168.2.108.

Procedure

Step 1 Open the browser, enter the default IP address of the control panel, and then press the Enter key.

Step 2 Set **Language** (support English, Russian, Latin American, Arabic), **Time Zone** and **System Time**, and then click **Next**.

Figure 5-1 Initialize



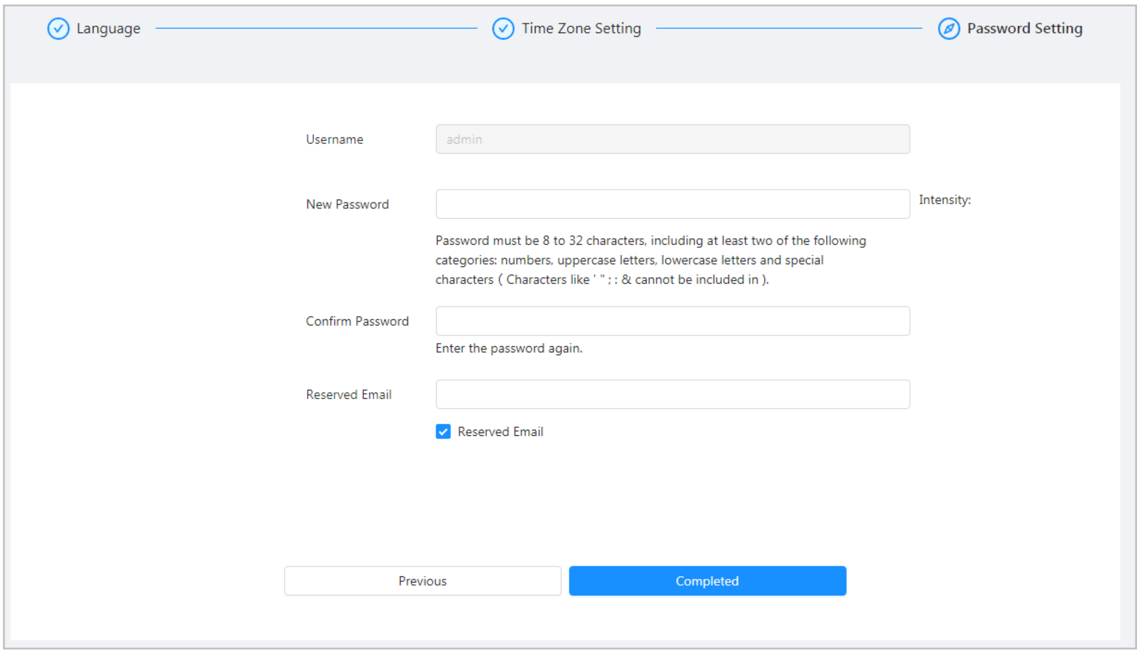
Date Format: DD-MM-YYYY

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

System Time: □ 31/05/2021 18:55:30

Step 3 Set the login password for the admin.

Figure 5-2 Set admin password



Username: admin

New Password

Intensity:

Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' " ; : & cannot be included in).

Confirm Password

Enter the password again.

Reserved Email

☑ Reserved Email

Step 4 Select **Reserved Email** and then enter the email address.

Step 5 Click **Completed**.

A prompt of successful initialization is displayed, and then the login page is displayed.

5.1.2 Logging in to Web Manager

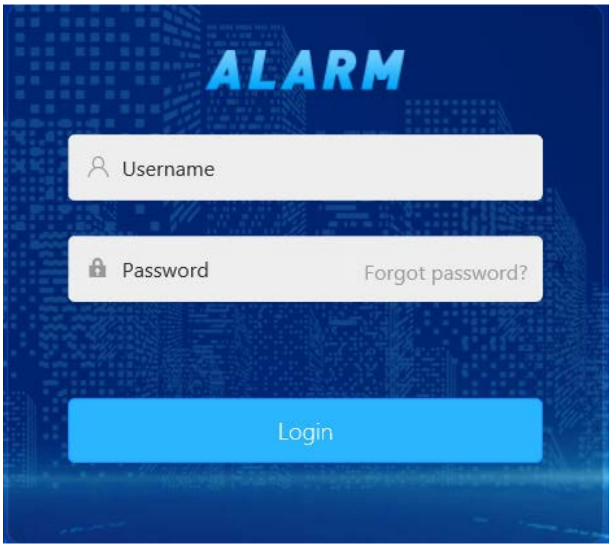
Make sure that the local computer and the control panel are on the same network segment.

- The default IP address of LAN1 is 192.168.1.108, and LAN2 is 192.168.2.108.
- The browser version is recommended to be Chrome 41.0 or later, IE9.0 or later, or Firefox 50.0 or later.

Step 1 Enter the Device IP address in the address bar of the browser, and then press Enter.

Step 2 Enter the user name and password, and then click **Login**.

Figure 5-3 Login



ALARM

Username

Password

Forgot password?

Login

5.1.3 Configuration Guide

Config Wizard is available for quick configuration of related parameters for basic arming and disarming of a single zone and subsystem, and to configure output alarm and alarm receiving center settings.

5.1.3.1 Configuring Zone and Subsystem

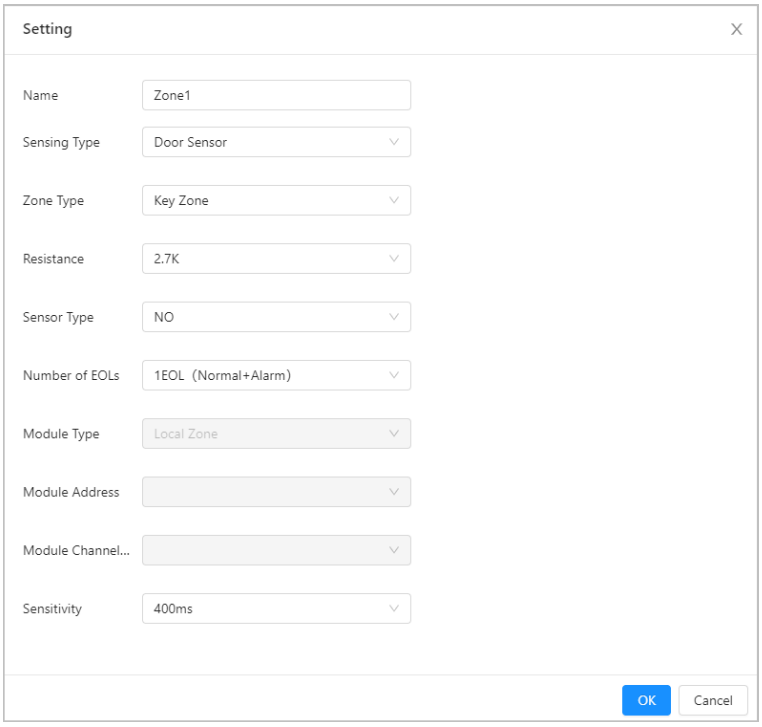
5.1.3.1.1 Configuring Zone

Configure the sensing method of sensors, zone type and sensor type of each zone.

Step 1 Click ◀ on the upper-right corner of the main page.

Step 2 Click ✎ to configure the zone parameters.

Figure 5-4 Zone settings



Setting

Name: Zone1

Sensing Type: Door Sensor

Zone Type: Key Zone

Resistance: 2.7K

Sensor Type: NO

Number of EOLs: 1EOL（Normal+Alarm）

Module Type: Local Zone

Module Address:

Module Channel...:

Sensitivity: 400ms

Table 5-1 Zone parameters description

Parameter	Description
Name	Custom zone name.
Sensing Type	Select according to the type of the connected detector.
Zone Type	Select zone as needed. For details, see "Appendix 1 Glossary".
Resistance	Select 10 K for M-BUS module and others as needed. 2.7 K, 4.7 K, 6.8 K, 10 K (M-BUS).
Sensor Type	Select **Normally Open** or **Normally Closed** according to the sensor type.
Number of EOL	● 0 EOL (Normal + Alarm): **No resistor**. ● 1 EOL (Normal + Alarm): **Default**. ● 2 EOL (Normal + Alarm + Short Circuit + Tamper): **Supports short circuit and tamper alarms**. ● 3 EOL (Normal + Alarm + Short Circuit + Tamper + Masked): **Supports mask alarm**.
Entry Delay	Unit is second. When the system is in the armed state, the zone with enter delay is triggered, but alarms cannot immediately go off. You can disarm the system during period. Otherwise the system will alarm right after the delay time ends.
Exit Delay	Unit is second. A time period when the system is in the armed state, the zone is triggered, but no alarms can go off until the period ends.
Module Type	Select matching module as needed. ● MBUS ● RS-808

Parameter	Description
Module Address	Enter the address as needed. We recommend configuring the address in sequence starting from 0. ● **ARM801**: 0–254. ● **ARM802**: 0–254. ● **ARM808**: 0–127. ● **ARM911**: 0–254. ● **RS-808**: 0–15.
Module Channel No.	Enter as needed. ● **ARM801**: 1. ● **ARM802**: 1–2. ● **ARM808**: 1–8. ● **ARM911**: 1. ● **RS-808**: 1–8.
Sensitivity	● Set the sensitivity value. You can select from 200 ms, 400 ms, 600 ms or 800 ms. The sensitivity value is 400 ms by default. ● Support setting sensitivity value for a single zone. ● Support modifying the sensitivity values of the following expansion modules: RS-808, and RS-708.

Step 3 Click **OK**.

Step 4 Click **Next**.

5.1.3.1.2 Configuring Subsystem

Configure the daily arming and disarming schedule, time and mode for the subsystem.

Step 1 In the **Subsystem** section, select a subsystem from the drop-down list.

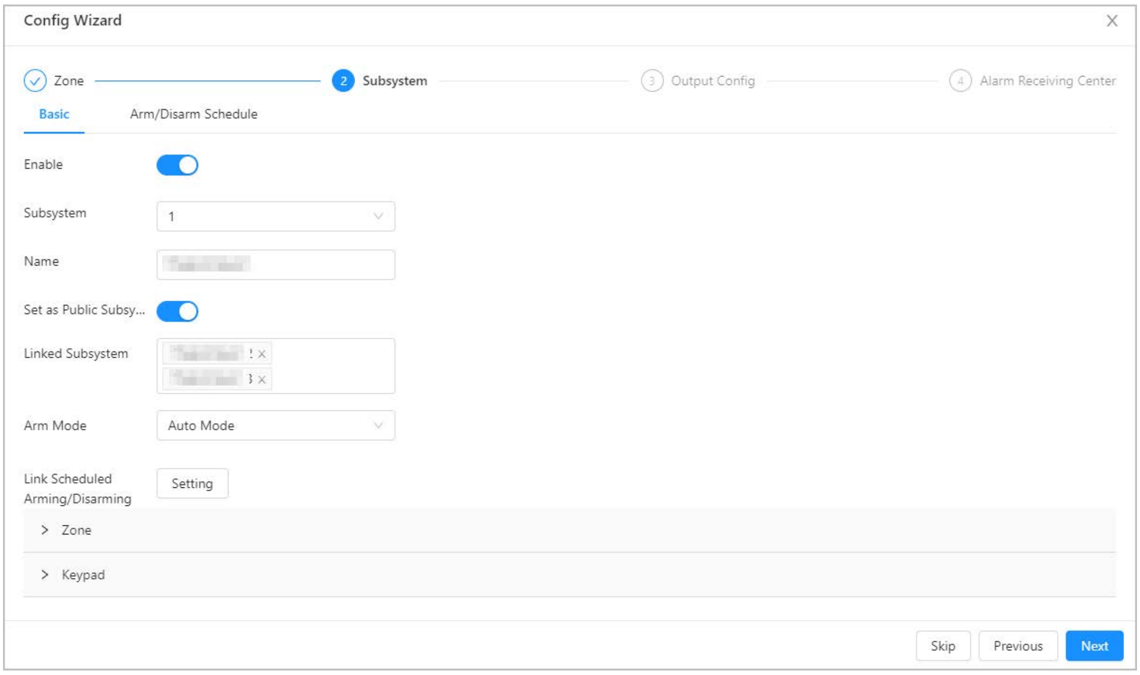
If you set **Subsystem** to 1, you can set it as a public subsystem. Once set, you can link subsystem 1 to other subsystems, zones and the keypad. You can also set arming modes and schedules for arming and disarming the public subsystem.

1) Click ○ next to **Set as Public Subsystem** to enable the public subsystem function.

2) Select linked subsystems.

- Other than subsystem 1, you can select 2 subsystems at least.
- If all the linked subsystems are armed, the public system will be armed automatically. If all the linked subsystems are disarmed, the public system will be disarmed automatically.
- Set **Arm Mode** to **Auto Mode** or **Forced Mode**.

Figure 5-5 Arming/disarming configuration



Config Wizard

✓ Zone — 2 Subsystem — 3 Output Config — 4 Alarm Receiving Center

Basic | Arm/Disarm Schedule

Enable	●
Subsystem	1
Name	[redacted]
Set as Public Subsy...	●
Linked Subsystem	[redacted] × [redacted] ×
Arm Mode	Auto Mode
Link Scheduled Arming/Disarming	Setting

> Zone

> Keypad

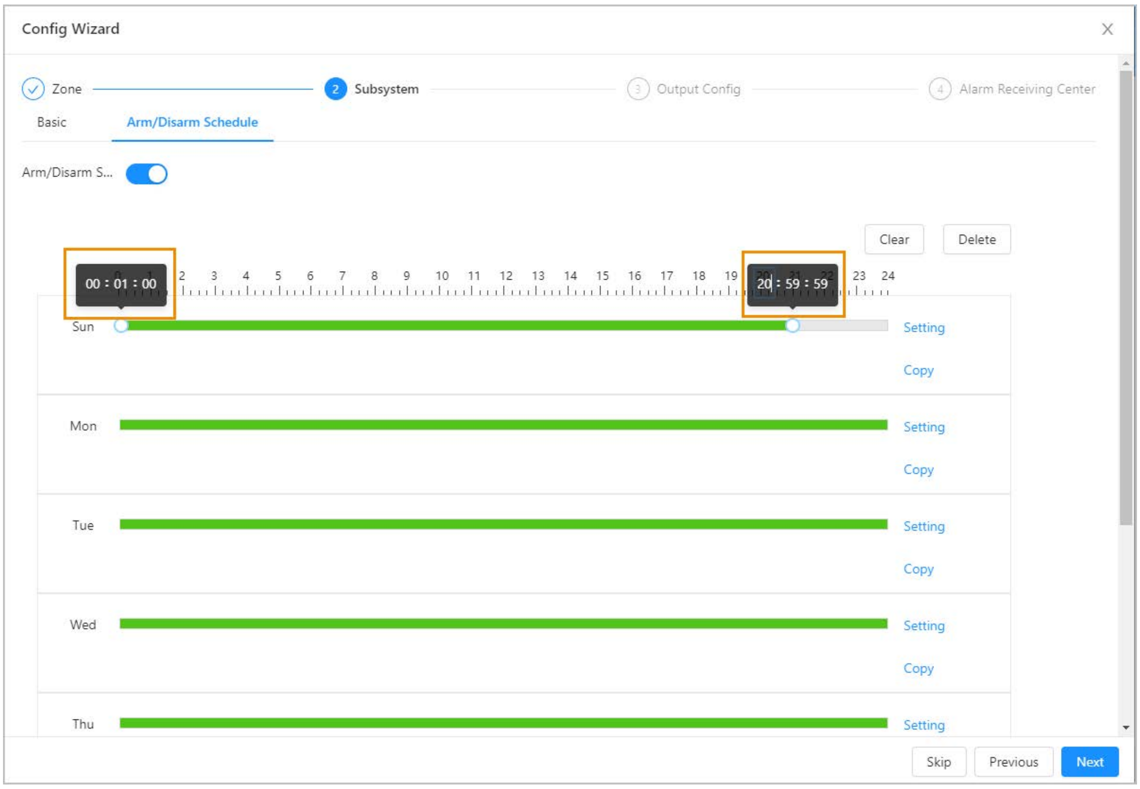
Step 2 Select **arm and disarm Schedule**, set arming/disarming time.

The green area in the slider indicates that the system will be armed during the defined periods.

- Click and hold the slider and adjust both its ends, in order to set the arming and disarming time.
- Click the slider, enter a specific time in the start and end time text box to set the arming and disarming period.

Click **Copy** to copy the schedule to other days.

Figure 5-6 arm and disarm schedule



Step 3 Click **Setting** to set the arming and disarming period and its mode.

By default, the start time is arming time, end is disarming.

Figure 5-7 Arming/disarming settings

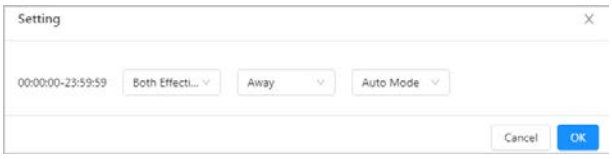


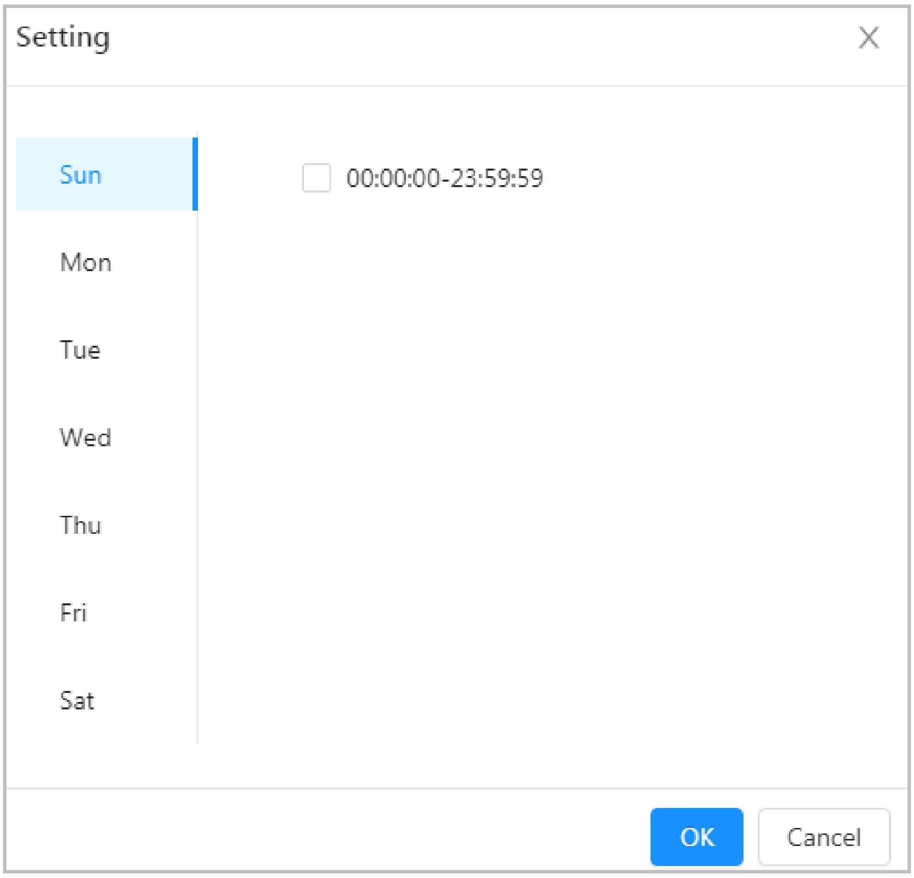
Table 5-2 Arming parameter description

Parameter	Description
Effective Start Time	Arms the system at the start time, but does not disarm at the end time.
Effective End Time	Disarms the system at end time.
Both Effective	Arms the system at the start time and disarm at end time.
Auto Mode	Arms/disarms automatically at the defined time when no errors occur (default). Fails to arm automatically when error happens.
Forced Mode	Force arm the subsystem.

Step 4 Click ○ to enable the arm and disarm schedule.

Step 5 Select **Basic** > **Setting**, and then select the day to set the time to enable the schedule.

Figure 5-8 Basic setting



Setting

- Sun
- Mon
- Tue
- Wed
- Thu
- Fri
- Sat

□ 00:00:00-23:59:59

Step 6 Click **OK**.

Step 7 Click **Next** to configure the relay and the siren.

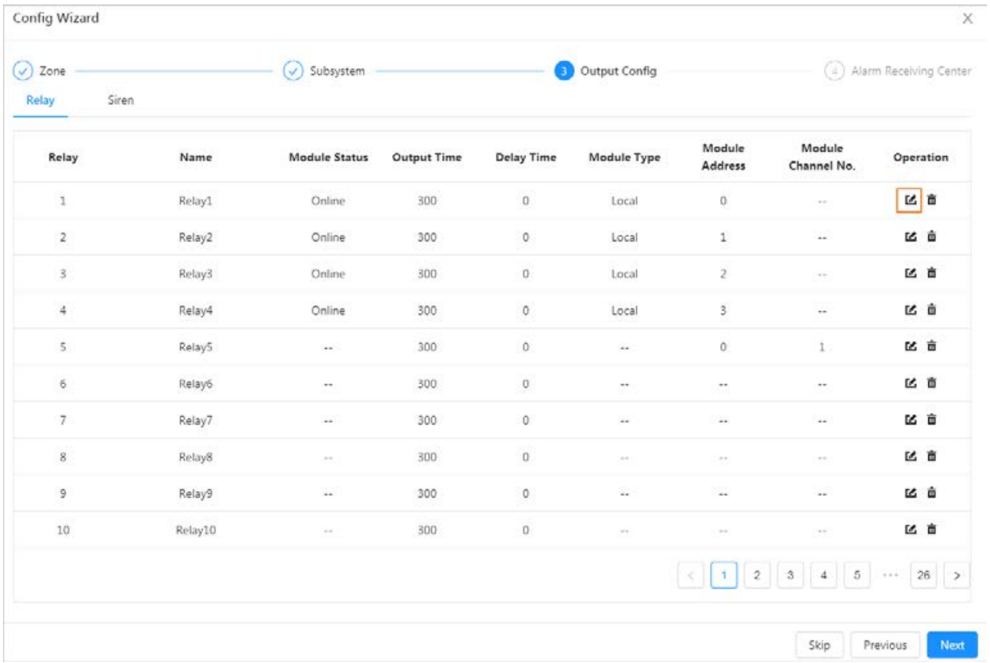
5.1.3.2 Output Configuration

5.1.3.2.1 Configuring Relay

Set the output status of the relay of each channel. When an alarm is triggered, the control panel links the relay to output.

Step 1 On the **Output Config** section, select **Relay**, and then click ✎.

Figure 5-9 Relay

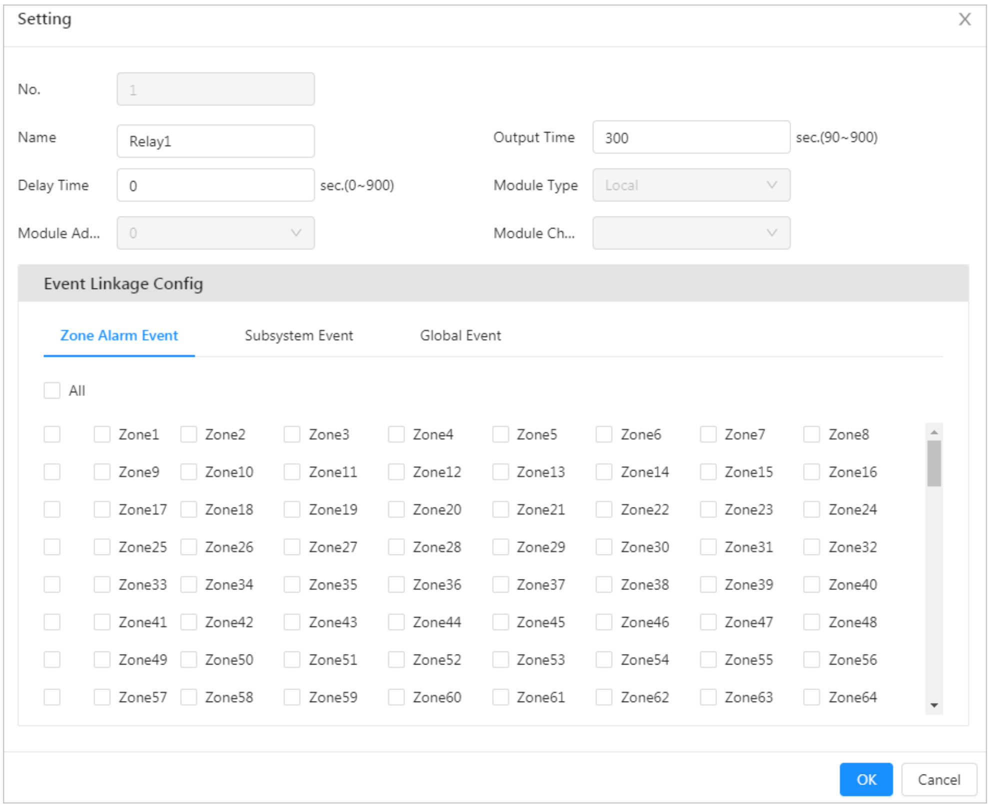


Config Wizard

Relay	Name	Module Status	Output Time	Delay Time	Module Type	Module Address	Module Channel No.	Operation
1	Relay1	Online	300	0	Local	0	--	
2	Relay2	Online	300	0	Local	1	--	
3	Relay3	Online	300	0	Local	2	--	
4	Relay4	Online	300	0	Local	3	--	
5	Relay5	--	300	0	--	0	1	
6	Relay6	--	300	0	--	--	--	
7	Relay7	--	300	0	--	--	--	
8	Relay8	--	300	0	--	--	--	
9	Relay9	--	300	0	--	--	--	
10	Relay10	--	300	0	--	--	--	

Step 2 Configure the parameters.

Figure 5-10 Setting



Setting

No. 1

Name Relay1

Output Time 300 sec.(90~900)

Delay Time 0 sec.(0~900)

Module Type Local

Module Ad... 0

Module Ch...

Event Linkage Config

□ All

□	□ Zone1	□ Zone2	□ Zone3	□ Zone4	□ Zone5	□ Zone6	□ Zone7	□ Zone8
□	□ Zone9	□ Zone10	□ Zone11	□ Zone12	□ Zone13	□ Zone14	□ Zone15	□ Zone16
□	□ Zone17	□ Zone18	□ Zone19	□ Zone20	□ Zone21	□ Zone22	□ Zone23	□ Zone24
□	□ Zone25	□ Zone26	□ Zone27	□ Zone28	□ Zone29	□ Zone30	□ Zone31	□ Zone32
□	□ Zone33	□ Zone34	□ Zone35	□ Zone36	□ Zone37	□ Zone38	□ Zone39	□ Zone40
□	□ Zone41	□ Zone42	□ Zone43	□ Zone44	□ Zone45	□ Zone46	□ Zone47	□ Zone48
□	□ Zone49	□ Zone50	□ Zone51	□ Zone52	□ Zone53	□ Zone54	□ Zone55	□ Zone56
□	□ Zone57	□ Zone58	□ Zone59	□ Zone60	□ Zone61	□ Zone62	□ Zone63	□ Zone64

Table 5-3 Relay parameter description

Parameter	Description
Name	Enter the relay name.
Output Time	The period when the relay returns to the disconnected status
Delay Time	The period the relay delays before another output again.

Parameter	Description
Event Linkage Config	When an event happens, the control panel links the relay to output. ● **Zone Alarm Event**: Select zones to be set. ● **Subsystem Event**: The linked output after the subsystem is armed or disarmed. For example, after subsystem 1 is armed, the control panel links relay 1 to output. ● **Global Event**: When a system event or emergency event occurs, the control panel links the relay to output.
Module Type	Select according to actual modules (no configuration needed for the 4 local relays). ● **MBUS**. ● **RS-708**. ● **RS-808**.
Module Address	Enter the address as needed. We recommend configuring the address starting from 0. ● **ARM801**: 0–254. ● **ARM802**: 0–254. ● **ARM808**: 0–127. ● **ARM911**: 0–254. ● **RS-708**: 0–15. ● **RS-808**: 0–15.
Module Channel No.	● **ARM808**: 1. ● **ARM911**: 1. ● **RS-708**: 1–8. ● **RS-808**: 1–2.

Step 3 Click **OK**.

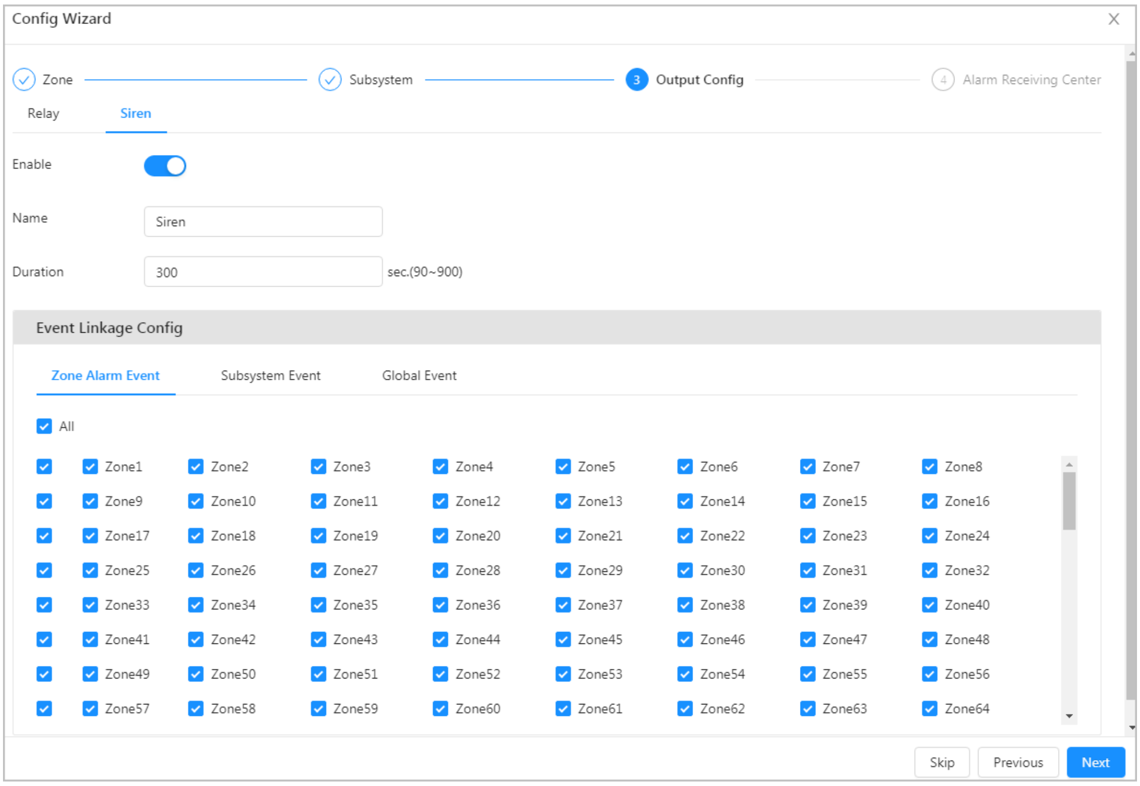
5.1.3.2.2 Configuring Siren

Set the output status of the relay for each channel. When an alarm event occurs, the control panel links the siren to output.

Step 1 On the **Output Config** section, select **Siren**, and then click ✎.

Step 2 Configure the parameters.

Figure 5-11 Siren



Enable ●

Name: Siren

Duration: 300 sec.(90~900)

Event Linkage Config

☑ All

☑	☑ Zone1	☑ Zone2	☑ Zone3	☑ Zone4	☑ Zone5	☑ Zone6	☑ Zone7	☑ Zone8
☑	☑ Zone9	☑ Zone10	☑ Zone11	☑ Zone12	☑ Zone13	☑ Zone14	☑ Zone15	☑ Zone16
☑	☑ Zone17	☑ Zone18	☑ Zone19	☑ Zone20	☑ Zone21	☑ Zone22	☑ Zone23	☑ Zone24
☑	☑ Zone25	☑ Zone26	☑ Zone27	☑ Zone28	☑ Zone29	☑ Zone30	☑ Zone31	☑ Zone32
☑	☑ Zone33	☑ Zone34	☑ Zone35	☑ Zone36	☑ Zone37	☑ Zone38	☑ Zone39	☑ Zone40
☑	☑ Zone41	☑ Zone42	☑ Zone43	☑ Zone44	☑ Zone45	☑ Zone46	☑ Zone47	☑ Zone48
☑	☑ Zone49	☑ Zone50	☑ Zone51	☑ Zone52	☑ Zone53	☑ Zone54	☑ Zone55	☑ Zone56
☑	☑ Zone57	☑ Zone58	☑ Zone59	☑ Zone60	☑ Zone61	☑ Zone62	☑ Zone63	☑ Zone64

Table 5-4 Description

Parameter	Description
Name	Enter the siren name.
Duration	The output duration of the siren.
Event Linkage Config	● **Zone Alarm Event**: Select zones to be set. ● **Subsystem Event**: The linked output after the subsystem is armed or disarmed. For example, after subsystem1 is armed, the control panel links siren to output. ● **Global Event**: When a system event or emergency event occurs, the control panel links the siren to output.

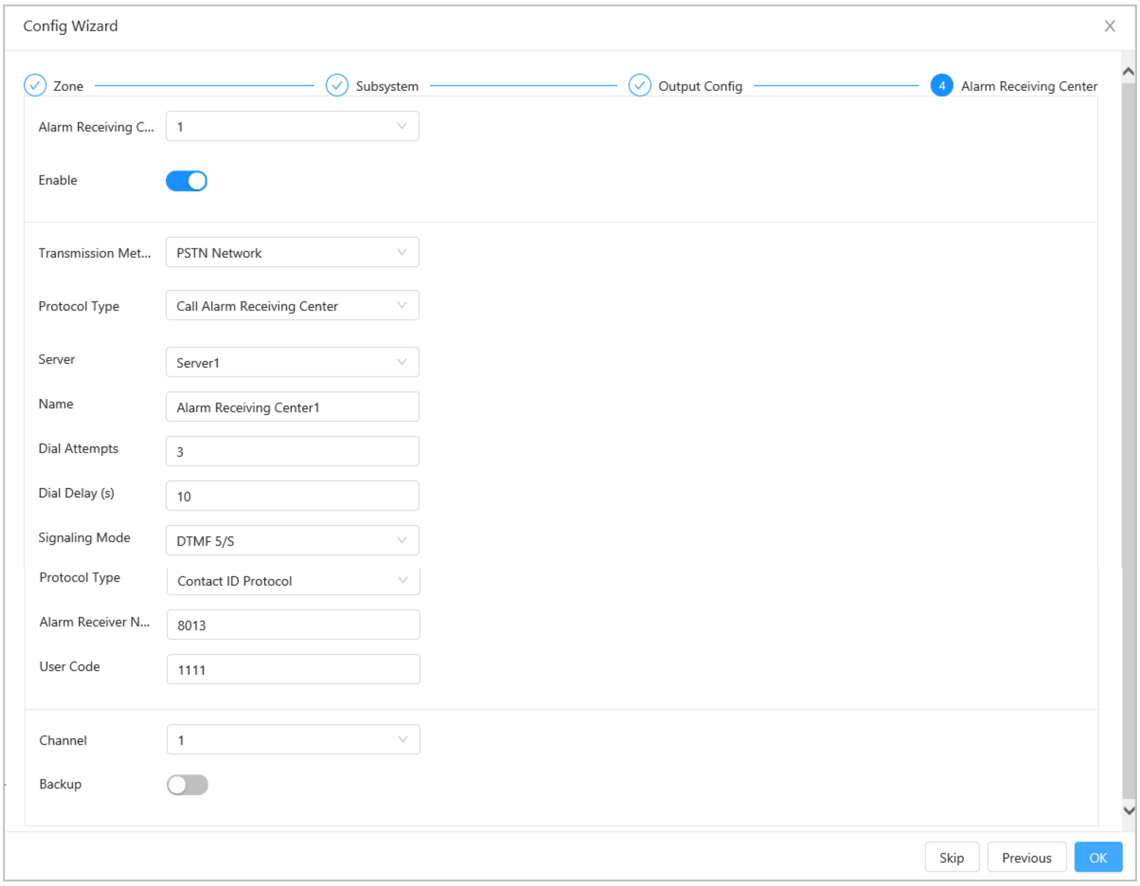
Step 3 Click **Next**.

5.1.3.3 Configuring Alarm Receiving Center

Configure the alarm transmission method. When an alarm is triggered, the control panel sends a message to the alarm receiving center.

Step 1 On the **Alarm Receiving Center** section, configure the parameters.

Figure 5-12 Alarm receiving center configuration



Alarm Receiving C... 1

Enable

Transmission Met... PSTN Network

Protocol Type Call Alarm Receiving Center

Server Server1

Name Alarm Receiving Center1

Dial Attempts 3

Dial Delay (s) 10

Signaling Mode DTMF 5/S

Protocol Type Contact ID Protocol

Alarm Receiver N... 8013

User Code 1111

Channel 1

Backup

Table 5-5 Alarm receiving center parameter description

Parameter	Description
Alarm Receiving Center No.	Click ○ to enable the alarm receiving center as needed.
Transmission Method	● **PSTN Network**: Sends CID messages to the call alarm receiving center. ● **Cellular Network**, **NIC 1** or **NIC 2**: Sends network messages to the network alarm receiving center.

Parameter	Description
Protocol Type	● None ● Call alarm receiving center ◇ **Server**: Select from server 1 and server 2 as needed. ◇ **Name**: Enter the center name. ◇ **Dial Attempts**: Attempts to send data to call alarm receiving center. If fails 3 times, the control panel will fail to send CID messages. ◇ **Dial Delay (s)**: Works with **Dial Attempts**. The time required before dialing again after dialing failure. ◇ **Signaling Mode**: Leave it as default. ◇ **Protocol Type**: It is **Contact ID Protocol** by default. ◇ **Alarm Receiver Number**: The number of the call alarm receiving center. ◇ **User Code**: The only code used when the control panel sends messages to the call alarm receiving center. It is 0000 by default. ● Register ◇ **Device ID**: Device ID that is assigned by the server and consistent with the registered ID on the server. ◇ **Server**: Server 1 and server 2. Select as needed. ◇ **Address**: The IP address of the server that needs to be registered to. ◇ **Port**: The port for auto-registration. ● Alarm center ◇ **Server**: Select from server 1 and server 2 as needed. ◇ **Address**: The IP address of server that needs to be registered to. ◇ **Port**: Server port number. 📖 ● You can set **Call Alarm Receiving Center** or **None** as **Protocol Type** when the **Transmission Method** is set to **PSTN Network**. ● You can set **Register**, **Alarm Center** or **None** as **Protocol Type** when the **Transmission Method** is set to **Cellular Network**, **NIC 1** or **NIC 2**.
Backup Channel	Click ○ to enable backup channel 1 or 2. Every center can set a main channel and backup channel. The backup channel can only be enabled when communication failed for the main channel.

Step 2 Click **OK**.

5.1.4 Resetting the Password

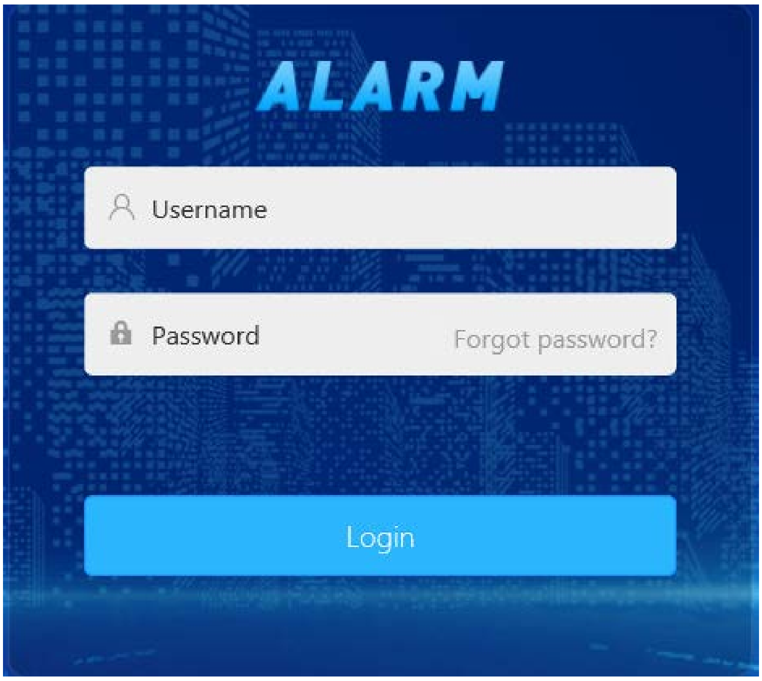
Prerequisites

- During device initialization, set an associate email. For details, see "5.1.1 Initializing the Control Panel".
- Make sure that you have enabled the **Password Reset** function on the **System** > **Account**.

Procedure

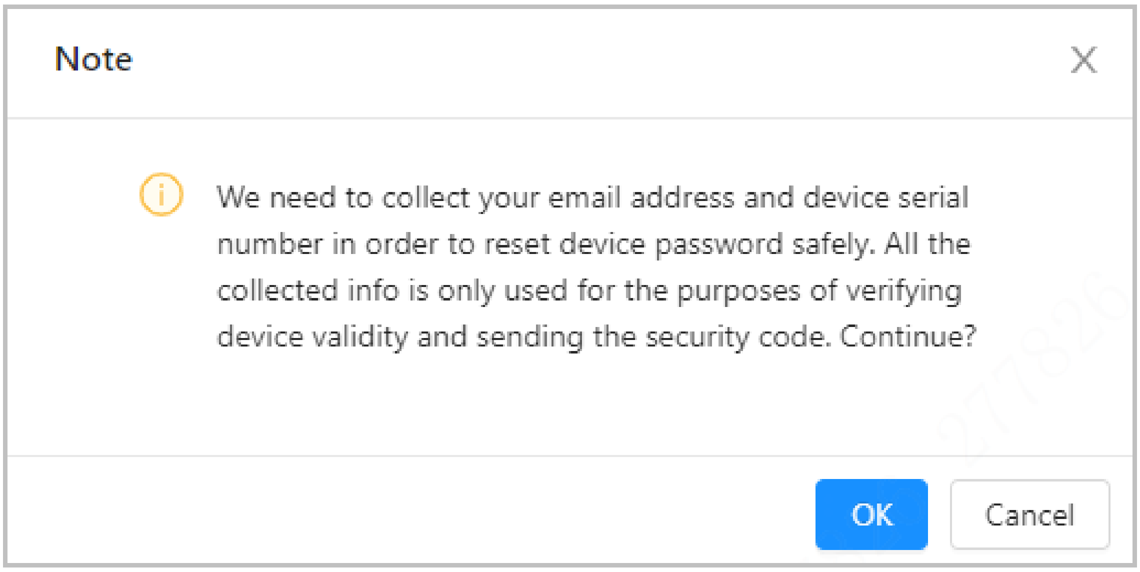
Step 1 On the web page, click **Forgot password?**.

Figure 5-13 Forgot password



Step 2 Click **OK**.

Figure 5-14 Reset password (1)



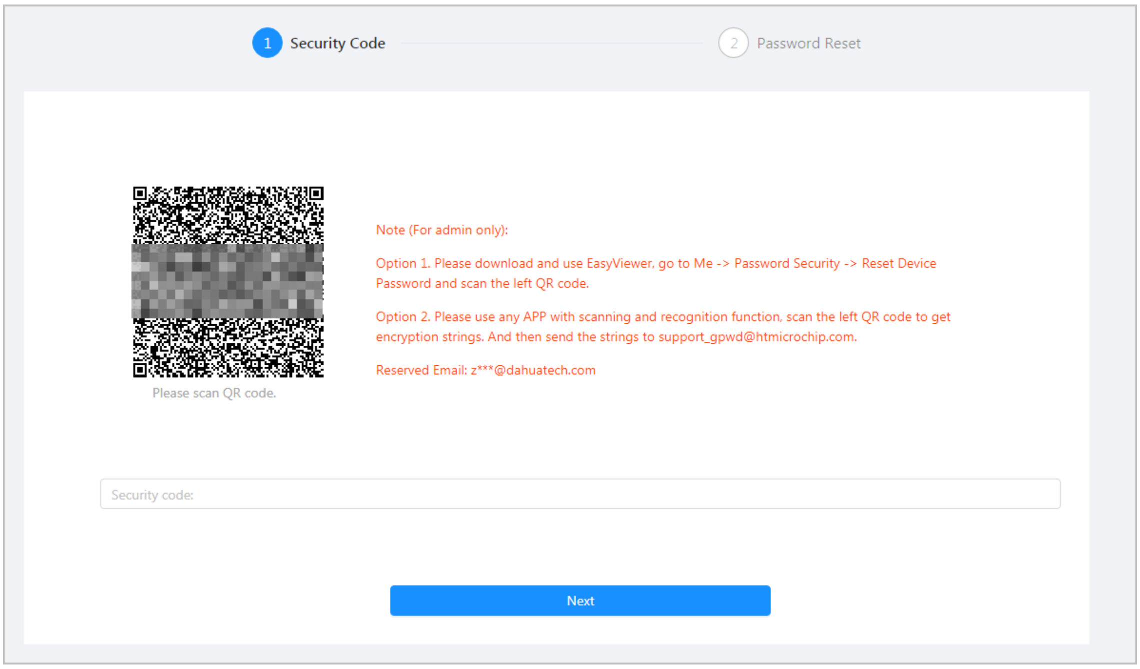
We need to collect your email address and device serial number in order to reset device password safely. All the collected info is only used for the purposes of verifying device validity and sending the security code. Continue?

Step 3 Scan the QR code, and you will get the security code.

Step 4 Enter the received security code in the **Security code** text box, and then click **Next**.

Use the security code within 24 hours after you receive it. Otherwise, it will be invalid.

Figure 5-15 Reset password (2)



Note (For admin only):

Option 1. Please download and use EasyViewer, go to Me -> Password Security -> Reset Device Password and scan the left QR code.

Option 2. Please use any APP with scanning and recognition function, scan the left QR code to get encryption strings. And then send the strings to support_gpwd@htmicrochip.com.

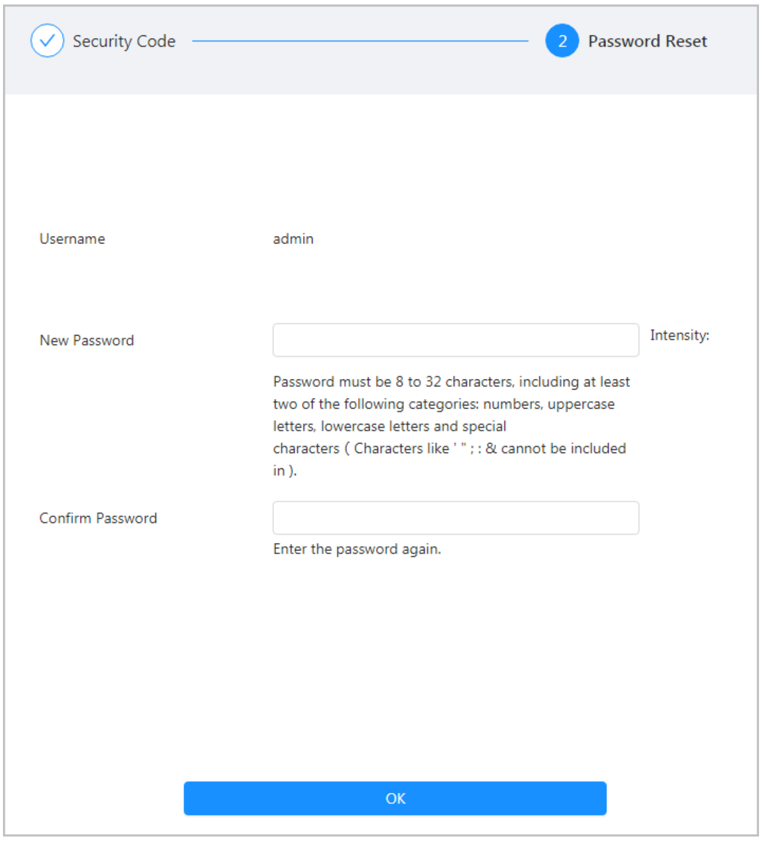
Reserved Email: z***@dahuatech.com

Security code:

Step 5 Set and confirm the new password.

The password can contain 8 to 32 non-empty characters and must have at least 2 types of the following characters: capital letters, lower-case letters, numbers, and special characters (excluding ' " ; , : &). The confirming password should be the same as the new password. Use the password strength prompt as a guide to set a strong password.

Figure 5-16 Password reset (3)



Username admin

New Password

Intensity:

Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' " ; : & cannot be included in).

Confirm Password

Enter the password again.

Step 6 Click **OK**.

5.2 Alarm Configuration

Configure basic functions such as arming/disarming single zone and subsystem, output alarm and alarm receiving center.

5.2.1 Zone

Log in to the web, and then select **Alarm Config** > **Zone**. For details, see "5.1.3.1.1 Configuring Zone".

5.2.2 Subsystem

Log in to the web, and then select **Alarm Config** > **Subsystem**. For details, see "5.1.3.1.2 Configuring Subsystem".

5.2.3 Siren

Log in to the web, and then select **Alarm Config** > **Siren**. For details, see "5.1.3.2.2 Configuring Siren".

5.2.4 Relay

Log in to the web, and then select **Alarm Config** > **Relay**. For details, see "5.1.3.2.1 Configuring Relay".

5.2.5 Printer

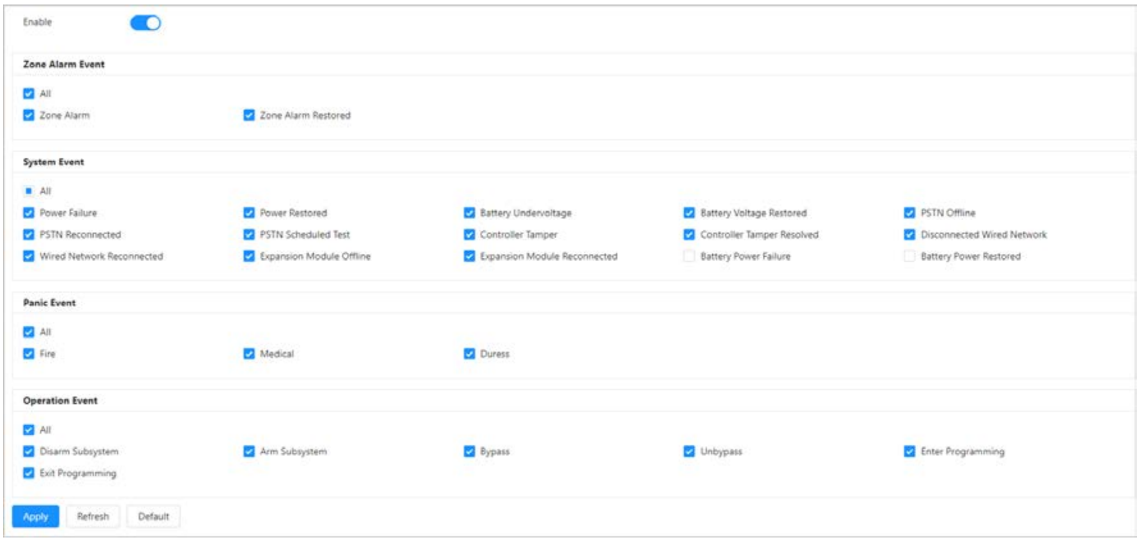
Set the printer to print event information when the defined event occurs.

Step 1 Log in to the web, and then select **Alarm Config** > **Printer**.

Step 2 Click **Enable**.

Step 3 Select an event to link to the printer.

Figure 5-17 Printer settings



Enable

Zone Alarm Event

☑ All
☑ Zone Alarm ☑ Zone Alarm Restored

System Event

■ All
☑ Power Failure ☑ Power Restored ☑ Battery Undervoltage ☑ Battery Voltage Restored ☑ PSTN Offline
☑ PSTN Reconnected ☑ PSTN Scheduled Test ☑ Controller Tamper ☑ Controller Tamper Resolved ☑ Disconnected Wired Network
☑ Wired Network Reconnected ☑ Expansion Module Offline ☑ Expansion Module Reconnected □ Battery Power Failure □ Battery Power Restored

Panic Event

☑ All
☑ Fire ☑ Medical ☑ Duress

Operation Event

☑ All
☑ Disarm Subsystem ☑ Arm Subsystem ☑ Bypass ☑ Unbypass ☑ Enter Programming
☑ Exit Programming

Step 4 Click **Apply**.

5.2.6 Buzzer

Set the buzzer to buzz when the defined event occurs.

Step 1 Log in to the web, and then select **Alarm Config** > **Buzzer**.

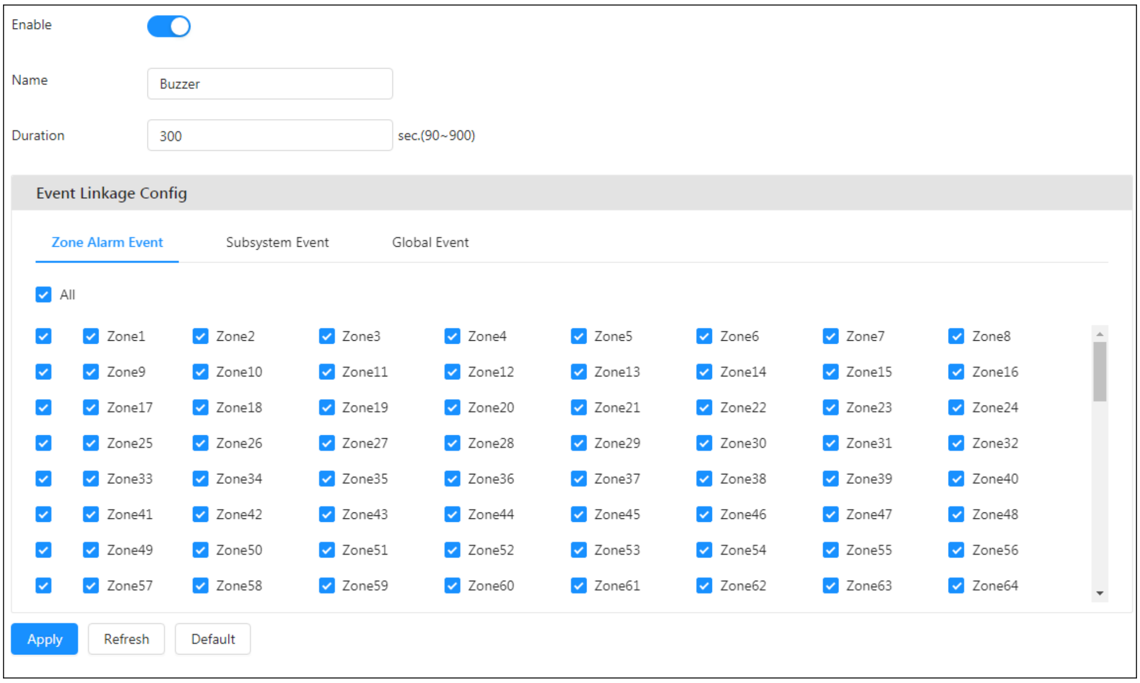
Step 2 Click **Enable**.

Step 3 Enter the buzzer name and set the duration.

Step 4 Select an event to link to the buzzer.

The parameters of the buzzer is the same as that of the siren. For parameter details, see Table 5-4.

Figure 5-18 Buzzer settings



Enable ●

Name: Buzzer

Duration: 300 sec.(90~900)

Event Linkage Config

☑ All

☑	☑ Zone1	☑ Zone2	☑ Zone3	☑ Zone4	☑ Zone5	☑ Zone6	☑ Zone7	☑ Zone8
☑	☑ Zone9	☑ Zone10	☑ Zone11	☑ Zone12	☑ Zone13	☑ Zone14	☑ Zone15	☑ Zone16
☑	☑ Zone17	☑ Zone18	☑ Zone19	☑ Zone20	☑ Zone21	☑ Zone22	☑ Zone23	☑ Zone24
☑	☑ Zone25	☑ Zone26	☑ Zone27	☑ Zone28	☑ Zone29	☑ Zone30	☑ Zone31	☑ Zone32
☑	☑ Zone33	☑ Zone34	☑ Zone35	☑ Zone36	☑ Zone37	☑ Zone38	☑ Zone39	☑ Zone40
☑	☑ Zone41	☑ Zone42	☑ Zone43	☑ Zone44	☑ Zone45	☑ Zone46	☑ Zone47	☑ Zone48
☑	☑ Zone49	☑ Zone50	☑ Zone51	☑ Zone52	☑ Zone53	☑ Zone54	☑ Zone55	☑ Zone56
☑	☑ Zone57	☑ Zone58	☑ Zone59	☑ Zone60	☑ Zone61	☑ Zone62	☑ Zone63	☑ Zone64

Step 5 Click **Apply**.

5.2.7 Audio

Set the linkage event. When a defined event occurs, an audio alarm will be triggered.

- Special characters are not supported, because they are difficult to be recognized.
- TTS voice broadcast does not support languages other than English and Chinese.

Step 1 Log in to the web, and select **Alarm Config** > **Audio.**

Step 2 Click **Sending Strategy**, and then select from the drop-down list.

- **PSTN Only**: Audio messages can only be sent through the PSTN module.
- **2G/4G Only**: Audio messages can only be sent through the 2G/4G module.
- **PSTN Preferred**: Select 2G/4G when the PSTN is unavailable.
- **2G/4G Preferred**: Select PSTN when the 2G/4G is unavailable.

When setting the **Sending Strategy** to **2G/4G Only** or **2G/4G Preferred**, make sure that the control panel supports 2G/4G module.

Step 3 Uploading audio files.

1) Select the audio file to upload.

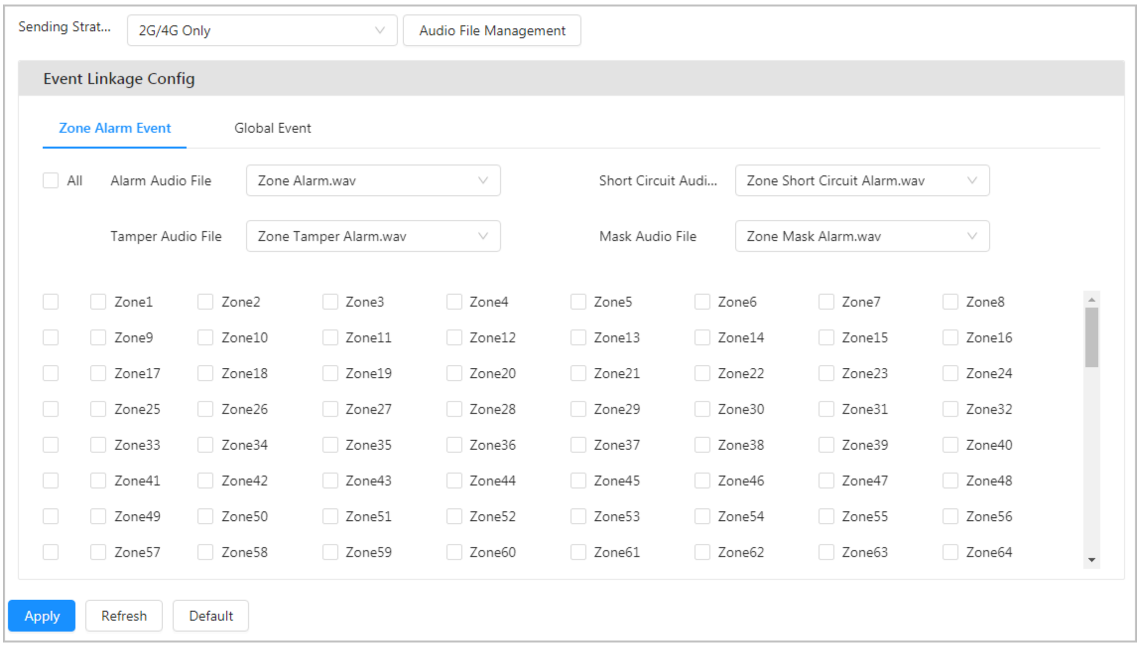
You can upload audio packages that are up to 3 M in size, in the .wav format. A single audio file can be up to 500 k.

2) Click **OK**.

Step 4 Select audio files from the **Audio File** list.

Step 5 Select an event to link to the audio.

Figure 5-19 Audio settings



Sending Strat... 2G/4G Only | Audio File Management

Event Linkage Config

Zone Alarm Event | Global Event

□ All

Alarm Audio File: Zone Alarm.wav

Short Circuit Audi...: Zone Short Circuit Alarm.wav

Tamper Audio File: Zone Tamper Alarm.wav

Mask Audio File: Zone Mask Alarm.wav

□	□ Zone1	□ Zone2	□ Zone3	□ Zone4	□ Zone5	□ Zone6	□ Zone7	□ Zone8
□	□ Zone9	□ Zone10	□ Zone11	□ Zone12	□ Zone13	□ Zone14	□ Zone15	□ Zone16
□	□ Zone17	□ Zone18	□ Zone19	□ Zone20	□ Zone21	□ Zone22	□ Zone23	□ Zone24
□	□ Zone25	□ Zone26	□ Zone27	□ Zone28	□ Zone29	□ Zone30	□ Zone31	□ Zone32
□	□ Zone33	□ Zone34	□ Zone35	□ Zone36	□ Zone37	□ Zone38	□ Zone39	□ Zone40
□	□ Zone41	□ Zone42	□ Zone43	□ Zone44	□ Zone45	□ Zone46	□ Zone47	□ Zone48
□	□ Zone49	□ Zone50	□ Zone51	□ Zone52	□ Zone53	□ Zone54	□ Zone55	□ Zone56
□	□ Zone57	□ Zone58	□ Zone59	□ Zone60	□ Zone61	□ Zone62	□ Zone63	□ Zone64

Apply | Refresh | Default

Step 6 Click **Apply**.

5.2.8 Fault Handing

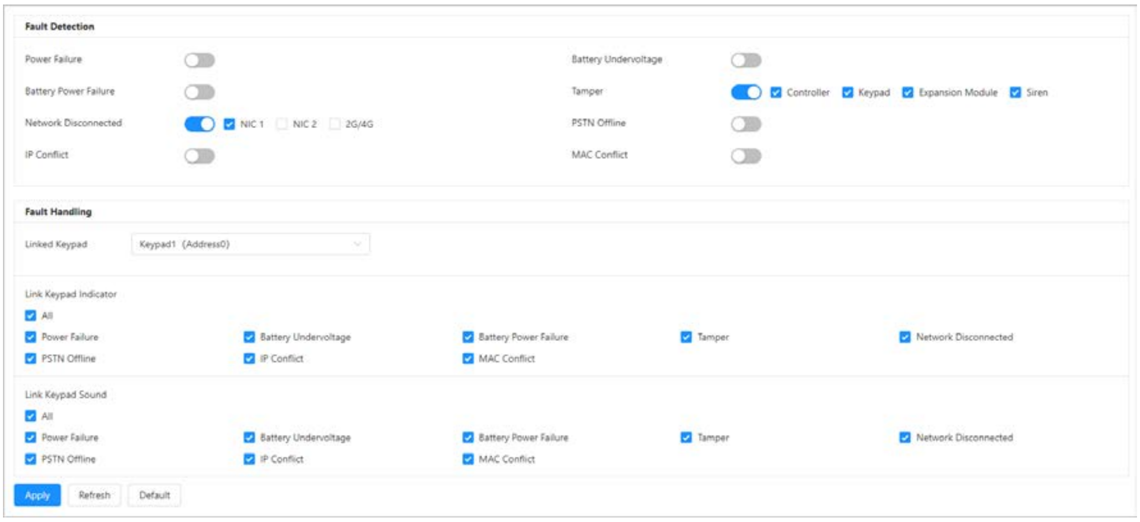
Set the detection event for the control panel. When the defined event occurs, an alarm is triggered, and then the linked keypad responds to it by lighting up the indicator or releasing an audio prompt.

Step 1 Log in to the web, and then select **Alarm Config** > **Fault Handing**.

Step 2 Enable events to be detected.

The following are enabled by default: tamper alarm events from the control panel and keypad, and network disconnected events from NIC 1.

Figure 5-20 Settings for fault handling



Fault Detection

Power Failure: Off

Battery Undervoltage: Off

Battery Power Failure: Off

Tamper: On ☑ Controller ☑ Keypad ☑ Expansion Module ☑ Siren

Network Disconnected: On ☑ NIC 1 □ NIC 2 □ 2G/4G

PSTN Offline: Off

IP Conflict: Off

MAC Conflict: Off

Fault Handling

Linked Keypad: Keypad1 (Address0)

Link Keypad Indicator

☑ All

☑ Power Failure ☑ Battery Undervoltage ☑ Battery Power Failure ☑ Tamper ☑ Network Disconnected

☑ PSTN Offline ☑ IP Conflict ☑ MAC Conflict

Link Keypad Sound

☑ All

☑ Power Failure ☑ Battery Undervoltage ☑ Battery Power Failure ☑ Tamper ☑ Network Disconnected

☑ PSTN Offline ☑ IP Conflict ☑ MAC Conflict

Apply | Refresh | Default

Step 3 Select keypad to link it.

- Set the event that triggers the keypad indicator when detected.
- Set the event that triggers the keypad audio prompt when detected.

Step 4 Click **Apply**.

5.2.9 SMS Linkage

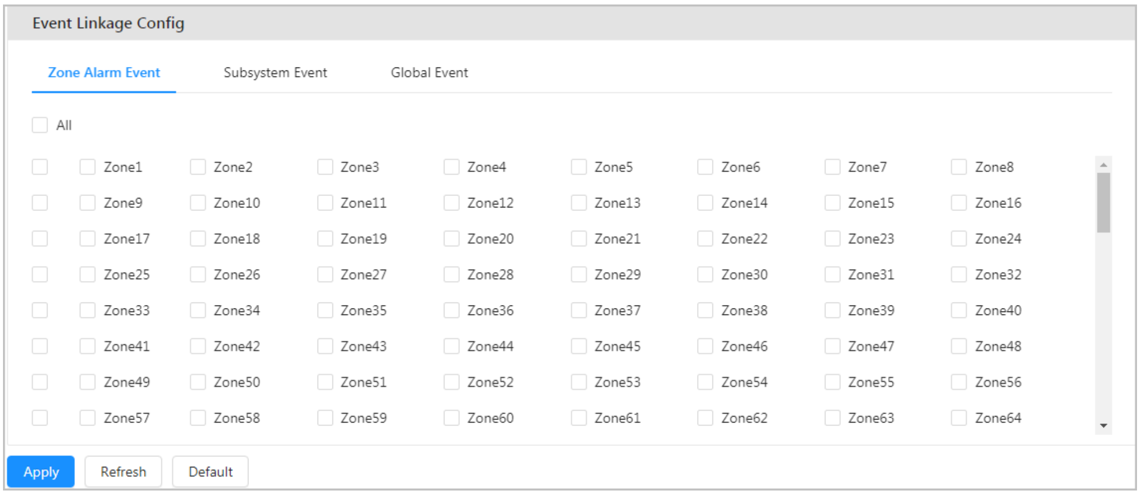
The control panel supports SMS. You can bind a telephone number to receive messages when an exception happens to the storage battery, power supply or network, or if an alarm is triggered, the control panel will send SMS to you.

Step 1 Log in to the web, and then select **Alarm Config** > **SMS Linkage**.

Step 2 Select the zone and event to be linked.

The parameters of the SMS linkage is the same as that of the siren. For parameter details, see Table 5-4

Figure 5-21 SMS linkage settings



□ All

□	□ Zone1	□ Zone2	□ Zone3	□ Zone4	□ Zone5	□ Zone6	□ Zone7	□ Zone8
□	□ Zone9	□ Zone10	□ Zone11	□ Zone12	□ Zone13	□ Zone14	□ Zone15	□ Zone16
□	□ Zone17	□ Zone18	□ Zone19	□ Zone20	□ Zone21	□ Zone22	□ Zone23	□ Zone24
□	□ Zone25	□ Zone26	□ Zone27	□ Zone28	□ Zone29	□ Zone30	□ Zone31	□ Zone32
□	□ Zone33	□ Zone34	□ Zone35	□ Zone36	□ Zone37	□ Zone38	□ Zone39	□ Zone40
□	□ Zone41	□ Zone42	□ Zone43	□ Zone44	□ Zone45	□ Zone46	□ Zone47	□ Zone48
□	□ Zone49	□ Zone50	□ Zone51	□ Zone52	□ Zone53	□ Zone54	□ Zone55	□ Zone56
□	□ Zone57	□ Zone58	□ Zone59	□ Zone60	□ Zone61	□ Zone62	□ Zone63	□ Zone64

Step 3 Click **Apply**.

5.2.10 CID Linkage

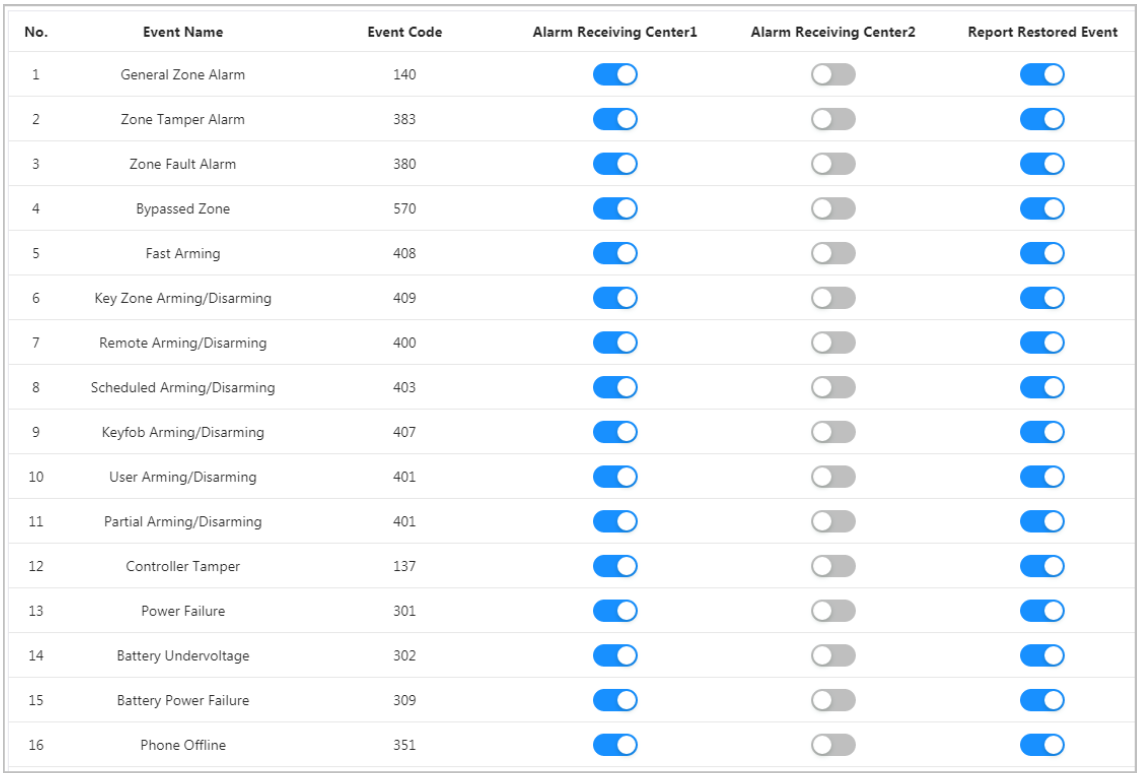
Set the event to link with the alarm receiving center. When the defined event occurs, the linked center gets the alarm message.

Step 1 Log in to the web, and then select **Alarm Config** > **CID Linkage.**

Step 2 Select and enable the alarm receiving center for each event as needed.

Step 3 Enable **Report Restored Event**.

Figure 5-22 CID linkage settings



No.	Event Name	Event Code	Alarm Receiving Center1	Alarm Receiving Center2	Report Restored Event
1	General Zone Alarm	140	●	○	●
2	Zone Tamper Alarm	383	●	○	●
3	Zone Fault Alarm	380	●	○	●
4	Bypassed Zone	570	●	○	●
5	Fast Arming	408	●	○	●
6	Key Zone Arming/Disarming	409	●	○	●
7	Remote Arming/Disarming	400	●	○	●
8	Scheduled Arming/Disarming	403	●	○	●
9	Keyfob Arming/Disarming	407	●	○	●
10	User Arming/Disarming	401	●	○	●
11	Partial Arming/Disarming	401	●	○	●
12	Controller Tamper	137	●	○	●
13	Power Failure	301	●	○	●
14	Battery Undervoltage	302	●	○	●
15	Battery Power Failure	309	●	○	●
16	Phone Offline	351	●	○	●

5.2.11 Alarm Receiving Center

Set the transmission method of the alarm receiving center, the report period for test reports, and the link to call the alarm receiving center.

Step 1 Log in to the web, and then select **Alarm Config** > **Alarm Receiving Center.**

Step 2 After setting **Sending Strategy**, click **Test Report**.

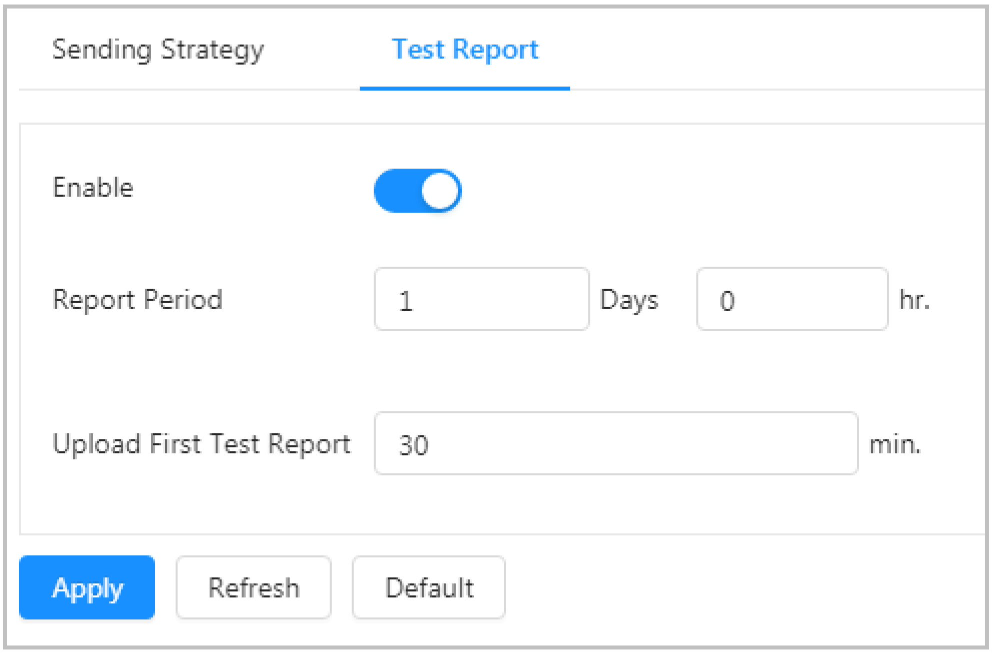
Set and back up the transmission method of the alarm receiving center. For details, see "5.1.3.3 Configuring Alarm Receiving Center".

Step 3 Click **Enable**.

Step 4 Configure the parameters.

- **Report Period**: Set the time interval for test reports to be uploaded.
- **Upload First Test Report**: Set the time needed for uploading the first test report after enabling it.

Figure 5-23 Test report



Enable: ●

Report Period: 1 Days 0 hr.

Upload First Test Report: 30 min.

5.3 Alarm Management

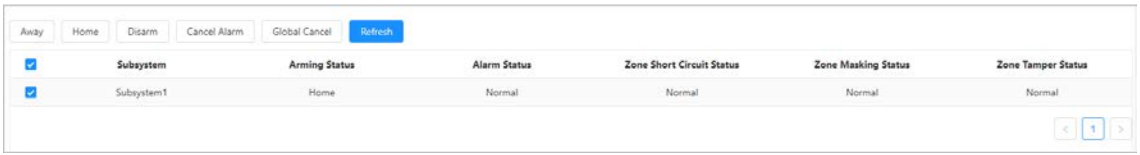
5.3.1 Subsystem

Arm and disarm subsystems and you can cancel alarms that occurred in subsystems.

Step 1 Log in to the web, and then select **Alarm Management** > **Subsystem.**

Step 2 Select a subsystem.

Figure 5-24 Subsystem configuration



☑	Subsystem	Arming Status	Alarm Status	Zone Short Circuit Status	Zone Masking Status	Zone Tamper Status
☑	Subsystem1	Home	Normal	Normal	Normal	Normal

Step 3 Click **Away**, **Home**, **Disarm** or **Cancel Alarm**.

The arming status of the subsystem changes after arming/disarming operations.

Global Cancel does not require selecting subsystem data. Click it to cancel all linked alarms of subsystems.

5.3.2 Zone

You can arm and disarm and bypass the zone.

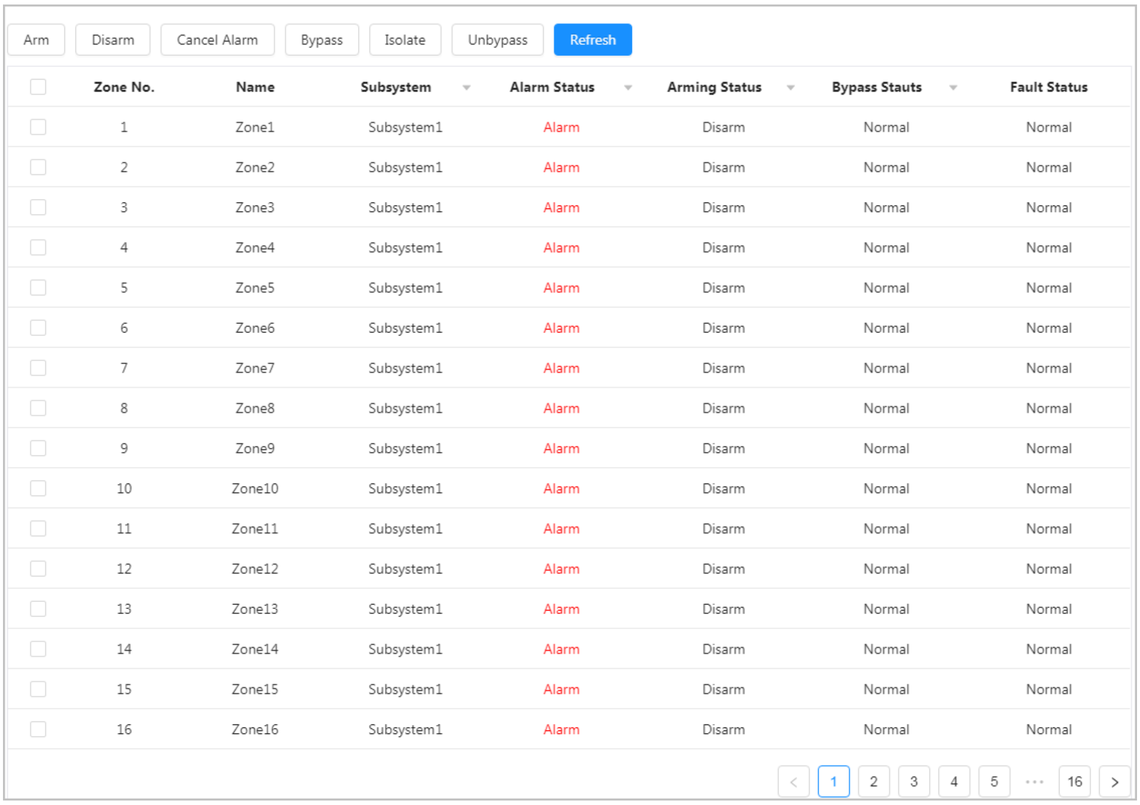
Step 1 Log in to the web, and then select **Alarm Management** > **Zone**.

Step 2 Select a zone.

Step 3 Click **Arm**, **Disarm**, **Cancel Alarm**, **Bypass**, **Isolate** or **Unbypass**.

The arming and bypass status of the zone changes after arming and disarming, and bypassing operations.

Figure 5-25 Zone settings



□	Zone No.	Name	Subsystem	Alarm Status	Arming Status	Bypass Stauts	Fault Status
□	1	Zone1	Subsystem1	Alarm	Disarm	Normal	Normal
□	2	Zone2	Subsystem1	Alarm	Disarm	Normal	Normal
□	3	Zone3	Subsystem1	Alarm	Disarm	Normal	Normal
□	4	Zone4	Subsystem1	Alarm	Disarm	Normal	Normal
□	5	Zone5	Subsystem1	Alarm	Disarm	Normal	Normal
□	6	Zone6	Subsystem1	Alarm	Disarm	Normal	Normal
□	7	Zone7	Subsystem1	Alarm	Disarm	Normal	Normal
□	8	Zone8	Subsystem1	Alarm	Disarm	Normal	Normal
□	9	Zone9	Subsystem1	Alarm	Disarm	Normal	Normal
□	10	Zone10	Subsystem1	Alarm	Disarm	Normal	Normal
□	11	Zone11	Subsystem1	Alarm	Disarm	Normal	Normal
□	12	Zone12	Subsystem1	Alarm	Disarm	Normal	Normal
□	13	Zone13	Subsystem1	Alarm	Disarm	Normal	Normal
□	14	Zone14	Subsystem1	Alarm	Disarm	Normal	Normal
□	15	Zone15	Subsystem1	Alarm	Disarm	Normal	Normal
□	16	Zone16	Subsystem1	Alarm	Disarm	Normal	Normal

5.3.3 Relay Output

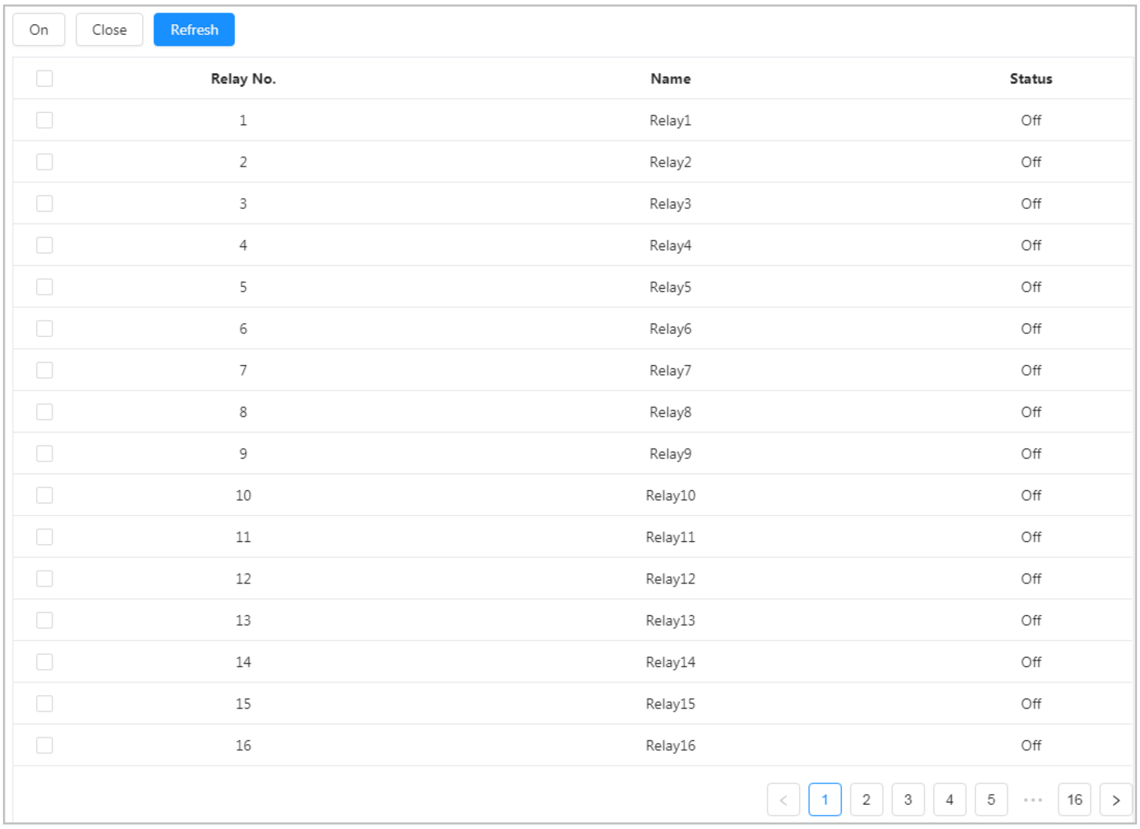
Turn on or off relays.

Step 1 Log in to the web, and then select **Alarm Management** > **Relay**.

Step 2 Select a relay.

Step 3 Click **On** or **Close** to turn on or off the relay.

Figure 5-26 Relay configuration



□	Relay No.	Name	Status
□	1	Relay1	Off
□	2	Relay2	Off
□	3	Relay3	Off
□	4	Relay4	Off
□	5	Relay5	Off
□	6	Relay6	Off
□	7	Relay7	Off
□	8	Relay8	Off
□	9	Relay9	Off
□	10	Relay10	Off
□	11	Relay11	Off
□	12	Relay12	Off
□	13	Relay13	Off
□	14	Relay14	Off
□	15	Relay15	Off
□	16	Relay16	Off

5.3.4 Siren

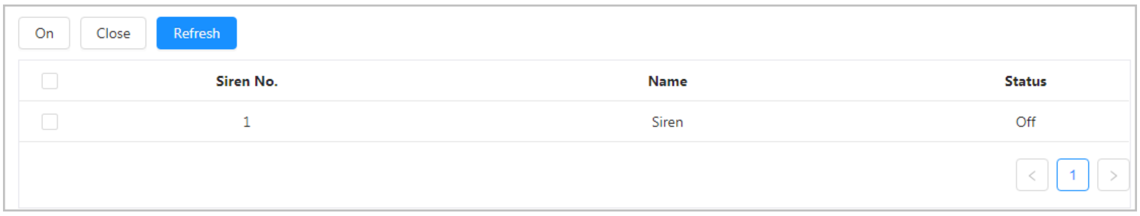
Turn on or off a siren.

Step 1 Log in to the web, and then select **Alarm Management** > **Siren**.

Step 2 Select a siren.

Step 3 Click **On** or **Close** to turn on or off the siren.

Figure 5-27 Siren



□	Siren No.	Name	Status
□	1	Siren	Off

5.4 Network Management

5.4.1 TCP/IP

You can configure the IP address, DNS (Domain Name System) server and more according to the network plan.

Prerequisites

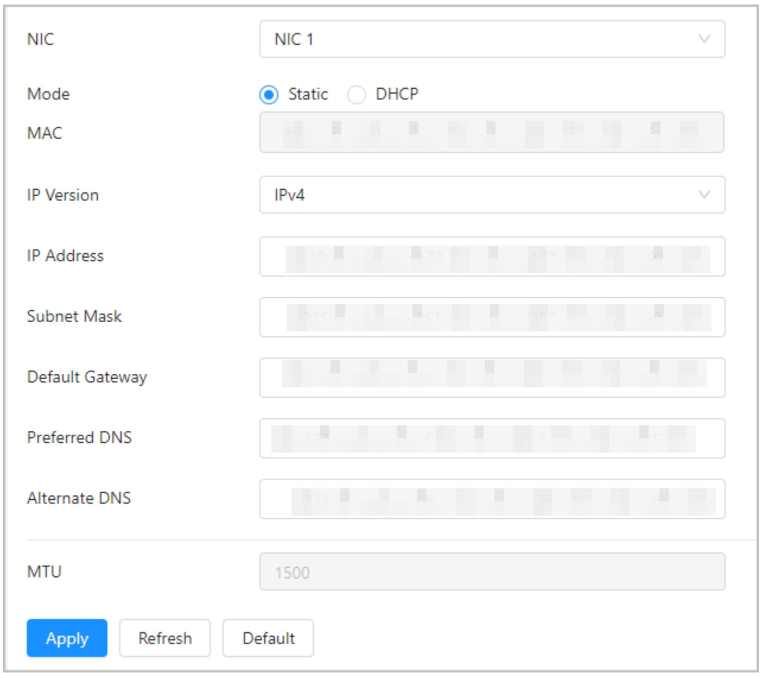
The control panel is connected to the network.

Procedure

Step 1 Log in to the web, and then select **Network** > **TCP/IP**.

Step 2 Configure the TCP/IP parameters.

Figure 5-28 TCP/IP



NIC: NIC 1

Mode: ● Static ○ DHCP

MAC: [redacted]

IP Version: IPv4

IP Address: [redacted]

Subnet Mask: [redacted]

Default Gateway: [redacted]

Preferred DNS: [redacted]

Alternate DNS: [redacted]

MTU: 1500

Table 5-6 Description of TCP/IP parameters

Parameter	Description
NIC	Select **NIC1** or **NIC2** for devices with two network cards. The default IP address of LAN1 is 192.168.1.108, and LAN2 is 192.168.2.108.
Mode	● **Static** Configure **IP Address**, **Subnet Mask**, and **Default Gateway** manually, and then click **Save**, the login page with the configured IP address is displayed. ● **DHCP (Dynamic Host Configuration Protocol)** If there is a DHCP server on the network, select **DHCP**, and the control panel acquires the network information such as the IP address automatically.
MAC Address	Displays the MAC address (Media Access Control) of the control panel.
IP Version	Select **IPv4** or **IPv6**.
IP Address	Select **Static** in **Mode**, and enter the IP address and subnet mask that you need. 📖 ● IPv6 does not have a subnet mask. ● The default gateway must be in the same network segment as the IP address.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the alternate DNS.

Parameter	Description
MTU	Adjust the MTU value according to the network environment and communication conditions to obtain good transmission rate. The default MTU value is 1500 bytes. The recommended MTU values for different situations are as follows. ● 1500: By default. It is the typical settings for network connections that do not have PPPOE and VPN. It is also the default setting of some routers, network adapters and switches. ● 1492: The optimum value for PPPOE. ● 1468: The optimum value for DHCP. ● 1450: The optimum value for VPN.

Step 3 Click **Apply**.

5.4.2 2G/4G

Prerequisites

Install 2G/4G modules first.

Background Information

Connect the device to a 2G/4G network through the dial-up method of different operators. Then you can receive information on alarms and the status of devices on your mobile device.

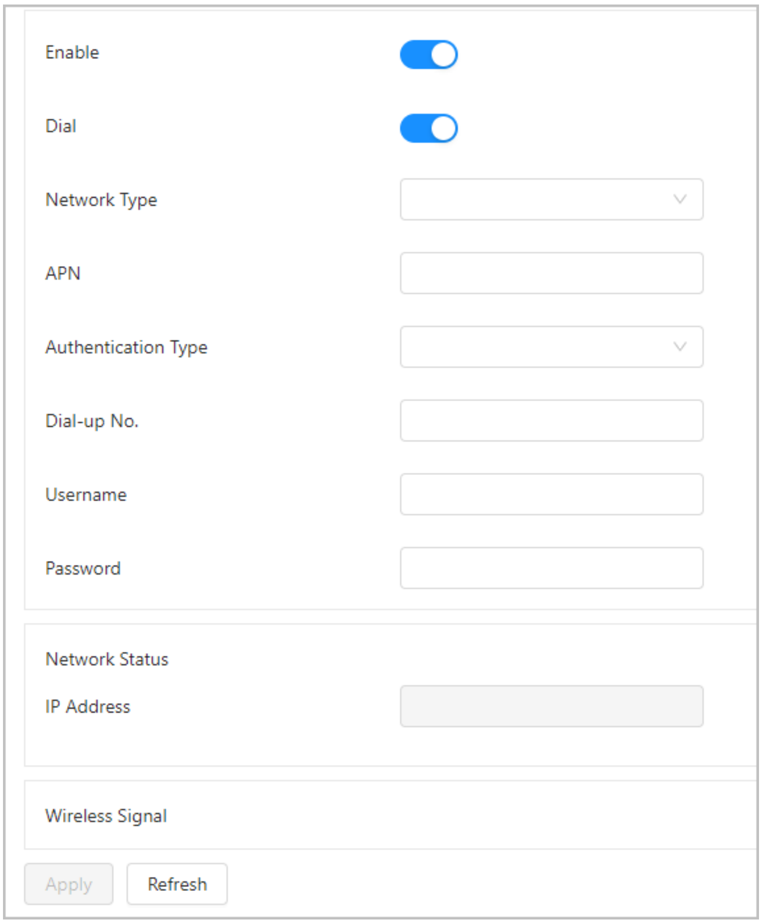
Procedure

Step 1 Log in to the web, and then select **Network** > **2G/4G**.

Step 2 Enable the module and **Dial**.

Step 3 Configure the parameters.

Figure 5-29 2G/4G



Enable
Dial
Network Type
APN
Authentication Type
Dial-up No.
Username
Password
Network Status
IP Address
Wireless Signal

Table 5-7 Description of 2G/4G parameters

Parameter	Description
Network Type	It is **Auto** by default.
APN	Displays the MAC address (Media Access Control) of the control panel.
Authentication Type	The control panel fills in the dial information automatically after recognizing 2G/4G module. You only need to manually enter the dial information if you use a special card.
Dial-up Number	
Username, Password	
Network Status, IP Address, Wireless Signal	—

Step 4 Click **Apply**.

5.4.2.1 Arming and Disarming Via SMS

Function

Send a text message to arm and disarm the subsystem.

Command

Enter the operation code + # + subsystem number (1 digit).

The operation code includes:

- Cancel alarms: 00
- Disarm: 01
- Arm: 02

Example

- Cancel the alarm for subsystem 1: Enter 00#1.
- Disarm subsystem 1: Enter 01#1.
- Arm subsystem 1: Enter 02#1.

5.4.2.2 Bypassing and Isolating Zones Via SMS

Function

Send a text message to bypass the zone.

Command

Enter the operation code + # + zone number.

The operation code includes:

- Unbypass: 04
- Bypass: 05
- Isolate: 06

Example

- Unbypass zone 1: Enter 04#1.
- Bypass zone 1: Enter 05#1.
- Isolate zone 1: Enter 06#1.
- Unbypass zone 256: Enter 04#256.
- Bypass zone 256: Enter 05#256.
- Isolate zone 256: Enter 06#256.

5.4.2.3 Voice Prompt

Function

Make a voice call and perform operations according to the voice prompt. Operations include arming and disarming the subsystem, cancelling the alarm, bypassing and isolating zones.

Voice Prompt

After you make a voice call, perform operations according to the voice prompt.

Voice prompt includes:

- Cancel alarms: Enter 1
- Arm and disarm: Enter 2
- Bypass: Enter 3
- Repeat voice prompt: Enter 4

Command

- Cancel alarms: Enter 1 + subsystem number (2 digits).
- Disarm the subsystem: Enter 2 + 1 + subsystem number (2 digits).
- Away arm the subsystem: Enter 2 + 2 + subsystem number (2 digits).
- Home arm the subsystem: Enter 2 + 3 + subsystem number (2 digits).
- Unbypass the zone: Enter 3 + 1 + zone number (3 digits).
- Bypass the zone: Enter 3 + 2 + zone number (3 digits).
- Isolate the zone: Enter 3 + 3 + zone number (3 digits).

Example

- Cancel the alarms for subsystem 1: Enter 1 + 01 in sequence according to the voice prompt.
- Disarm subsystem 1: Enter 2 + 1 + 01 in sequence according to the voice prompt.
- Away arm subsystem 1: Enter 2 + 2 + 01 in sequence according to the voice prompt.
- Home arm subsystem 1: Enter 2 + 3 + 01 in sequence according to the voice prompt.
- Unbypass zone 1: Enter 3 + 1 + 001 in sequence according to the voice prompt.
- Bypass zone 1: Enter 3 + 2 + 001 in sequence according to the voice prompt.
- Isolate zone 1: Enter 3 + 3 + 001 in sequence according to the voice prompt.

5.4.3 Port

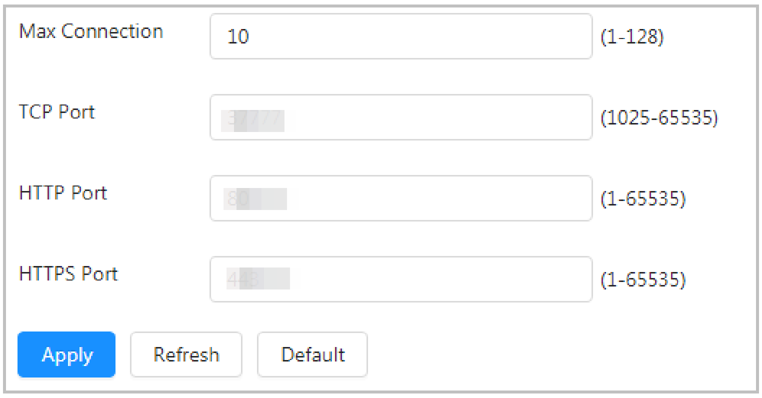
Configure the maximum port numbers and values.

Step 1 Log in to the web, and then select **Network** > **Port**.

Step 2 Configure each port of the control panel.

Except **Max Connection**, modifications of other parameters will take effect after restart.

Figure 5-30 Port



Max Connection	10	(1-128)
TCP Port	[redacted]	(1025-65535)
HTTP Port	[redacted]	(1-65535)
HTTPS Port	[redacted]	(1-65535)

Table 5-8 Port parameters description

Parameter	Description
Max. Connection	The maximum number of clients accessing the Device at the same time, such as clients accessing through the web, platform, and mobile phone.
TCP port	TCP service port. You can enter the value as needed. It is 37777 by default.
UDP Port	User datagram protocol port. You can enter the value as needed. It is 37778 by default.
HTTP Port	HTTP communication port. You can enter the value as needed. It is 80 by default. If you enter other values, enter the modified port number after the IP address when logging in to the Device in the browser.
HTTPS Port	HTTPS communication port. You can enter the value as needed. It is 443 by default.

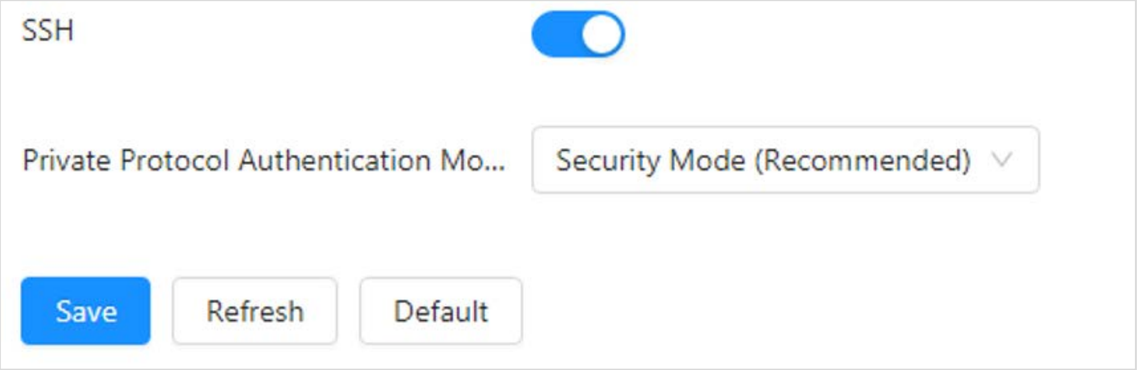
Step 3 Click **Apply**.

5.4.4 Basic Services

SSH (Secure Shell) protocol provides security protection for remote dialog login and network services. Through configuring system services, it can secure the system. It is disabled by default, and it needs authentication after being enabled to access security management and encrypt data during transmission. **Security Mode** is recommended for **Private Protocol Authentication Mode**.

Log in to the web, and then select **Network** > **Basic Services**.

Figure 5-31 Basic services



SSH

Private Protocol Authentication Mo... Security Mode (Recommended)

5.5 Device Information

Log in to the web, select **Device Info**, and then the control panel features, version, system status, module and legal information will be displayed.

- **Features**: Displays the number of alarm input, alarm output and sirens.
- **Version**: Displays the device model, SN, system version and other information.
- **System Status**: Displays the undervoltage status, battery status, power supply, control panel tamper, PSTN offline and other information.
- **Module**: Displays information on the keypad and RS-485 module of the control panel.
- **Legal Info**: The open source software agreement of the control panel.

5.6 System Management

5.6.1 Account

5.6.1.1 Web User

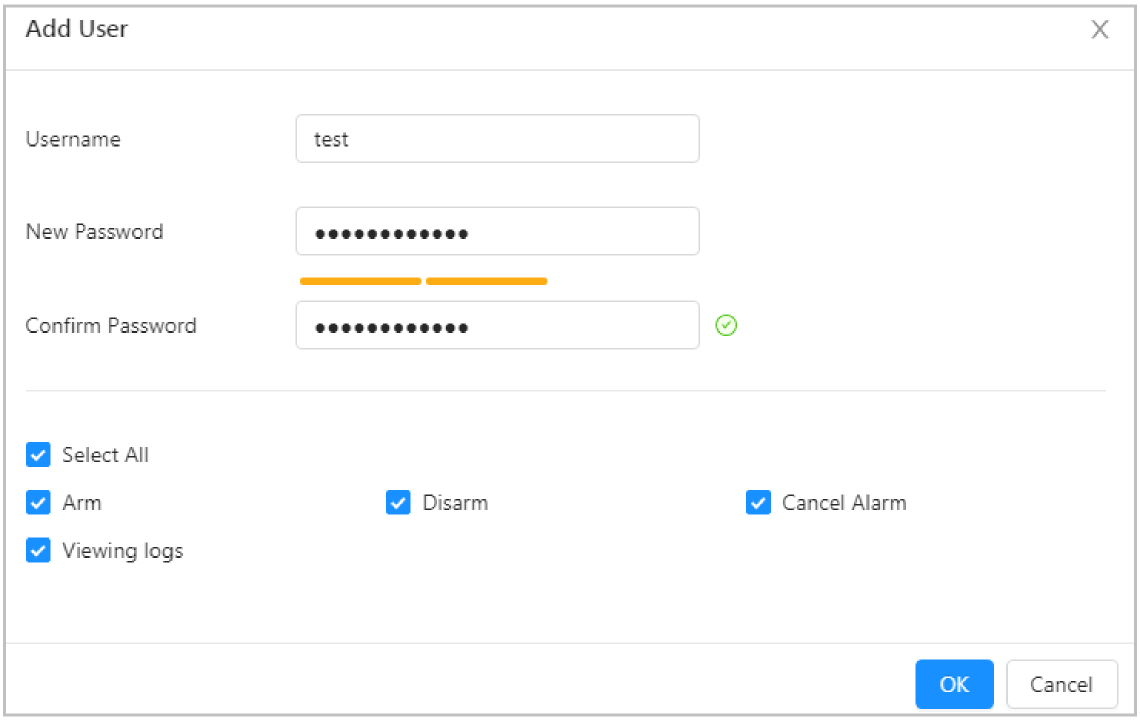
You can add, edit and delete user accounts which can log in to the control panel web page.

Step 1 Log in to the web, and then select **System** > **Account** > **Web User**.

Step 2 Click **Add**.

Step 3 Configure the parameters.

Figure 5-32 Add web user



Add User

Username: test

New Password: ●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●

☑ Select All

☑ Arm ☑ Disarm ☑ Cancel Alarm

☑ Viewing logs

Table 5-9 Web user parameters description

Parameter	Description
Username, New Password, Confirm Password	Enter the user name and password, and confirm the password.
User permissions	Grant the user permissions to arm, disarm and cancel alarms and to view logs.

Step 4 Click **OK**.

5.6.1.2 Keypad User

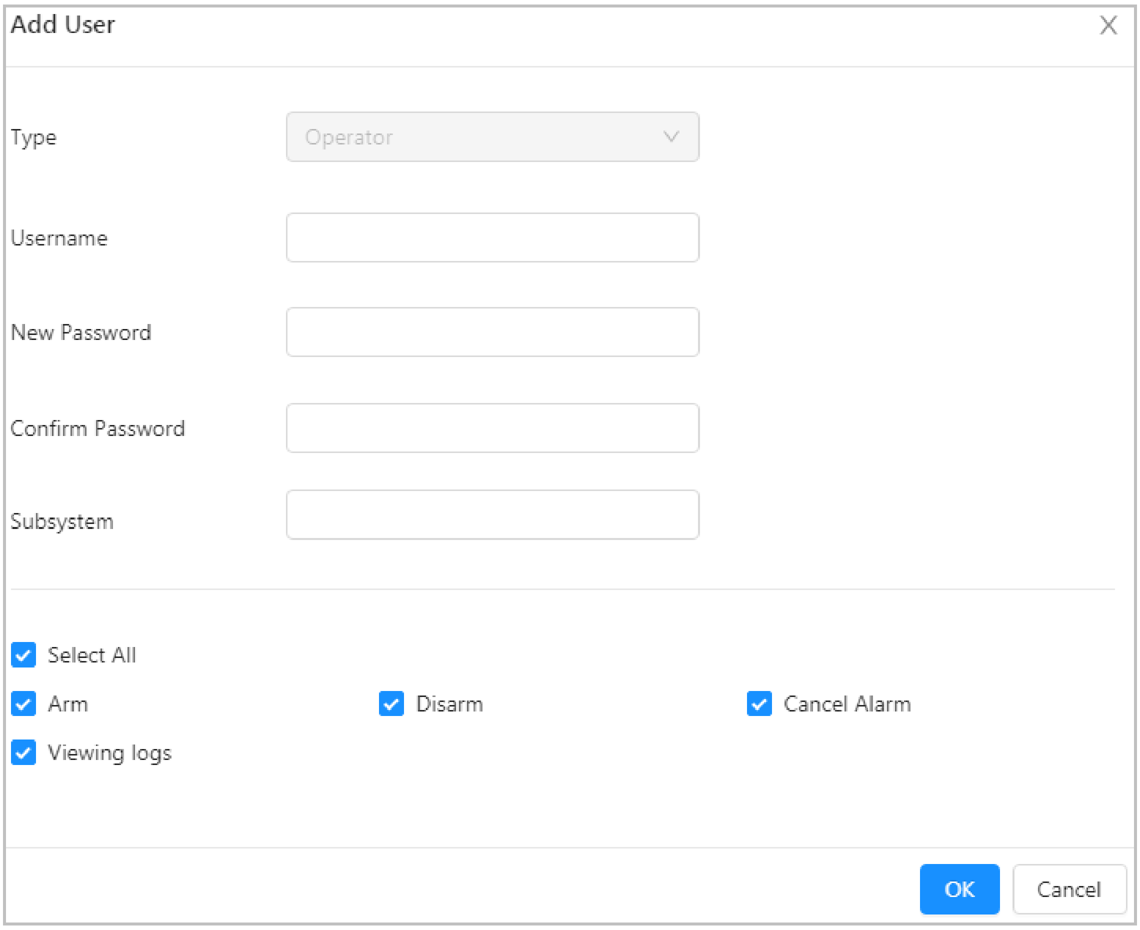
Keypad user can execute operations such as arming/disarming, alarm cancel and viewing logs through the keypad.

Step 1 Log in to the web, and then select **System** > **Account** > **Keypad User**.

Step 2 Click **Add**.

Step 3 Configure the parameters.

Figure 5-33 Add keypad user


Add User

Type: Operator

Username:

New Password:

Confirm Password:

Subsystem:

☑ Select All

☑ Arm ☑ Disarm ☑ Cancel Alarm

☑ Viewing logs

Table 5-10 Keypad user parameters description

Parameter	Description
Type	It is **Operator** by default.
Username, New Password, Confirm Password	Enter the username, password and confirm password.
Subsystem	Link subsystems of the keypad user. Multiple selections are available.
User permissions	Grant the user permissions to arm, disarm and cancel alarms and to view logs.

Step 4 Click **OK**.

5.6.1.3 Keyfob User

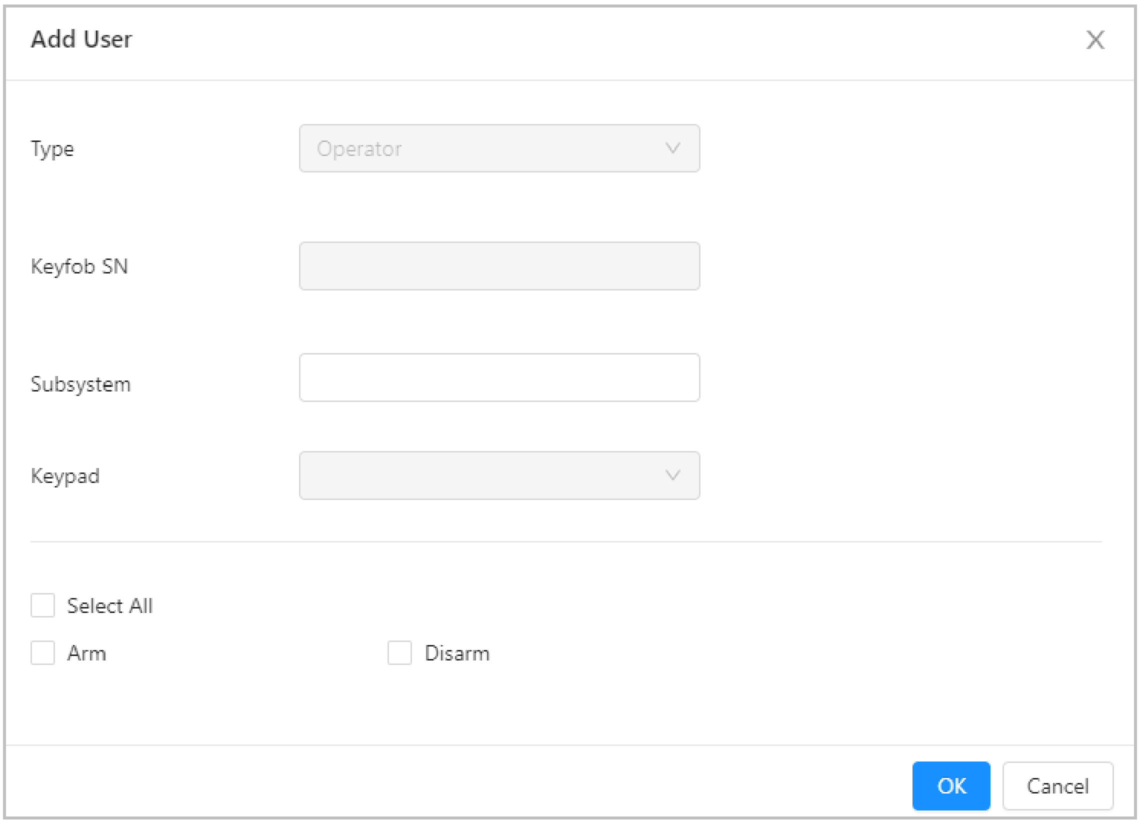
You can arm and disarm the control panel, and upload panic alarm through the keyfob.

Step 1 Log in to the web, and then select **System** > **Account** > **Keyfob User**.

Step 2 Click **Add**, and then press and hold the keyfob until the indicator lights up. The control panel automatically obtains the keyfob SN.

Step 3 Configure the parameters.

Figure 5-34 Add keyfob user



Add User

Type: Operator

Keyfob SN

Subsystem

Keypad

□ Select All

□ Arm □ Disarm

Table 5-11 Keyfob user parameters description

Parameter	Description
Type	It is **Operator** by default.
Keyfob SN	Automatically obtained from the keyfob after it is turned on.
Subsystem	Link subsystems of the keyfob user. Multiple selections are available.
Keypad	The control panel can be paired with up to 32 different keypads, but each keyfob can only be bound to a keypad. You cannot change the keypad that is bound to the keyfob.
User permissions	Grant the keyfob user permissions to arm (such as home arm and away arm) and disarm.

Step 4 Click **OK**.

Step 5 Press **Home**, **Away**, **Disarm** or **SOS** on the keyfob.

5.6.1.4 Card Owner

IC card owner can arm and disarm the control panel after being added to the system.

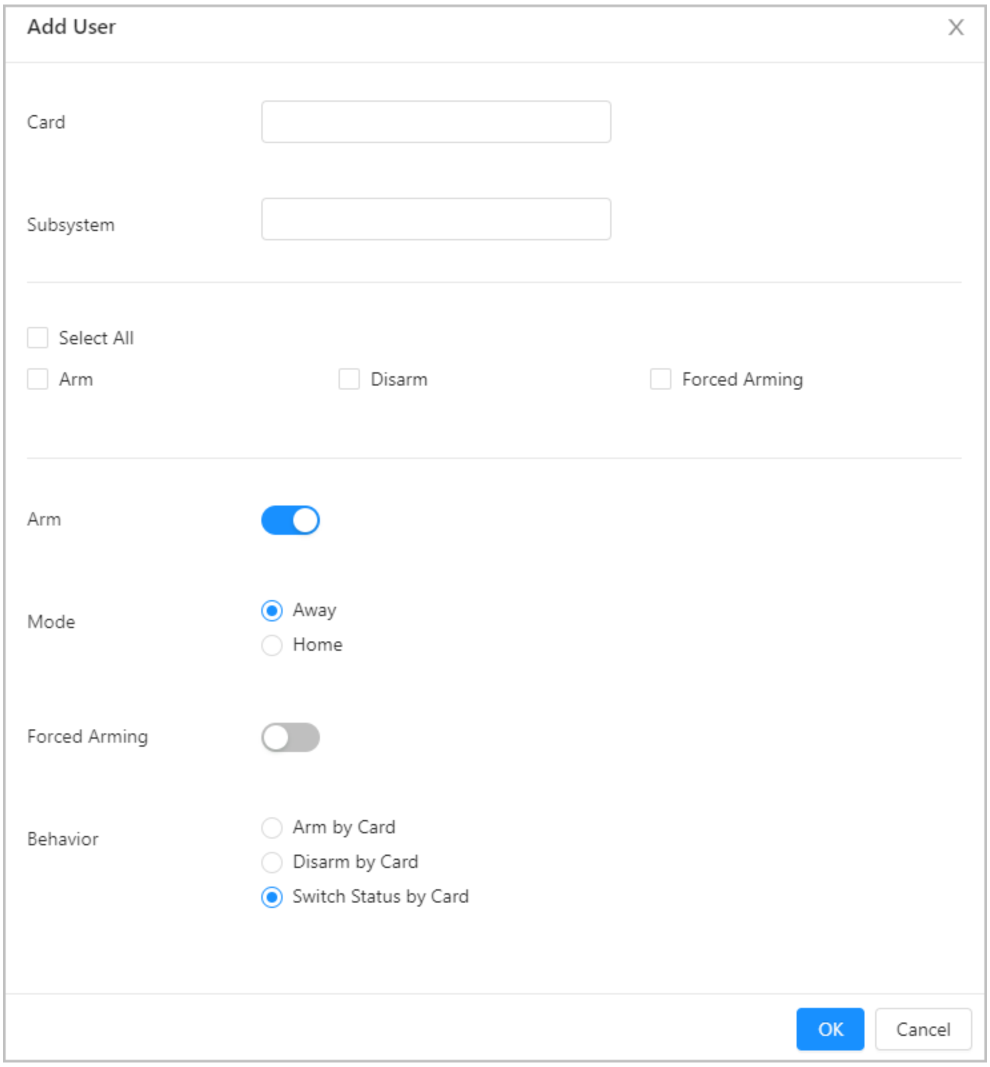
Connect a keypad to the alarm control panel.

Step 1 Log in to the web, and then select **System** > **Account** > **Card Owner**.

Step 2 Click **Add**, and then swipe the card on the keypad to have its card number read.

Step 3 Configure the parameters.

Figure 5-35 Add card owner



Add User

Card

Subsystem

□ Select All

□ Arm □ Disarm □ Forced Arming

Arm: on

Mode: ● Away ○ Home

Forced Arming: off

Behavior: ○ Arm by Card ○ Disarm by Card ● Switch Status by Card

Table 5-12 Add card owner parameters description

Parameter	Description
Card	Automatically obtained by the control panel when swiping it on the keypad.
Subsystem	Link subsystems of the card owner. Multiple selections are available.
User permissions	Grant the card owner permissions to arm and disarm.
Arm	Enable arm. ● **Mode**: Select between **Home** and **Away**. ● **Forced Arming**: You can arm the subsystem when an alarm is being triggered. ● Behavior ◇ **Arm by Card**: Arm. ◇ **Disarm by Card**: Disarm. ◇ **Switch Status by Card**: Switch the current arming status of the control panel by swiping the card.

Step 4 Click **OK**.

5.6.1.5 Mobile User

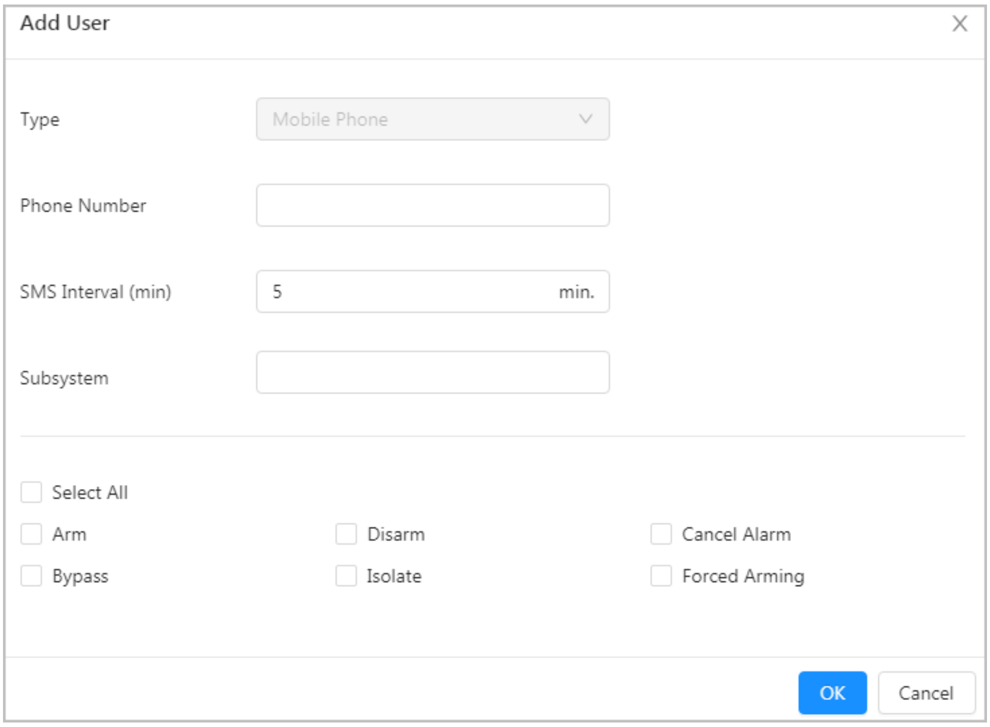
You can arm and disarm the control panel, and report an alarm through your mobile phone after it is added to the system.

Step 1 Log in to the web, and then select **System** > **Account** > **Mobile User.**

Step 2 Click **Add**.

Step 3 Configure the parameters.

Figure 5-36 Add mobile user



Add User ×

Type: Mobile Phone

Phone Number:

SMS Interval (min): 5 min.

Subsystem:

□ Select All

□ Arm □ Disarm □ Cancel Alarm

□ Bypass □ Isolate □ Forced Arming

Table 5-13 Mobile user parameters description

Parameter	Description
Type	It is **Mobile Phone** by default.
Phone Number	Enter the mobile phone number.
SMS Interval (min)	The time interval for when the same alarm SMS is sent to your mobile phone. It needs to be an integer between 0 and 5.
Subsystem	Select the subsystem to which the mobile user belongs to. Multiple selections are available.
User permission	Grant the user permission to arm, disarm, and cancel alarms, to bypass and more.

Step 4 Click **OK**.

5.6.1.6 Key User

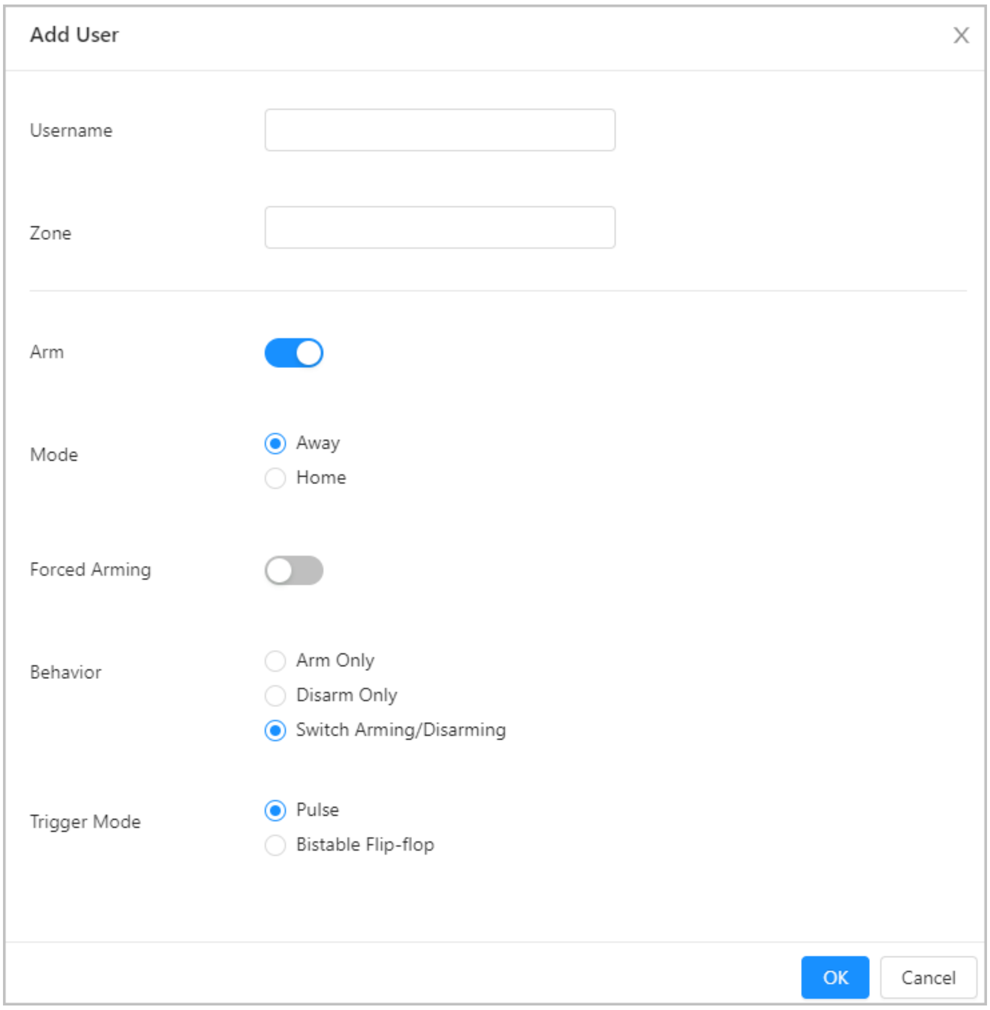
Add key users and link them to key zones, and then these key users will be able to arm and disarm the subsystems of the zone.

Step 1 Log in to the web, and then select **System** > **Account** > **Key User.**

Step 2 Click **Add**.

Step 3 Configure the parameters.

Figure 5-37 Add key user



Add User

Username

Zone

Arm: ● (on)

Mode: ● Away ○ Home

Forced Arming: ○ (off)

Behavior: ○ Arm Only ○ Disarm Only ● Switch Arming/Disarming

Trigger Mode: ● Pulse ○ Bistable Flip-flop

Table 5-14 Add key user parameters description

Parameter	Description
Username	Enter the username.
Zone	Links zone to the key user. Multiple selections are available.
Arm	Enable arm. ● **Mode**: Select between **Home** and **Away**. ● **Forced Arming**: You can arm the subsystem when errors happen in zones under the subsystem. ● Behavior ◇ **Arm Only**: Arm. ◇ **Disarm Only**: Disarm. ◇ **Switch Arming/Disarming**: Switch the arming status of the subsystem corresponding with the key zone. ● Trigger Mode ◇ **Pulse**: Variable type. The status of the key zone from before-triggering to triggered. ◇ **Bistable Flip-flop**: Fixed type. Disarm when the key zone changes from triggered to before-triggering, and arm when it changes from before-triggering to triggered.

Step 4 Click **OK**.

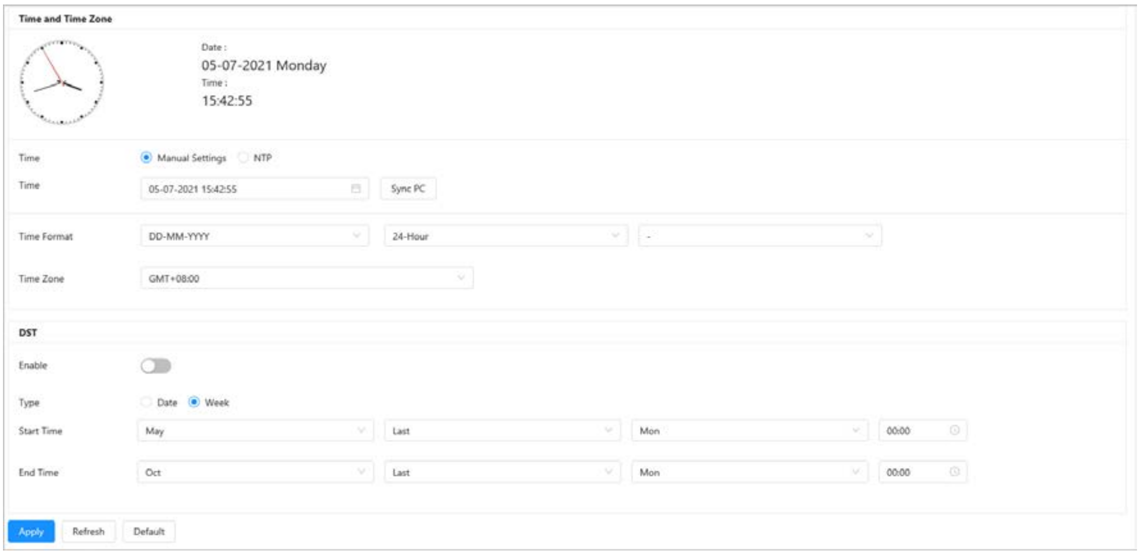
5.6.2 Time Settings

Configure the date and time zone, DST and other parameters of the Device.

Step 1 Log in to the web, and then select **System** > **Time**.

Step 2 Configure the parameters.

Figure 5-38 Time settings



Time and Time Zone

Date : 05-07-2021 Monday

Time : 15:42:55

Time: ● Manual Settings ○ NTP

Time: 05-07-2021 15:42:55 Sync PC

Time Format: DD-MM-YYYY 24-Hour -

Time Zone: GMT+08:00

DST

Enable

Type: ○ Date ● Week

Start Time: May Last Mon 00:00

End Time: Oct Last Mon 00:00

Apply Refresh Default

Table 5-15 Time settings parameter description

Parameter	Description
Time	Select **Manual Settings** or **NTP**.
Manual Settings	Set the time manually. Set the date and time of the current system for the Device. Click **Sync local computer** to sync with the time of local computer.
NTP	Enable the NTP function to sync the control panel time with the NTP server. ● **Server**: Enter the IP address of the server that has NTP services installed, or click **Manual Update** to sync the Device time with NTP server. ● **Port**: The system only supports TCP protocol and the default setting is 123 (1–65535). ● **Interval**: Enter the time interval when you want the control panel to sync its time with the NTP server. The maximum value is 65535 minutes.
Time Format	● Select a date format, including **YYYY-MM-DD**, **MM-DD-YYYY**, and **DD-MM-YYYY**. ● Select **24-Hour** or **12-Hour**. ● Set separator for the time format.
Time Zone	Select a time zone according to the location of the control panel.

Parameter	Description
DST	Some countries or regions adopt DST system. You can enable this function as needed. 1. Enable **DST**. 2. Select type from **Date** or **Week**. 3. Set start time and end time.

Step 3 Click **Apply**.

5.6.3 Device Maintenance

5.6.3.1 Device Maintenance

Automatic Restart

Select **System** > **Maintenance** > **Maintenance** to set week and time of automatic restart. Click **Apply** to save the configurations. The system automatically restarts at the set time.

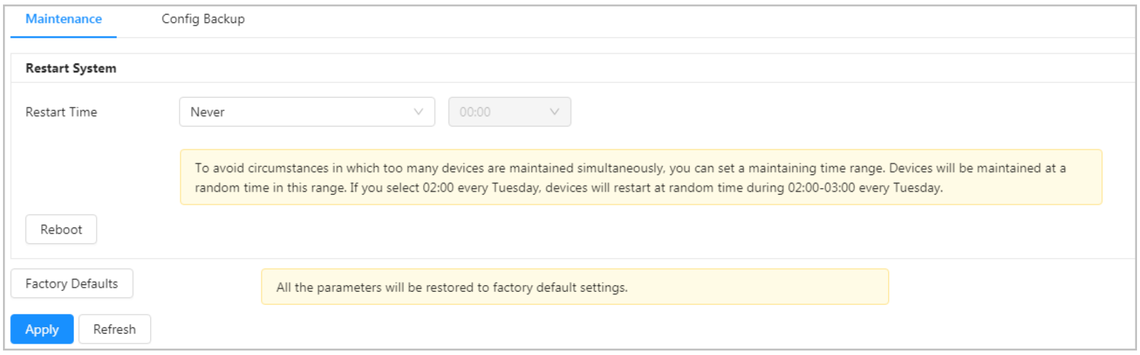
Manual Restart

Select **System** > **Maintenance** > **Maintenance**, and then click **Reboot**. The system restarts immediately when you confirm to restart as prompted.

Restore Default

Select **System** > **Maintenance** > **Maintenance**, and then click **Factory Defaults**, enter the password of admin account and then click **OK**. The system restarts and restores all parameters (other than IP) to the factory default after you confirm to do so as prompted.

Figure 5-39 Maintenance



Restart Time: Never 00:00

To avoid circumstances in which too many devices are maintained simultaneously, you can set a maintaining time range. Devices will be maintained at a random time in this range. If you select 02:00 every Tuesday, devices will restart at random time during 02:00-03:00 every Tuesday.

All the parameters will be restored to factory default settings.

5.6.3.2 Configuring Backup

Import or export a system profile. You can apply the same parameters to multiple devices by using a configuration backup file.

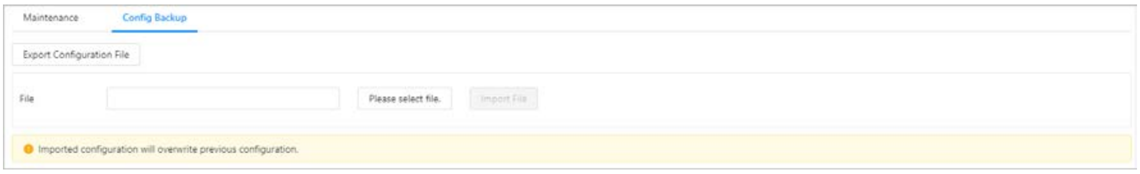
Step 1 Logging in to web, and then select **System** > **Maintenance** > **Maintenance** > **Config Backup**.

Step 2 Click **Please Select File** to select a profile to import.

Step 3 Click **Import File** to complete import of the backup data.

Step 4 Click **Export Configuration File** to save all profiles on the web locally as prompted.

Figure 5-40 Configure backup



Imported configuration will overwrite previous configuration.

5.6.3.3 Walk Test (Installer)

Test the work status of installed detectors, and the reaction of the control panel when triggering or turning off the detector. Walk test mode can test the validity of one or more detectors.

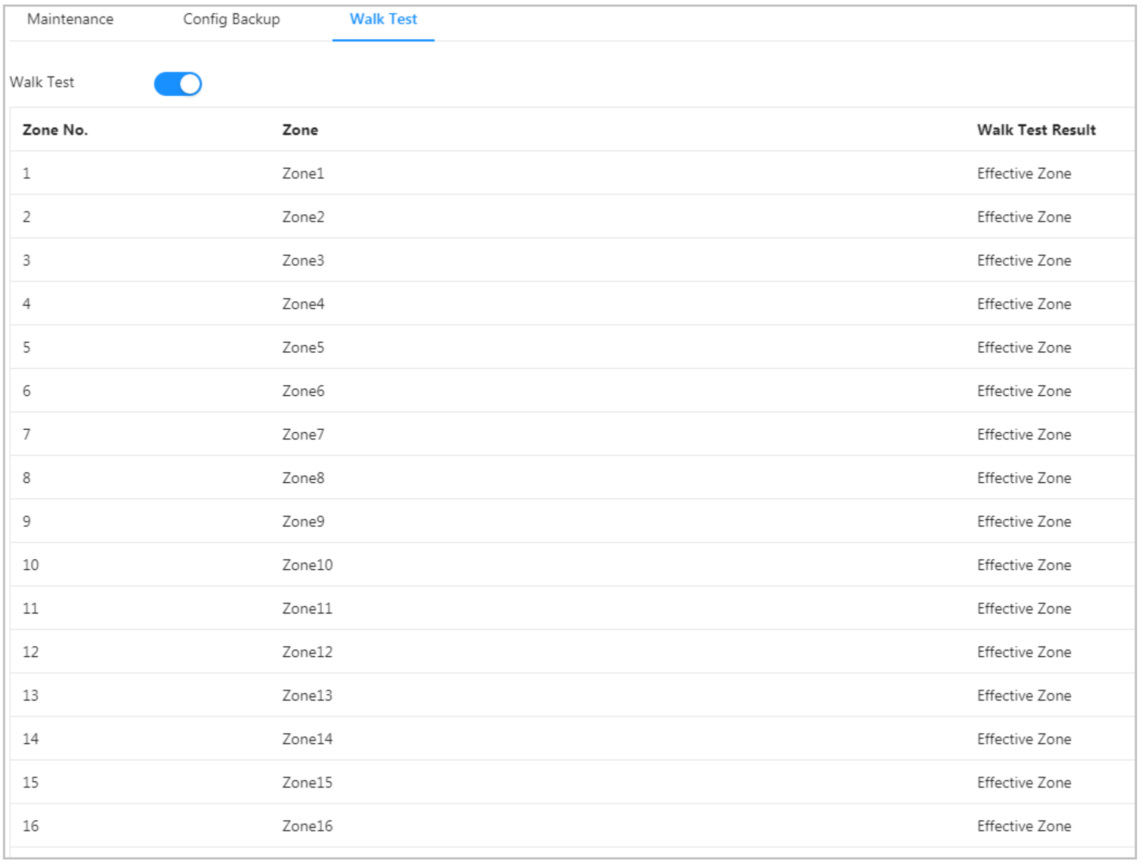
Walk test function is only available to the installer.

Step 1 Log in to the web, and then select **System** > **Maintenance** > **Walk Test**.

Step 2 Enable **Walk Test**, and then check for the test results.

- **Effective Zone**: Detectors were triggered.
- **Ineffective Zone**: Detectors were not triggered.

Figure 5-41 Walk test



Walk Test ●

Zone No.	Zone	Walk Test Result
1	Zone1	Effective Zone
2	Zone2	Effective Zone
3	Zone3	Effective Zone
4	Zone4	Effective Zone
5	Zone5	Effective Zone
6	Zone6	Effective Zone
7	Zone7	Effective Zone
8	Zone8	Effective Zone
9	Zone9	Effective Zone
10	Zone10	Effective Zone
11	Zone11	Effective Zone
12	Zone12	Effective Zone
13	Zone13	Effective Zone
14	Zone14	Effective Zone
15	Zone15	Effective Zone
16	Zone16	Effective Zone

5.6.4 System Update

Background Information

⚠

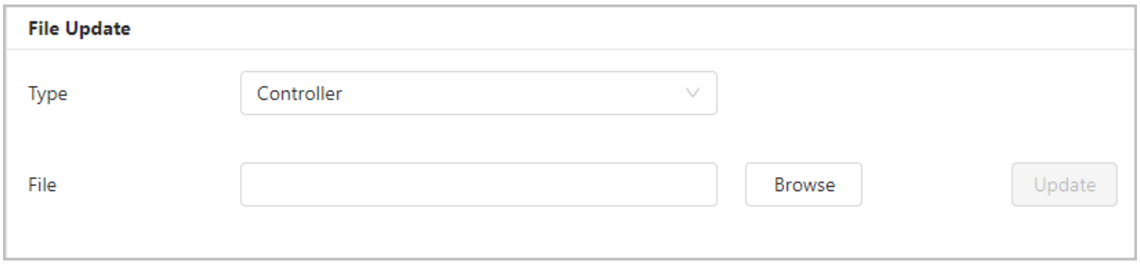
- Only administrator and manufacturer can perform system updates. The zone must be disarmed when the system is being updated.
- During an update, do not power off, restart or shut down the control panel, or disconnect the system from the network.
- Please select the correct update files. Updating the wrong program will cause the control panel to behave abnormally.

Procedure

Step 1 Log in to the web with the manufacturer account, and then select **System** > **Update**.

Step 2 Configure the parameters.

Figure 5-42 System update



File Update

Type: Controller

File:

Table 5-16 Alarm receiving center parameter description

Parameter	Description
Please select type	Select upgrade method as needed.
Address	Only the following three update types require address. ● **Alarm Keypad**: Keypad address. ● **ARM808-RS Module**: DIP address. ● **ARM708-RS Module**: DIP address.

Step 3 Click **Browse**, and then select the upgrade file (.bin file) to be imported.

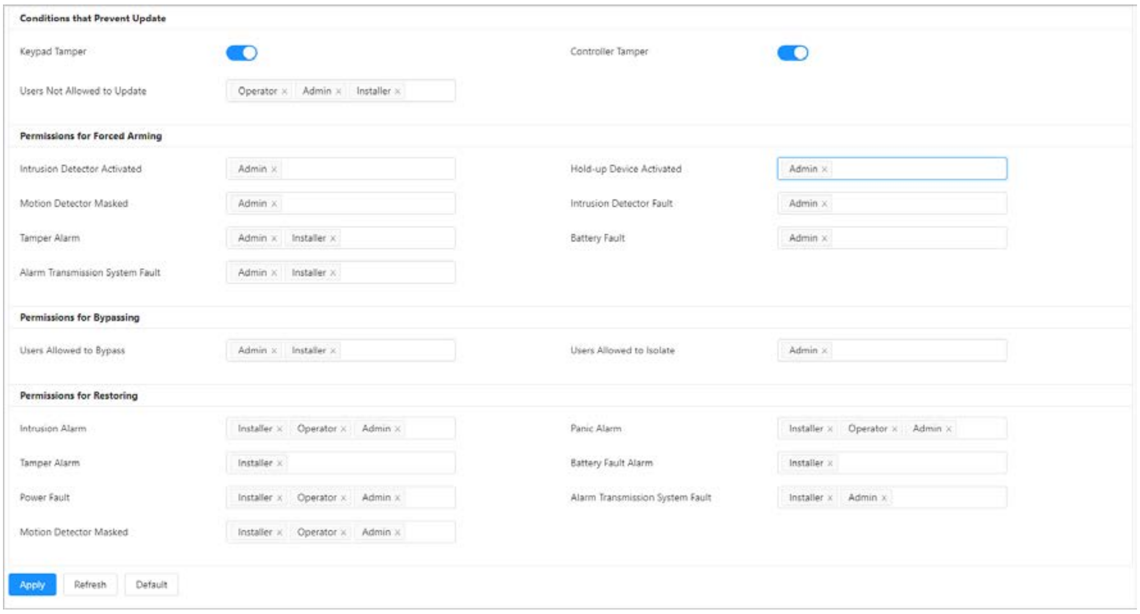
Step 4 Click **Update** to upgrade the system.

After the upgrade is complete, the control panel and the web Manager will restart.

5.6.5 System Detection

After enabling the system detection feature, the entire business logics of the control panel conform to standards. Default values are recommended.

Figure 5-43 System detection



Conditions that Prevent Update

Keypad Tamper: On
Controller Tamper: On
Users Not Allowed to Update: Operator ×, Admin ×, Installer ×

Permissions for Forced Arming

Intrusion Detector Activated: Admin ×
Hold-up Device Activated: Admin ×
Motion Detector Masked: Admin ×
Intrusion Detector Fault: Admin ×
Tamper Alarm: Admin ×, Installer ×
Battery Fault: Admin ×
Alarm Transmission System Fault: Admin ×, Installer ×

Permissions for Bypassing

Users Allowed to Bypass: Admin ×, Installer ×
Users Allowed to Isolate: Admin ×

Permissions for Restoring

Intrusion Alarm: Installer ×, Operator ×, Admin ×
Panic Alarm: Installer ×, Operator ×, Admin ×
Tamper Alarm: Installer ×
Battery Fault Alarm: Installer ×
Power Fault: Installer ×, Operator ×, Admin ×
Alarm Transmission System Fault: Installer ×, Admin ×
Motion Detector Masked: Installer ×, Operator ×, Admin ×

5.7 Log

5.7.1 Viewing and Backing Up Logs

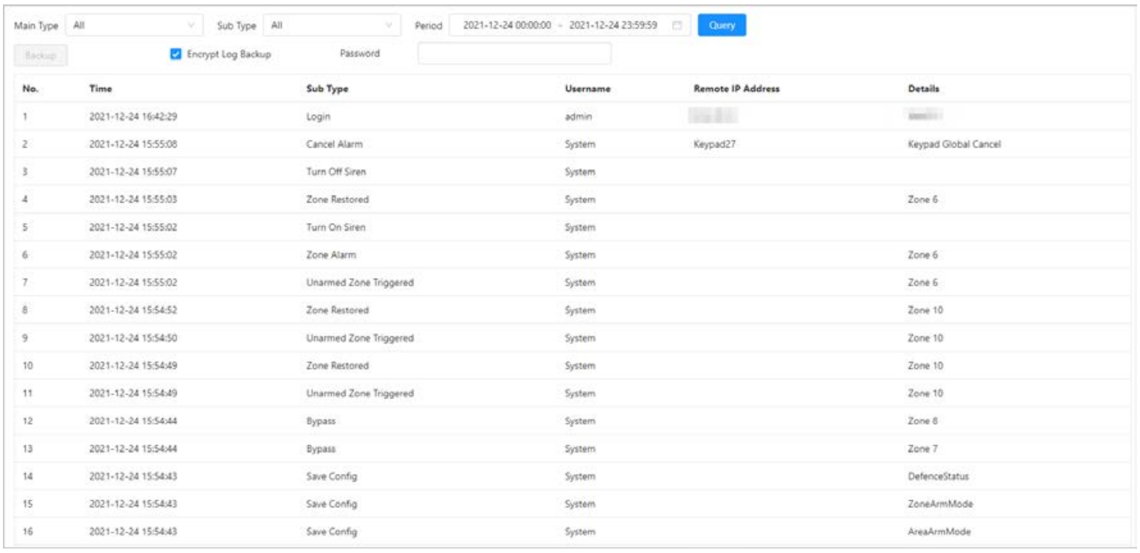
You can view and backup logs.

Step 1 Log in to the web, and then select **Log** > **Log**.

Step 2 Set **Main Type**, **Sub Type** and **Period**.

Step 3 Click **Query**.

Figure 5-44 Log



Main Type: All
Sub Type: All
Period: 2021-12-24 00:00:00 - 2021-12-24 23:59:59
☑ Encrypt Log Backup
Password:

No.	Time	Sub Type	Username	Remote IP Address	Details
1	2021-12-24 16:42:29	Login	admin	[redacted]	[redacted]
2	2021-12-24 15:55:08	Cancel Alarm	System	Keypad27	Keypad Global Cancel
3	2021-12-24 15:55:07	Turn Off Siren	System		
4	2021-12-24 15:55:03	Zone Restored	System		Zone 6
5	2021-12-24 15:55:02	Turn On Siren	System		
6	2021-12-24 15:55:02	Zone Alarm	System		Zone 6
7	2021-12-24 15:55:02	Unarmed Zone Triggered	System		Zone 6
8	2021-12-24 15:54:52	Zone Restored	System		Zone 10
9	2021-12-24 15:54:50	Unarmed Zone Triggered	System		Zone 10
10	2021-12-24 15:54:49	Zone Restored	System		Zone 10
11	2021-12-24 15:54:49	Unarmed Zone Triggered	System		Zone 10
12	2021-12-24 15:54:44	Bypass	System		Zone 8
13	2021-12-24 15:54:44	Bypass	System		Zone 7
14	2021-12-24 15:54:43	Save Config	System		DefenceStatus
15	2021-12-24 15:54:43	Save Config	System		ZoneArmMode
16	2021-12-24 15:54:43	Save Config	System		AreaArmMode

Step 4 Click **Backup** directly, or click **Encrypt Log Backup**, enter the password, and then click **Backup** to backup logs.

5.7.2 Remote Log

You can configure the remote syslog server to have the logs uploaded to it, and then you can view them on syslog server.

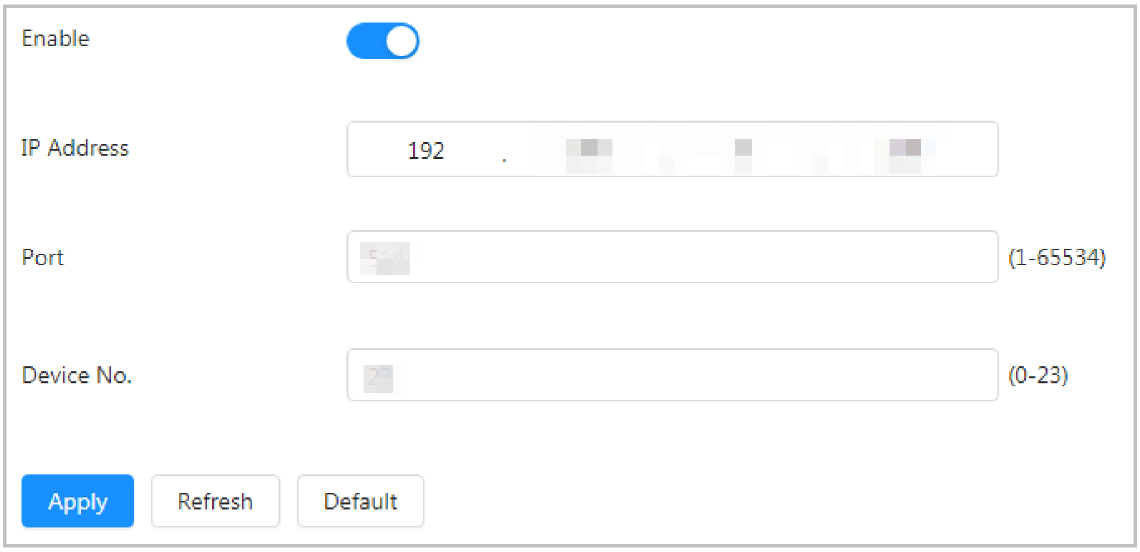
Step 1 Log in to the web, and then select **Log** > **Remote Log**.

Step 2 Click ○ next to **Enable** to enable the function.

Step 3 Set **IP Address**, **Port** and **Device No.** of the remote server.

Step 4 Click **Apply**.

Figure 5-45 Remote log



Enable	●	
IP Address	192 . [redacted]	
Port	[redacted]	(1-65534)
Device No.	[redacted]	(0-23)

5.7.3 Log Scraping

You can apply log scraping to view and analyze issues through logs.

Step 1 Log in to the web, and then, and then select **Log** > **Log Scraping**.

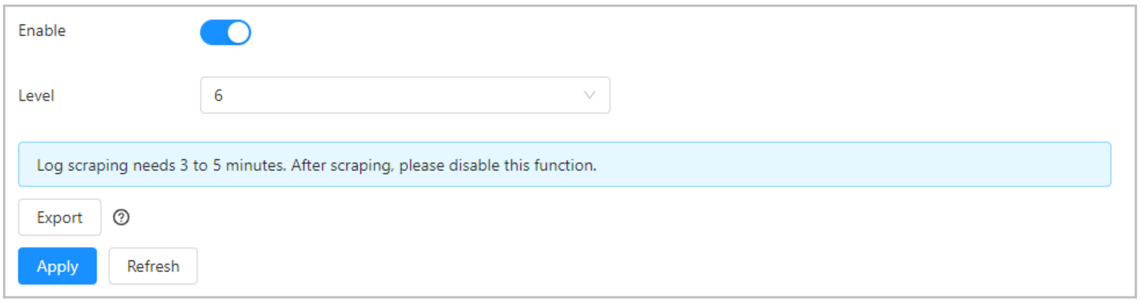
Step 2 Click ○ next to **Enable** to enable the function.

The higher the level of the logged in account, the greater the quantity of log information available.

Step 3 Click **Save**.

Step 4 Disable the function, click **Save** and then click **Export** to export scraped logs.

Figure 5-46 Log scraping



Enable: ●

Level: 6

Log scraping needs 3 to 5 minutes. After scraping, please disable this function.

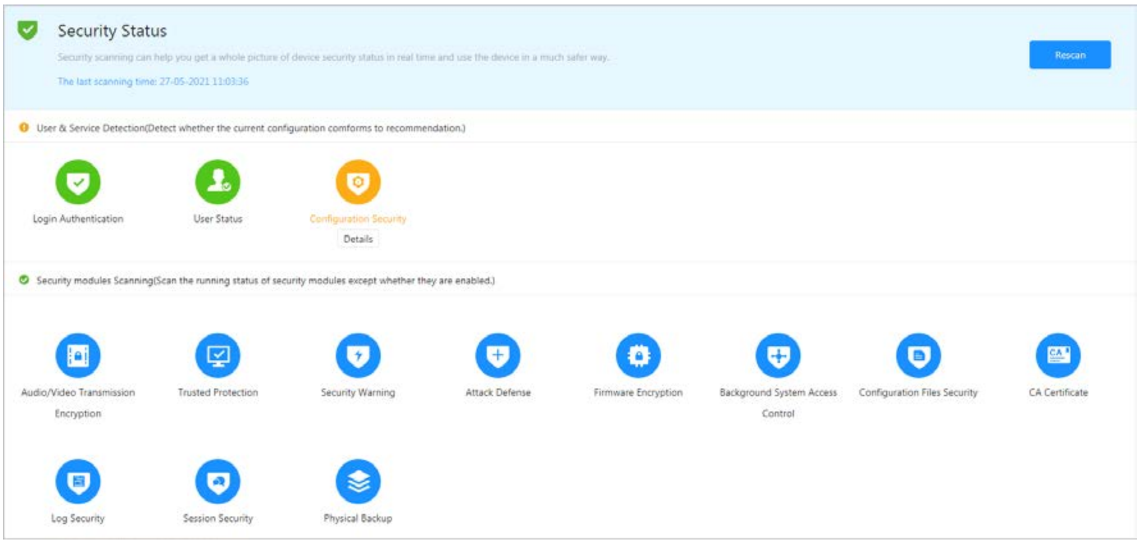
5.8 Security

View device security status and set security functions.

5.8.1 Security Status

Read the current security status of the control panel to use it more securely, log in to the web, and then select **Security** > **Security Status** to check whether the current device meets the requirements of recommended configurations. If not, click **Details** to check and optimize. You can also click **Rescan** to refresh the security status result.

Figure 5-47 Security status



Security Status

Security scanning can help you get a whole picture of device security status in real time and use the device in a much safer way.

The last scanning time: 27-05-2021 11:03:36

User & Service Detection(Detect whether the current configuration comforms to recommendation.)

Security modules Scanning(Scan the running status of security modules except whether they are enabled.)

5.8.2 Configuring System Service

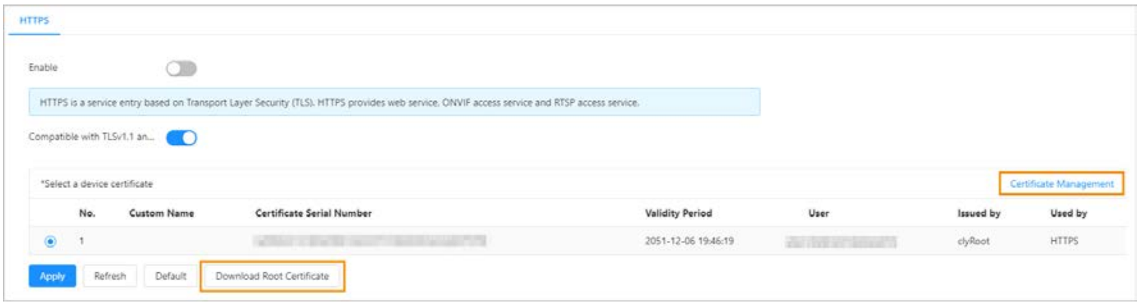
Background Information

Through installing the root certificate, the local computer can log in to the control panel by HTTPS to ensure the security of communication data and guard the user information and device security with stable technology measures.

Procedure

Step 1 Log in to the web, and then select **Security** > **System Service**.

Figure 5-48 System service



HTTPS

Enable ○

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Compatible with TLSv1.1 an... ●

*Select a device certificate

Certificate Management

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
●	1		[redacted]	2051-12-06 19:46:19	[redacted]	clyRoot	HTTPS

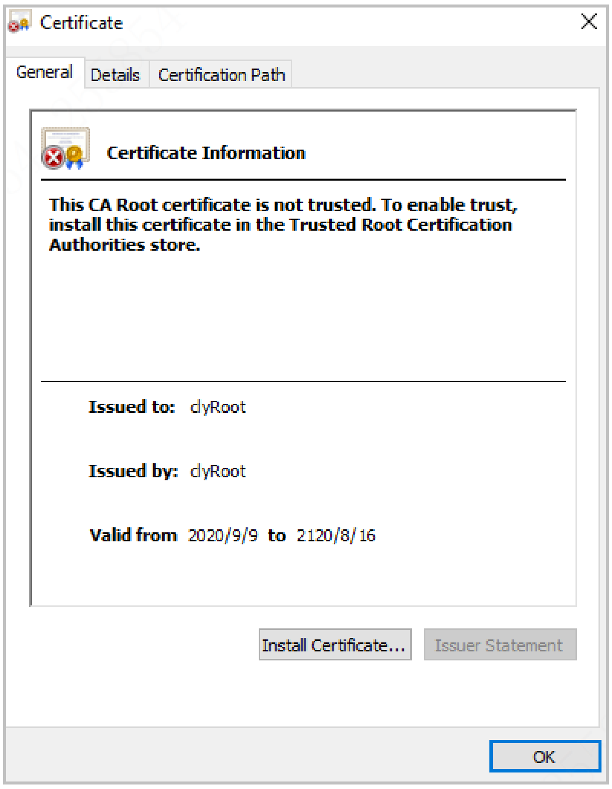
Step 2 Download and install the root certificate.

1) Click **Download Root Certificate** and save the root certificate by following the instructions on the page.

2) Double-click the downloaded **RootCert.cer** file to open the certificate.

3) Click **Install Certificate**.

Figure 5-49 Certificate



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: dyRoot

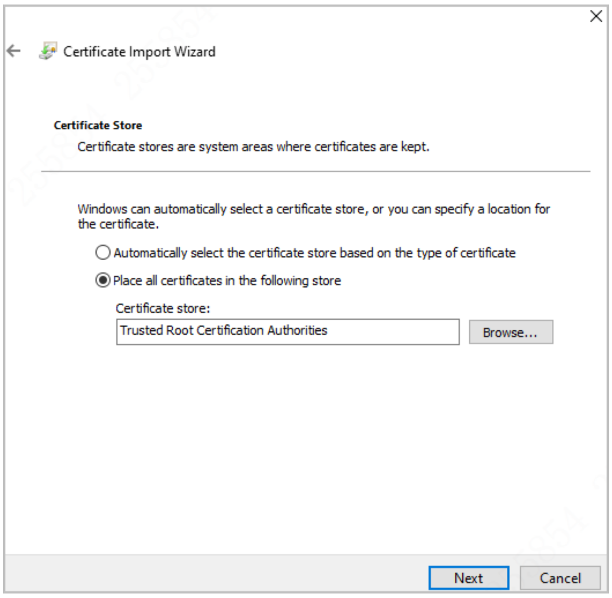
Issued by: dyRoot

Valid from 2020/9/9 to 2120/8/16

4) Click **Next** on the prompted window.

5) Select **Place all certificates in the following store**, and then click **Browse**.

Figure 5-50 Certificate storage location



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

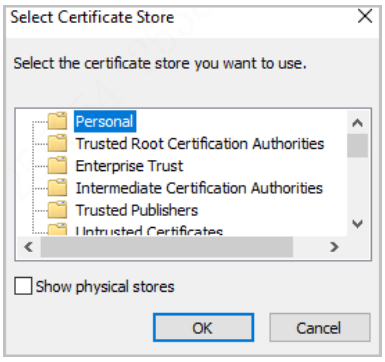
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

6) Select **Trusted Root Certification Authorities** and click **OK**.

Figure 5-51 Select certificate store



Select Certificate Store

Select the certificate store you want to use.

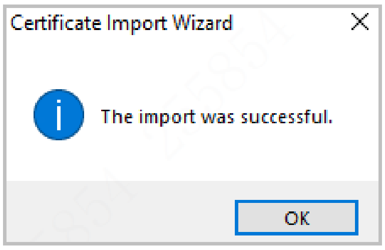
- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

7) Click **Next** and then click **Finish**.
8) The certificate installation completes.

   Enter https://IP *address* in the browser to open the login page, which indicates that the certificate was installed. If no certificate installed, the browser will prompt a certificate error.

Figure 5-52 Certificate imported successfully



Certificate Import Wizard

The import was successful.

Related Operations

Click **Certificate Management** to go to **CA Certificate** page. For details, see "5.8.4 CA Certificate".

5.8.3 Setting Attack Defense

5.8.3.1 Configuring Firewall

Set the block list and allow list to restrict the access rights of users, thus safeguarding the security of network gateway.

Step 1 Log in to the web, and then select **Security** > **Attack Defense** > **Firewall**.

Step 2 Enable the allow list or block list.

Step 3 Set **Allow List** or **Block List** as the **Mode**.

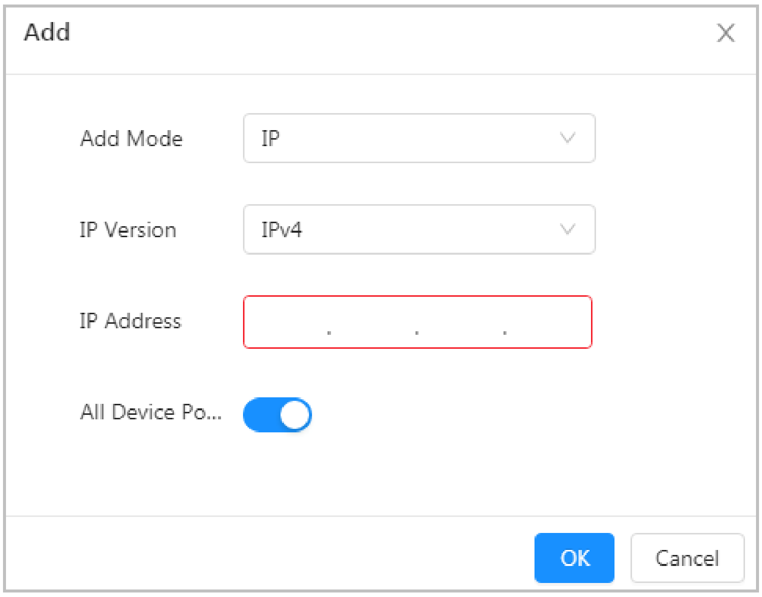
Step 4 Click **Add**.

- **Allow List**: Only if the IP or MAC address of the user is in the allow list, can the Terminal be accessed. If a port is also set, the user can only access the specified port.
- **Block List**: If the IP or MAC address of the user is in the block list, the Terminal cannot be accessed. If a port is also set, the user cannot access the specified port.

📖

- The device IP/MAC shall not be included in the block list and allow list.
- When adding MAC address, you cannot set the port.
- MAC address verification takes effect only when the IP address of the Terminal and local computer of the user are in the same LAN.
- When the Terminal is accessed through WAN, the system can only verify the MAC address of the router.

Figure 5-53 Add allow list or block list



Add

Add Mode: IP

IP Version: IPv4

IP Address: . . .

All Device Po...

Step 5 Configure the parameters.

Table 5-17 Firewall parameters description

Parameter	Description
Add Mode	● **IP**: Select the IP version and enter the IP address of the host. ● **IP Segment**: Select the IP version, and then enter the start address and end address of the segment. ● **MAC**: Enter the MAC address to be added.
IP Address	The IP address of the devices included in the allow list or block list.
Add Device Ports	Set the access port. Control IP and MAC addresses to access designated ports. You can enable **All Device Ports**, or disable this function, and then configure the **Start Port** and the **End Port**.
Start Port	
End Port	

Step 6 Click **OK**.

The system goes back to the **Firewall** section.

Step 7 Click **Apply**.

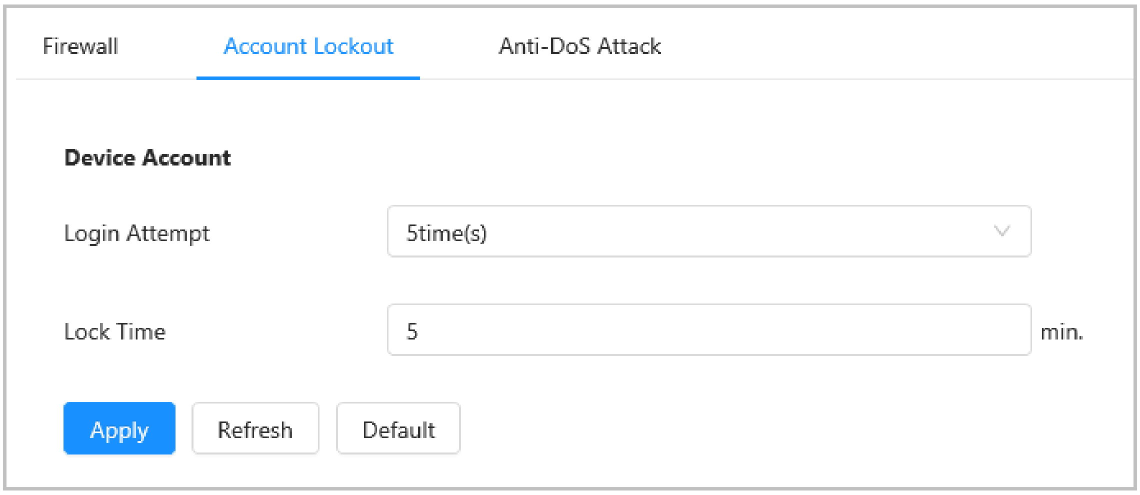
5.8.3.2 Account Lockout

Set the allowed times of login attempts and lock time to improve security.

Step 1 Log in to the web, and then select **Security** > **Attack Defense** > **Account Lockout**.

Step 2 Set the **Login Attempts** and **Lock Time**.

Figure 5-54 Account lockout configuration



Device Account

Login Attempt: 5time(s)

Lock Time: 5 min.

Step 3 Click **Apply**.

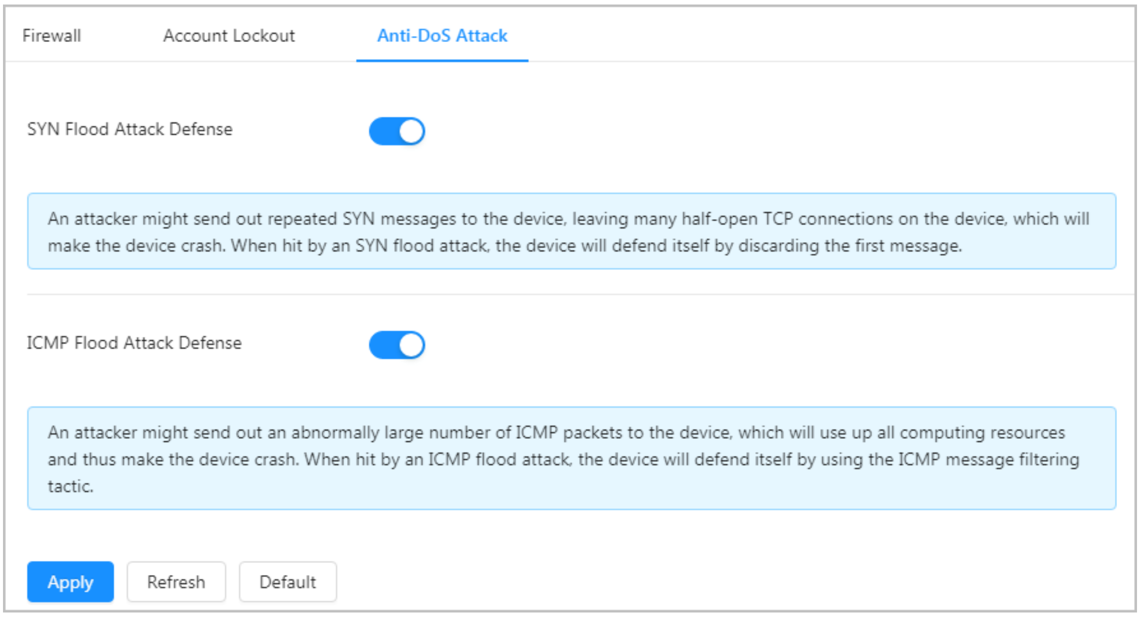
5.8.3.3 Setting Anti-DoS Attack

Anti-DoS attack includes SYN flood attack defense and ICMP flood attack defense.

Step 1 Log in to the web, and then select **Security** > **Attack Defense** > **Anti-DoS Attack**.

Step 2 Click ○ corresponding to **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to enable the defense.

Figure 5-55 Anti-DoS attack



SYN Flood Attack Defense: on

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack Defense: on

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

Step 3 Click **Apply**.

5.8.4 CA Certificate

5.8.4.1 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your local computer.

5.8.4.1.1 Creating Certificate

Create certificate in the control panel.

Procedure

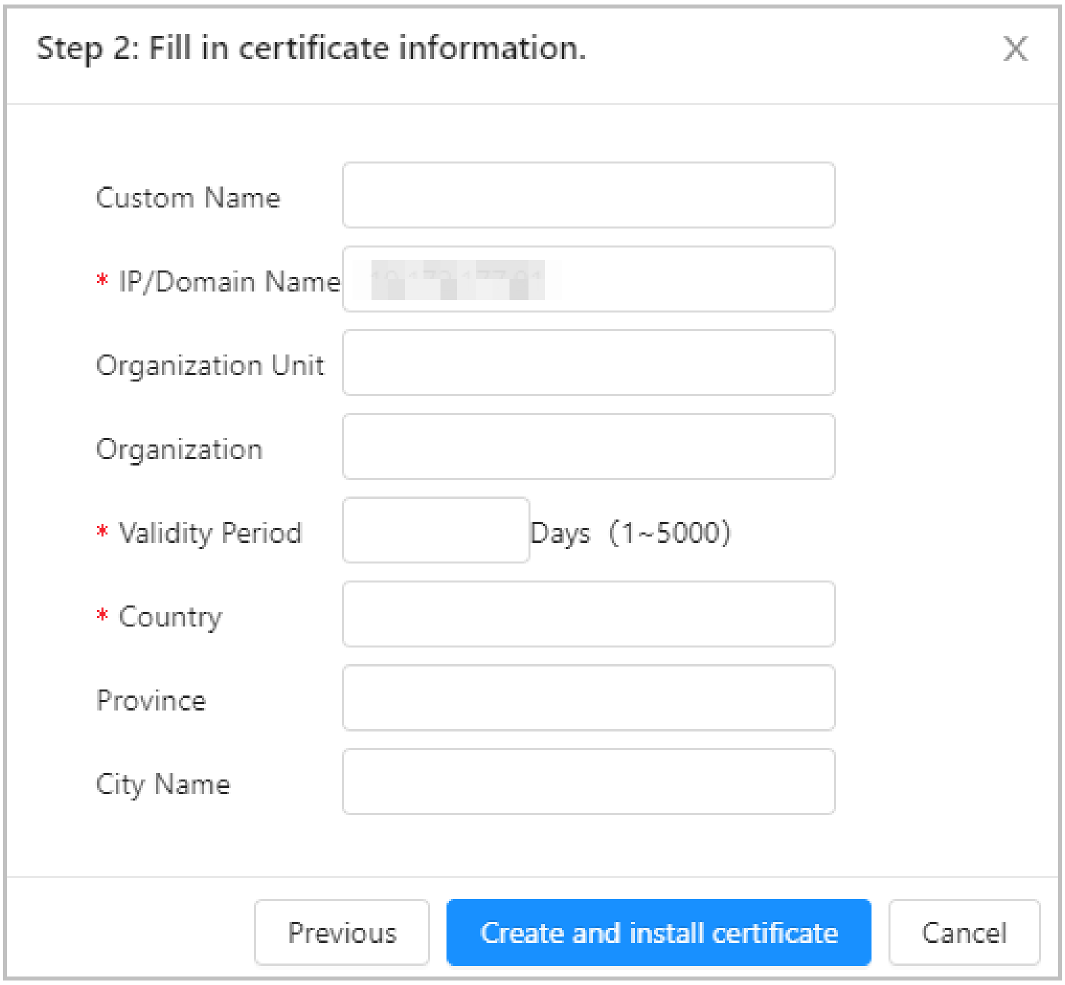
Step 1 Log in to the web, and then select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

Step 3 Select **Create Certificate**, and click **Next**.

Step 4 Enter the certificate information.

Figure 5-56 Certificate information (1)



Step 2: Fill in certificate information.

Custom Name

* IP/Domain Name [redacted]

Organization Unit

Organization

* Validity Period Days (1~5000)

* Country

Province

City Name

Step 5 Click **Create and install certificate**.
After the certificate is created successfully, you can view the created certificate on the **Device Certificate** section.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click 📥 to download the certificate.
- Click 🗑 to delete the certificate.

5.8.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the control panel.

Procedure

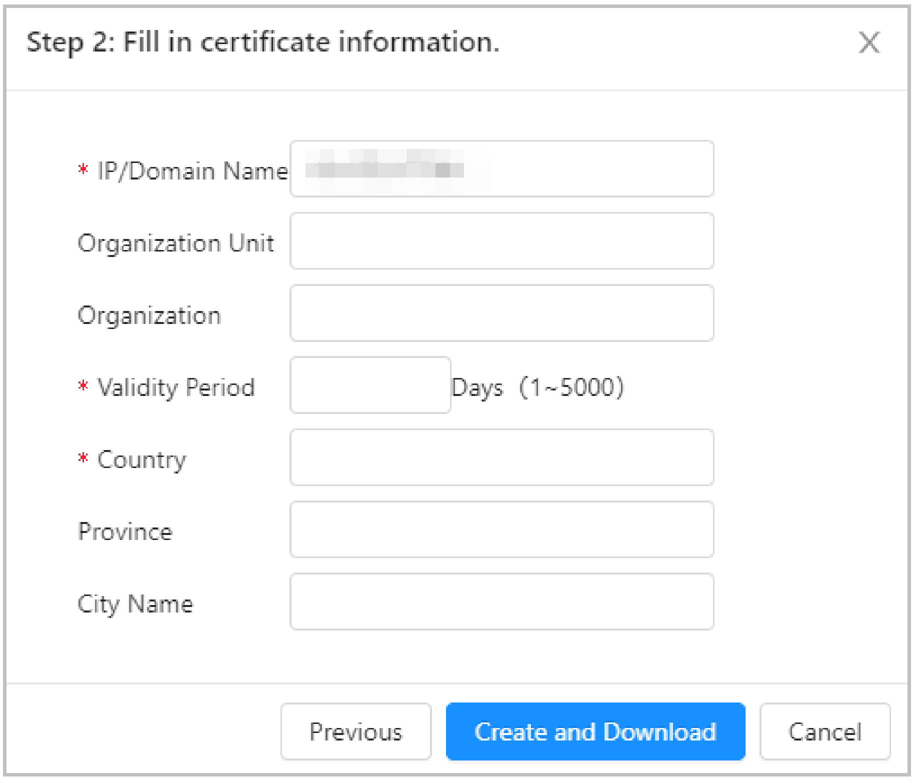
Step 1 Log in to the web, and then select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Device Certificate**.

Step 3 Select **Apply for CA Certificate and Import (Recommended)**, and click **Next**.

Step 4 Enter the certificate information.

Figure 5-57 Certificate information (2)



Step 2: Fill in certificate information.

* IP/Domain Name [redacted]

Organization Unit

Organization

* Validity Period Days (1~5000)

* Country

Province

City Name

Step 5 Click **Create and Download**.

Save the request file to your local computer.

Step 6 Apply the CA certificate from the third-party certificate authority.

Step 7 Import the signed CA certificate.

1) Save the CA certificate to the local computer.
2) Do Step1 to Step3, and click **Browse** to select the signed CE certificate.
3) Click **Install and Import**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** section.

- Click **Recreate** to create the request file again.
- Click **Import Later** to import the certificate next time.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click 📥 to download the certificate.
- Click 🗑 to delete the certificate.

5.8.4.1.3 Installing Existing Certificate

CA certificate is a digital certificate for the legal identity of the camera. For example, when the camera accesses the LAN through 802.1x, the CA certificate is required.

Procedure

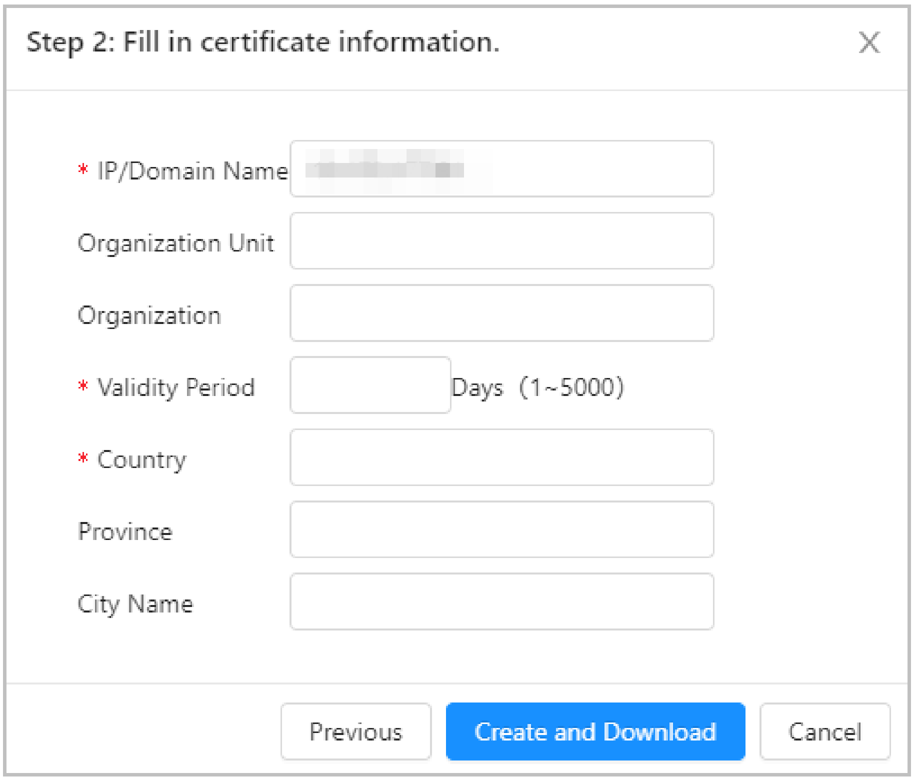
Step 1 Log in to the web, and then select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Installing Device Certificate**.

Step 3 Select **Install Existing Certificate**, and click **Next**.

Step 4 Click **Browse** to select the certificate and private key file, and enter the private key password.

Figure 5-58 Certificate and private key



Step 2: Fill in certificate information.

* IP/Domain Name [redacted]

Organization Unit

Organization

* Validity Period Days (1~5000)

* Country

Province

City Name

Step 5 Click **Import and Install**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** section.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click 📥 to download the certificate.
- Click 🗑 to delete the certificate.

5.8.4.2 Installing Trusted CA Certificate

Background Information

CA certificate is a digital certificate for the legal identity of the device. For example, when the control panel accesses the LAN through 802.1x, the CA certificate is required.

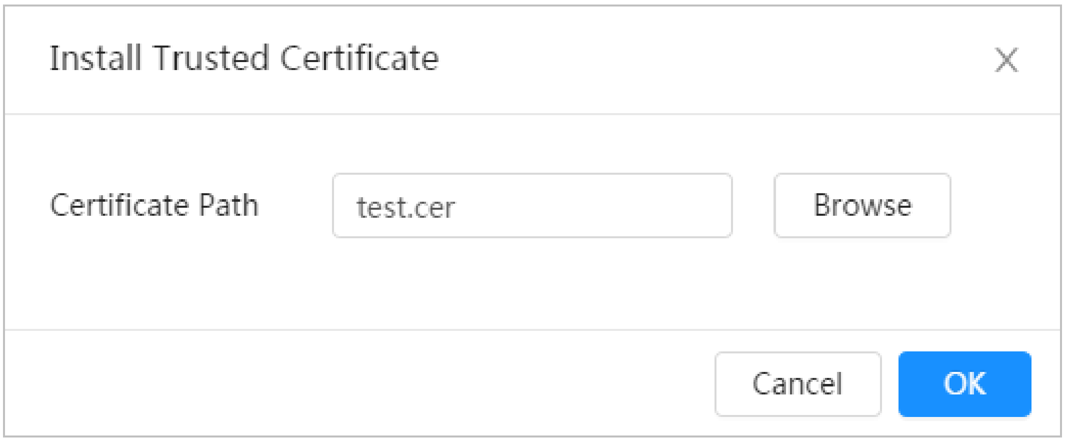
Procedure

Step 1 Log in to the web, and then select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Install Trusted Certificate**.

Step 3 Click **Browse** to select the certificate.

Figure 5-59 Installing trusted certificate



Install Trusted Certificate

Certificate Path: test.cer

Step 4 Click **OK**.

After the certificate is created successfully, you can view the created certificate on the **Trusted CA Certificate** section.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click 📥 to download the certificate.
- Click 🗑 to delete the certificate.

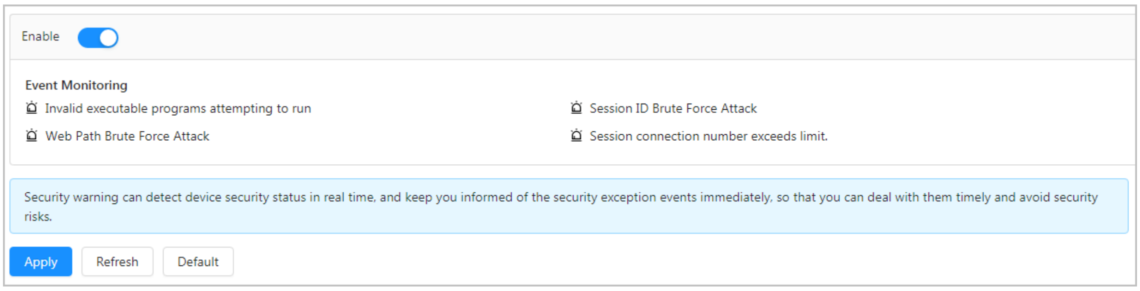
5.8.5 Security Warning

Security warning can detect device status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

Step 1 Log in to the web, and then select **Security** > **Security Warning**.

Step 2 Click **Enable**.

Figure 5-60 Security warning



Enable: ●

Event Monitoring

- Invalid executable programs attempting to run
- Web Path Brute Force Attack
- Session ID Brute Force Attack
- Session connection number exceeds limit.

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

Step 3 Click **Apply**.

6 Keypad Operations

This section introduces basic features of the keypad. For specific operation, refer to the user's manual of the keypad.

6.1 Initialization

Prerequisites

- The control panel works normally.
- The control panel and keypad were correctly connected. You successfully connected port B and A of the keypad to ports B and A of the control panel, port– to GND–, and port + to +12 VDC of the control panel. For details, see "4.2.5 Keypad Cable Connection".

Procedure

Step 1 Power off the keypad while the control panel is still powered on, and check if the control panel works normally.

Supply independent power for each of them when multiple keypads are connected.

Step 2 Press and hold both ENTER and ENTER keys to power on the keypad. Release ENTER when the keypad lights up and displays operating language options (Chinese and English).

Step 3 Select a proper language through ∧ or ∨, and then press ENTER.

Step 4 Select **RS-485 Address** through ∧ or ∨, press ENTER, enter keypad address and then press ENTER.

Step 5 Restart the keypad

6.2 Operation Mode and User Passcodes

Use the keypad by directly entering command under operation mode. Operation mode is divided into programming and walk test modes which cannot be logged into at the same time. When exiting from the programming mode, the keypad returns to global mode by default. When there are no operations for 3 minutes under programming mode, the keypad returns to global mode automatically.

The default password is different for each user type, which includes administrator, installer, manufacturer and operator.

- The default password of admin is 1234.
- The default password of installer is 9090.
- The default password of manufacturer 2008.

6.3 User Permission

Permissions vary for different users.

Table 6-1 Description of user permissions

User	Description
Administrator	Arm, disarm, cancel alarm, restore alarm cancellation, bypass, isolate, configure forced arm, manage users, add or edit configuration parameters.
Installer	All permissions of the admin (including walk test) except disarming.
Manufacturer	Manage users, edit basic programs, such as updating program.
Operator	Arm, disarm, cancel alarm, restore alarm cancellation.

6.4 Global Mode

- The zone number contains 3 digits, ranging from 001 to 256. It uses 0 as placeholder in front when there are less than 3 digits (e.g. 10 becomes 010).
- The subsystem number contains 2 digits, ranging from 01 to 08. It uses 0 as placeholder in front when there are less than 2 digits (e.g. 8 becomes 08).
- The relay number contains 3 digits, ranging from 001 to 256. It uses 0 as placeholder in front when there are less than 3 digits (e.g. 10 becomes 010).
- All objects with the consecutive operation function support up to 16 operations in a row. For example, bypass zone can bypass up to 16 zones at the same time.

6.4.1 Arming and Disarming

Function

- Arming: When the control panel and the detectors work properly, arm the zone, and then the control panel will respond to alarm signals in the zone.
- Disarming: Disarm the zone when it is in the armed status.

Command

- Switch system status: Enter passcode.
- Disarm subsystem: Enter passcode + * + 2 + * + subsystem number.
- Away arm subsystem: Enter passcode + * + 3 + * + subsystem number.
- Forced away arm subsystem: Enter passcode + * + 4 + * + subsystem number.
- Home arm subsystem: Enter passcode + * + 5 + * + subsystem number.
- Forced home arm subsystem: Enter passcode + * + 6 + * + subsystem number.
- Arm single zone: Enter passcode + * + 10 + * + zone number.
- Disarm single zone: Enter passcode + * + 11 + * + zone number.

Switching system status means that you can switch the arming/disarming status of each active subsystem. For example, if the current subsystem is in the armed status, enter the command and the subsystem changes to the disarmed status.

Example

Admin (default passcode is 1234) performs away arming on subsystem1.

1. Under global mode, enter 1234 * 3 * 01.
2. Press Enter.

6.4.2 Cancel Alarm

Function

Cancel the alarm through the keypad when an alarm is triggered.

Command

- Cancel all alarms: Enter passcode + * + 1.
- Cancel zone alarm: Enter passcode + * + 1 + * + zone number.
- Cancel subsystem alarm: Enter passcode + * + 23 + * + subsystem number.

Example

Admin (default passcode is 1234) cancels all alarms.

1. Under global mode, enter 1234 * 1.
2. Press Enter.

6.4.3 Bypass and Isolate

Function

When the whole system fails to be armed due to detector faults or human activities in some zones, you are allowed to bypass these zones by selectively removing detectors from the security system. For example, a detector may be bypassed in order to arm the perimeter with a window open.

- Bypass: If one or more zones are bypasses, they are disabled for one arming cycle. After one arming cycle, they are automatically unbypassed.
- Isolate: If one or more zones are isolated, they are disabled until they are unbypassed.
- Unbypass: Manually restores a zone to normal functioning by removing a bypass condition.

Command

- Unbypass: Enter passcode + * + 7 + * + zone number.
- Bypass: Enter passcode + * + 8 + * + zone number.
- Isolate: Enter passcode + * + 9 + * + zone number.

Example

Admin (default passcode is 1234) bypass zone1.

1. Under the global mode, enter 1234*8*001.
2. Press Enter.

6.4.4 Relay

Function

Manually turn on or off the relay output.

Command

- Manually turn on the relay output: Enter passcode + * + 13 + * + relay number.
- Manually turn off the relay output: Enter passcode + * + 14 + * + relay number.

The 3-digit relay number ranges from 001 to 256, and it uses 0 as placeholder in front when there are less than 3 digits (e.g. 10 becomes 010).

Example

Installer (default passcode is 1234) turns off the relay1 output function.

1. Under global mode, enter 1234*14*001.
2. Press Enter.

6.4.5 PSTN Test

Function

- With the correct configuration, the control panel tries to send a test message to the configured alarm receiving center after executing the PSTN manual test command. The successful test prompt only means that the command was sent successfully, but not that the alarm receiving center received the message.
- After executing SMS or the call manual test command, the control panel sends a test message or makes a test call to the phone to check whether the 2G/4G module, or SMS and call functions of the control panel are available.

Command

- PSTN manual test: Enter passcode + * + 15.
- SMS manual test: Enter passcode + * + 16 + * + phone number.
- Call manual test: Enter passcode + * + 17 + * + phone number.

Example

Installer (default passcode is 1234) manually tests PSTN.

1. Under global mode, enter 1234*15.
2. Press Enter.

6.4.6 Restarting Control Panel

Function

Restart the alarm control panel.

Command

Enter passcode + * + 20.

Example

Admin (default passcode is 1234) restarts the control panel.

1. Under global mode, enter 1234 * 20.
2. Press Enter.

6.4.7 Initializing Control Panel

Function

Initialize the alarm control panel.

Due to the inconvenience of entering letters on the keypad, the passcode of the admin account which initializes the control panel uses the following rules.

- After executing the command with a digital passcode (3–27 digits) to successfully initialize the control panel, the actual passcode is admin + the digital passcode.
- If the passcode is a mix of numbers and letters (8–32), after successful initialization, the actual passcode is the mixed passcode.

Command

Enter passcode * + 21 + * + passcode of admin.

Example

Admin (default password is 1234) initializes the control panel, and sets the admin user passcode to admin123.

1. Under global mode, enter 1234*21*123.
2. Press Enter.

6.4.8 Restoring to Default

Function

Restore parameters to default settings, including alarm, alarm output, alarm subsystem, keypad, arm and disarm, main battery failure, undervoltage, tamper alarm, call alarm receiving center, PSTN offline, subsystem status, network disconnection, IP conflict, MAC conflict and emergency alarm.

Command

Enter passcode + * + 22.

Example

Admin (default passcode is 1234) restores the control panel to default settings.

1. Under the global mode, enter 1234*22.
2. Press Enter.

Appendix 1 Glossary

Appendix Table 1-1 Glossary

Term	Description
Subsystem	Subsystem is an independent area distributed by the alarm control panel, which functions as an independent system that can arm and disarm the area.
24-hour Auxiliary Zone	Frequently applied to the emergency button, water leak detector, temperature detector and more. Detectors working in this zone are in an armed state 24 hours a day. They are also unaffected by arm and disarm operations and no bypass. When an alarm event is detected, the zone triggers sound and light alarm prompts on the keypad, triggering a siren if siren linkage is enabled. Meanwhile, it generates an event report and sends it to the alarm receiving center (the uploaded report code differs from that of the 24-hour audible zone). You can view the alarm status of the zone on the client.
24-hour Vibration Zone	Frequently applied to the emergency button, smoke detector and glass break detector. Applicable for us with ATMs and on other scenes. Detectors working in this zone are in an armed state 24 hours a day. They are also unaffected by arm and disarm operations and no bypass. When an alarm event is detected, the zone triggers sound and light alarm prompts on the keypad and triggers the siren if siren linkage is enabled. Meanwhile, it generates an event report and sends it to the alarm receiving center. You can view the status of the alarm for the zone on the client.
24-hour Audible Zone	Frequently applied to the emergency button, smoke detector and glass break detector. Detectors working in this zone are in an armed status 24 hours a day and are unaffected by arm and disarm operations and no bypass. When an alarm event is detected, the zone triggers sound and light alarm prompts on the keypad and triggers the siren if siren linkage is enabled. Meanwhile, it generates an event report and sends it to the alarm receiving center. You can view the status of the alarm for the zone on the client.
24-hour Silent Zone	Frequently applied to the emergency button in banks, at jewelry counters, and in other scenes. It can trigger and report alarms to the center station, without displaying the zone number on the keypad. No alarm tone, only communication reports of telephone line programming and serial port. Unaffected by arm and disarm operations.
Delayed Zone	Used at main entrances and exits (such as front doors). It takes effect when away delay ends after arming. When the zone is triggered, entry delay is enabled. You must disarm the system before the delay ends to avoid triggering an alarm. The control panel will buzz during entry delay period as a reminder to disarm the system.

Term	Description
Instant Zone	Applicable for use in scenarios where immediate reports are closely followed by a triggered alarm. Entry and exit delay are not supported. Detectors working in this zone are in an armed state 24 hours a day, and can be affected by arm and disarm operations and bypass allowed. When an alarm event is detected, the zone triggers sound and light alarm prompts on the keypad and triggers the siren if siren linkage is enabled. Meanwhile, it generates an event report and sends it to the alarm receiving center (report code uploaded differs from that of the 24-hour audible zone). You can view the status of the alarm for the zone on the client. Usually use with smoke detectors.
Fire Zone	Used in areas with smoke and heat detectors and is armed for 24 hours a day. When the zone is triggered, it generates a fire alarm signal, the keypad displays the zone number, triggers the external siren and reports to the center station. It is unaffected by arm and disarm operations.
Burglar Zone	Used in defense areas such as in places where external doors or windows are normally closed, on fence perimeters and in off-limit passages. An immediate alarm is triggered when an intrusion occurs. It is unaffected by arm and disarm operations.
Perimeter Zone	Mostly used on external doors or windows. When the system is armed, detectors in the zone are in an armed state. An alarm is triggered and reported immediately after an alarm event is detected. When a zone is disarmed but remains in an armed state, the system sends an operation log to the alarm receiving center automatically. The zone status then changes to failure.
Not Alarm Input Zone	The control panel does not generate alarms when this zone is triggered. It only collects, as an input status, indicating the working status of the control panel. It can also be used to execute linked actions, to display the open status of doors, turn on lights through the corresponding output module programming, and more.
Fixed Key Zone	Specially designed for changing system arming/disarming status. When the zone is normal, the system is in a disarmed state, and when triggered, the system status changes to armed.
Variable Key Zone	Specially designed for changing system arming/disarming status. Each time the zone is triggered, the system status changes.
Arming	Turn the system on. The security system can be turned on (armed) in many different ways, depending on the arming command used.
Home Arming	An arming mode that allows the user to arm the system when inside the area of the alarm system. Under this mode, all perimeter zones (such as outdoor perimeter detectors) in the system are in an armed state, but internal zones (such as the indoor IR detector) are bypassed by the system, so alarms will not be triggered when people move freely in the zone because the internal zones of the subsystem are disarmed.

Term	Description
Away Arming	Arm the system when all the users leave the zone of the alarm system. Under this mode, all zones of the system are under the working status, which means all zones of the subsystem are armed.
Disarming	Turn the security system off. The opposite of arming.
Cancel Alarm	Cancel linked alarms of subsystems or zones.
Global Cancel	Cancel all alarms linked to subsystems or zones, including alarms linked to control panel failure.
Bypass	When the whole system fails to be armed due to detector faults or human activities in some zones, users are allowed to bypass these zones by selectively removing detectors from the security system. For example, a detector may be bypassed in order to arm the perimeter with a window open.
Isolate	If one or more zones are isolated, they are disabled until they are unbypassed.
Unbypass	Manually restores a zone to normal functioning by removing a bypass condition.
Exit Delay	A programmed delay in the system alarm response that allows an individual to exit after arming an area. Failure to exit before the delay time expires causes entry delay to begin. The system must then be disarmed. If it is not disarmed before the delay time expires, the system will produce an alarm response that might include the sending of reports to the central station.
Entry Delay	A programmed delay in the system alarm response that allows an individual to enter an armed area through the correct detector and disarm the area. If the system is not disarmed before the delay time expires, the system will initiate an alarm response which may include sending reports to the central station.
0 or 1 EOL	The detector type can be NO or NC, and returns two statuses: Normal and alarm (short circuit and broken circuit are considered to be alarm
2 EOL	The detector type can be NO or NC, and returns four statuses: Normal,
3 EOL	The detector type can be NO or NC, and returns five statuses: Normal,
Case Tamper	The alarm is activated when the case is opened.
Wall Tamper	The alarm is activated when the case is detached from the wall.

Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it’s something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883