



Hybrid Panel

User Manual



Foreword

General

This manual introduces the installation, functions and operations of the Hybrid Panel (hereinafter referred to as the "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, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	January 2026

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user manual, use our CD-ROM, scan the QR code or visit

our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Operation Requirements

**DANGER**

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

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

Preventive measures (including but not limited to):

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



- 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.
- Please follow the electrical requirements to power the device.
 - ◇ Followings are the requirements for selecting a power adapter.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.

- ◇ We recommend using the power adapter provided with the device.
- ◇ When you select the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.



- 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.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Overview.....	1
1.2 Technical Specifications.....	1
1.3 Checklist.....	7
2 Design.....	8
2.1 Appearance.....	8
2.2 Dimensions.....	10
3 Installation and Wiring.....	11
3.1 Installing the Panel.....	11
3.2 Cable Connection.....	14
3.2.1 Wired Input Cable Connection.....	14
3.2.2 Wired Output Cable Connection.....	14
3.2.3 RS-485 Cable Connection.....	15
3.2.4 Keypad Cable Connection.....	15
3.2.5 Siren Cable Connection.....	16
4 DMSS Operations for End Users.....	18
4.1 Signing Up and Logging in to DMSS.....	18
4.2 User Overview.....	20
4.3 Adding Devices.....	21
4.3.1 Adding the Panel.....	21
4.3.2 Introduction of Peripheral Devices to be Added.....	23
4.3.3 Adding Bus Devices.....	24
4.3.4 Adding Wired Devices.....	25
4.3.5 Adding Wireless Devices.....	27
4.3.6 Adding IPC.....	28
4.3.7 Adding Card.....	31
4.4 Configuring Alarm Linkage Video.....	31
4.5 Panel General Settings.....	32
4.5.1 Viewing Panel Status.....	33
4.5.2 Configuring the Panel Parameters.....	35
4.6 Network Configuration.....	40
4.6.1 Wired Network Configuration.....	40
4.6.2 Wi-Fi Network Configuration.....	41
4.6.3 (Optional) Cellular Configuration.....	41
4.7 Managing Devices.....	42

4.7.1	Entrusting Devices.....	42
4.7.2	Unbinding Devices.....	45
4.7.3	Applying for Security Services.....	45
4.8	Managing Areas.....	46
4.8.1	Adding Areas.....	47
4.8.2	Setting Area as Public Area.....	47
4.8.3	Configuring Maintenance Mode.....	48
5	General Operations.....	50
5.1	Single Arming and Disarming.....	50
5.2	Global Arming and Disarming.....	51
5.3	Manual Arming and Disarming.....	52
5.4	Scheduled Arming and Disarming.....	53
6	Web Operations.....	54
6.1	Starting the Device.....	54
6.1.1	Initializing the Hybrid Panel.....	54
6.1.2	Logging in to Webpage.....	55
6.1.3	Resetting the Password.....	56
6.2	Overview.....	58
6.3	Adding Areas.....	59
6.4	Device Setting.....	60
6.4.1	Adding Bus Devices.....	60
6.4.2	Adding Wired Devices.....	60
6.4.3	Adding Wireless Devices.....	63
6.4.4	Adding IPC.....	65
6.4.5	Adding Card.....	68
6.5	Person Management.....	69
6.5.1	Adding Users.....	69
6.5.2	Resetting the Password.....	71
6.6	Panel.....	71
6.6.1	Basic Settings.....	72
6.6.2	System Settings.....	73
6.6.3	Network Settings.....	78
6.6.4	Alarm Receiving Center.....	81
6.6.5	Intercom Service.....	84
6.7	Maintenance Center.....	86
6.7.1	Installation and Maintenance Mode.....	86
6.7.2	Detector Test.....	86
6.7.3	One-click Diagnosis.....	87
6.7.4	System Information.....	88
6.7.5	Viewing Logs.....	88

6.7.6 Maintenance Management.....	90
6.7.7 Updating.....	91
6.7.8 Advanced Maintenance.....	91
6.8 Security.....	92
6.8.1 Security Status.....	93
6.8.2 Configuring System Service.....	93
6.8.3 Setting Attack Defense.....	95
6.8.4 Data Encryption.....	98
6.8.5 Security Warning.....	99
Appendix 1 Arming Failure Events and Description.....	100
Appendix 2 SIA Event Codes and Description.....	102
Appendix 3 Security Commitment and Recommendation.....	107

1 Introduction

1.1 Overview

The hybrid panel is an alarm control panel that manages both wired and wireless peripherals. It comes with built-in wired inputs and outputs, which can be expanded through extension modules, and can connect to wireless peripherals through RF expansion modules. The panel provides control over devices connected to interact with users and security companies. The panel is ideal for indoor installation.

1.2 Technical Specifications

This section contains technical specifications of the device. Please refer to the ones that correspond with your model.

Table 1-1 Technical specifications

Type	Parameter	Description	
Port	Alarm Input	DHI-ARC3808H: 128 channels (8 local channels) Wired input: A maximum of 500 m. Cable: Twisted pair (oxygen-free copper wire, 57/0.145±0.007 mm, 1000 m, ≤19.5Ω).	DHI-ARC3408H: 64 channels (8 local channels) Wired input: A maximum of 500 m. Cable: Twisted pair (oxygen-free copper wire, 57/0.145±0.007 mm, 1000 m, ≤19.5Ω).
	Alarm Output	DHI-ARC3808H: 128 channels (4 local channels) Wired output: A maximum of 500 m. Cable: Twisted pair (oxygen-free copper wire, 57/0.145±0.007 mm, 1000 m, ≤19.5Ω).	DHI-ARC3408H: 64 channels (4 local channels) Wired output: A maximum of 500 m. Cable: Twisted pair (oxygen-free copper wire, 57/0.145±0.007 mm, 1000 m, ≤19.5Ω).

Type	Parameter	Description	
	Connected Peripheral	DHI-ARC3808H: Up to 16 wired keypads Up to 8 wireless sirens (ARA12 series, ARA13 series) and 1 local siren Up to 128 wireless keyfobs (ARA24 series) Up to 16 expansion modules Up to 120 wireless door detectors (ARD323 series, ARD333 series. The quantity depends on actual alarm input connections) Up to 120 wireless PIR Detectors (ARD1233 series. The quantity depends on actual alarm input connections) Up to 120 wireless Dual-Tech Detectors (ARD2231 series. The quantity depends on actual alarm input connections)	DHI-ARC3408H: Up to 8 wired keypads Up to 8 wireless sirens (ARA12 series, ARA13 series) and 1 local siren Up to 64 wireless keyfobs (ARA24 series) Up to 8 expansion modules Up to 56 wireless door detectors (ARD323 series, ARD333 series. The quantity depends on actual alarm input connections) Up to 56 wireless PIR Detectors (ARD1233 series. The quantity depends on actual alarm input connections) Up to 56 wireless Dual-Tech Detectors (ARD2231 series. The quantity depends on actual alarm input connections)
	Area	DHI-ARC3808H: 32 areas (rooms)	DHI-ARC3408H: 16 areas (rooms)
	Network Mode	DHI-ARC3808H: Ethernet, Wi-Fi and 2G/3G/4G networks (optional)	DHI-ARC3408H: Ethernet and 2G/3G/4G networks (optional)
	Network Port	1 × RJ-45, 10 Mbps/100 Mbps Ethernet port.	
	Telephone Line	Yes (optional)	
	RS-485	2 channels. The maximum distance for one RS-485 bus is 1000m, and intercom devices must be limited to within 300m. Cable: Twisted pair (oxygen-free copper wire, 57/0.145±0.007 mm, 1000 m, ≤19.5Ω).	
	Storage Battery	Yes (12 V, 7 Ah. The backup battery is not included in the set)	
	Auxiliary Power Output	3 channels (2 × auxiliary power output and 1 × siren power output); total current: 2 A	
Video & Audio	Video Input	DHI-ARC3808H: 8 channels	DHI-ARC3408H: 4 channels

Type	Parameter	Description	
Function	Indicator Light	DHI-ARC3808H: 5 indicators (1 × power status indicator, 1 × storage battery status indicator, 1 × 2 G/4 G status indicator, 1 × PSTN status indicator, and 1 × AP mode indicator)	DHI-ARC3408H: 4 indicators (1 × power status indicator, 1 × storage battery status indicator, 1 × 2 G/4 G status indicator, and 1 × PSTN status indicator)
	Button	DHI-ARC3808H: 3 buttons (1 reset button, 1 power switch button, and 1 AP button)	DHI-ARC3408H: 2 buttons (1 × reset button, 1 × power switch button)
	Buzzer	Yes	
	SMS	Yes (up to 12 phone numbers)	
	Phone Call	Yes (up to 12 phone numbers)	
	Video Linkage	Yes	
	Offline Cache	Stores up to 50 alarm messages	
	Arm and Disarm	App, keyboard, keyfob, card, scheduled arming and disarming	
	Remote Update	Cloud update Web	
	Network Protocol	SIA SoftGuard	
	Low Battery Detection	Yes	
	Battery Level Display	Yes	
	Tamper	Yes (1 × case tamper and 1 × wall tamper)	
	Signal Strength	Yes	
	User Management	32 app users (30 × general users, 1 × admin user and 1 × installer) and 32 × keypad users	
	Power Failure Protection for Configured Parameters	Yes	
	Logs	5, 000 entries	
Technical	Operating Current	132 mA/220 VAC	
	Operating Frequency	50 Hz/60 Hz	

Type	Parameter	Description
Wireless	Wi-Fi	Wi-Fi
General	Language	English, Spanish (Latin America), Spanish, French, Italian, Arabic, Turkish, Danish, Czech, Slovak, Russian, Portuguese, German, Dutch, Greek, Bulgarian, Polish
	Power Supply	100 -240 VAC supply (standard) 13-15 VDC power adapter supply (optional)
	Power Supply Type	Type A
	Standby Time	36 hours (disarming, arming, and alarm once a day. Supports wired, Wi-Fi (select models) and 4 G connection. Does not supply power externally)
	Low Battery Threshold	11,000 mV
	Battery Restore Threshold	12,000 mV
	Power Consumption	45W (max) 2.7 W (standby)
	Operating Temperature	-10 °C to +55 °C (+14 °F to +131 °F)
	Operating Humidity	10%–90% (RH)
	Product Dimensions	304 mm × 235 mm × 90.8 mm (11.97" × 9.25" × 3.57")
	Net Weight	1361 g (3.00 lb)
	Gross Weight	1758 g (3.88 lb)
	Installation	Wall mount
	Casing Material	PC + ABS
	Appearance Color	White
	Protection	IP30
	Anti-corrosion Level	Basic Protection *The products are designed for general use and are applicable even in areas with no specific requirements for anti-corrosion protection.
	Storage Temperature	-10 °C to +55 °C (+14 °F to +131 °F)
	Storage Humidity	10%–90% (RH)
	Packaging Dimensions	369 mm × 140 mm × 280 mm (14.53" × 5.51" × 11.02")

Type	Parameter	Description
Wi-Fi	Wi-Fi Standard	IEEE 802.11b/g/n
	Wi-Fi Frequency Range	2400-2483.5 MHz
	Wi-Fi Power Transmission	≤20 dBm@2400 MHz–2483.5 MHz
Cellular Network	Cellular Network Standard	GSM/WCDMA/LTE
	Frequency Range	EU: 4G: FDD-LTE: B1/B3/B7/B8/B20/B28A; TDD-LTE: B38/B40/B41; 3G: WCDMA: B1/B8; 2G: GSM: 1800/900MHz; LA: 4G: FDD-LTE: B1/B2/B3/B4/B5/B7/B8/B28; TDD-LTE: B40; 3G: WCDMA: B1/B2/B4/B5/B8; 2G: GSM: 850/900/1800/1900 MHz
	Transmitter Power (EIRP)	4G: Power class 3: 23 dBm±2dB 3G: Power class 3: 24 dBm+1/-3dB 2G: Power class 0: 30 dBm±3dB (GSM900) Power class 5: 33 dBm±3dB (GSM1800)

Table 1-2 ATE category

ATE Category	Reporting Time	Protocols	Communication Devices			Communication Device to be Used
			PSTN	2G/3G	IP	
SP2	25 h	Standard	√			The check marked communication device
SP3	30 min	Standard		√	√	Only one of the two check marked communication devices
SP4	3 min	Encrypted		√	√	Only one of the two check marked communication devices

ATE Category	Reporting Time	Protocols	Communication Devices			Communication Device to be Used
			PSTN	2G/3G	IP	
SP5	90 s	Encrypted		√	√	Only one of the two check marked communication devices
DP1	25 h	Standard	√	√	√	Only two of the three check marked communication devices
DP2	30 min	Standard	√	√	√	Only two of the three check marked communication devices
DP3	3 min	Encrypted		√	√	The two check marked communication devices
DP4	90 s	Encrypted		√	√	The two check marked communication devices

ATE: AI-arm transmission equipment.

SPx (Single Path): A value that indicates the performance level achieved by a single communication device, according to the EN 50136–1 standard.

DPx (Double Path): A value that indicates the performance level achieved by a combination of two communication devices, according to the EN 50136–1 standard.

Reporting time: The reporting time is prescribed based on the standard of each level of performance. Reporting time is the maximum time available to report when an alarm transmission device fails. AI-arm transmission devices meet this requirement by regularly reporting their status through a specific symbolic test function.

Protocols: Indicates the security level of the protocols to be used for the notification of failures. Standard protocols and voice protocols are encrypted. High security protocols are encrypted with an AES 128 bit or AES 256 bit encryption key.

Communication devices: Implemented communication devices.

Communication devices to be used: Indicates the number of and which communication devices are to be used based on the ATE category.

SP2: **LAN/WIFI** using CLOUD, **APP DMSS** (reporting time default 150") or **ARC** reporting time min. 25 h);

DP2: primary **LAN/WIFI** using CLOUD, **APP DMSS** (reporting time default 150") or **ARC** reporting time min. 30 min) and secondary **GPRS/4G** using CLOUD **APP DMSS** (reporting time default 150") or **ARC** reporting time min. 30 min)/

1.3 Checklist

Check the package against the following list. If any of the items are damaged or missing, contact customer service.

Figure 1-1 Checklist

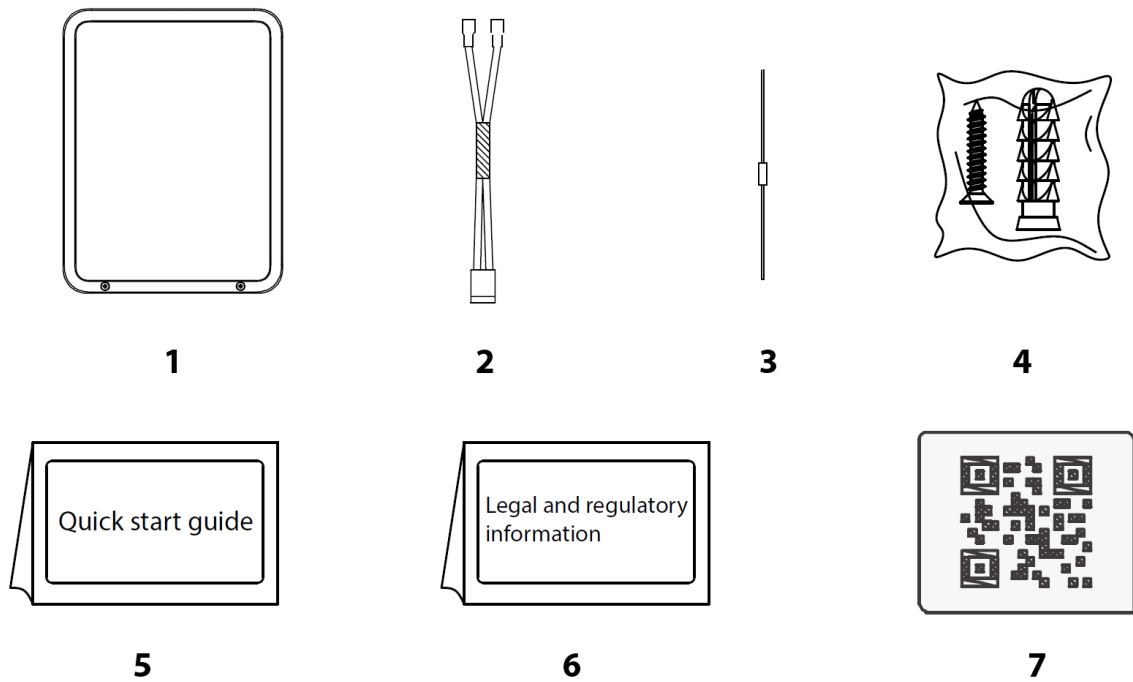


Table 1-3 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Hybrid panel	1	5	Quick start guide	1
2	Battery cable	1	6	Legal and regulatory information	1
3	2.2k resistance 6.8k resistance	1	7	QR code	1
4	Package of screws	1	—	—	—

2 Design

2.1 Appearance

Figure 2-1 Appearance

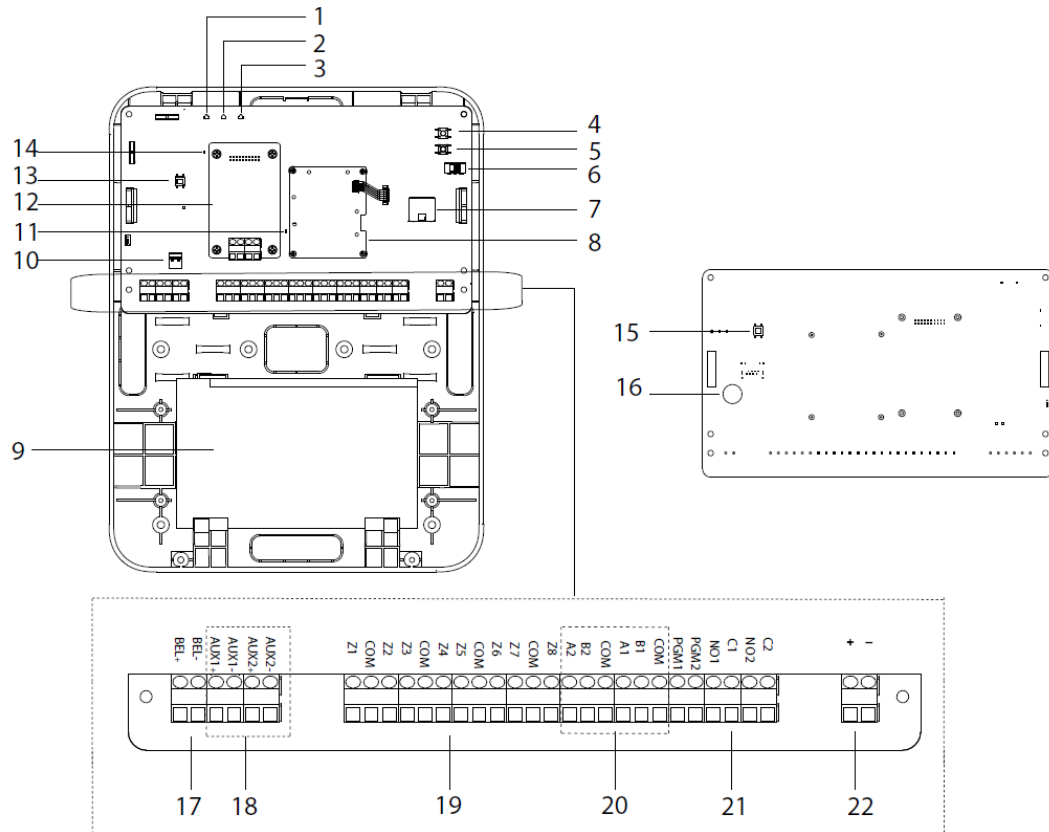


Table 2-1 Structure

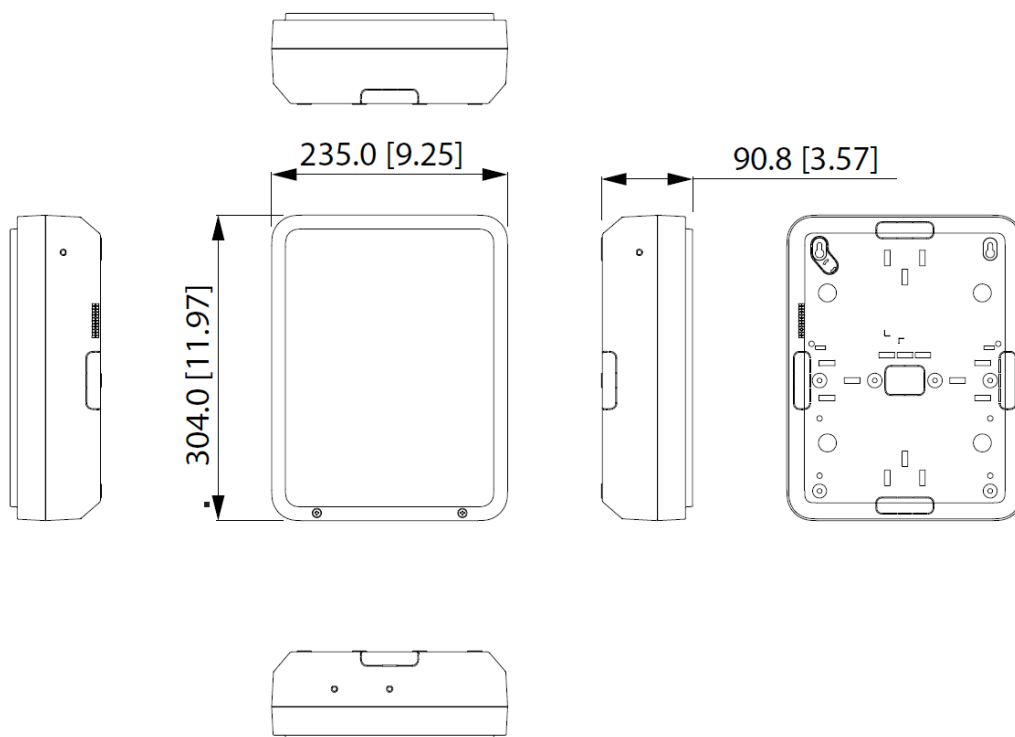
No.	Name	Description
1	Battery indicator	● Solid green: Connected to the battery. ● Off: Disconnected to the battery.
2	4G indicator	● Solid green: 4G communication is normal. ● Solid red: 4G communication is abnormal. ● Off: Disconnected to the 4G module.
3	PSTN indicator	● Solid green: PSTN communication is normal. ● Solid red: PSTN communication is abnormal. ● Off: Disconnected to the PSTN module.

No.	Name	Description
4	AP button	Press and hold the button for 2 seconds to turn on the AP function, and the phone will connect to the hotspot from the panel, and then sync Wi-Fi user name and password to the panel. You can also turn off the AP through pressing and holding the button for 2 seconds when AP is enabled.  Only supported on select models.
5	Reset button	Press and hold the button for 10 seconds to restart the panel and restore to factory defaults.
6	Power switch	Connects to the power supply.
7	LAN port	Connects to the wired network. Light on when connection is normal, and off when abnormal.
8	(Optional) 4G module	The panel can connect to the network and communicate through 4G. Inserting a SIM card allows the panel to use cellular data, and push alarm notifications.
9	Battery compartment	Used to place storage battery. When necessary, you can insert batteries into the compartment to use as a backup power for the panel.  The lead-acid battery used must meet airtightness requirements, include external connection wires and protective devices, and comply with IEC 60896-21, IEC 60896-22, or IEC 60896-11 standards.
10	BAT port	Connects to a battery for power supply or charging.
11	Power indicator	Solid green after the panel is powered on.
12	(Optional) PSTN module	Used for PSTN communication.
13	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
14	AP indicator	● Flashes blue: In AP mode. ● Off: In STA mode.  Only supported on select models.
15	Wall tamper switch	When the tamper switch is released, a tamper alarm will be triggered.
16	Buzzer	Sounds alarm when an alarm is triggered.
17	Bell	Connects to sirens.
18	Auxiliary power output	Provides auxiliary power to external devices.

No.	Name	Description
19	Alarm input	Supports connecting to external wired detectors (up to 8 channels).
20	RS-485 port	Supports connecting to RS-485 expansion modules, keypads, and other external devices.
21	Alarm output	Supports connecting to external alarm output devices (2 PGM channels and 2 relay channels).

2.2 Dimensions

Figure 2-2 Dimensions (Unit: mm[inch])



3 Installation and Wiring



The circuit connecting the hybrid panel to the power grid must include an overcurrent protection device with a rated current of not less than 16 A. 16 AWG is recommended for the ground wire. For the battery power supply port, a 12 V/7 AH battery is recommended.

3.1 Installing the Panel

Install the hybrid panel.

Procedure

Step 1 Power on the hybrid panel.

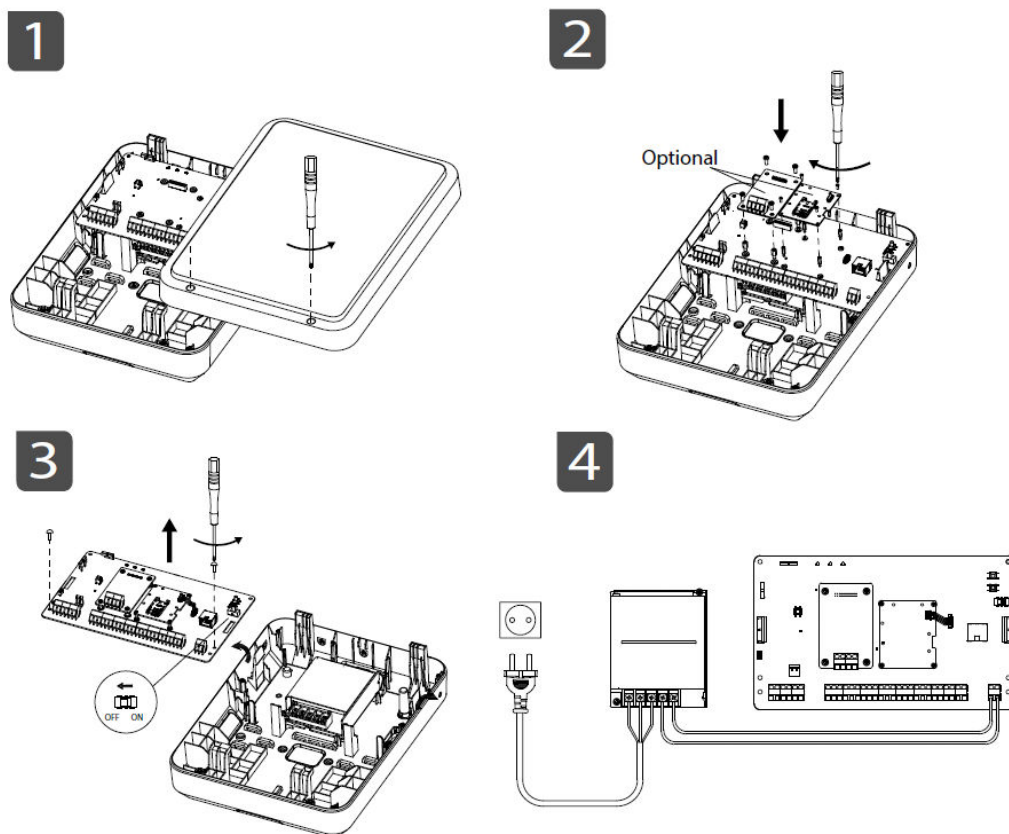
1. Use a screwdriver to remove the screws from the top cover of the panel and to expose the mainboard.
2. (Optional) Install the PSTN module and 4G module on to the mainboard.



The PSTN module and 4G module are not included in the package. You need to purchase them separately.

3. Turn on the power switch.
4. Connect to a power source using the provided power cord.

Figure 3-1 Power on

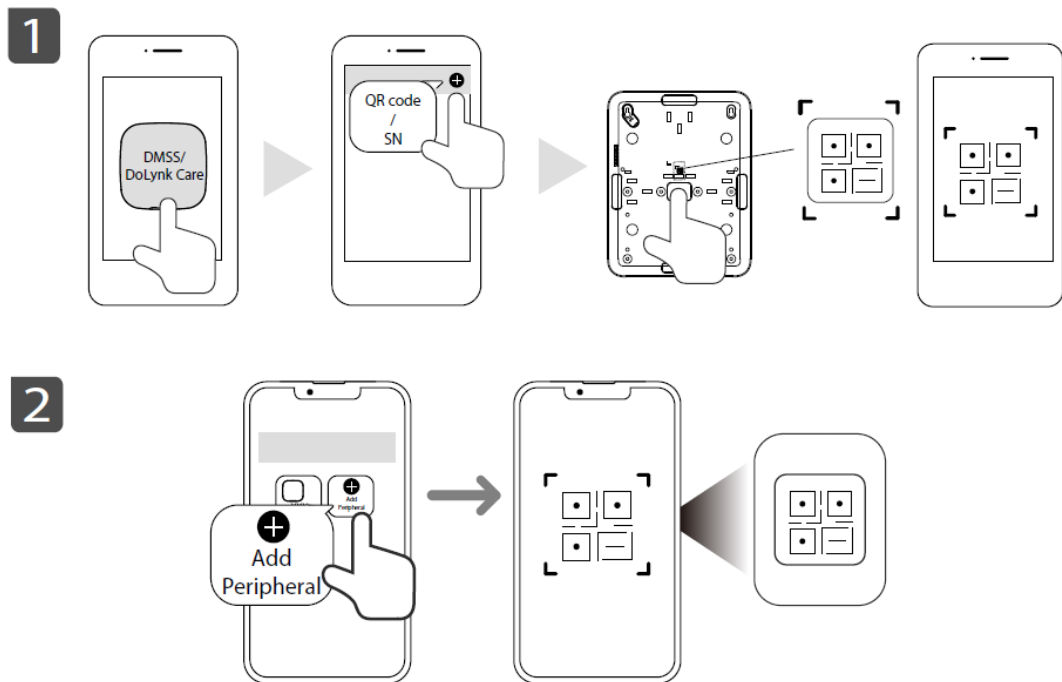


Step 2 Add the hybrid panel to DMSS or DoLink Care app, and then add peripherals to the hybrid panel.



Make sure that the version of the DMSS app is V2.3.10 or later, and DoLink Care is V2.530.10 or later.

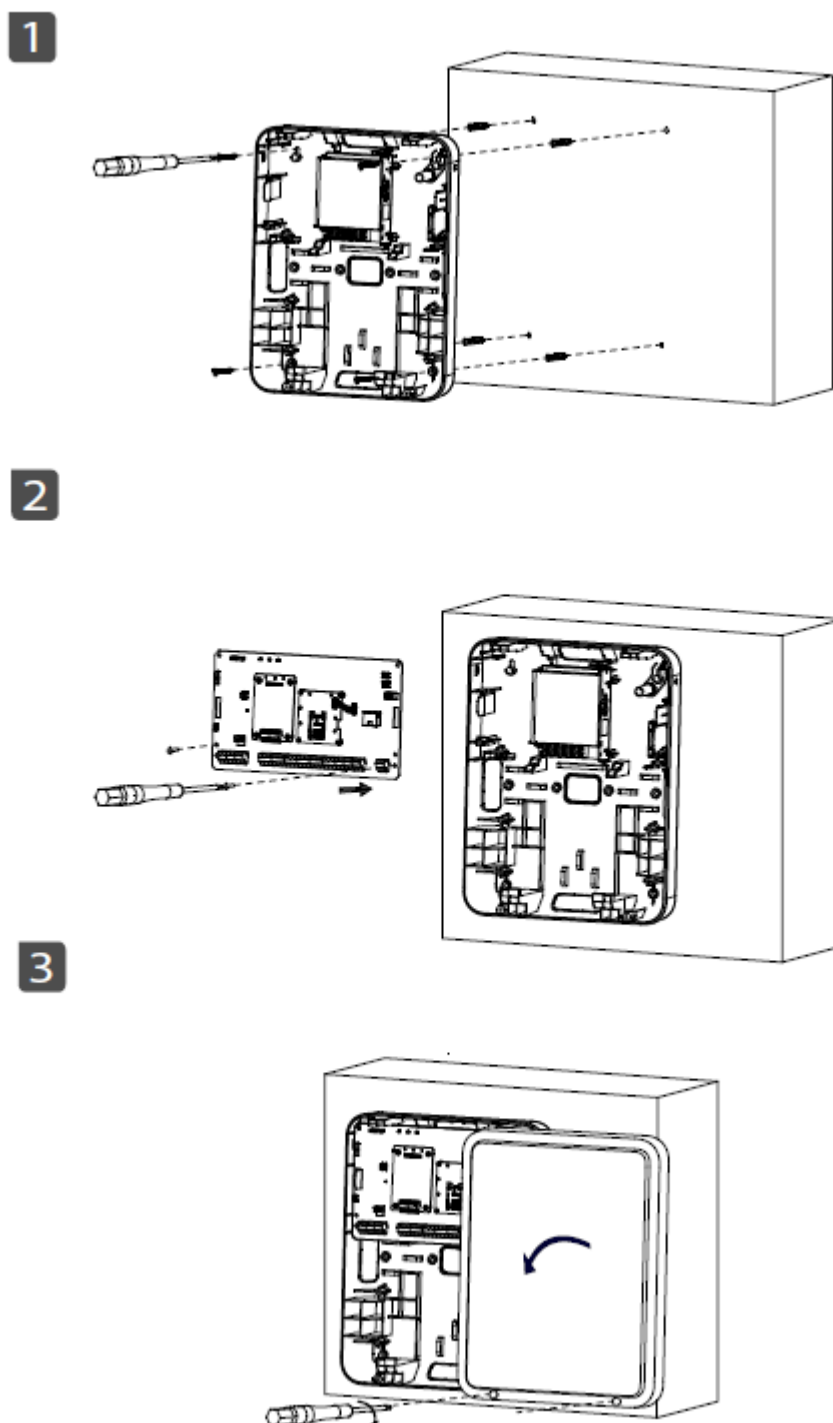
Figure 3-2 Add hybrid panel



Step 3 Install the hybrid panel.

1. Fix the back cover of the panel onto the wall.
2. Secure the mainboard onto the internal of the hybrid panel. Make sure it is properly seated and connected.
3. Attach the cover and secure it with the screws using a screwdriver.

Figure 3-3 Install the hybrid panel

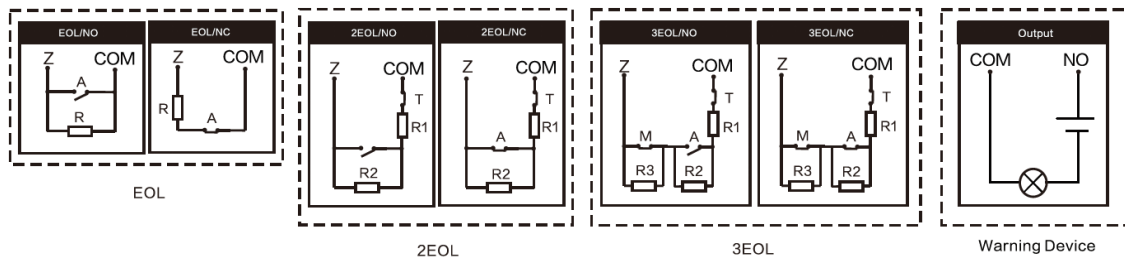


3.2 Cable Connection

3.2.1 Wired Input Cable Connection

This section uses 8-channel alarm input as an example, the corresponding ports are Z1 to Z8. 0 or 1 EOL, 2 EOL and 3 EOL are available for detectors that are normally open and closed. Set the hybrid 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 3-4 Detector wiring



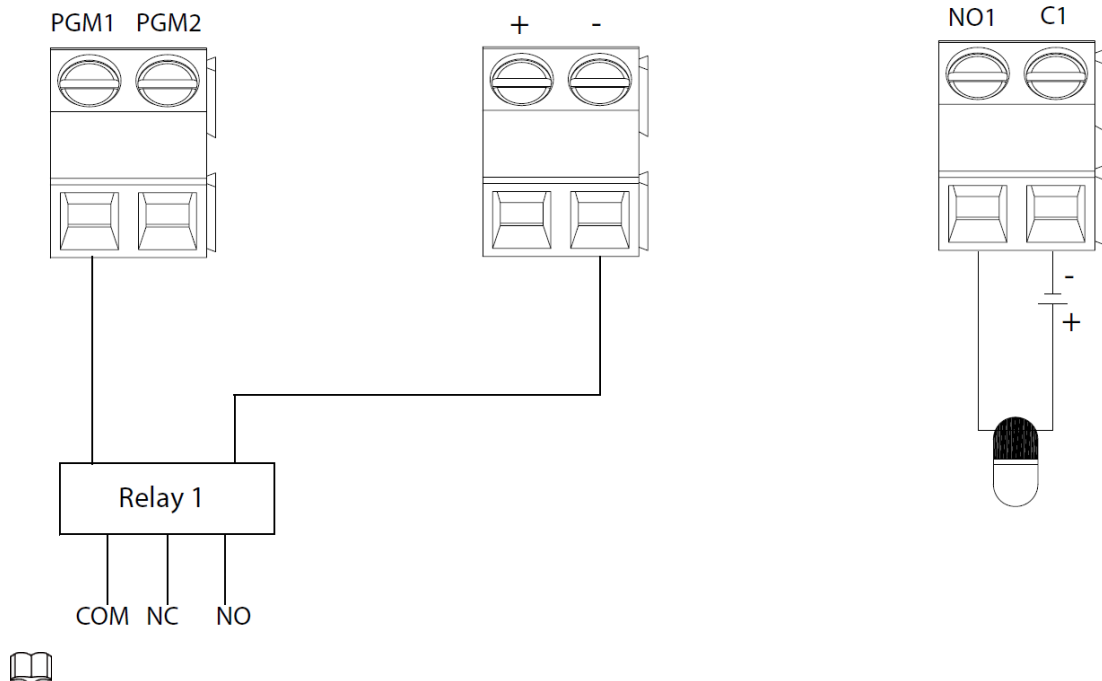
3.2.2 Wired Output Cable Connection



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 3 A). If you need to use large power loads, use a relay.

- NO1/C1: Normally open alarm outputs (dry contact) for triggering external alarm devices.
- PGM1/PGM2: Wet contact outputs (60 mA max), supporting positive/negative triggering. It can be configured as NO or NC. If the current exceeds the limit, it is recommended that you connect a relay expansion.

Figure 3-5 Local alarm output cable connection

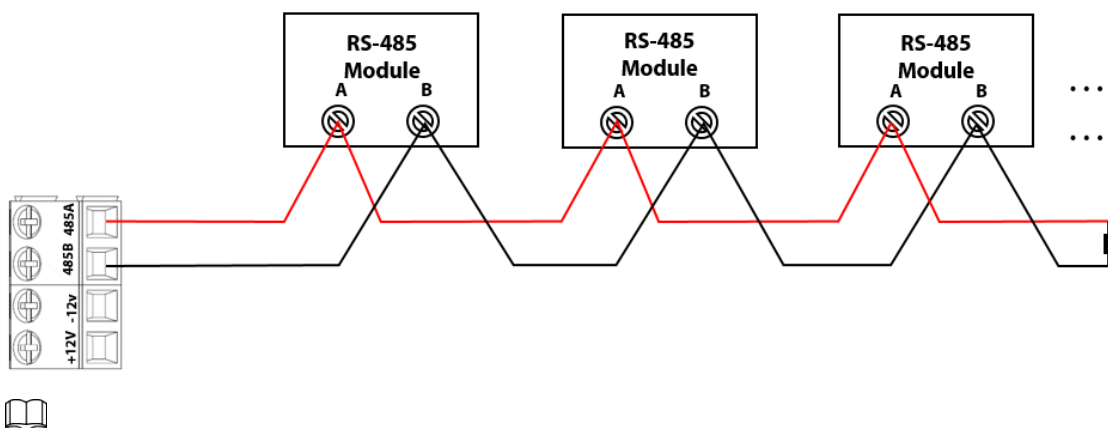


External devices need extra power supply. The load capacity of the alarm light is no more than 12 VDC and 3 A.

3.2.3 RS-485 Cable Connection

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

Figure 3-6 RS-485 cable connection

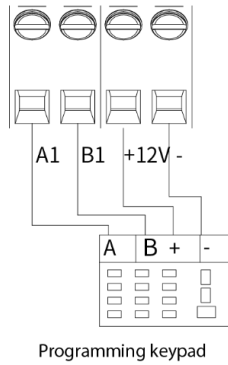


Terminating resistor for RS-485 bus of the end module needs to be switched to position 7 and 8.

3.2.4 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 panel.

Figure 3-7 Keypad cable connection



The end keypad connected to the panel must have its terminating resistor for RS-485 bus switch on the back of the keypad set to **ON**.

3.2.5 Siren Cable Connection

The load capacity of the siren port is 12 VDC.

The total maximum current output capacity for both auxiliary power output and siren output is 2 A.

There are 2 methods to connect the siren.

Figure 3-8 Siren cable connection-method 1

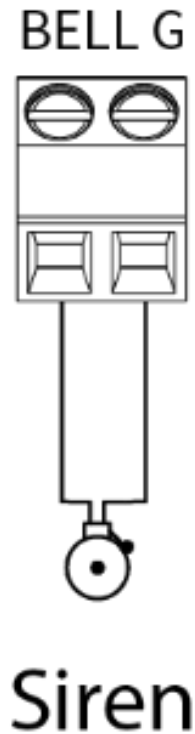
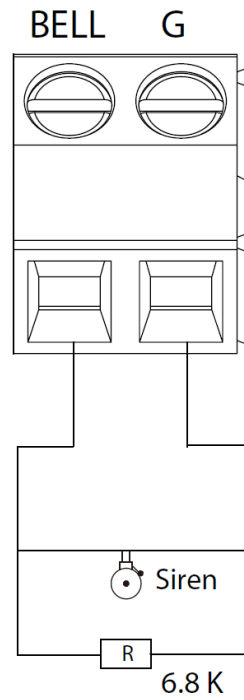


Figure 3-9 Siren cable connection-method 2



Using a 6.8 K terminating resistor for cable anti-cut and anti-short circuit protection.

4 DMSS Operations for End Users

DMSS app provides professional security surveillance services for end users. For DMSS admin users, you can share the panel with DMSS general users and entrust it to one enterprise. Peripherals that come with the panel can be shared and entrusted at the same time. To share and entrust the panel by yourself, you need to install the latest version of DMSS app.



The figures are for reference only and might differ from the actual interface.

4.1 Signing Up and Logging in to DMSS

The security system is configured and controlled through DMSS app. You can access to DMSS app on iOS and Android. This section uses the operations on iOS as an example.



Make sure that you have installed the latest version of the app.

Procedure

Step 1 Search for DMSS in the app store, and then download the app.



For Android users, you can go to Google Play to download DMSS.

Step 2 On your phone, tap  to start the app.

Step 3 Create an account.

1. Tap **Sign Up**.
2. Select a country or region from the list.
3. Enter the email and password for registration.



Tap  to show the password, and the icon will become .

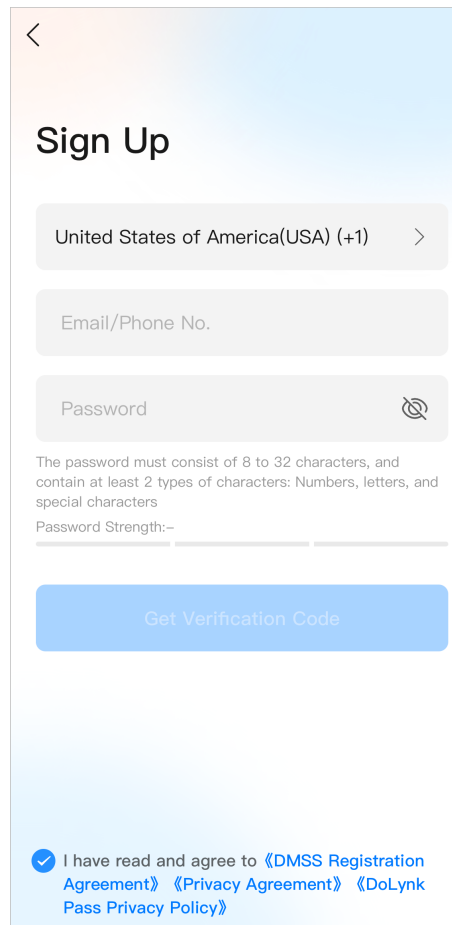
4. Select the **I have read and agree to DMSS Registration Agreement, Privacy Policy and DoLink Pass Privacy Policy**.
5. Tap **Get Verification Code**, check your email box for the verification code, and then enter the code.



Use the verification code within 60 seconds of receiving it. Otherwise, the verification code will become invalid.

6. Tap **OK**.

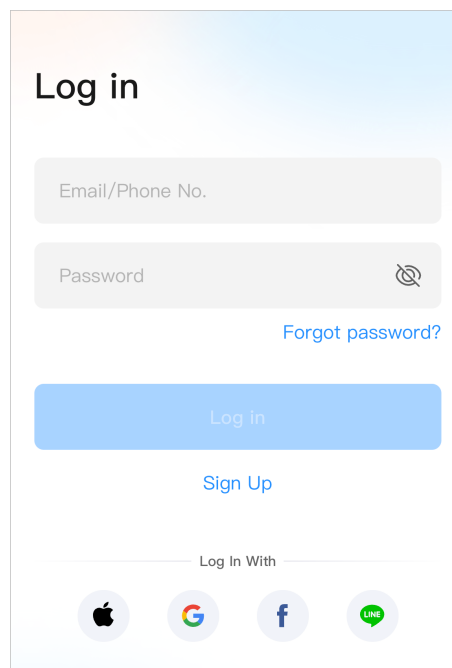
Figure 4-1 Sign up



The Sign Up screen features a light blue gradient background. At the top left is a back arrow. The title "Sign Up" is centered. Below it is a country selection dropdown showing "United States of America(USA) (+1)" with a right arrow. This is followed by input fields for "Email/Phone No." and "Password". The password field has an eye icon for toggling visibility. Below the password field, a text block states: "The password must consist of 8 to 32 characters, and contain at least 2 types of characters: Numbers, letters, and special characters". Below this is a "Password Strength:-" indicator with two progress bars. A large blue button labeled "Get Verification Code" is positioned below the strength indicator. At the bottom, there is a checked checkbox and the text: "I have read and agree to 《DMSS Registration Agreement》 《Privacy Agreement》 《DoLink Pass Privacy Policy》".

Step 4 Go back to the **Login** screen, enter your email and password, and then tap **Log In**.

Figure 4-2 Login



The Log in screen has a light blue gradient background. It features the title "Log in" at the top. Below the title are input fields for "Email/Phone No." and "Password". The password field includes an eye icon for visibility toggle. A blue link "Forgot password?" is located to the right of the password field. A large blue button labeled "Log in" is centered below the input fields. Below the "Log in" button is a blue link "Sign Up". At the bottom, there is a section titled "Log In With" with four circular icons for social login: Apple, Google, Facebook, and LINE.



You can modify the password on the **Me > Account Management > Modify Password**.

4.2 User Overview

Users can only be created on the DMSS app. Classify the users into different roles so that they can have different access levels for operating the devices.

For Certification IMQ-SISTEMI DI SICUREZZA is mandatory manage system with the DMSS for access level 2, and DoLynk Care for access level 3.

User Access Level

Table 4-1 User access level

User	Access Level
DMSS admin user	L2
DMSS general user	L2
Installer	L3

- **Installer:** Installers provide end users with operation and maintenance services. This role has to apply for permissions from the end user (DMSS admin user) to operate the device. They can receive permissions such as device configuration and user management.
- **DMSS admin user:** The administrator user would be an end user. This role cannot be modified and has permissions, such as device configuration and user management. The DMSS admin users does not have permission to configure the device when installers lend the panel to them, or when they entrust the panel to the installer.
- **DMSS general user:** These are users whom a DMSS admin user shares devices to through the DMSS app. This role can be modified and only has basic permissions, such as viewing device status, and arming and disarming rooms.

Business Flow

Following is the entrusting and sharing process on the DMSS app. Installers and end users can follow the process to share and entrust devices.

Figure 4-3 Business flow (DMSS user)

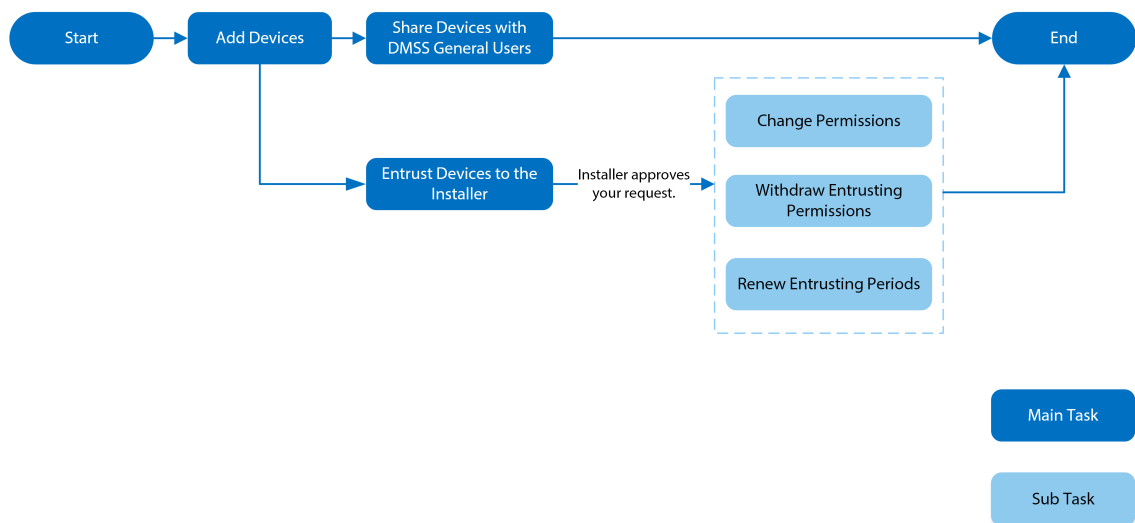
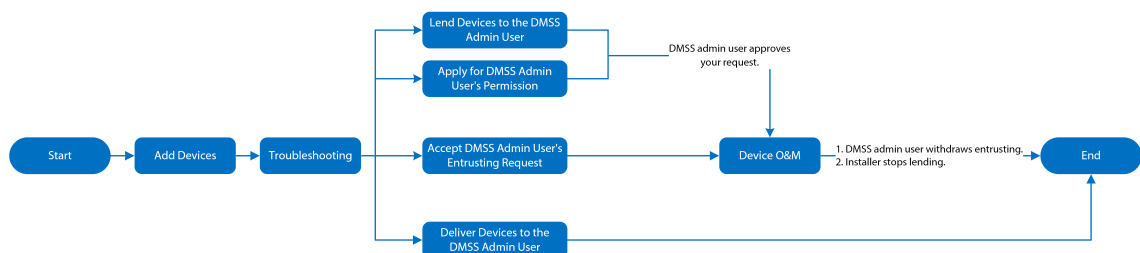


Figure 4-4 Business flow (Installer)



4.3 Adding Devices

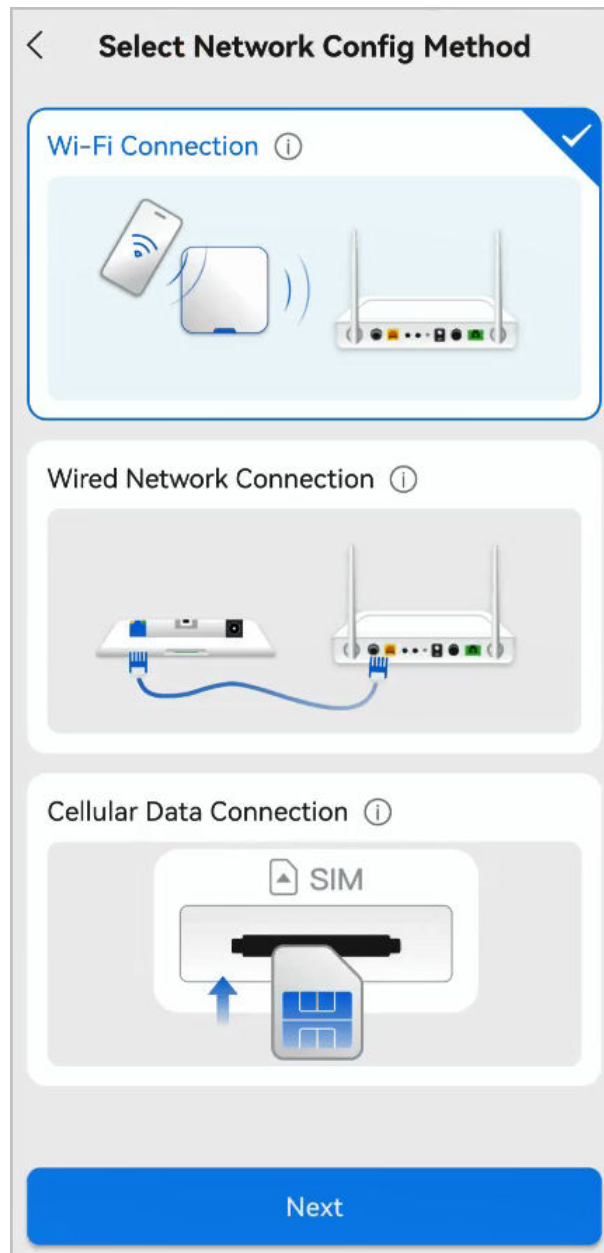
For end users, you can add alarm devices to DMSS app.

4.3.1 Adding the Panel

Procedure

- Step 1** On the **Device** screen, tap , and then select **Scan QR Code**.
- Step 2** Add a device.
- Scan the device QR code directly, or tap  and import the QR code picture to add a device.
 - Tap **Manually Enter SN**, and then enter the device SN to manually add a device.
- Step 3** Select network configuration mode.
- Wi-Fi connection: Make sure that you have available Wi-Fi to connect to and the panel supports Wi-Fi function.
 - Wired network connection: Make sure that you have connect the panel to the router using a network cable.
 - Cellular data connection: Make sure that you have inserted a SIM card and the 4G module into the panel.

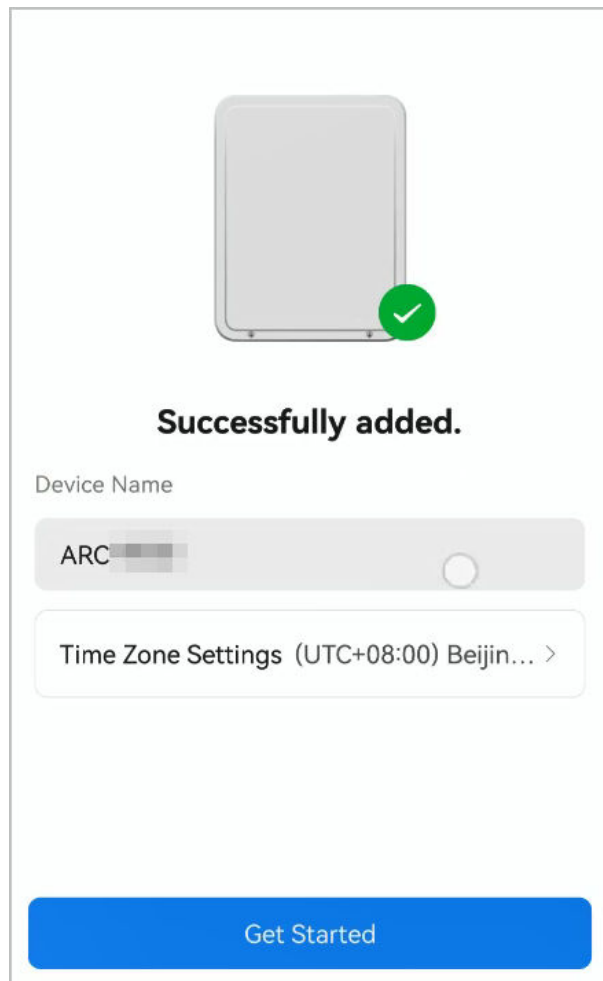
Figure 4-5 Network mode



Step 4 Follow the on-screen prompts to add the panel, and then tap **Next** .
Wait for the pairing to complete.

Step 5 Configure the panel name and select the time zone, and then tap **Get Started**.

Figure 4-6 Added successfully



4.3.2 Introduction of Peripheral Devices to be Added

Different peripheral devices are added differently to the hybrid panel on the DMSS app. The following is how to add them separately.

Table 4-2 Description for adding devices

Entry	Device Types
⊕ > Wired Device	Sirens, alarm input, alarm output, expansion input and expansion output
⊕ > Bus Device	LCD keypads and expansion modules
⊕ > Wireless Device	Wireless detectors, keyfobs, and wireless sirens
⊕ > IPC	IPC devices

4.3.3 Adding Bus Devices

Add bus devices to the hybrid panel.

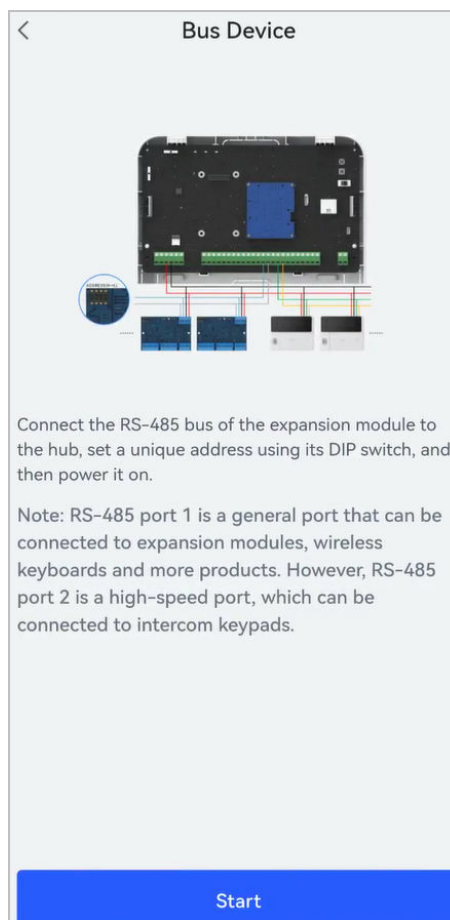
Prerequisites

Make sure that you have connected the bus devices to the panel through the RS-485 port before you add the bus devices on DMSS app.

Procedure

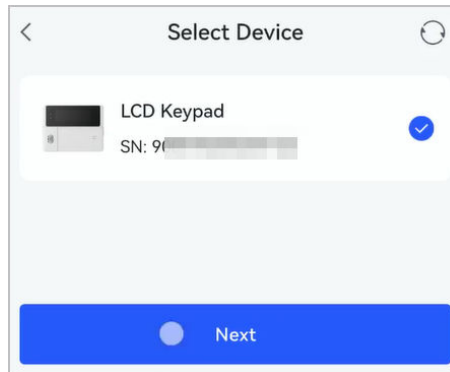
- Step 1 Go to the **Devices** screen of the panel, and then select  > **Bus Device**.
- Step 2 Tap **Start**, and then wait for the pairing to be complete.

Figure 4-7 Add bus device



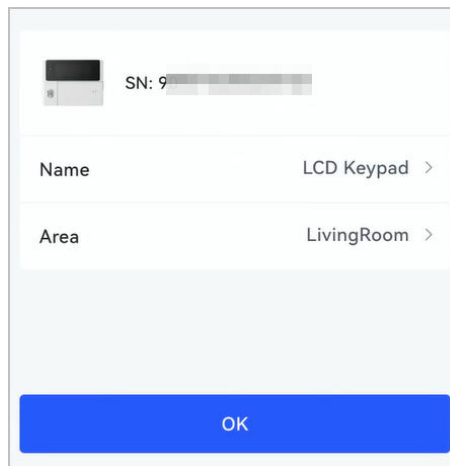
- Step 3 Select the paired bus device, and then tap **Next**.

Figure 4-8 Pairing complete



- Step 4 Custom the device name and select area for the device, and then tap **OK**.
The bus device is added successfully.

Figure 4-9 Custom device name and area



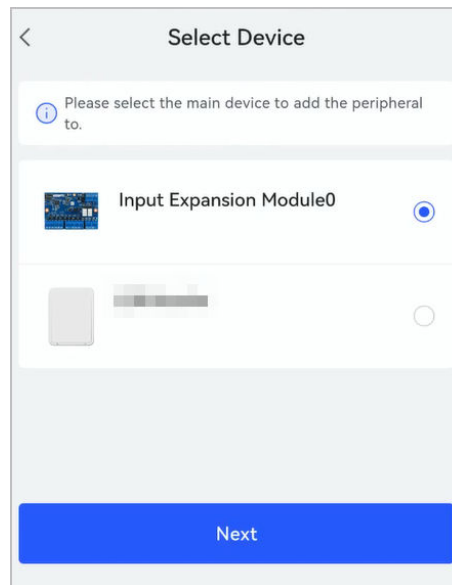
4.3.4 Adding Wired Devices

You can add wired devices and sirens to the hybrid panel.

Procedure

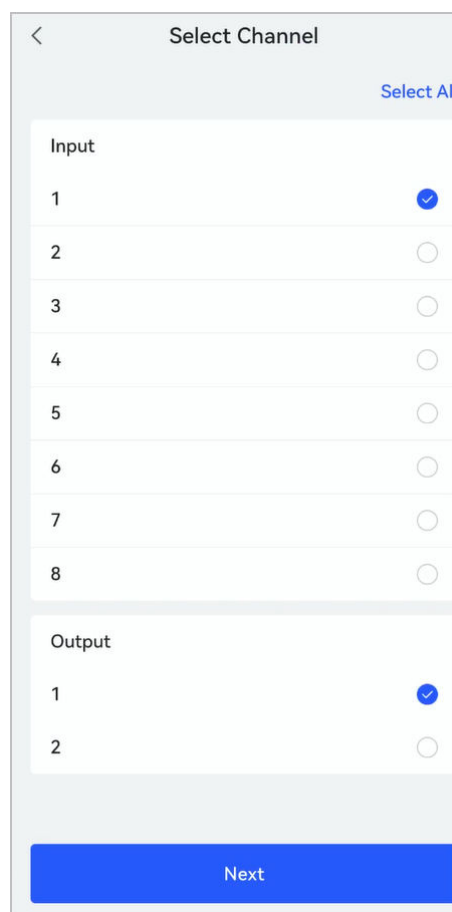
- Step 1 Go to the **Devices** screen of the panel, and then select  > **Wired Device**.
Step 2 Select the device from the list, and then tap **Next**.

Figure 4-10 Add wired device



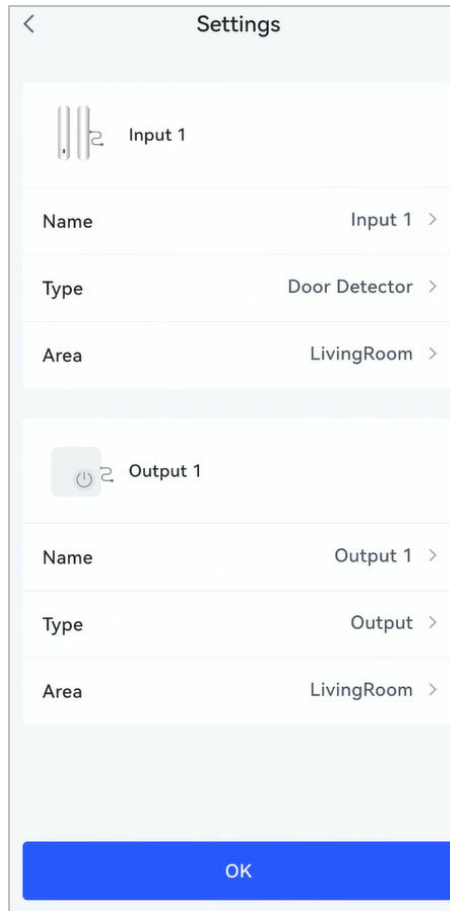
Step 3 Select the input or output channel, and then tap **Next**.

Figure 4-11 Add input or output channels



Step 4 Configure the name, type and assign area for the channels, and then tap **OK**.

Figure 4-12 Configure information



Settings

Input 1

Name Input 1 >

Type Door Detector >

Area LivingRoom >

Output 1

Name Output 1 >

Type Output >

Area LivingRoom >

OK

4.3.5 Adding Wireless Devices

You can add multiple wireless detectors, wireless sirens and keyfobs into the panel. For details on adding peripherals, see user manuals of respective peripherals.



Make sure that you have added devices with RF receiving function to the hybrid panel. Otherwise you cannot add wireless devices to the panel. For details, see "4.3.3 Adding Bus Devices".

Go to the **Devices** screen of the panel, and then select  > **Wireless Device**.

Add One by One

1. Scan the QR code at the bottom of the device, and then tap **Next**.
You can also enter the serial number of the peripheral by tapping **SN**, select a QR code image from **My Files** to add the peripherals.
2. Follow the on-screen instructions and switch the device to on, and then tap **Next**.
3. Wait for the pairing.
4. Customize the name of the device, and select the area, and then tap **Completed**.

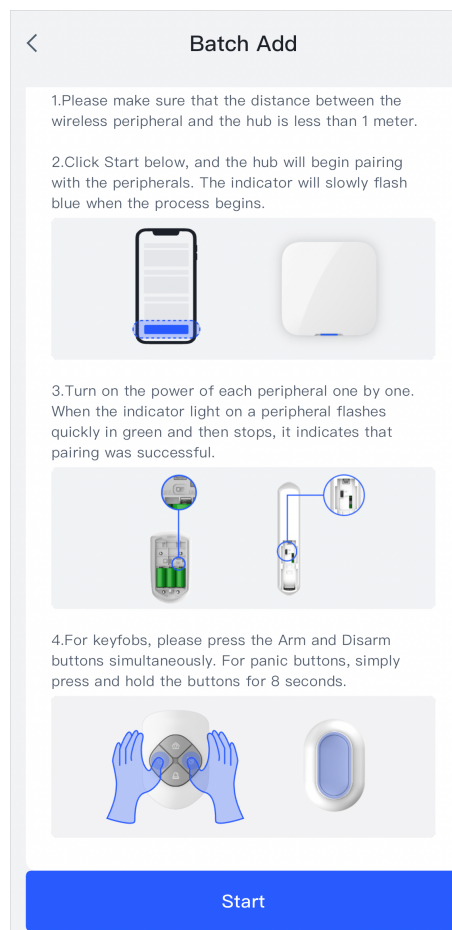
Add in Batches

Tap **Bach Add** , and then tap **Start** to start pairing.



- Make sure that the distance between the peripherals and the hub should be less than 1 meter.
- Turn on the power of the peripheral. When the indicator light on the peripheral flashes quickly in green and then stops, it indicates the pairing is successful. Repeat this step to add peripherals one by one. Be cautious that you must not power on peripherals at a time.
- For keyfobs, press the **Arm** and **Disarm** buttons simultaneously to start pairing. For panic buttons, press and hold the button for 8 seconds to go to pairing mode.

Figure 4-13 Batch add



4.3.6 Adding IPC

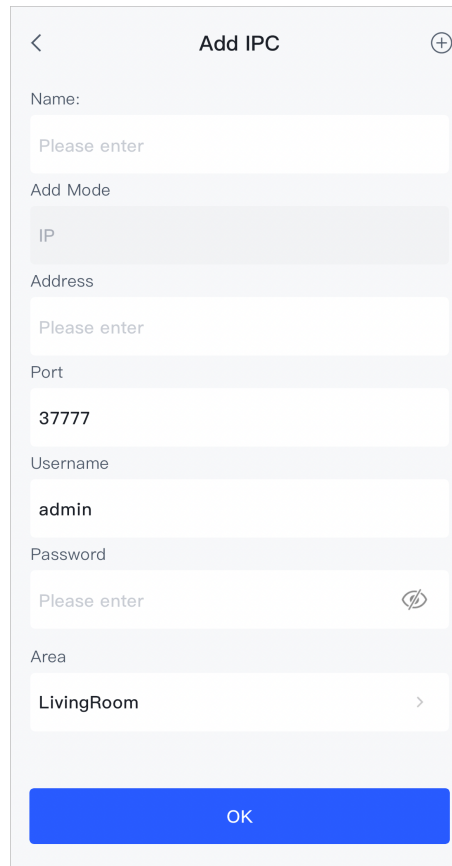
Add IPCs to the panel.

Procedure

- Step 1** Go to the **Devices** screen of the panel, and then select  > **Add IPC**.
- Step 2** Add an IPC to the panel.
- Manually add:

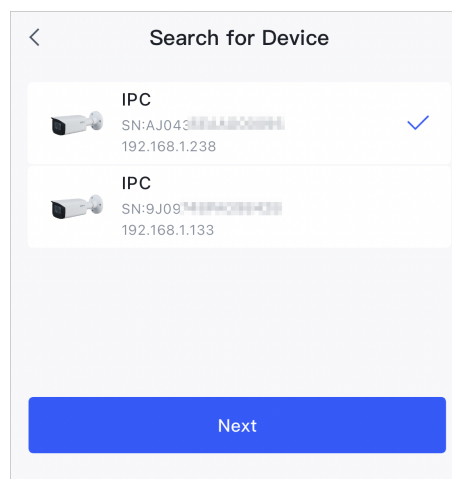
1. Configure the device name, IP address of the IPC, port number, username and the password of the IPC, and select the area where the IPC is assigned to, and then tap **OK**.

Figure 4-14 Manually add



2. Select the channel of the IPC, and then tap **OK**.
- Online search:
 1. Tap  and select **Search on LAN** to search for the IPC in the same network segment.

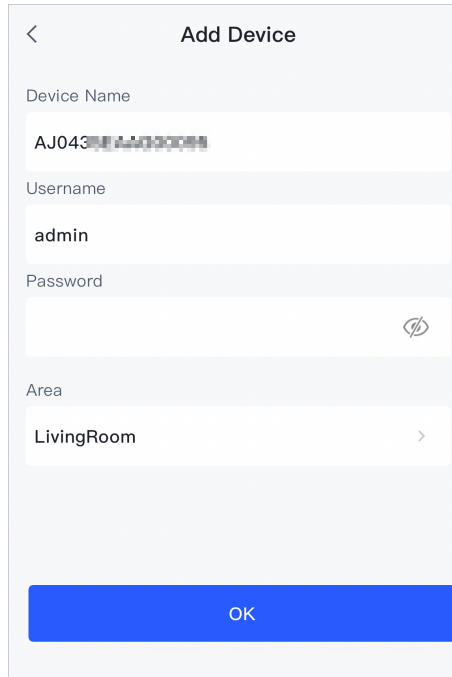
Figure 4-15 Online search



2. Tap **Next**.

3. Enter the password of the IPC and select the area where the IPC is assigned to, and then tap **OK**.

Figure 4-16 Enter password



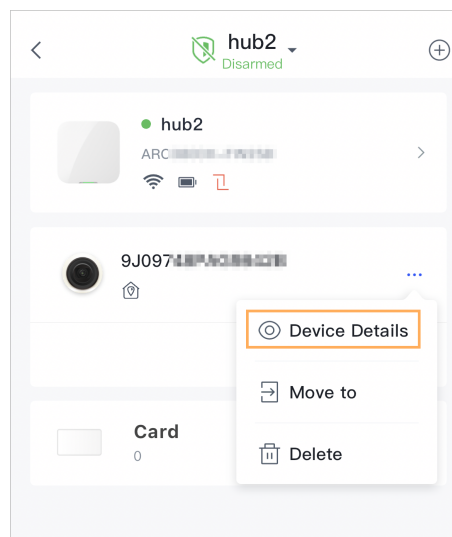
4. Select the channel of the IPC, and then tap **OK**.

Related Operations

You can configure the parameters of the added IPC.

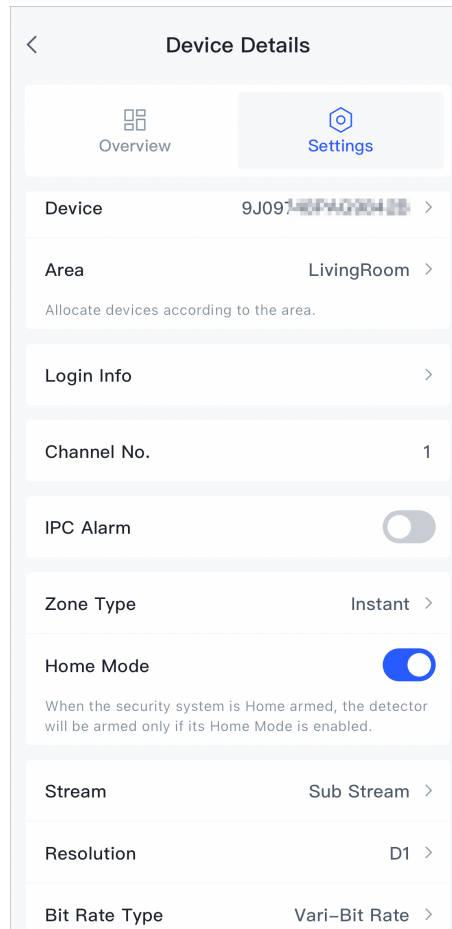
1. Select **Device Details** of the IPC.

Figure 4-17 Device details



2. Select **Settings** to configure the parameters of the IPC.

Figure 4-18 Configure parameters



4.3.7 Adding Card

Add card to hybrid panel.

Procedure

- Step 1** Go to the **Devices** screen of the panel, and then select  > **Add Card**.
- Step 2** Press any button on the LCD keypad to wake it up, and then swipe the card over the card swiping area.

4.4 Configuring Alarm Linkage Video

Configure the alarm linkage for peripherals so that you can view video clips when the alarm is triggered.

Prerequisites

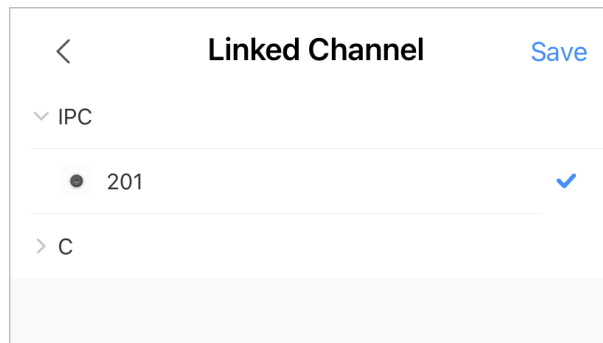
- Make sure that the panel is armed before you configure the alarm-video linkage.
- Make sure that you have added peripherals to the panel.

Procedure

- Step 1** On the **Devices** screen of the panel, select a peripheral, and then go to **Device Details** > **Settings** to configure the parameters.
- Step 2** Enable **Alarm and Video Linkage**, and then select **Video Channel**.

Step 3 Select a video channel from the **Linked Channel** list, and tap **Save**.

Figure 4-19 Linked channel



4.5 Panel General Settings

You can view and edit basic device information.

Procedure

Step 1 On panel screen, tap **Settings** to view device details.

Table 4-3 Parameter description

Parameter	Description
Device	- View name, type, SN and device model of the panel. - Edit device name, and then tap Save to save configuration.
Hub Setting	Configure parameters of the panel.
Network	Tap Network to view your present network information.
Time Zone	Tap Time Zone to select your time zone, and enable DST (daylight saving time) if necessary. Time Zone : Select the time zone in which the panel operates. DST : Select date or week, and then select start time and end time.
Language	Select the language linking to SMS voice. It supports 18 languages: Arabic, Czech, Danish, Dutch, English, French, German, Italian, Portuguese (Europe), Russian, Spanish (Latin America), Spanish (Europe), Turkish, Slovak, Polish, Greek, Bulgarian and Estonian. It is set as English by default.
User's Manual	Tap User's Manual to obtain the user manual of the hybrid panel.
Firmware Update	Update online.  Update is not allowed when the panel is in armed status or the battery level is low.

Parameter	Description
View Logs	View device and app logs. - Device log: Select View Logs > Device Log to view alarm logs of the device. You can also tap  on the Device Log screen to send alarm logs to the linked email. - App log: Select View Logs > App Log to view alarm logs. You can also tap  on the App Log screen to send alarm logs to the linked email.
Collect Logs	Collect logs for device and app.

4.5.1 Viewing Panel Status

Panel Icon Description

Introduces the meaning of icons for the door detector. You can view these icons on the panel screen.

Table 4-4 Device icon description

Parameter	Icon	Description
LTE Signal Strength		Ultra weak
		Weak
		Good
		No signal
		Excellent
Wi-Fi Signal Strength		Ultra weak
		Weak
		Good
		Excellent
		No signal
SIM Card		SIM card is active
		No SIM card
		The SIM card is unlocked
		The SIM card is locked

Parameter	Icon	Description
Battery Level		100%
		80%
		60%
		40%
		20%
		No battery
Tamper		Opened
Ethernet		Connected

Hybrid Panel Status Description

On the **Devices** screen of the panel, select a panel, and then select **Overview** or **Status** to view the panel information and status.

Table 4-5 Overview

Parameter	Description
Basic Info	Displays the basic information of the panel.
Online Status	Displays the online status of the panel.
Type	Displays the device type.
SN	Displays the serial number of the panel.
Model	Displays the device model of the panel.

Table 4-6 Status

Parameter	Description
Wi-Fi Signal Strength	Internet connection status of the panel through Wi-Fi. For greater reliability, we recommend installing the panel in places with the signal strength of at least 2 bars.
LTE Signal Strength	The signal strength of the mobile network for the active SIM card.
Battery Level	Shows the remaining electricity of the battery in the form of percentage.
Tamper	Displays the anti-tamper status of the panel. The types include: • Opened • Disconnected

Parameter	Description
External power	Shows external power connection status. The types include: • Connected • Disconnected
Wi-Fi	Displays Wi-Fi status of the panel. The types include: • Connected • Disconnected
Ethernet	Displays Ethernet status of the panel. The types include: • Connected • Disconnected
4G	Displays 4G status of the panel. The types include: • Connected • Disconnected
SIM Card	Displays the connection status of the SIM card. The types include: • SIM • None • Locked (This status bar is only supported when there is a SIM card inserted into the panel).
Firmware Version	The program version of the panel.

4.5.2 Configuring the Panel Parameters

Procedure

- Step 1 On the **Devices** screen of the panel, select the panel.
- Step 2 Select **Settings** > **Hub Setting** to view and edit general information of the panel.

Table 4-7 Panel parameter description

Parameter	Description
User Manager	You can add, modify, delete app or keypad users when the panel is disarmed. ● Keypad User : Tap Add to add a keypad user. Enter user name, operation code (4 to 6 digits), and duress passcode (optional), and then select arm and disarm permissions for the room.  ◇ Up to 64 keypad users are allowed (32 manually added users and 32 automatically created users). The first manually created user is the admin user by default. All the permissions are available to admin user. ◇ DMSS automatically creates a keypad user every time when a device is added for the first time. The sequence number of keypad users created by the system automatically starts from 33, and has an icon  next to its account. ◇ A keypad user will be automatically created for shared users. ● App User : Select the user to modify their permissions, including SOS, switch control, bypass, notification, keypad code, snapshot and alarm video.  Select Share Devices, enter the DMSS account to which the device is to be shared, and select the permissions for the account.
SOS Alarm	Configure SOS alarm types, including panic alarm, link to siren, medical alarm and fire alarm. After configuration, tap SOS on the Operation screen of the panel to trigger alarm. When multiple alarm types are selected, a pop-up window prompts to remind you select one alarm to trigger this time.
Installer	Entrust service providers. Tap Entrusting , enter the service provider account, entrusting period, and select the devices to be entrusted, select I have read and agree User Agreement, and then tap Next.
Global Arming/Disarming	Arm or disarm all the detectors in all the areas with one tap.
Scheduled Arming/Disarming	Arm or disarm the areas by schedule. ● Area : Select the area in which the panel operates. ● Command Settings : Select an armed mode as needed by tapping Home, Away, or Disarm. ● Time Point : Select the time period in which the panel operates. ● Repeat : Select the day(s) of the week as the repeat period. ● Forced Arming : You can arm the system when errors happen in zones.

Parameter	Description
Sound Settings	● Volume : Select the volume for alarm. ● Alarm/Tamper Sound : Enable the function so that there will be sound when the alarm or tamper event occurs. ● Duration : Configure the duration for the alarm sound. ● Play Sound for Delay Time and Arming/Disarming : Enable the function so that the ringtone will be applied in these scenarios.
Intercom Service	Enable Intercom Service to achieve the function. ● Intercom Time Limit : When an alarm is triggered, intercom services can be initiated within the configured time interval. Once the time goes expired, a new intercom session cannot be started again.  The duration of every intercom session cannot be over 20 minutes. ● Intercom : Select at least 1 intercom device regardless of the method you select. ◇ App intercom: Intercom between the keypad and DMSS app. Enable App , select the keypad assigned to different areas, or select Do Not Link. ◇ Alarm receiving center: Intercom between the keypad and the platform. Enable Alarm Receiving Center, and then configure parameters. ○ Protocol: Select SIP or VOIP. ○ Select by Intercom Device : Only one device with the intercom function under the panel can be selected for intercom. ○ Select by Zone : For each room, only one LCD keypad with the intercom function added under the panel can be selected. ○ Server Config : Configure the server information.
Test Mode	Tap Start to test the status of the peripherals connecting to the panel in different areas, and then tap Stop to complete detection.
Cloud Service Connection	Set the server-panel ping interval with the range from 150 to 900 seconds (150 seconds by default). If the D-cloud detects that the panel's offline duration exceeds 150 seconds, it will report the panel status to the user through app.

Parameter	Description
Heartbeat	Configure the panel-detector ping interval. The settings determine how frequently the panel communicates with the peripherals and how quickly the loss of connection is detected. ● Detector Ping Interval (s) : The frequency of connected peripherals operated by the panel is configured in the range of 12 seconds to 300 seconds (60 seconds by default).  The shorter the detector ping interval, the shorter the life span of the battery. ● Number of Dropped Packets : A counter of undelivered packets is configured in the range of 3 to 60 (15 packets by default).  ◇ The smaller the number, the more frequently the offline status of peripherals is detected and reported. ◇ If the panel constantly loses connection with the peripherals and cannot detect their defined heartbeats, it will report their offline status to the system.
Link Siren for Tamper	● Link Siren for Tamper : In the arming status, when the Link Siren for Tamper is enabled, the panel will link the alarm sound.  The siren will alert when the lids of the panel and peripherals are open. ● Disarm linkage: The alarm linkage is enabled in disarming mode.  Enabling this function is not compliant with EN50131-1 standard.
System Integrity Check	When enabled, the panel checks whether the current system is abnormal during arming. If it is abnormal, arming will be prevented. The items checked include arm with faults, main power failure, main power failure delay, alarm panel tamper, connection to cloud platform, wired network error, Wi-Fi error, RF jamming and ARC connection.  ● For the keyfob, the indicator flashes green, and then turns red. ● For the app, an alarm message pops up. ● For the keypad, it beeps for 1 second, the arming and disarming indicator flashes green for 2 seconds, and then it turns to the normal status.

Parameter		Description
Alarm Receiving Center	Basic	Select Alarm Receiving Center 1 or Alarm Receiving Center 2, and go to the respective configuration screen. Enable the function, and then configure parameters. ● Primary Channel : Enable the function, and then you can configure parameters. ● Connection Method : Select from PSTN and IP.  You need to connect the PSTN module to the panel before you use PSTN for communication.
	Connection Mode (PSTN)	● Communication Protocol : Select from ContactID and Phone.  In Phone mode, calls will only be made when an alarm is triggered. ● Central Account : Enter the account number that created by the alarm receiving center , which is used to identify the panel when the panel sends information to the alarm receiving center . ● ARC Name : The name of the alarm receiving center, which is used for keeping logs and subsequent message push. ● Alarm Receiver No. : Configure the phone number of the alarm controller in the alarm receiving center. ● Dialing Delay : The time of dialing delay. ● Number of Redials : The time of redials. ● Transmission Mode : Select from DTMF Slow Dial and DTMF Fast Dial. ● Phone number : Enter the phone number if you select Phone for Communication Protocol. ● Secondary channel : Enable the channel and then configure parameters if you select Phone for Communication Protocol.

Parameter		Description
	Connection Mode (IP)	● Communication Protocol : Select from SIA-DC09 (SIA-CID) , SIA-DC09(SIA-DCS), Softgard, Converter. ● Central Account : Enter the account number that created by the alarm receiving center , which is to be used to identify the panel when the panel sends information to the alarm receiving center . ● IP Protocol : It is TCP by default. ● IP/Domain/Port : The IP/domain name and port of the alarm receiving center. ● Heartbeat Interval :The heartbeat interval between the panel and the alarm receiving center.  Heartbeat interval is disabled when you enter 0 seconds. ● Encryption : Enable the function and enter the key for encrypting the messages. ● Retransmissions : Configure the number of retransmission for failed event uploads (when the alarm receiving center is online). ● Retransmission Interval : Configure the interval of retransmission for failed event reuploads (when the alarm receiving center is online). ● Communication Test : Click Test to test the connection status with the alarm receiving center. ● Scheduled Test : When enabled, the panel reports periodic test event regularly. You can configure the auto report period for sending test. The default period is 24 hours.

4.6 Network Configuration

On the **Device Details** screen, select **Basic Config** > **Network Configuration**, and then you can select network for the panel: wired network, wireless network, or cellular network.

4.6.1 Wired Network Configuration

Procedure

- Step 1 Select **Network Settings** > **Wired Network Config**.
- Step 2 Configure wired network connection parameters.

Table 4-8 Description of wired network parameters

Parameter	Description
DHCP	When there is a DHCP server on the network, you can enable DHCP , and then the panel gets a dynamic IP address automatically.
IP Address	Set the IP address manually: Set IP address, subnet mask, default gateway, DNS and MAC address manually for the panel.
Subnet Mask	

Parameter	Description
Gateway	
DNS	
DNS 2	
MAC Address	

4.6.2 Wi-Fi Network Configuration

Background Information



The Wi-Fi function is available on select models.

Procedure

- Step 1 Select **Network Settings** > **Wi-Fi Network Configuration**.
- Step 2 Select an available Wi-Fi network in the area, and then enter the network password to connect to the network.

4.6.3 (Optional) Cellular Configuration

Procedure

- Step 1 Select **Network Settings** > **Cellular**.
- Step 2 Configure cellular parameters.

Table 4-9 Description of cellular parameters

Parameter	Description
Cellular	Tap ☐ next to the Cellular to enable the cellular.
Priority	Tap ☐ next to the Priority to set the cellular as the priority when selecting the network.
SIM	The SIM card allows the panel to use cellular data, and push alarm notifications.
APN	The Access Point Name (APN) is the name of the settings your device reads to set up a connection for the gateway between your carrier's cellular network and the public internet.
Auth Mode	Authentication mode of the cellular networking.
Username	The user name and password of the cellular network.
Password	
Dial Number	The number that the panel is to call.
Roaming Data	Enable the function when you travel outside the coverage region to access internet connection.
Mobile Data Usage	View the usage of the mobile data.
Reset Statistics	Reset mobile data usage to restart the count.

Parameter	Description
PIN	Supports to enter the PIN of SIM 1 and SIM 2 respectively for privacy protection when necessary.  It is prohibited to enter the PIN code when the SIM card status is unlocked. Lock it when you want to enter the PIN.

4.7 Managing Devices

4.7.1 Entrusting Devices

You can entrust devices one by one or in batches.



Device entrusting services are available in some countries or areas, including France, Benelux, Italy, Spanish Portuguese, Germany, Hungary, Czech Republic, Turkey, Baltic Sea, Poland, Latin America, Russia, Myanmar, Thailand, Vietnam, Algeria, Tunisia, Tanzania, South Africa, Australia, and India.

4.7.1.1 Entrusting the Device One by One

You can entrust a device to DoLink Care users. You can configure the entrusting permissions.

Prerequisites

You have bound with a service provider.

Procedure

- Step 1** On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2** On the **Device Details** page, tap the device icon to go to the **Device Info** screen, and then tap **Entrust**.
- Step 3** On the **Entrust** screen, confirm the information of the bound service provider, or you can also tap  to scan the corresponding QR code of the installer.
- Step 4** Select entrusting periods and permissions, and then tap **OK**.

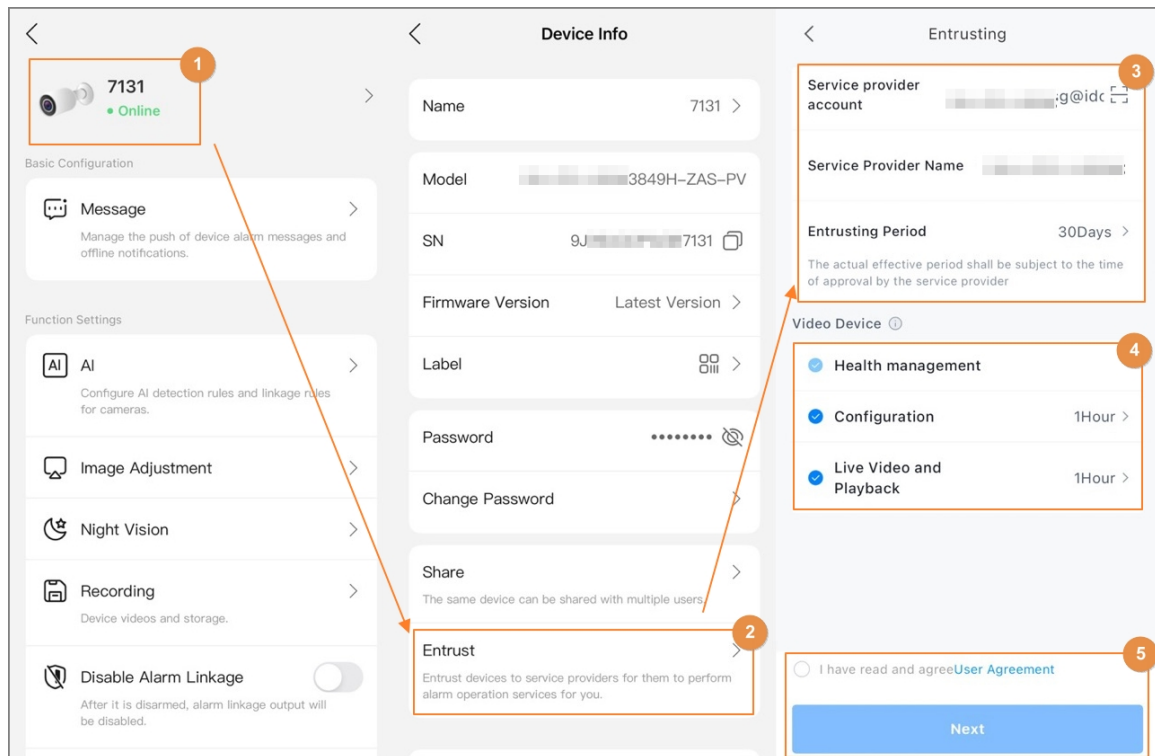
Table 4-10 Instruction of permissions

Permission	Description	Note
Health Management	It is selected by default, which cannot be canceled, including the permissions for one-click health check, error reporting, error fixing, data statistics, and health report.	—

Permission	Description	Note
Video Devices	You can request for the permissions of device configuration, live video and playback. ● Configuration permissions: Including restarting and upgrading the device, formatting SD card and configuring plug-in. ● Live video and playback: View the live video, play back the recordings and the view video permission of the plug-in.	You can choose temporary permissions, such as 1 hour or 4 hours, or opt for authorization during the whole entrusting period. For example, if the entrusting period is 30 days, you will have the permissions for the entire 30-day duration.
Alarm Devices	You can request for the permissions of device configuration and operation. ● Configuration permissions: Including adding, deleting and configuring the peripherals, adding, deleting and configuring the rooms, editing the device information, configuring the device network and time zone, upgrading the device, adding and deleting users, changing device password and binding with converter account. ● Operation permissions: Including arming or disarming (including SOS), testing alarm hub and peripherals, and alarm output control (plug, switch and relay).	
Video Interconnect Devices	You can request for the permissions of device configuration and operation. ● Configuration permissions: Including network transmission, SIP configuration and device maintenance. ● Operation permissions: Including talk and opening doors.	

Step 5 Read and select **I have read and agree User Agreement**, and then tap **Next**.

Figure 4-20 Entrust a device



Results

You can view entrusting status on device list screen. When successfully entrusted, the device status changes from **Under Reviewing** to **Entrusting to ******.



After an entrusting request has been successfully sent, a message will pop up on the **Home** screen. You need to wait for a response from the installer, which will be displayed on the **Message > Mailbox > Personal Information**.

Related Operations

- To change permissions, go to the **Entrust to Company** screen, and then tap **Change Permissions**.
- To withdraw entrusting permissions, go to the **Entrust to Company** screen, and then tap **Withdraw**.
- To renew entrusting periods, go to the **Entrust to Company** screen, and then tap **Renew**.

4.7.1.2 Entrusting Devices in Batches

You can entrust devices to the service provider in batches.

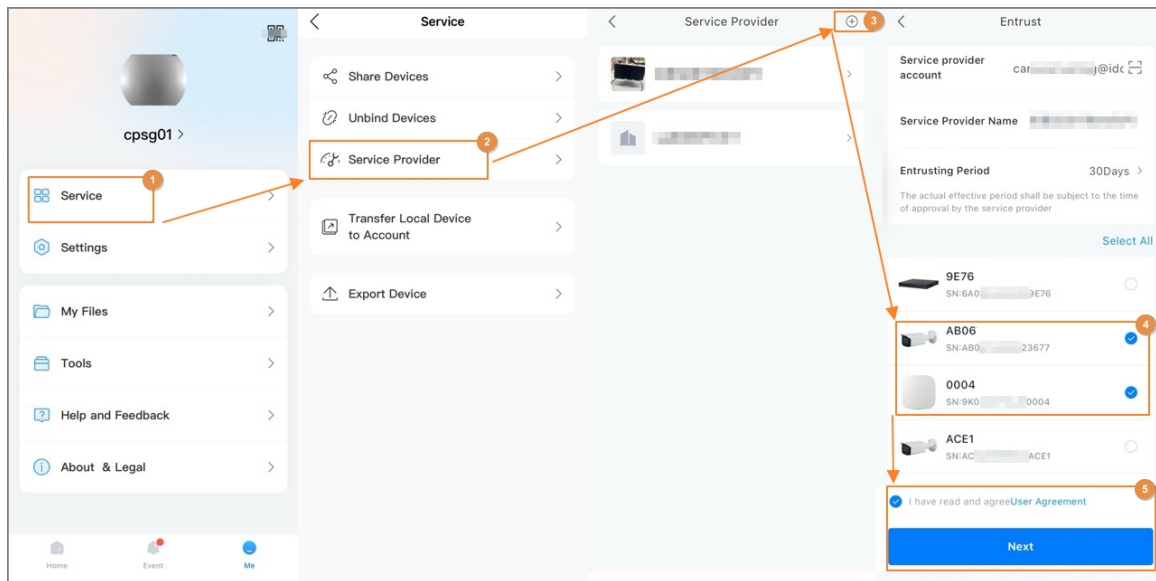
Prerequisites

You have bound with a service provider.

Procedure

- Step 1** On the **Device** screen, select **Me > Service > Service Provider**, and then tap .
- Step 2** On the **Device Entrusting** screen, confirm the information of the bound service provider, or you can also tap  to scan the QR code of the service provider.
- Step 3** Select the devices to be entrusted, and then entrust those to DoLink Care. The process for entrusting multiple devices is the same as entrusting a single device.

Figure 4-21 Entrust devices in batches



4.7.2 Unbinding Devices

When you add the device, if the device has been bound to another account, you can unbind the device first. Then you can add the device successfully.

Procedure

- Step 1** Tap **Unbind** on the home screen.
- Step 2** Tap **Apply Unbind**.
- Step 3** Scan the QR code or enter the SN of the device manually. There are following 2 methods:
 - Request to unbind:
 1. The system displays the authorization code. Follow the on-screen instructions to upload the required images.
 2. The system verifies the submitted information. The device can be unbound after the system verifies the information successfully.
 - Unbind with device password: If you have the device password, you can enter the device password to unbind the device.



The device must be online. If you forgot the password or the password is incorrect, you can request to unbind the device.

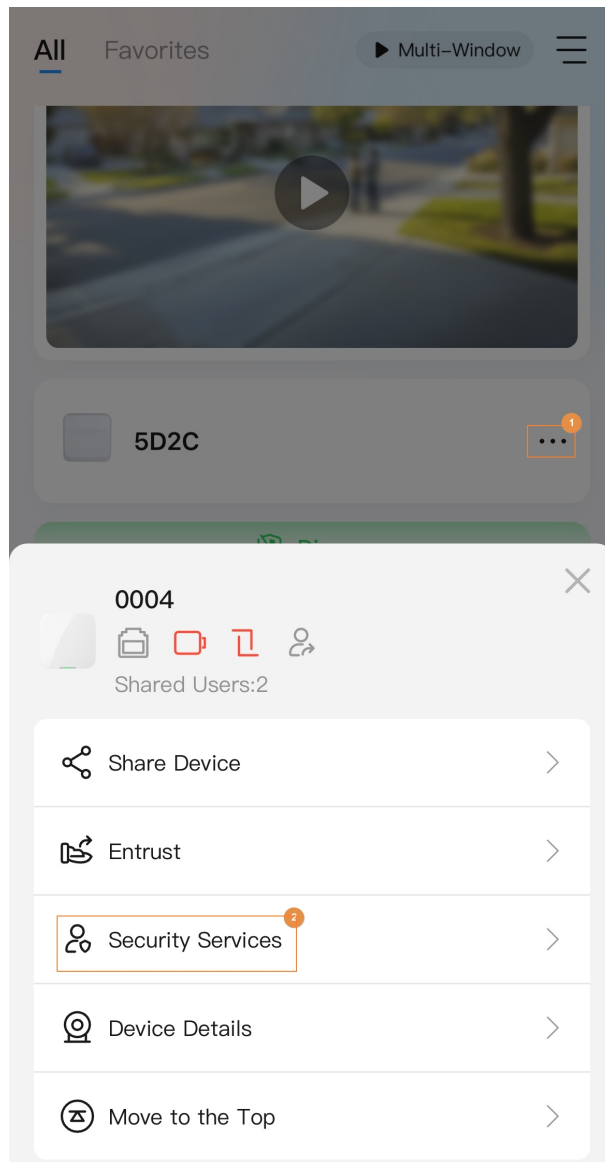
4.7.3 Applying for Security Services

You can apply for security services for the alarm hubs and CCTV devices. Bind the device to a Converter account in the region. After you bound the alarm hub to a Converter account, all the alarm messages, errors and notifications will be sent to the Converter.

Procedure

- Step 1** On the **Device** screen, tap **...** next to an alarm hub, and then tap **Security Services**.

Figure 4-22 Apply for security services



Step 2 Tap **Apply**.

Step 3 Displays all the security companies which are in the same city as the current DMSS account, including the company name, email and logo. Tap the company to view the company details, and then tap **Apply**.



- You can select the country or area on the top of **Security Company** screen.
- Supports searching for the company by entering the company name.

Step 4 Confirm your account information, and then tap **Apply**.

Related Operations

After the binding application is sent, the Converter account must review and activate the service. After the application is accepted, you can receive a message.

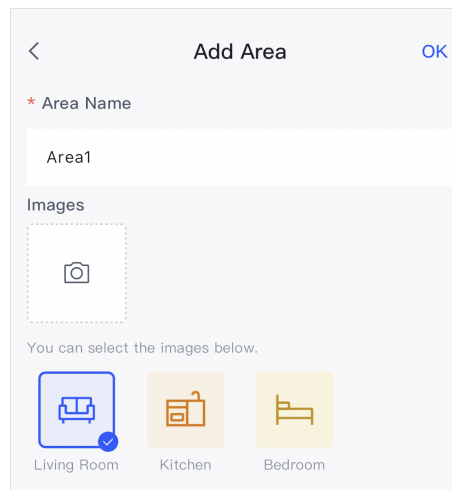
4.8 Managing Areas

4.8.1 Adding Areas

Procedure

- Step 1 On the **Area** screen of the panel, tap **+** at the upper-right corner to add areas.
- Step 2 Configure the area, select image for the area, and then tap **OK**.

Figure 4-23 Add area



4.8.2 Setting Area as Public Area

Set the area as public area, and then it can be linked to other areas.

Background Information

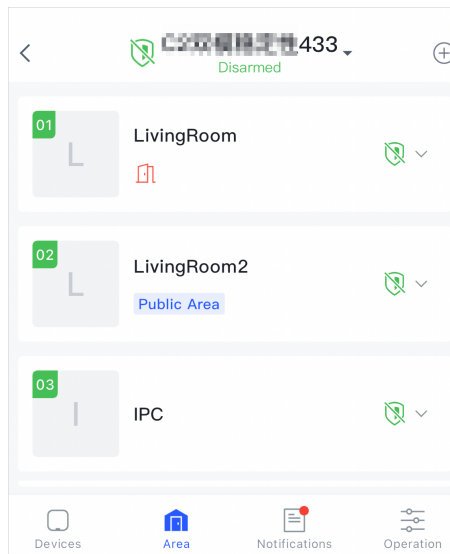
A public area must have linked to at least 2 other areas.

- If all linked areas are armed, the public area will automatically arm itself.
- If any one of the linked areas is disarmed, the public area will automatically disarm itself.

Procedure

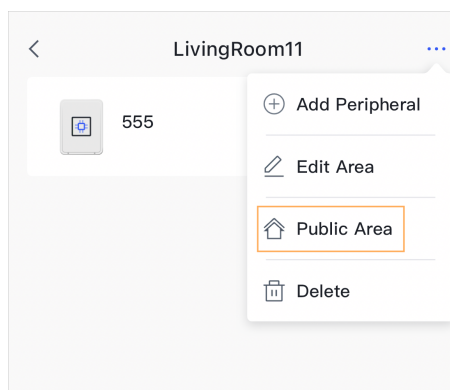
- Step 1 On the **Area** screen of the panel, select an area to go to its details screen.

Figure 4-24 Select an area



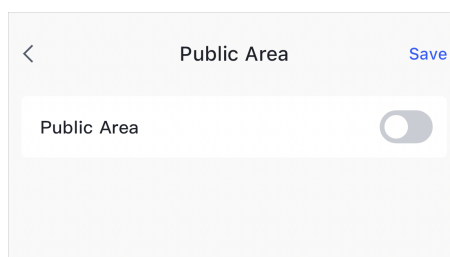
Step 2 Tap ... at the upper-right corner, and then tap **Public Area**.

Figure 4-25 Set as public area



Step 3 Enable **Public Area**, and then tap **Save**.

Figure 4-26 Enable public area

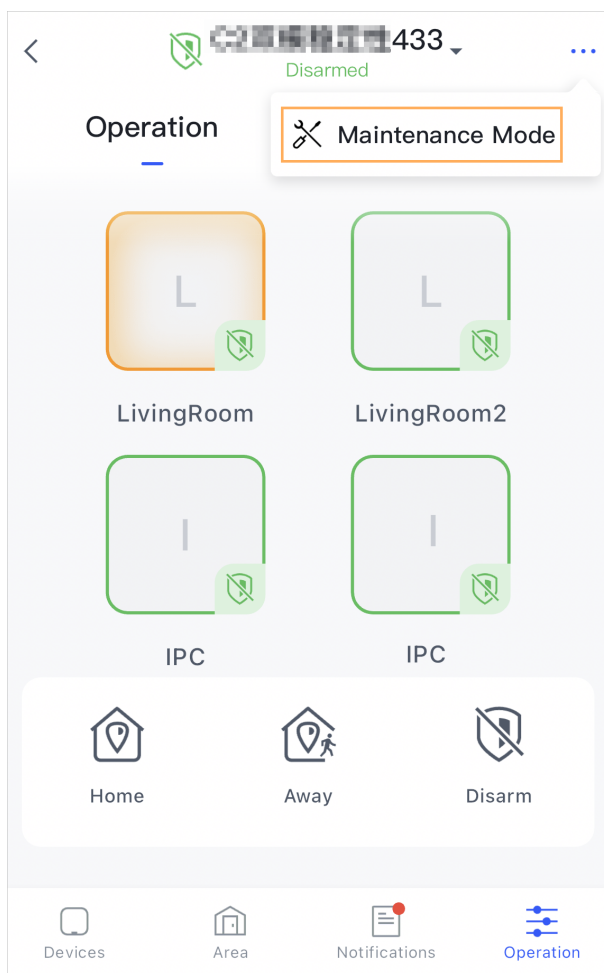


4.8.3 Configuring Maintenance Mode

Maintenance mode is designed for device servicing and updates. In the maintenance mode, the system suspends all alarm and fault reporting to the areas to avoid unnecessary notifications during maintenance tasks.

On the **Operation** screen, tap ... at the upper-right corner, and then tap **Maintenance Mode**.

Figure 4-27 Maintenance mode



5 General Operations

The user in level 2 or 3 has the permission to arm and disarm the system. This section uses end user's operation on DMSS as an example.

Prerequisites

- Make sure that you have added a panel before performing configurations.
- Make sure that the panel has a stable internet connection.
- Make sure that the panel is disarmed.

Background Information

You can manage alarm panels and peripherals, and perform operations such as arming and disarming, configuring alarm devices.

Procedure

- Step 1 On the panel screen, tap **Peripheral** to add the peripherals. For details on adding the peripherals, see the user manual of the corresponding device.
- Step 2 Arm and disarm the detectors in a single area or all the areas through manual or scheduled operations.
- **Single Arming and Disarming** : Arm and disarm the detectors in a single area.
 - **Global Arming and Disarming** : Arm and disarm the detectors in all the areas.
 - **Manual Arming and Disarming** : Arm the security system through the DMSS app, keypad or keyfob.
 - **Schedule Arming and Disarming** : Arm and disarm the detectors by schedule.

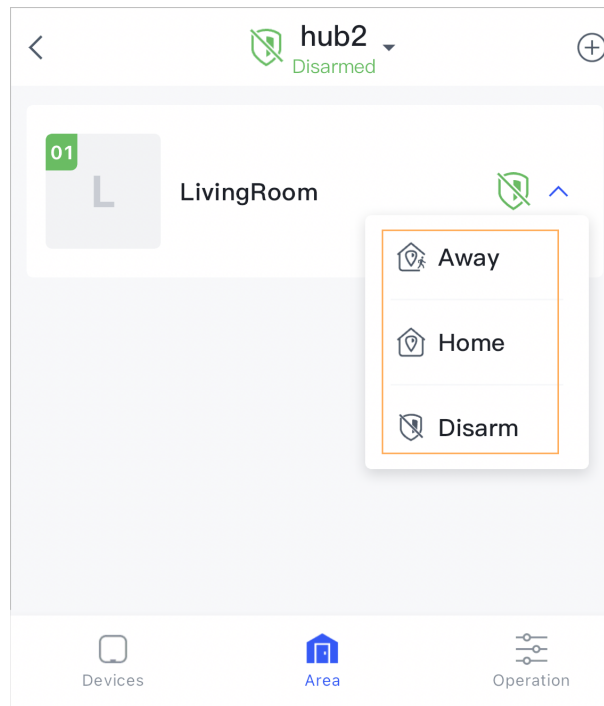
5.1 Single Arming and Disarming

You can arm and disarm the detectors in a single area.

Procedure

- Step 1 On the panel screen, tap **Area**.
- Step 2 Tap  next to an area, and then select from **Home** , **Away**, **Disarm**.
- **Home** : Arm the system when inside the area of the alarm system.
 - **Away** : Arm the system when you leave the area of the alarm system.
 - **Disarm** : Turn the security system off. The opposite of arming.

Figure 5-1 Single arming and disarming



5.2 Global Arming and Disarming

You can arm and disarm the detectors in all the areas.

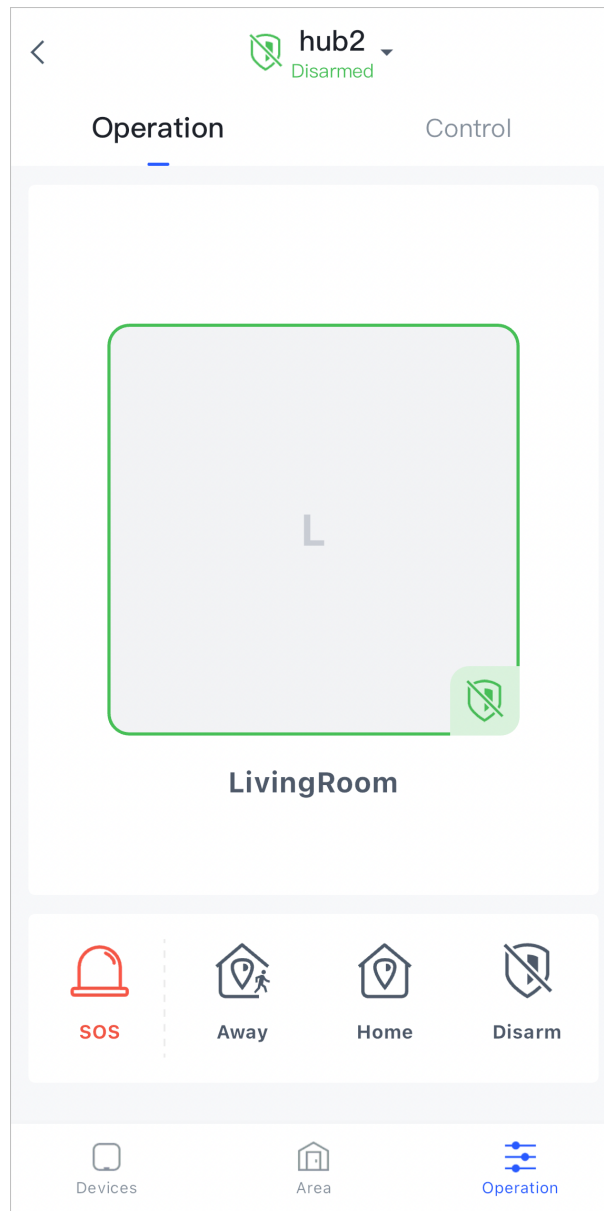
Prerequisites

Make sure that you have enabled the **Global Arming/Disarming** function.

Procedure

- Step 1 On the **Operation** screen of the panel, select from **Home**, **Away** to global arm the detectors.
- Step 2 Tap **Disarm** to global disarm the detectors.
- Step 3 Tap **SOS** to trigger alarms.

Figure 5-2 Global arming and disarming



5.3 Manual Arming and Disarming

You can arm the security system through the DMSS app or keyfob.

- To arm and disarm the detectors in a single area or all the areas, see "5.1 Single Arming and Disarming", and "5.2 Global Arming and Disarming".
- To operate through the keyfob and keypad, you need to assign the control permissions of the areas to the keyfob and keypad first. For details, see the user manual of the corresponding keyfob and keypad.

5.4 Scheduled Arming and Disarming

You can set a schedule to arm and disarm detectors. You can configure arming plans, including arming area, modes and periods.

Procedure

- Step 1** On the panel screen, select **Device Details** > **Settings** > **Hub Setting**.
- Step 2** Select **Scheduled Arming/Disarming** screen, tap **Add**, and then configure arming plans.

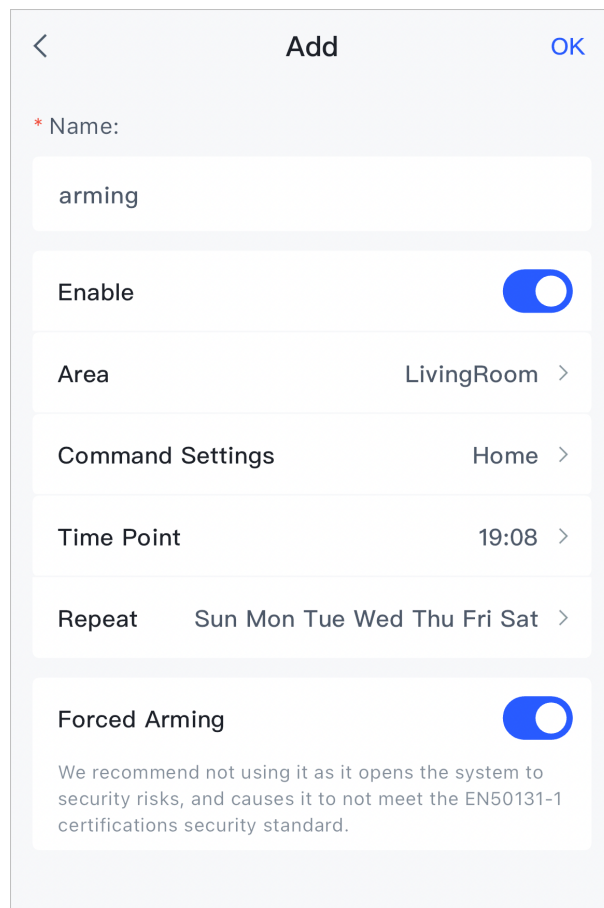
- **Name** : Customize a name for the arming plans.
- **Area** : Select a single or multiple areas that you want to arm.
- **Command Setting** : Select from **Home**, **Away**, and **Disarm**.
- **Time** : Set an arming time.



To apply the arming time to other days, tap **Repeat** and select the days you want.

- **Forced Arming** : Select as needed.

Figure 5-3 Scheduled arming and disarming



The screenshot shows the 'Add' screen for configuring a scheduled arming plan. The screen has a light gray background with white input fields and blue toggle switches. The top bar has a back arrow, the title 'Add', and an 'OK' button. The form contains the following elements:

- Name:** A text input field with the value 'arming'.
- Enable:** A toggle switch that is currently turned on (blue).
- Area:** A dropdown menu showing 'LivingRoom' with a right arrow.
- Command Settings:** A dropdown menu showing 'Home' with a right arrow.
- Time Point:** A dropdown menu showing '19:08' with a right arrow.
- Repeat:** A dropdown menu showing 'Sun Mon Tue Wed Thu Fri Sat' with a right arrow.
- Forced Arming:** A toggle switch that is currently turned on (blue).

Below the 'Forced Arming' toggle, there is a warning message: 'We recommend not using it as it opens the system to security risks, and causes it to not meet the EN50131-1 certifications security standard.'

- Step 3** Tap **OK**.

6 Web Operations

6.1 Starting the Device

6.1.1 Initializing the Hybrid Panel

Background Information

When using hybrid 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.

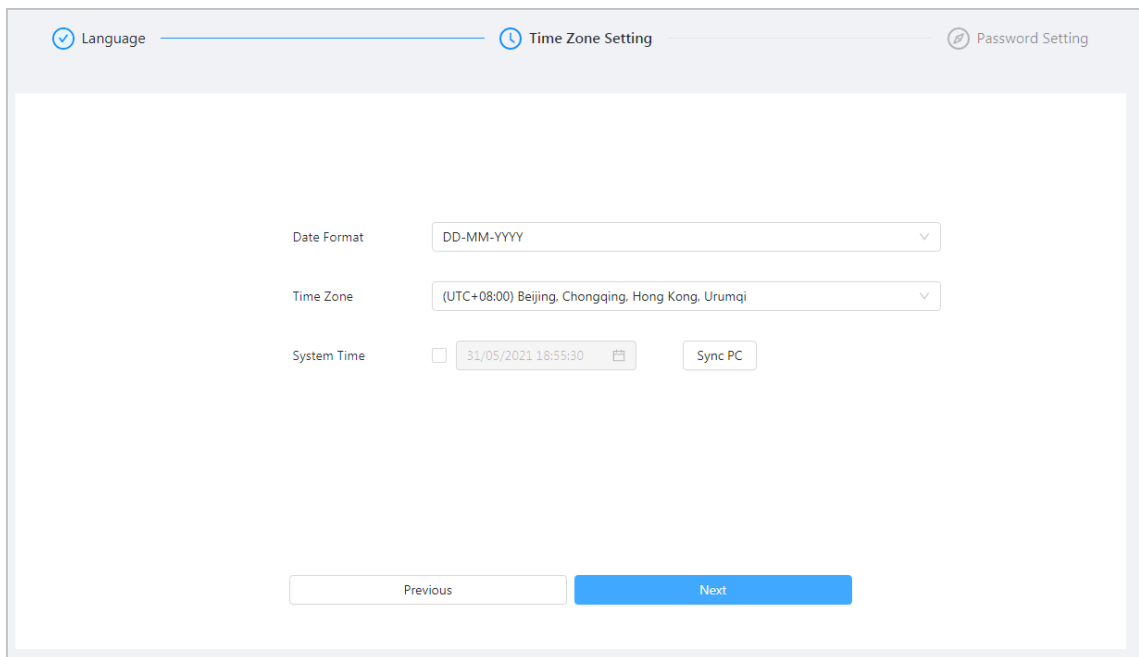


- To protect your device, keep your admin login password safe after completing the initialization steps, and change the password regularly.
- The default IP address of LAN1 is 192.168.1.108, and LAN2 is 192.168.2.108.

Procedure

- Step 1** Open the browser, enter the default IP address of the hybrid panel, and then press the Enter key.
- Step 2** Set **Language** , **Time Zone** and **System Time**, and then click **Next**.

Figure 6-1 Initialize



The screenshot shows the 'Time Zone Setting' step of the initialization process. At the top, there are three tabs: 'Language' (checked), 'Time Zone Setting' (active), and 'Password Setting'. The main content area contains the following settings:

- Date Format:** A dropdown menu showing 'DD-MM-YYYY'.
- Time Zone:** A dropdown menu showing '(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi'.
- System Time:** A checkbox is unchecked, followed by a text box showing '31/05/2021 18:55:30' and a 'Sync PC' button.

At the bottom, there are two buttons: 'Previous' and 'Next'.

- Step 3** Set the login password for the admin.

Figure 6-2 Set admin password

Language Time Zone Setting Password Setting

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

Previous Completed

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.

6.1.2 Logging in to Webpage

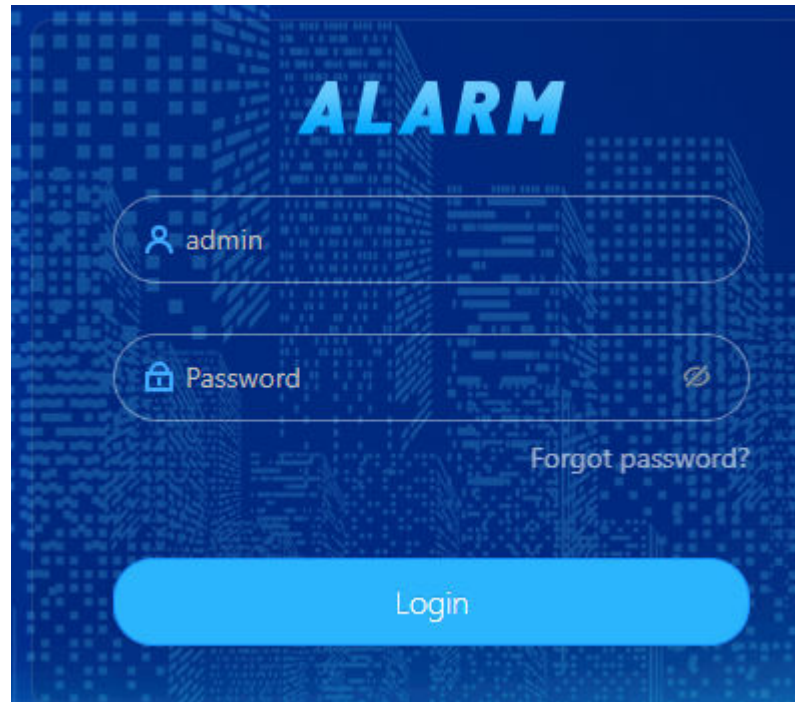
Make sure that the local computer and the hybrid panel are on the same network segment.

Procedure

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

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

Figure 6-3 Login



6.1.3 Resetting the Password

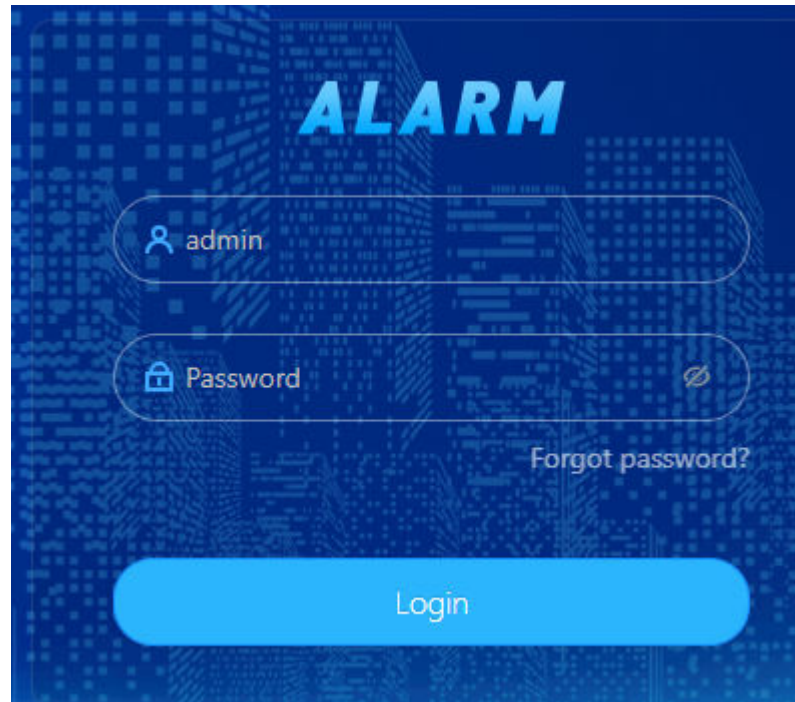
Prerequisites

- During device initialization, set a reserved email.
- Make sure that you have enabled the **Password Reset** function on the **Person Management** page.

Procedure

- Step 1 On the webpage, click **Forgot password?**.

Figure 6-4 Forgot password



Step 2 Click **OK**.

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.

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 6-5 Password reset

✓ Security Code

2 Password Reset

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.

OK

Step 6 Click **OK**.

6.2 Overview

Click **Overview** to go to the overview page.

Figure 6-6 Home page

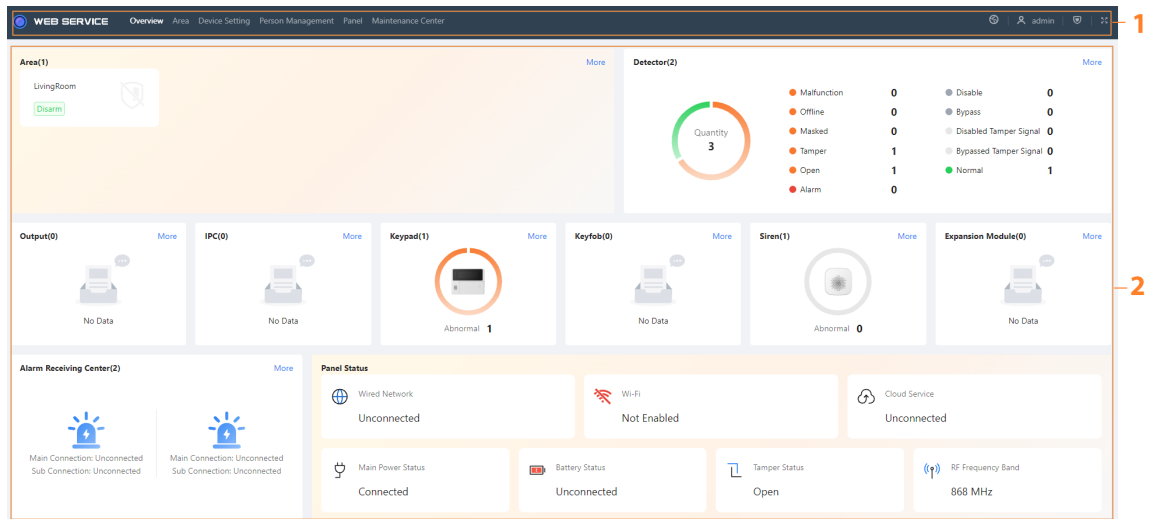


Table 6-1 Home page description

No.	Description
1	• : Select a language on the device. • : Log out or restart the device. • : Enter the Security page. • : Display in full screen.
2	Displays area, detector quantity and status, types of detectors, alarm receiving center, and panel status.

6.3 Adding Areas

Create areas, and set the area as public area according to your needs.

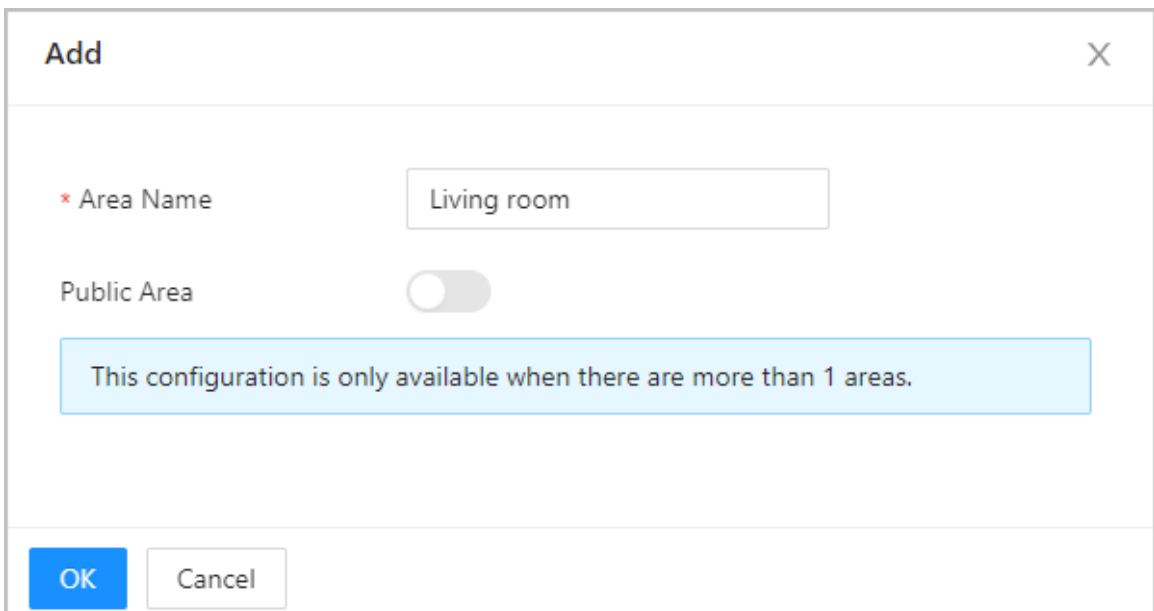
Background Information

A public area must have linked to at least 2 other areas. If all linked areas are armed, the public area will automatically arm itself. If any one of the linked areas is disarmed, the public area will automatically disarm itself.

Procedure

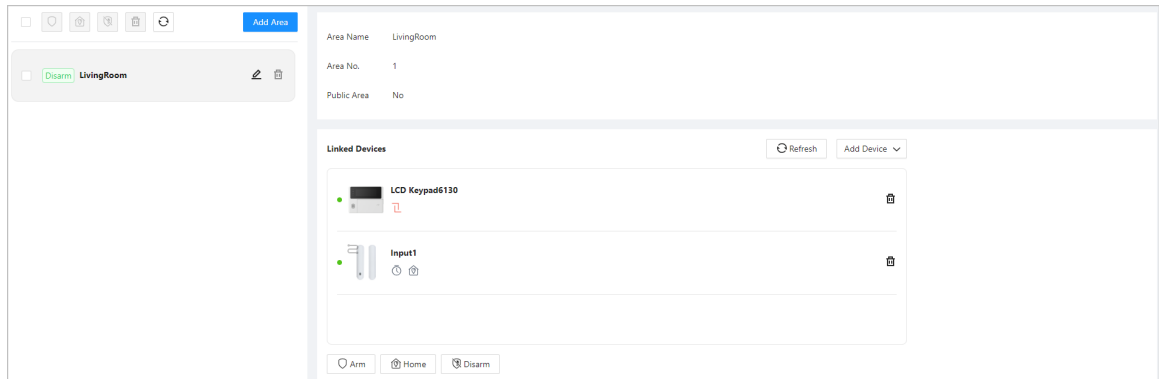
- Step 1** Log in to the webpage of the hybrid panel.
- Step 2** Select **Area**, and then click **Add**.
- Step 3** Configure area name, enable **Public Area** according to your needs, and then click **OK**.

Figure 6-7 Configure area name



- Step 4** Add devices for the area.
- Click **Add Device**, select the device type, and then add devices according to prompts.

Figure 6-8 Add devices



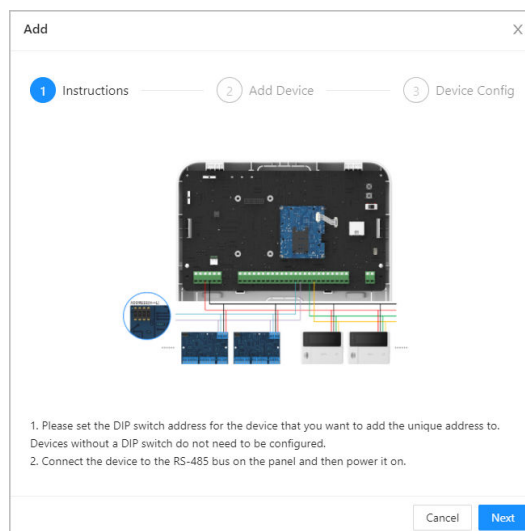
6.4 Device Setting

6.4.1 Adding Bus Devices

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Device Settings**.
- Step 3 Click **Add Device**, and then select **Bus Device**.

Figure 6-9 Add bus device



- Step 4 Click **Next**, select the device, and then click **Add**.
- Step 5 Configure the device name, assign the area for the device, and then click **OK**.

6.4.2 Adding Wired Devices

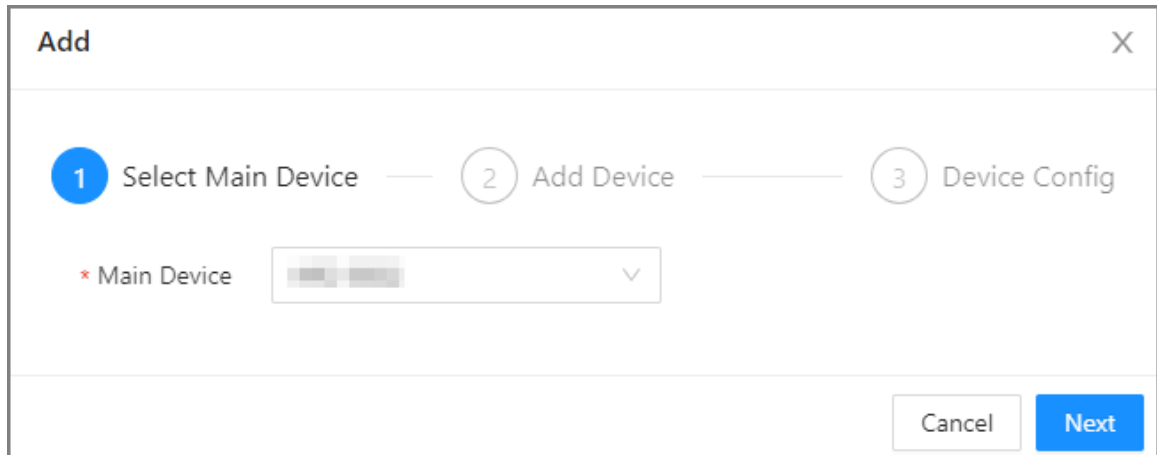
Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Device Settings**.

Step 3 Click **Add Device** , and then select **Wired Device**.

Step 4 Select the main device, and then click **Next**.

Figure 6-10 Select main device

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there is a progress bar with three steps: "1 Select Main Device" (highlighted with a blue circle), "2 Add Device" (in a grey circle), and "3 Device Config" (in a grey circle). Below the progress bar, there is a label "* Main Device" followed by a dropdown menu showing a blurred selection. At the bottom right of the dialog, there are two buttons: "Cancel" and "Next" (highlighted in blue).

Step 5 Select input or output channels, and then click **Add**.

Figure 6-11 Select input or output channels

Add
✕

✓ Select Main Device

2 Add Device

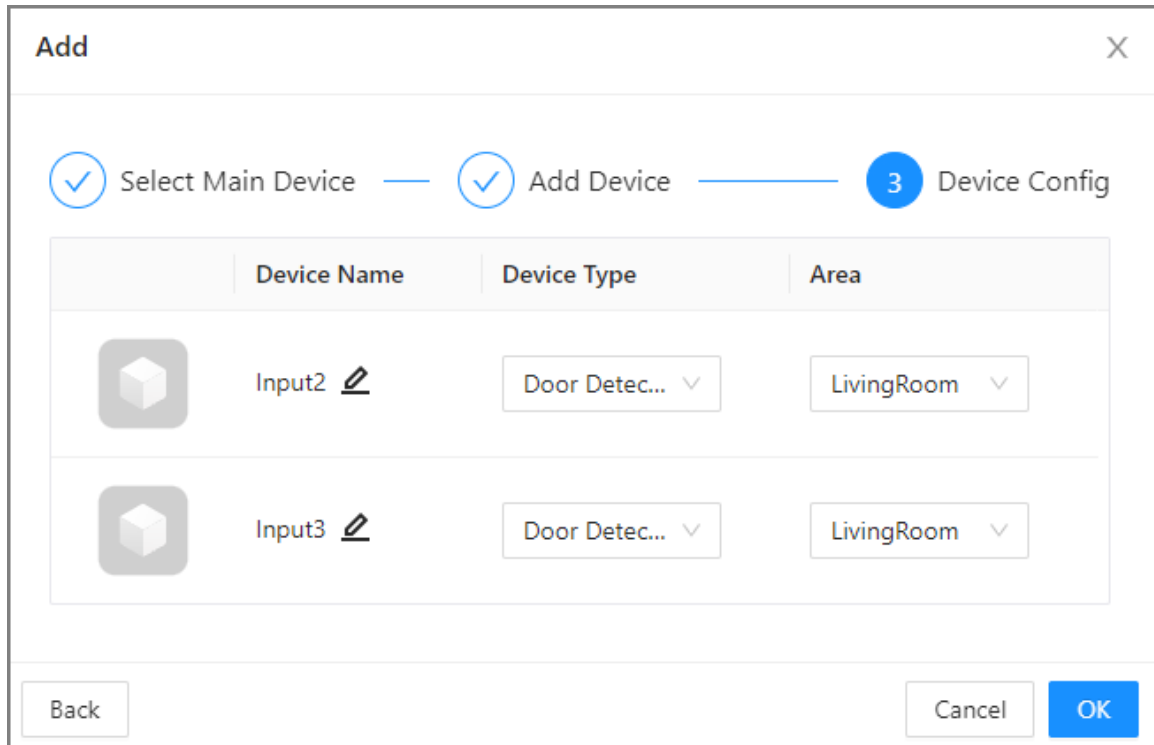
3 Device Config

☐		Device Name	Channel No.	Type
☒		Input2	2	Input
☒		Input3	3	Input
☐		Input4	4	Input
☐		Input5	5	Input
☐		Input6	6	Input
☐		Input7	7	Input

Back
Cancel
Add

Step 6 Configure the device name, select device type and assign area, and then click **OK**.

Figure 6-12 Configure device information



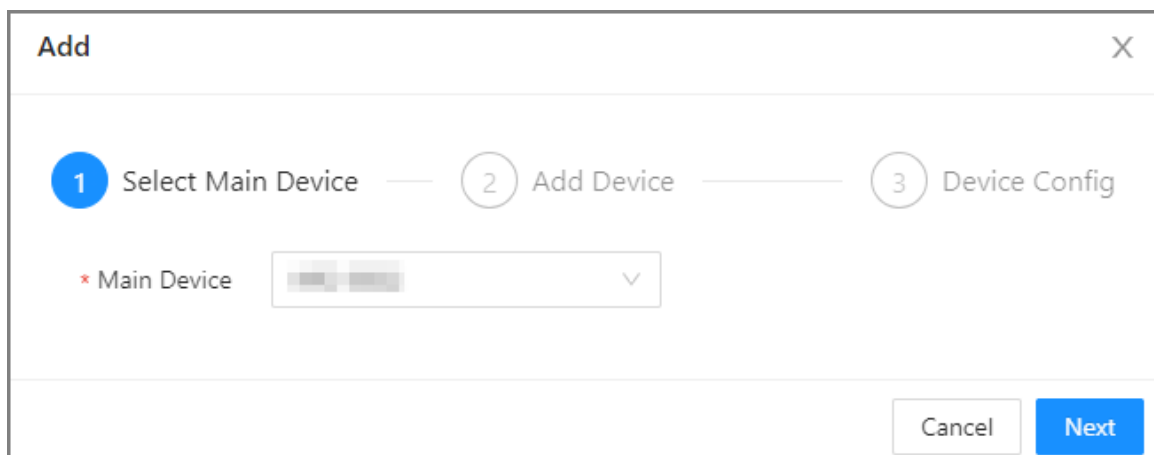
	Device Name	Device Type	Area
	Input2 	Door Detec... 	LivingRoom 
	Input3 	Door Detec... 	LivingRoom 

6.4.3 Adding Wireless Devices

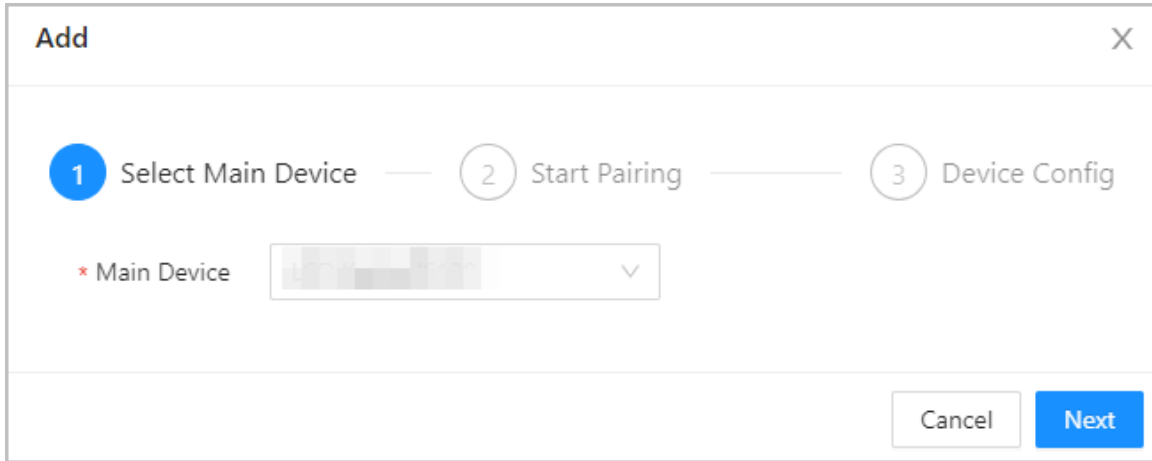
Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Device Settings**.
- Step 3 Select the main device (LCD keypad), and then click **Next**.

Figure 6-13 Select main device



* Main Device 

A screenshot of a software dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains a progress indicator with three steps: "1 Select Main Device" (highlighted with a blue circle), "2 Start Pairing" (in a grey circle), and "3 Device Config" (in a grey circle). Below the progress bar, there is a label "* Main Device" followed by a dropdown menu showing a blurred list of device names. At the bottom right, there are two buttons: "Cancel" and "Next".

Add

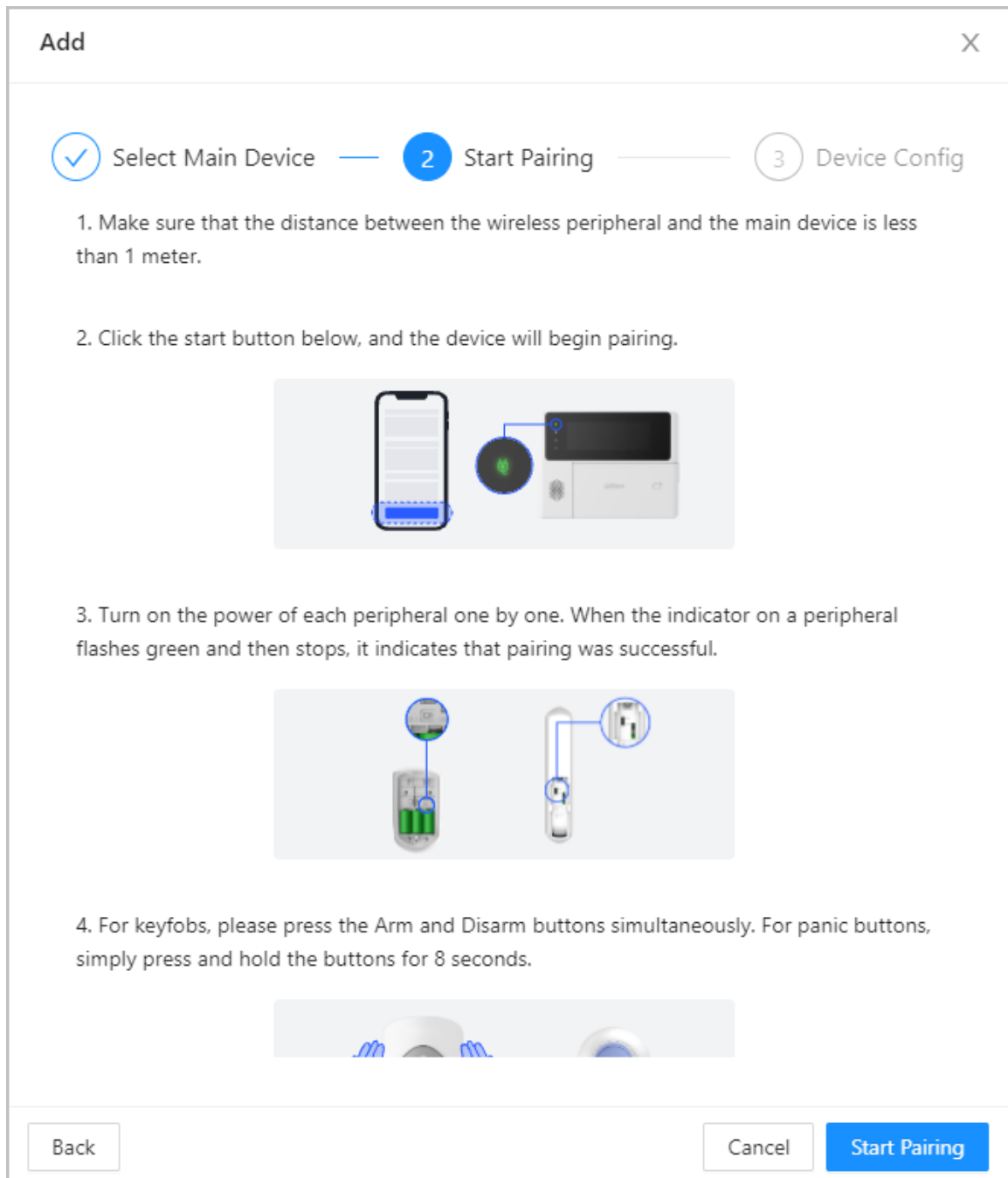
1 Select Main Device — 2 Start Pairing — 3 Device Config

* Main Device

Cancel Next

Step 4 Click **Start Pairing**.

Figure 6-14 Start pairing



Step 5 Configure the device name, select device type and assign area, and then click **OK**.

6.4.4 Adding IPC

Log in to the webpage of the panel, select **Device Settings**. Click **Add Device**, and then select **IPC**.

Adding by LAN Searching

1. The page displays the IPC devices that are on the same network segment with the panel, select the IPC, and then click +.

Figure 6-15 Add IPC (1)

Add
X

SN	IP Address	Port	Operation
A	172.24.2.100	37777	+
B	172.24.2.101	37777	+
C	172.24.2.102	37777	+
D	172.24.2.103	37777	+
E	172.24.2.104	37777	+

Manual Add
Cancel

2. Enter the user name, password used to log in to the webpage of the IPC, enter the name of the IPC, select the area, and then click **Next**.

Figure 6-16 Add IPC (2)

Add
X

1 IPC Info
2 Select Channel

* Username 123

* Password *****

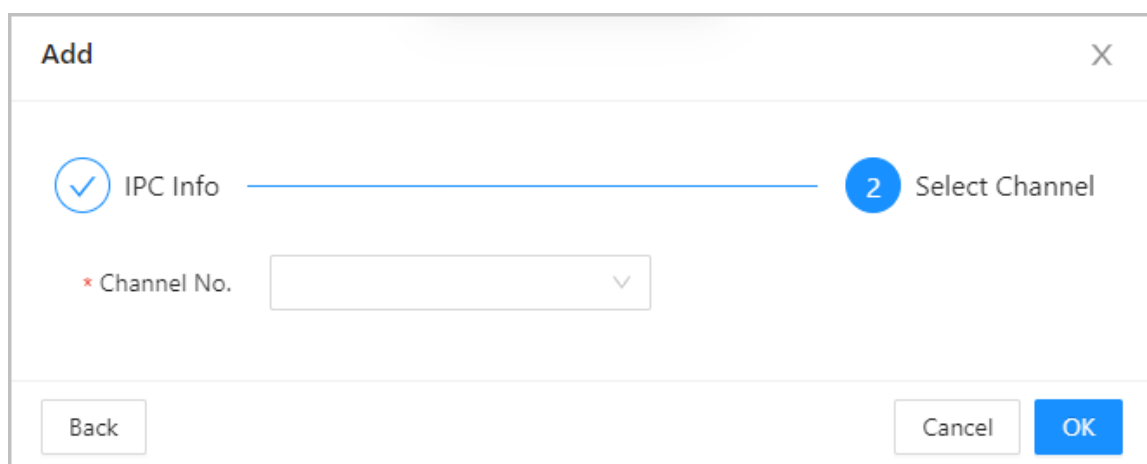
* Device Name

* Area LivingRoom

Cancel Next

3. Select the channel, and then click **OK**.

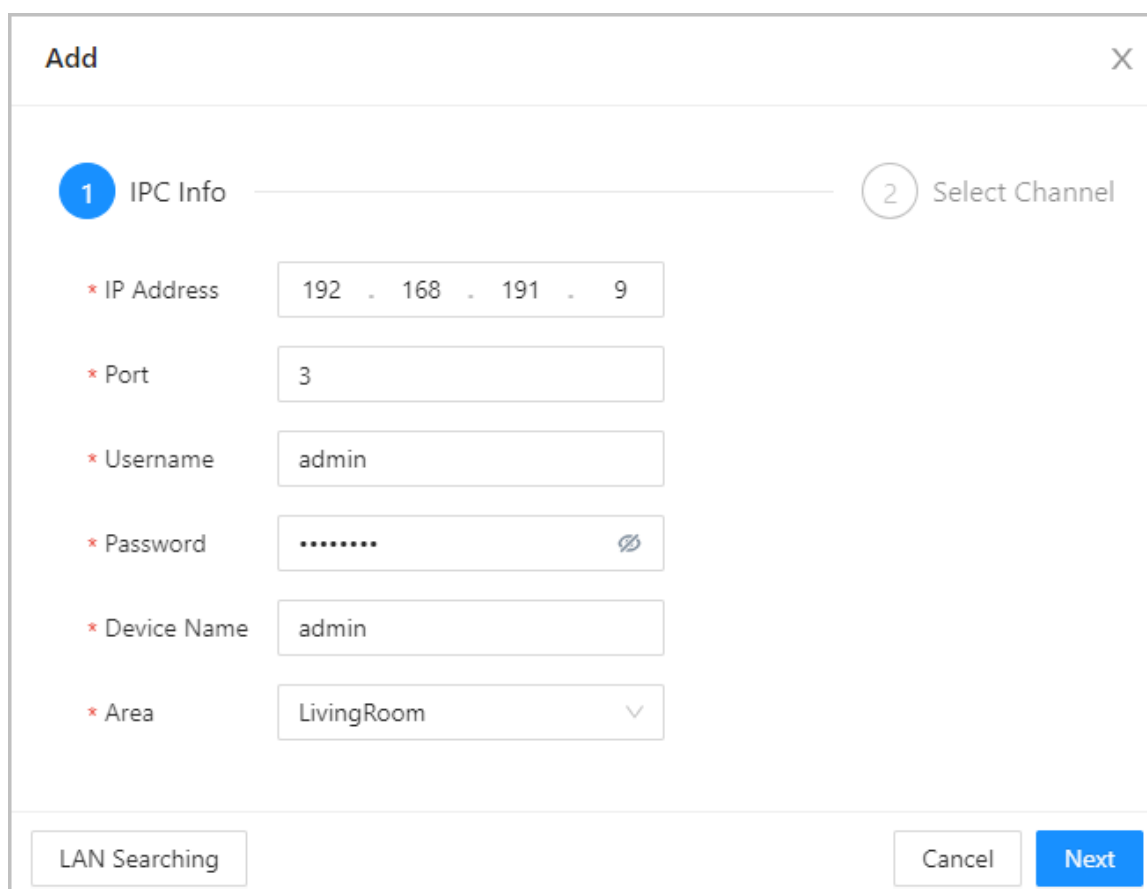
Figure 6-17 Add IPC (3)



Adding by Manually Entering Information

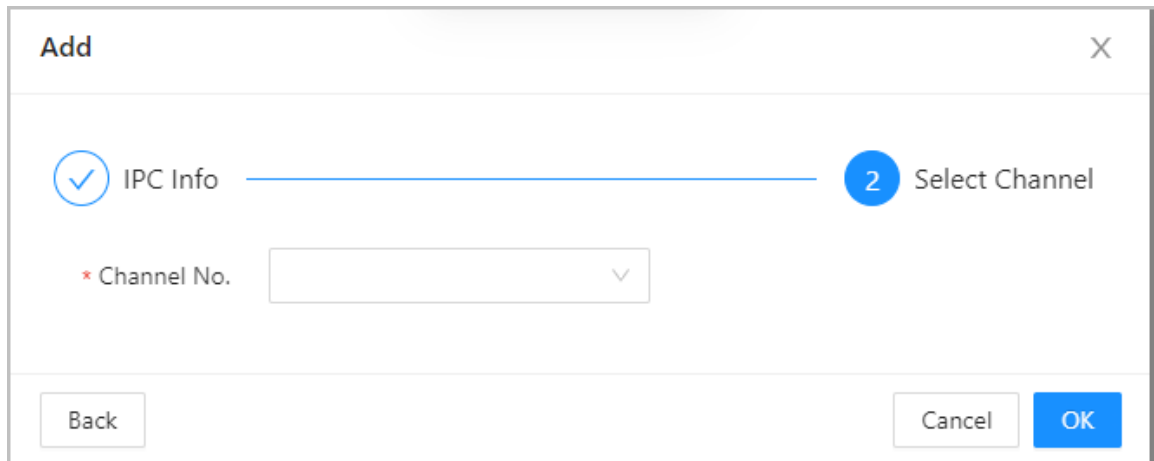
1. Click **Manual Add** on the device searching page.
2. Configure the IPC information, and then click **Next**.

Figure 6-18 Add IPC



3. Select the channel, and then click **OK**.

Figure 6-19 Add IPC (2)

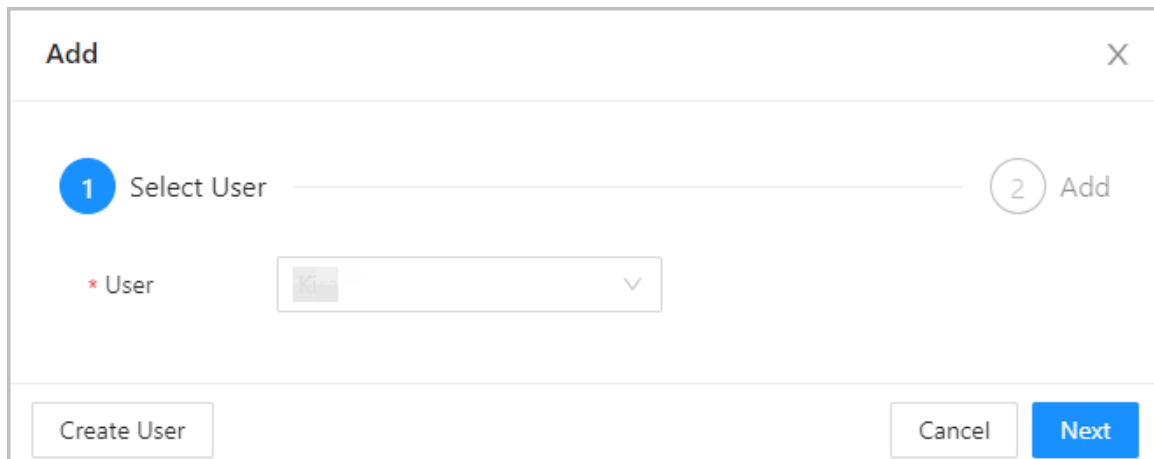


6.4.5 Adding Card

Procedure

- Step 1 Log in to the webpage of the panel, select **Device Settings**.
- Step 2 Click **Add Device**, and then select **IPC**.
- Step 3 Select the user, and then click **Next**.

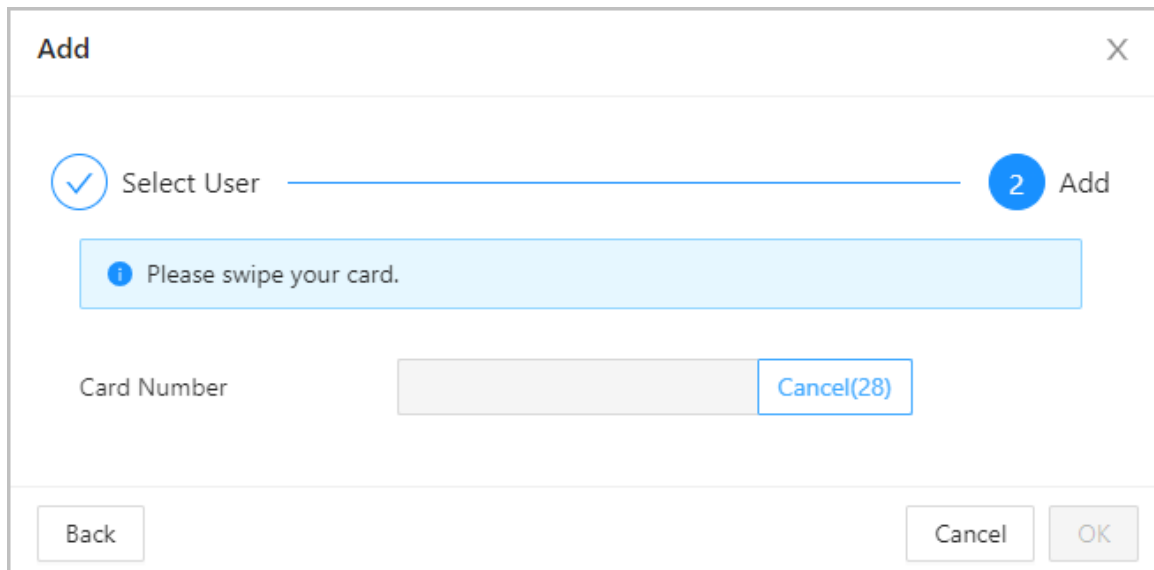
Figure 6-20 Select user



- Step 4 Press any button on the LCD keypad to wake it up, and then swipe the card over the card swiping area.

The card number will be filled in automatically, and then click **OK**.

Figure 6-21 Add card



6.5 Person Management

6.5.1 Adding Users

Background Information

There are 3 types of users: Administrator, installer and operator (keypad). The administrator and installer (the default password for the installer user is installer9090) are created by the panel by default, and operator can be added through webpage or app.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Person Management**, and then click **Add** to add new users.
- Step 3 Configure parameters.

Figure 6-22 Add users

Add
X

* Username

Jack

Operation Code

•••••

Duress Password

•••••

* Related Area

☐ All (Including All New Areas Added)

Select

☒ LivingRoom

Card

+ Add

* Permission

☒ Arm
☒ Disarm
☒ Output Control
☒ Bypass

OK

Cancel

Table 6-2 Parameter description of person

Parameter	Description
Username	The name of the keypad user.
Operation Code	When performing certain commands on the LCD keypad, the user must first enter the operation password before pressing the corresponding function key.

Parameter	Description
Duress Password	An alarm will be triggered when a duress password is used to unlock the keypad.
Related Area	Select the area that the person can have operation permission.  You need to create an area in Area .
Card	Click Add , and swipe your card on the keypad within the countdown to add the card.
Permission	Select the permission for the person to have on the webpage or app. • Arm/Disarm: Arm and disarm the area where the hybrid panel is linked to. • Output control: Controls the output of the keypad. • Bypass: When bypass is enabled, information will not be sent to the hybrid panel.

Step 4 Click **OK**.

6.5.2 Resetting the Password

Reset the password through the linked email when you forget your password.

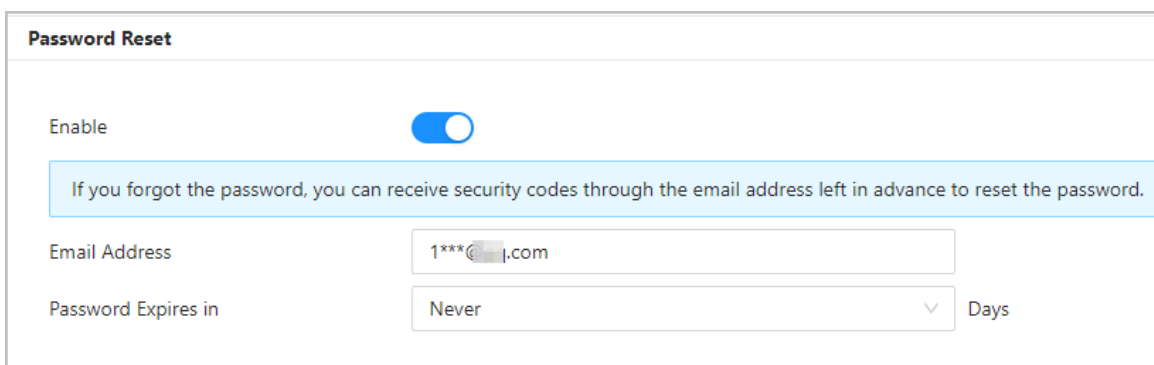
Procedure

Step 1 Select **Person Management** > **Password Reset**.

Step 2 Enter the email address, and set the password expiration time.

Step 3 Turn on the password reset function.

Figure 6-23 Reset Password




If you forgot the password, you can receive security codes through the linked email address to reset the password.

Step 4 Click **Apply**.

6.6 Panel

6.6.1 Basic Settings

6.6.1.1 Configuring Panel Name

Configure the panel name.

Procedure

- Step 1 On the home page, select **Panel** > **Basic Settings** > **Panel Name**.
Step 2 Configure the panel name, and then click **Apply**.

6.6.1.2 Configuring Time

Procedure

- Step 1 On the home page, select **Panel** > **Basic Settings** > **Time**.
Step 2 Configure the time of the panel.

Figure 6-24 Date settings

Time and Time Zone



Date :
2024-11-04 Monday
Time :
5:44:03 PM

Time
☒ Manually Set
☐ NTP

System Time

2024-11-04 5:44:03 PM

Sync PC

Time Format

YYYY-MM-DD

12-Hour

Time Zone

DST

Enable
☐

Type
☒ Date
☐ Week

Start Time

Jan

1

12:00 AM

End Time

Jan

2

12:00 AM

Apply

Refresh

Default

Table 6-3 Time settings description

Parameter	Description
Time	- Manual Set: Manually enter the time or you can click Sync Time to sync time with computer. - NTP: The Device will automatically sync the time with the NTP server. ◇ Server : Enter the domain of the NTP server. ◇ Port : Enter the port of the NTP server. ◇ Interval : Enter its time with the synchronization interval.
Time format	Select the time format.
Time Zone	Enter the time zone.
DST	(Optional) Enable DST. - Select Date or Week from the Type. - Configure the start time and end time of the DST.

Step 3 Click **Apply**.

6.6.2 System Settings

6.6.2.1 System Integrity Check

When enabled, the panel checks whether the current system is abnormal during arming. If it is abnormal, arming will be prevented.

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Panel** > **System Settings** > **System Integrity Check**.
- Step 3 Enable the functions according to your needs.

Figure 6-25 System integrity check

System Integrity Check
☒

Arm With Faults
☒

Fault Detection

Disabling any of these functions will cause the system to not comply with EN50131-1.

Main Power Failure
☒

Time to Accept Power Fail...
30min

Set the delay time for all the devices on the system to push notifications, when the main power supply is disconnected.

Panel Tamper Detection
☒

Connections to Cloud
☒

Wi-Fi Error
☒

RF Jamming
☒

ARC Connection Error
☒

Wired Network Error
☒

Cellular Network Error
☒

Apply
Refresh

Table 6-4 Description of parameters

Parameter	Description
System Integrity Check	When enabled, the panel checks whether the current system is abnormal during arming. If it is abnormal, arming will be prevented.
Arm With Faults	Allows the panel to arm even when faults are detected.
Main Power Failure	Reports alarm when detecting a main power disconnection.
Time to Accept Power Failure	Configure the delay time for all devices on the system to push notifications when the main power supply is disconnected. This allows a grace period before the system considers the power failure.
Panel Tamper Detection	Reports alarm when detecting the panel is detached from the location where it is installed.
Connections to Cloud	Reports alarm when detecting failure in communicating with cloud services.
Wi-Fi Error	Reports a fault message when detecting a Wi-Fi disconnection.
RF Jamming	Reports alarm when detecting radio frequency (RF) jamming, which is a type of interference that can disrupt wireless communication.
ARC Connection Error	Reports a fault message when detecting a disconnection with the alarm receiving center.
Wired Network Error	Reports a fault message when detecting a wired network disconnection.
Cellular Network Error	Reports a SIM card fault or mobile network fault if no SIM card is detected or the mobile network cannot connect.

Step 4 Click **Apply**.

6.6.2.2 Link Tamper to Siren

Procedure

Step 1 Log in to the webpage of the panel.

Step 2 Select **Panel** > **System Settings** > **Link Tamper to Siren**.

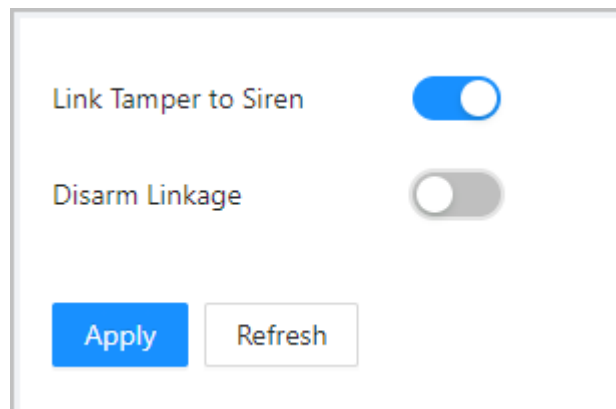
Step 3 Enable functions according to your needs.

- Link tamper to siren: When enabled and the system is armed, panel tampering triggers the siren alarm to deter intruders and alert users.
- Disarm linkage: The alarm linkage is enabled in disarming mode.



Enabling this function is not compliant with EN50131-1 standard.

Figure 6-26 Link tamper to siren



Step 4 Click **Apply**.

6.6.2.3 Peripheral Connection

Procedure

Step 1 Log in to the webpage of the panel.

Step 2 Select **Panel** > **System Settings** > **Peripheral Connection**.

Step 3 Enable functions according to your needs.

- Wireless peripheral heartbeat interval: The regular time interval at which wireless peripherals send heartbeat signals to the panel. It can verify that the peripheral is online and communicating properly.
- Packet loss count for reporting device offline: Defines how many consecutive heartbeat packets must be lost before the panel reports the peripheral as offline. It prevents false offline alarms due to temporary signal interference.

Figure 6-27 Heartbeat

Heartbeat

Wireless Peripheral Heart...

sec (12~300)

Packet Loss Count for Rep...

time(s) (3~60)

Apply

Refresh

Step 4 Click **Apply**.

6.6.2.4 Scheduled Arming and Disarming

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Panel** > **System Settings** > **Scheduled Arming/Disarming**.
- Step 3 Click **Add**, configure the parameters.

Figure 6-28 Configure parameters

Add
X

* Name

Jack

* Mode

Arm

* Related Area

☐ All (Including All New Areas Added)

Select

☒ LivingRoom

* Select time

Select time

* Repeat

☐ All
☒ Mon
☒ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat
☐ Sun

Forced Arming

☒

Forced arming does not comply with the EEN50131-1 standard.

Enable

☒

OK

Cancel

Table 6-5 Parameter description

Parameter	Description
Name	The name of the schedule. Custom.
Mode	Select from Arm , Home and Disarm .

Parameter	Description
Related Area	Select the area linked to the schedule.  Supports multiple selection of areas.
Select time	Select the time at which the schedules takes effect.
Repeat	Select the repeat weekdays for the schedule.
Forced Arming	When enabled, the system will force arm for the areas according to the schedule.
Enable	Enable the schedule.

Step 4 Click **Apply**.

6.6.3 Network Settings

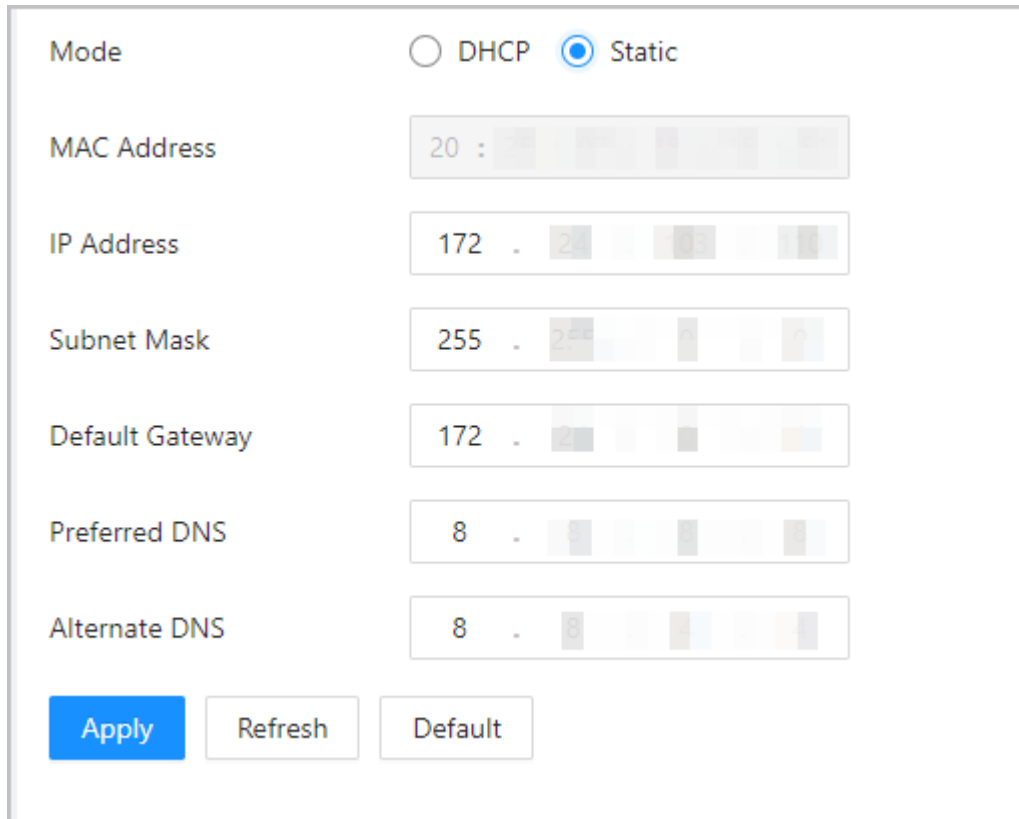
6.6.3.1 Configuring Wired Network

You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Panel** > **Network Settings** > **Wired Network**.
- Step 3 Configure the parameters.

Figure 6-29 IP



Mode: ☐ DHCP ☒ Static

MAC Address: 20 : [] [] [] [] [] []

IP Address: 172 . [24] [] [] [1] []

Subnet Mask: 255 . [255] [] [] [] []

Default Gateway: 172 . [24] [] [] [1] []

Preferred DNS: 8 . [8] [8] [8] [8] []

Alternate DNS: 8 . [8] [8] [8] [8] []

[Apply](#) [Refresh](#) [Default](#)

Table 6-6 Description of IP

Parameter	Description
Mode	- Static: Manually enter IP address, subnet mask, and gateway. - DHCP: It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Address	If you set the mode to Static , configure the IP address, subnet mask and gateway.
Subnet Mask	
Default Gateway	 - IPv6 address is represented in hexadecimal. - IPv6 version do not require setting subnet masks. - The IP address and default gateway must be in the same network segment.
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.

Step 4 Click **Apply**.

6.6.3.2 Configuring Wi-Fi

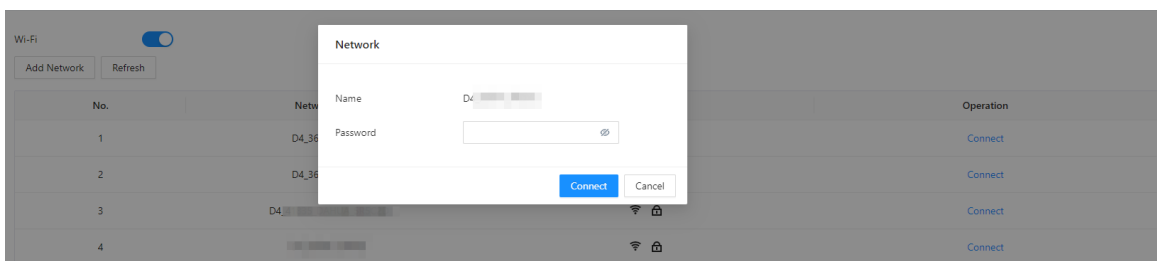


Wi-Fi function is only available on select models.

Procedure

- Step 1** Select **Panel** > **Network Settings** > **Wi-Fi**.
- Step 2** Turn on **Wi-Fi**.
All available Wi-Fi are displayed.
- Step 3** Click **Connect**, and then enter the password of the Wi-Fi.
The Wi-Fi is connected.

Figure 6-30 Wi-Fi



Related Operations

If the Wi-Fi you want to connect is not displayed in the list, you can manually add and connect to it.

1. Click **Add Network**, enter the name of the Wi-Fi, and select the security mode.
If you select **No** for **Security**, you do not need to enter the password. Otherwise, you need to enter the password of this Wi-Fi.
2. Click **Connect**.

Figure 6-31 Add Wi-Fi

Other Networks

Network

Wi-Fi

Security

On

Password

.....

Connect

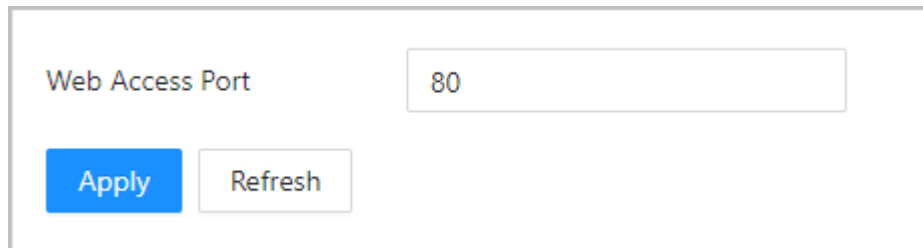
Cancel

6.6.3.3 Configuring HTTP

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Panel** > **Network Settings** > **HTTP**.
- Step 3 Enter the port to access the webpage.

Figure 6-32 HTTP



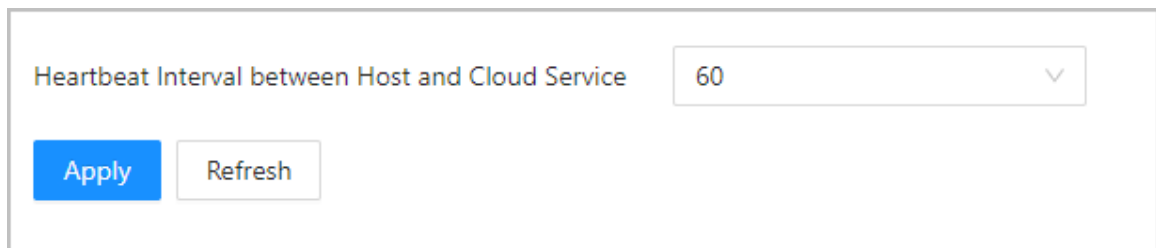
- Step 4 Click **Apply**.

6.6.3.4 Configuring Cloud Service

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Panel** > **Network Settings** > **Cloud Service**.
- Step 3 Configure the heartbeat interval.

Figure 6-33 Cloud service



- Step 4 Click **Apply**.

6.6.4 Alarm Receiving Center

Establish connection between the panel and alarm receiving center, and the event messages can be reported to the alarm receiving center.

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Panel** > **Alarm Receiving Center**.
- Step 3 Configure parameters for ARC1 and ARC2.

Figure 6-34 Configure parameters

ARC 1

ARC 2

Enable

☐

Connection Mode

☒ IP
 ☐ PSTN

Protocol

SIA-DC09(SIA-CID)

Central Account

Length 3-16 characters (numbers and letters A-F)

IP Protocol

TCP

IP or Domain Name

Port

0

Heartbeat Interval

60

sec (0~86400)

Retransmission Times

3

time(s) (1~15)

Reupload Interval

10

sec (5~60)

Encryption

None

Communication Test

Test

Scheduled Test

☒

Frequency for Sending Test...

24h

Backup Config

☐

Connection Mode

☒ IP
 ☐ PSTN

Protocol

SIA-DC09(SIA-CID)

Central Account

Length 3-16 characters (numbers and letters A-F)

IP Protocol

TCP

IP or Domain Name

Verify Video

☐

Upload Events

☒ Alarm
 ☒ Error
 ☒ Operation
 ☒ Arming and Disarming

Table 6-7 Description of alarm receiving center parameter

Parameter		Description
Enable		Enable the alarm receiving center function.
Connection Mode (IP)	Protocol	Select from SIA-DC09 (SIA-CID) , SIA-DC09(SIA-DCS) , Softgard , Converter .
	Central Account	Enter the account number that created by the alarm receiving center , which is to be used to identify the panel when the panel sends information to the alarm receiving center .
	IP Protocol	It is TCP by default.
	IP or Domain Name/Port	The IP/domain name and port of the alarm receiving center.

Parameter		Description
	Heartbeat Interval	The heartbeat interval between the panel and the alarm receiving center.  0 seconds means Heartbeat interval is disabled.
	Retransmission Times	Configure the number of retransmission for failed event uploads (when the alarm receiving center is online).
	Reupload Interval	Configure the interval of retransmission for failed event reuploads (when the alarm receiving center is online).
	Encryption	The panel uses an encryption format for information security when you configure the ARC. None is set by default.
	Communication Test	Click Test to test the connection status with the alarm receiving center.
	Scheduled Test/ Frequency for Sending Test	When enabled, the panel reports periodic test event regularly. You can configure the frequency for sending test. The default period is 24 hours.
Connection Mode (PSTN)	Protocol	Select from ContactID and Phone .  In Phone mode, calls will only be made when an alarm is triggered.
	ARC Name	The name of the alarm receiving center, which is used for keeping logs and subsequent message push.
	Central Account	Enter the account number that created by the alarm receiving center , which is to be used to identify the panel when the panel sends information to the alarm receiving center .
	ARC Phone No.	Configure the phone number of the alarm controller in the alarm receiving center.
	Dialing Delay	The time of dialing delay.
	Redials	The time of redials.
	Transmission Mode	Select from DTMF Slow Dial and DTMF Fast Dial .
	Communication Test	Click Test to test the connection status with the alarm receiving center.
	Scheduled Test/ Frequency for Sending Test	When enabled, the panel reports periodic test event regularly. You can configure the frequency for sending test. The default period is 24 hours.
Backup Config		Enable Backup Config , and repeat the above configuration items after they take effect.
Verify Video		When enabled, the panel reports the URL of images or videos to the alarm receiving center.

Parameter	Description
Upload Events	Select the events according to your needs.

Step 4 Click **Apply**.

6.6.5 Intercom Service

Configure intercom service.

Procedure

Step 1 Log in to the webpage of the panel.

Step 2 Select **Panel** > **Intercom Service**.

Step 3 Enable **Panel Intercom Service**, select the intercom method, and then configure parameters for intercom service.

When intercom service is enabled, it means the panel starts to provide intercom service. You can need to select the intercom target from App or the alarm receiving center. At least one must be selected, and you can also select both. The default method is app.

Figure 6-35 Configure intercom parameters

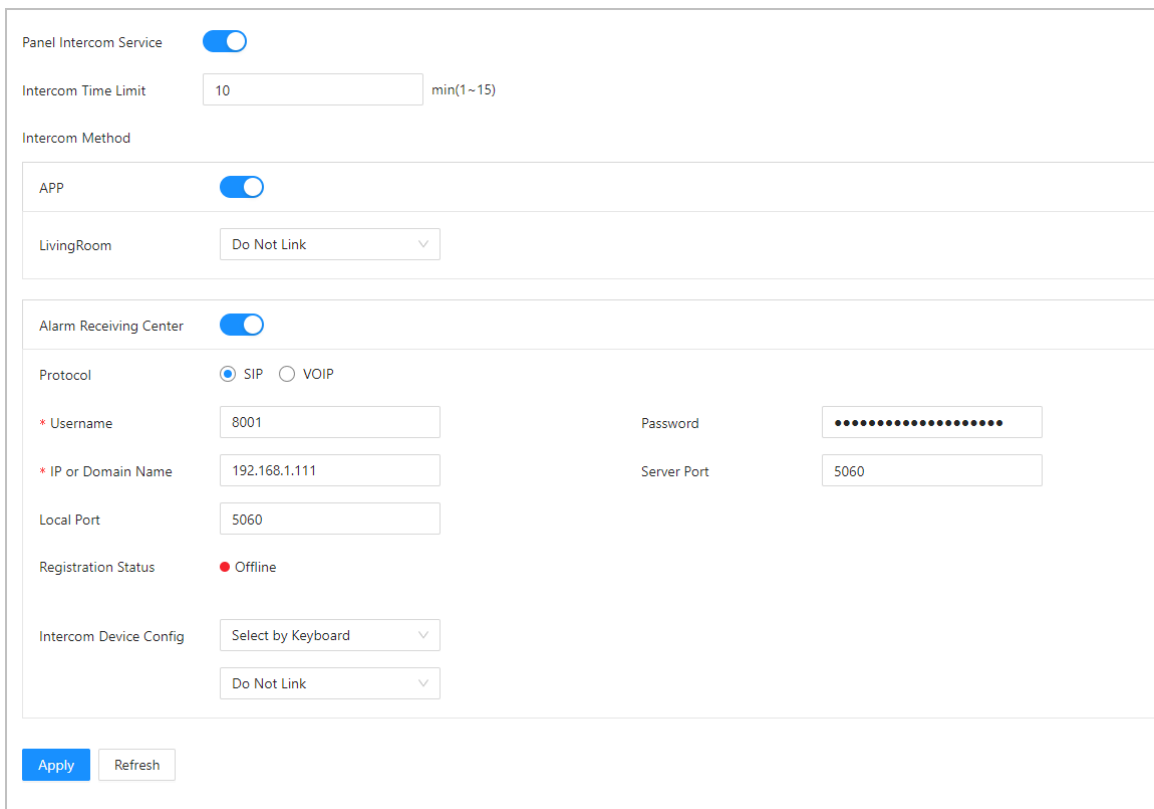


Table 6-8 Parameter description of intercom service

Module	Parameter	Description
Panel Intercom Service	Intercom Time Limit	The time limit for intercom between the panel and DMSS app. 
		The intercom time limit starts counting from the moment the alarm is triggered, and once the limit time is exceeded, the intercom cannot be initiated for that particular alarm.
Intercom Method (App)	Living Room	Select whether to link to the area or not.
Intercom Method (Alarm Receiving Center)	Protocol (SIP)	● Username/Password: Enter the user name and password to log in to the SIP server. ● IP or Domain Name: Enter the IP or domain name of the SIP server. ● Server Port: Enter the port of the SIP server. ● Local Port: Enter the local port. ● Registration Status: The system synchronizes whether the registration is online or offline. ● Intercom Device Config: ◇ Select by keyboard: Only one device with intercom function under the panel can be selected for intercom. ◇ Select by room: For each room, only one LCD keypad with intercom function added under the panel can be selected.
	Protocol (VOIP)	● Device ID: Enter the device ID: ● Username/Password: Enter the user name and password to log in to the server. ● IP or Domain Name: Enter the IP or domain name of the server. ● Server Port: Enter the port of the server. ● Local Port: Enter the local port. ● Wait Time for Answer: The required time for the alarm receiving center to build connection. ● Intercom Device Config ◇ Select by keyboard: Only one device with intercom function under the panel can be selected for intercom. ◇ Select by room: For each room, only one LCD keypad with intercom function added under the panel can be selected.

Step 4 Click **Apply**.

6.7 Maintenance Center

6.7.1 Installation and Maintenance Mode

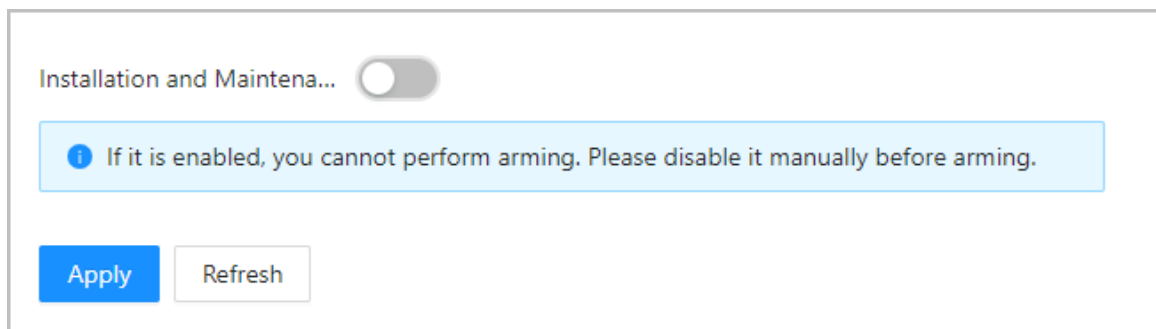
Background Information

- Enable installation and maintenance mode. During maintenance, the device will not report tamper, alarm, or fault messages, nor will it trigger sirens, SMS, phone calls, or SIA reporting.
- Installation and maintenance mode can only be enabled when all rooms are disarmed. After enabling, the panel's power indicator will flash green slowly to indicate it is in installation and maintenance mode. You must manually exit this mode.
- Arming cannot be successfully performed in installation and maintenance mode.

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Maintenance Center** > **Installation and Maintenance Mode**.
- Step 3 Enable **Installation and Maintenance Mode** based on your need.

Figure 6-36 Installation and maintenance mode



- Step 4 Click **Apply**.

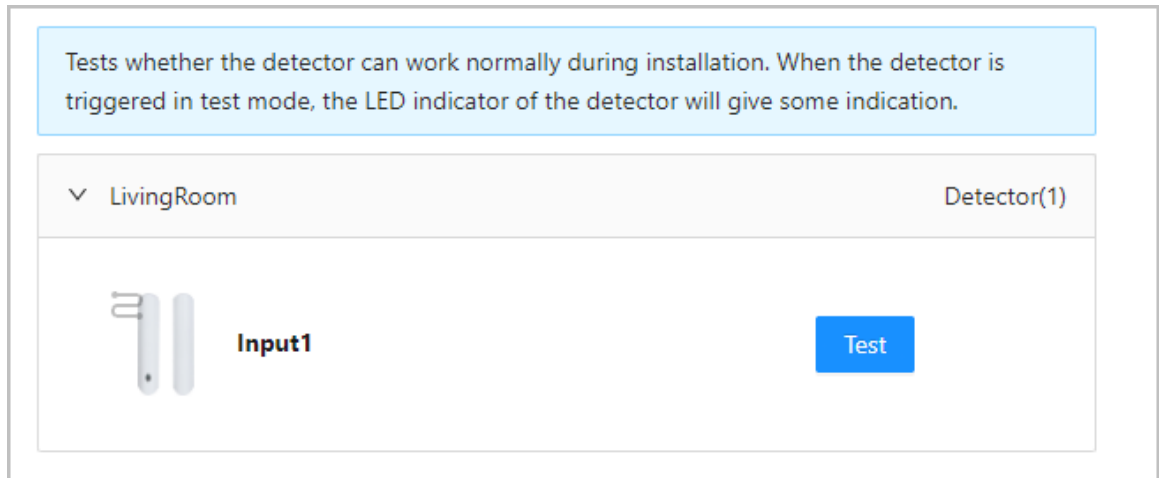
6.7.2 Detector Test

Test whether the detector can work normally during installation.

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Maintenance Center** > **Detector Test**.
- Step 3 Click **Test**.

Figure 6-37 Detector test



6.7.3 One-click Diagnosis

The system automatically diagnoses the configurations and the status of the device to improve its performance.

Procedure

Step 1 On the home page, select **Maintenance Center** > **One-click Diagnosis**.

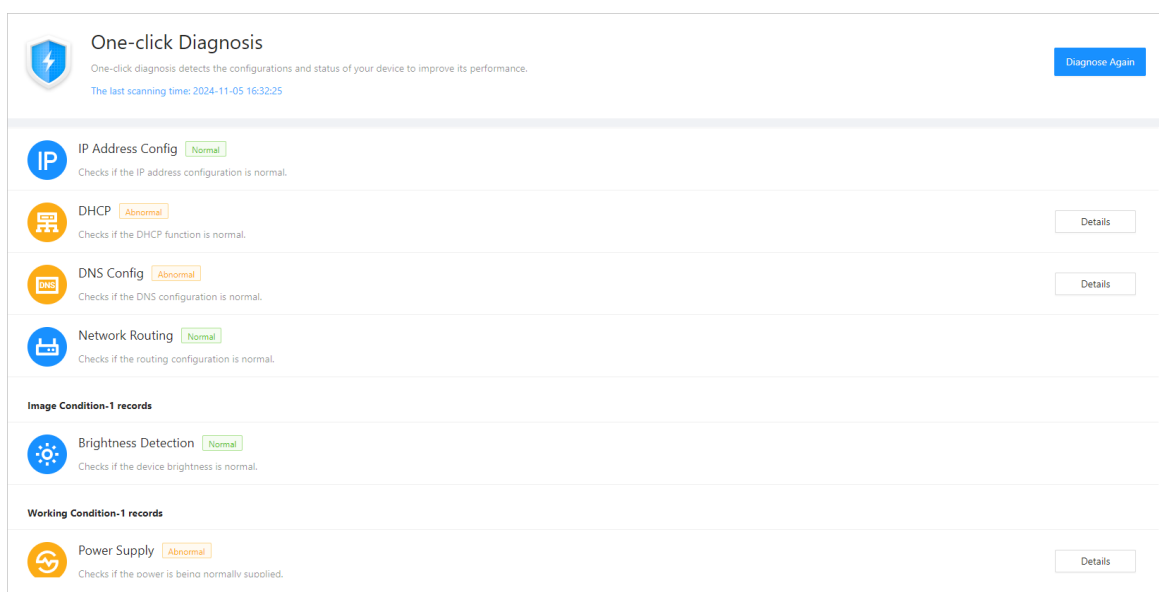
Step 2 Click **Diagnose**.

The system automatically diagnoses the configurations and the status of the device and display diagnosis results after it completes.

Step 3 (Optional) Click **Details** to view details of abnormal items.

You can ignore the abnormality or optimize it. You can also click **Diagnose Again** to perform automatic diagnosis again.

Figure 6-38 One-click diagnosis



6.7.4 System Information

6.7.4.1 Viewing Version Information

On the webpage, select **Maintenance Center** > **System Info** > **Version**, and you can view version information of the Device.

6.7.4.2 Viewing Legal Information

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

6.7.5 Viewing Logs

View logs such as system logs, admin logs, and unlock records.

6.7.5.1 System Logs

Search for and view system logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center** > **Log** > **Log**.
- Step 3 Select the time range and the log type, and then click **Search**.

Related Operations

- click **Export** to export the searched logs to your local computer.
- Click **Encrypt Log Backup**, and then enter a password. The exported file can be opened only after entering the password.
- Click  to view details of a log.

6.7.5.2 Remote Logs

Build connection with the server for transmission of remote logs.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Center** > **Log** > **Remote Log**.
- Step 3 Configure parameters.

Figure 6-39 Remote log

Enable
☐

IP Address

192 . 168 . 0 . 108

Port

514

(1-65534)

Device No.

22

(0-23)

Enable TLS
☐

i RTSP stream is encrypted by using TLS tunnel before transmission.

Apply

Refresh

Default

Table 6-9 Description of remote logs

Parameter	Description
Enable	When enabled, the panel will send log data to the server remotely.
IP Address	The IP address of the server where the log data will be sent.
Port	The port number of the server that will receive the log data.
Device No.	A unique identifier for the device. This number helps differentiate multiple devices when logs are received by the server.
Enable TLS	When enabled, the log data is encrypted using a TLS tunnel before being sent to ensure communication.

Step 4 Click **Apply**.

6.7.5.3 Log Scrapping

Configure log scrapping.

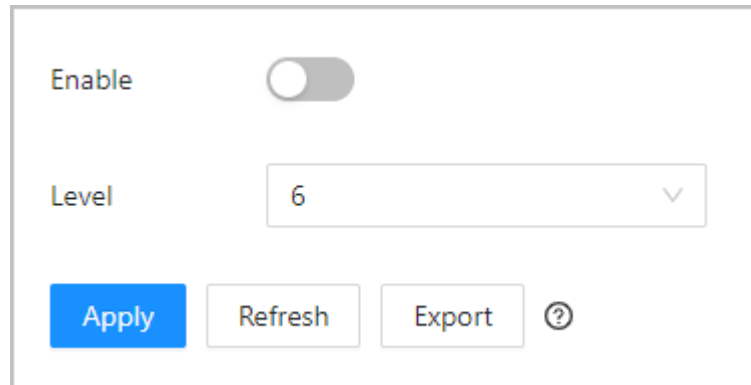
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center > Log > Log Scrapping**.

Step 3 Enable the function, configure the level, and then click **Apply**.

Figure 6-40 Log scrapping



The interface for log scrapping configuration. It includes an 'Enable' toggle switch currently turned off, a 'Level' dropdown menu set to '6', and three buttons: 'Apply' (blue), 'Refresh', and 'Export'. A help icon (?) is located next to the 'Export' button.

6.7.6 Maintenance Management

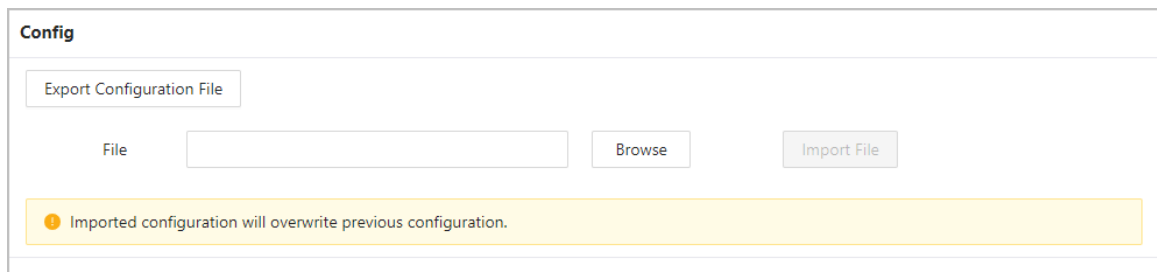
6.7.6.1 Configuration Management

You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Management** > **Config**.

Figure 6-41 Configuration management



The 'Config' interface for configuration management. It features a tab labeled 'Export Configuration File'. Below this, there is a 'File' input field, a 'Browse' button, and an 'Import File' button. A yellow warning box at the bottom states: 'Imported configuration will overwrite previous configuration.'

- Step 3 Export or import configuration files.

- Export the configuration file.
Click **Export Configuration File** to download the file to the local computer.



The IP will not be exported.

- Import the configuration file.
 - Click **Browse** to select the configuration file.
 - Click **Import configuration**.



Configuration files can only be imported to devices that have the same model.

6.7.6.2 Maintenance

Regularly restart the Device during its idle time to improve its performance.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Maintenance Management** > **Maintenance**.
- Step 3 Set the time, and then click **Apply**.

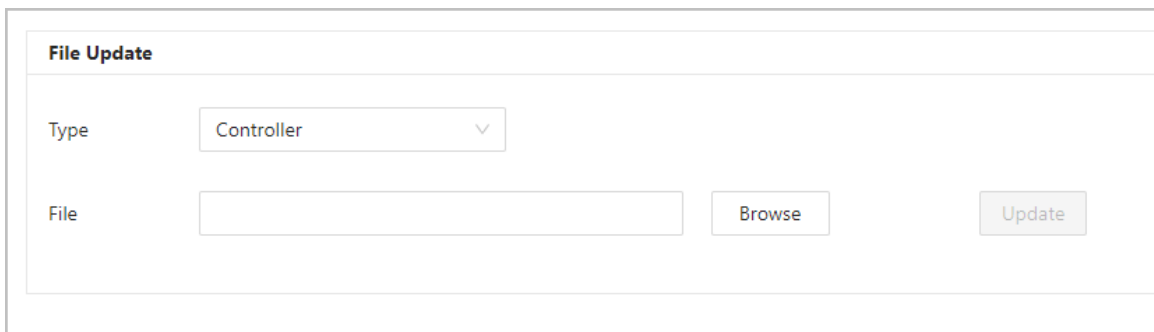
The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

6.7.7 Updating

Procedure

- Step 1 Log in to the webpage of the panel.
- Step 2 Select **Maintenance Center** > **Update**.
- Step 3 Select the type the device.

Figure 6-42 Select type



- Step 4 In **File Update**, click **Browse**, and then upload the update file.



The update file should be a .bin file.

- Step 5 Click **Update**.

The Device will restart after the update finishes.

6.7.8 Advanced Maintenance

Acquire device information and capture packet to make easier for maintenance personnel to perform troubleshooting.

6.7.8.1 Exporting

Procedure

- Step 1 On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Export**.
- Step 2 Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

6.7.8.2 Packet Capture

Packet Capture

1. On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 6-43 Packet capture

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	192.168.1.166	Optional	Optional	Optional	Optional	0.00MB	▶
eth2	192.168.1.101	Optional	Optional	Optional	Optional	0.00MB	▶

2. Enter the IP address, click .
- ▶ changes to .
3. After you acquired enough data, click .

Captured packets are automatically downloaded to your local computer.

Network Test

1. On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.
2. In the **Network Test** area, enter the destination address, and then configure data packet size.

Figure 6-44 Network test

Network Test

Destination Address

Data Packet Size
Byte (64-4096)

Test Result

3. Click **Test**.

The result is displayed in the **Test Result** area. You can copy the result.

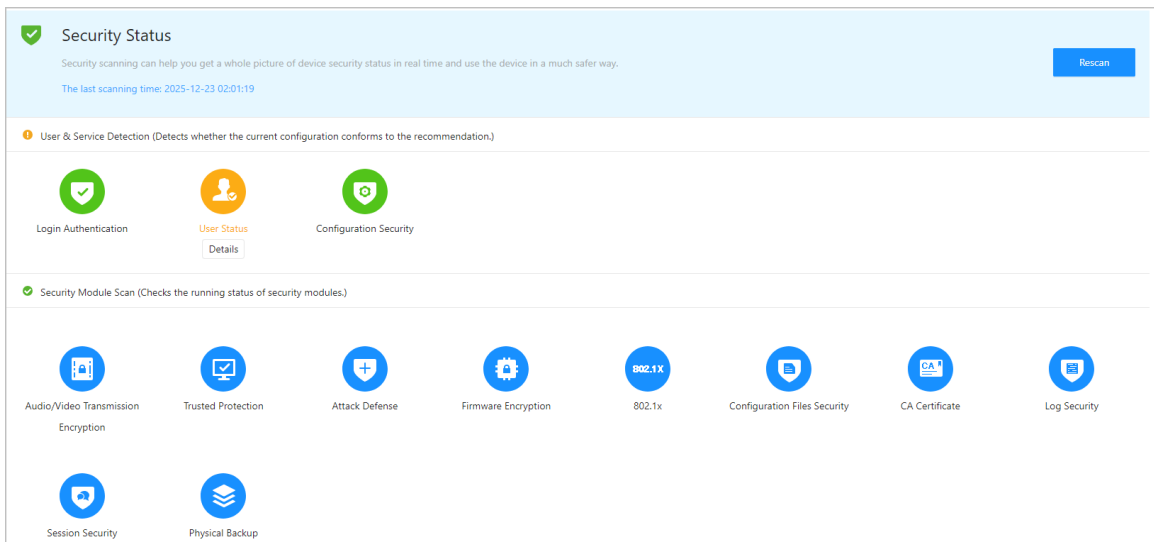
6.8 Security

View device security status and set security functions.

6.8.1 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 6-45 Security status



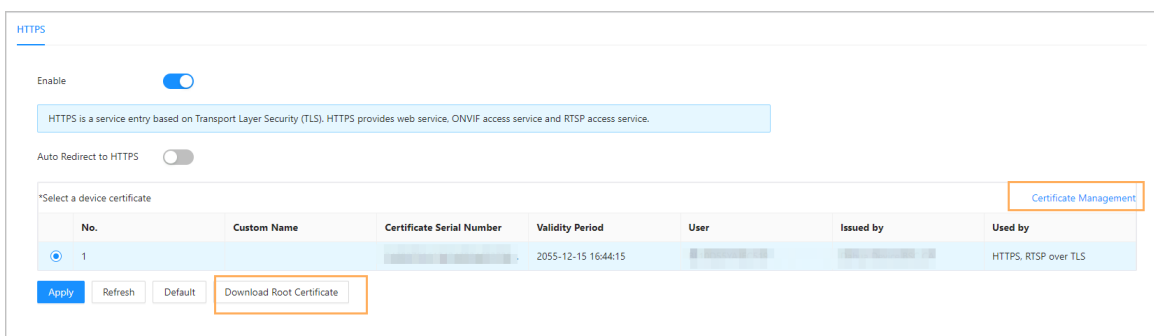
6.8.2 Configuring System Service

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**.

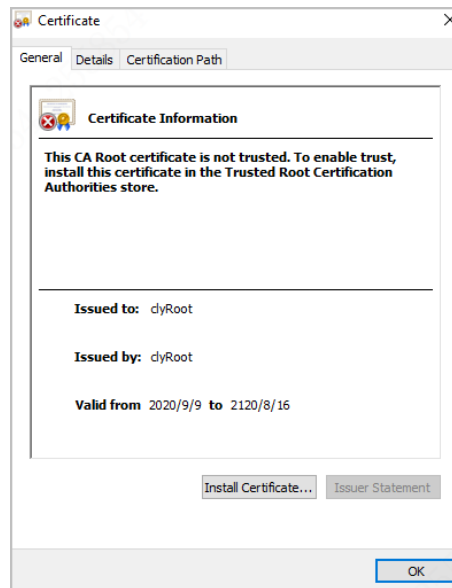
Figure 6-46 System service



Step 2 Download and install the root certificate.

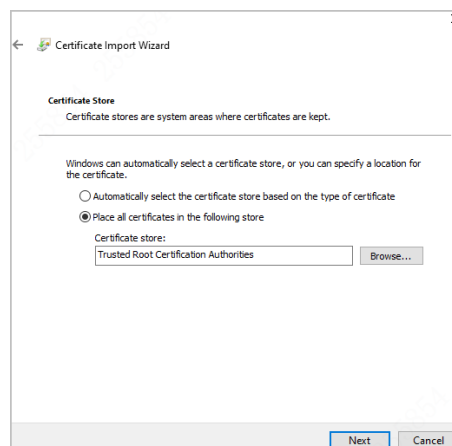
1. Click **Download Root Certificate** and save the root certificate by following the instructions on the page.
2. Double-click the downloaded **RootCert.cer** file to open the certificate.
3. Click **Install Certificate**.

Figure 6-47 Certificate



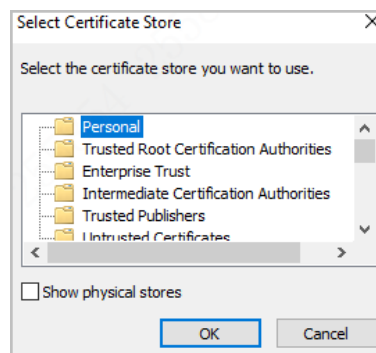
4. Click **Next** on the prompted window.
5. Select **Place all certificates in the following store**, and then click **Browse**.

Figure 6-48 Certificate storage location



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

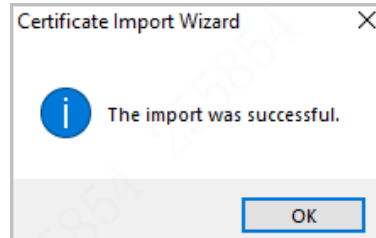
Figure 6-49 Select certificate store



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 6-50 Certificate imported successfully



Related Operations

Click **Certificate Management** to go to **CA Certificate** page.

6.8.3 Setting Attack Defense

6.8.3.1 Configuring Firewall

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

Procedure

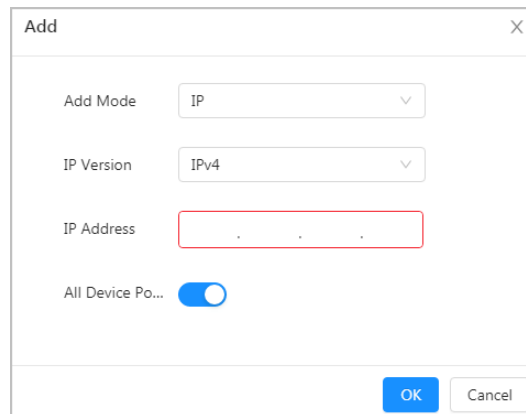
- Step 1 Log in to the webpage, and then select **Security** > **Attack Defense** > **Firewall**.
- Step 2 Enable the allow list or block list.
- Step 3 Set **Allow List** or **Block List** as the **Mode**.
- Step 4 Click **Add**.

- **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 6-51 Add allow list or block list



Step 5 Configure the parameters.

Table 6-10 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**.

6.8.3.2 Account Lockout

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

Procedure

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

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

Figure 6-52 Account lockout configuration

Step 3 Click **Apply**.

6.8.3.3 Setting Anti-DoS Attack

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

Procedure

- Step 1** Log in to the webpage, 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 6-53 Anti-DoS attack

Step 3 Click **Apply**.

6.8.4 Data Encryption

Background Information



You are recommended to enable **Data Encryption** function. There might be safety risk if this function is disabled.

Procedure

Step 1 Select **Security** > **Data Encryption**.

Step 2 Configure the parameters.

Figure 6-54 Data encryption

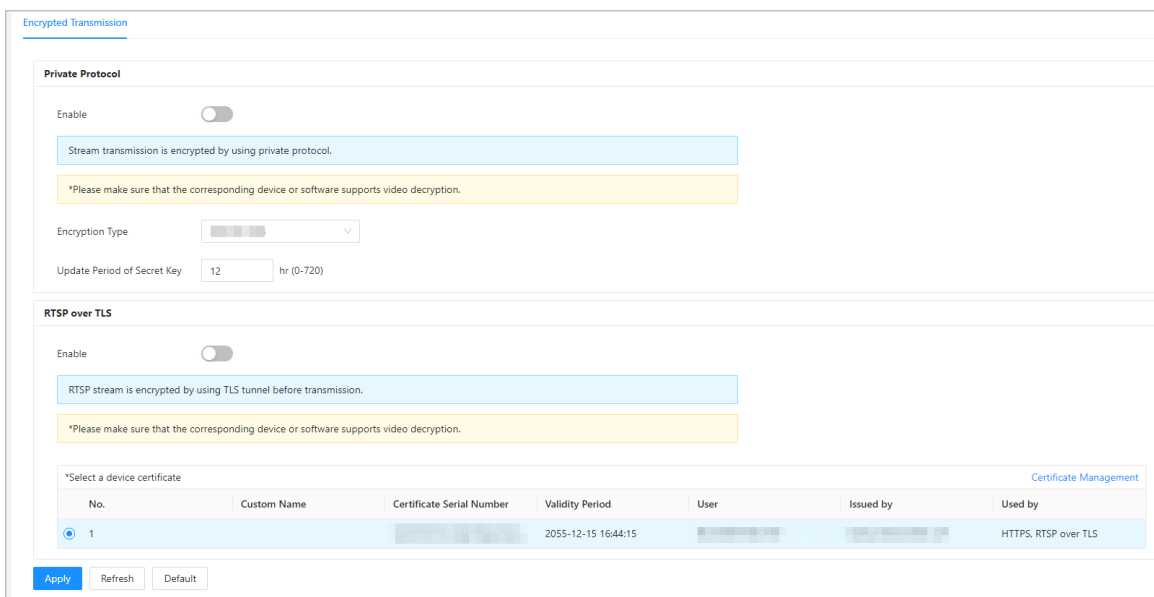


Table 6-11 Description of data encryption parameters

Area	Parameter	Description
Private Protocol	Enable	Enables encryption by using private protocol.  There might be safety risk if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.

Area	Parameter	Description
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS.  There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	View details about certificate management.

Step 3 Click **Apply**.

6.8.5 Security Warning

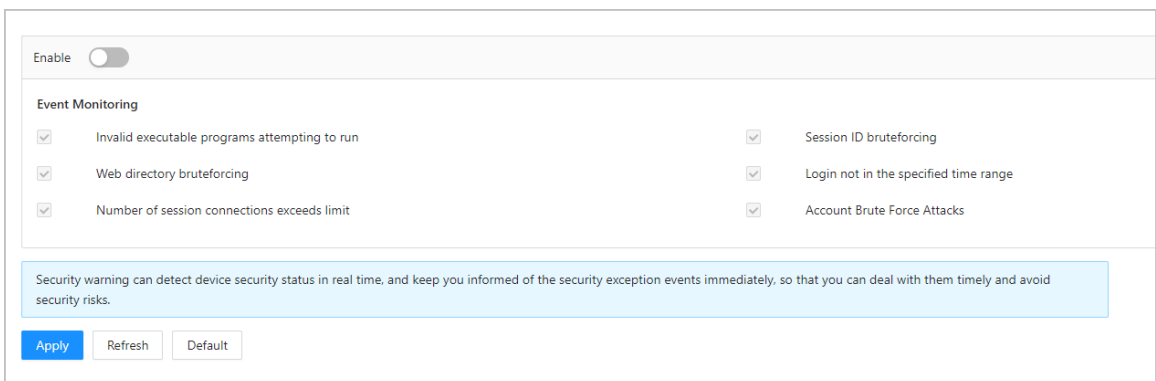
Security warning can detect device status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

Procedure

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

Step 2 Click **Enable**.

Figure 6-55 Security warning



Step 3 Click **Apply**.

Appendix 1 Arming Failure Events and Description

Appendix Table 1-1 Arming failure events and description (peripherals)

No.	Reason	Description
1	Module Loss	The peripheral was offline.
2	Heart Error	No heartbeat packets have been sent for more than 18 minutes.
3	Alarm	Alarm (24 hours).
4	Open	The back cover of the device was open.
5	Tamper	Peripheral tamper alarm was triggered.
6	Low Battery	Low battery of the device was detected.
7	PriPowerLoss	Peripheral main power failure was detected.
8	Battery Loss	Battery failure was detected.
9	Over Voltage	Overvoltage was detected.
10	Over Current	Overcurrent was detected.
11	Over Heat	Overheat was detected.
12	Fire Alarm	Fire alarm was triggered.
13	Medical Alarm	Medical alarm was triggered.
14	Panic Alarm	Panic alarm was triggered.
15	Gas Alarm	Gas leak alarm was triggered.
16	Intrusion Alarm	Intrusion alarm was triggered.
17	Hold Up Alarm	Panic alarm was triggered.

Appendix Table 1-2 Arming failure events and description (panel)

No.	Reason	Description
1	SOS Alert	Panic alarm can be triggered through the DMSS app.
2	Tamper	Hybrid panel tamper alarm was triggered.
3	Server Connect Error	The panel was offline.
4	SIA Server Connect Error	There is an error with the connection between the panel and the SIA alarm receiving center.
5	Low Battery	Low battery was detected.
6	Main Loss	Main power failure was detected.
7	Battery Loss	Battery failure was detected.
8	No GSM	2G/4G module errors was detected.
9	ATS Fault	Alarm transmission system fault was detected.

No.	Reason	Description
10	No SIM Card	No SIM card.
11	Mobile Network Fault	Cellular network failure was detected.
12	Wired Network Fault	Wired network failure was detected.
13	Wifi Network Fault	Wi-Fi network failure was detected.

Appendix 2 SIA Event Codes and Description

Appendix Table 2-1 SIA event codes and description

No.	Event	Original Code	SIA Code	Description
1	Medical Alarm	1100	MA	Medical Alarm Button Was Pressed
2	Medical Alarm Stopped	3100	MH	Medical Alarm Button Was Restored
3	Fire Alarm	1110	FA	Fire Alarm
4	Fire Alarm Stopped	3110	FH	Fire Alarm Stopped
5	Duress Alarm	1121	HA	Duress Alarm
6	Silent Panic Alarm	1122	HA	Panic Button Was Pressed Hold-Up Button Was Pressed
7	Silent Panic Alarm Stopped	3122	HH	Panic Button Was Restored Hold-Up Button Was Restored
8	Audible Panic Alarm	1123	PA	Panic Button Was Pressed Hold-Up Button Was Pressed
9	Audible Panic Alarm Stopped	3123	PH	Panic Button Was Restored Hold-Up Button Was Restored
10	Burglary Alarm	1130	BA	Motion Detected Opening Action Detected External Contact Was Opened Intrusion Alarm Glass Break Detected Tilt Detected Shock Detected
11	Burglary Alarm Stopped	3130	BR	Motion Stopped Closing Action Detected External Contact Was Closed Intrusion Alarm Stopped Glass Stopped Breaking Stopped Tilting Shock Stopped

No.	Event	Original Code	SIA Code	Description
12	Perimeter Alarm	1131	BA	Tripwire Alarm
13	Perimeter Alarm Stopped	3131	BR	Tripwire Alarm Stopped
14	24 Hour Alarm	1133	BA	Motion Detected Opening Action Detected External Contact Was Opened Glass Break Detected Tilt Detected Shock Detected
15	24 Hour Alarm Stopped	3133	BR	Motion Stopped Closing Action Detected External Contact Was Closed Intrusion Alarm Stopped Glass Stopped Breaking Stopped Tilting Shock Stopped
16	Entry Or Exit Alarm	1134	BA	Motion Detected Opening Action Detected External Contact Was Opened Glass Break Detected Tilt Detected Shock Detected
17	Entry Or Exit Alarm Stopped	3134	BR	Motion Stopped Closing Action Detected External Contact Was Closed Intrusion Alarm Stopped Glass Stopped Breaking Stopped Tilting Shock Stopped
18	Lid Was Opened	1137	TA	Lid Was Opened External Lid Was Opened Device Moved

No.	Event	Original Code	SIA Code	Description
19	Lid Was Closed	3137	TR	Lid Was Closed External Lid Was Closed Device Stopped Moving
20	Expansion Module Was Disconnected	1143	EM	Camera Module Is Connected
21	Expansion Module Was Connected	3143	EN	Camera Module Was Disconnected
22	Masking Alarm	1149	TA	Masking Alarm
23	Masking Alarm Stopped	3149	TR	Masking Alarm Stopped
24	Gas Leakage	1151	GA	Gas Leak Detected
25	Gas Leakage Stopped	3151	GH	Gas Leak Stopped
26	Water Leakage	1154	WA	Water Leak Detected
27	Water Leakage Stopped	3154	WH	Water Leak Stopped
28	High Temperature	1158	KA	High Temperature
29	Normal Temperature	3158	KH	Normal Temperature
30	Low Temperature	1159	ZA	Low Temperature
31	Normal Temperature	3159	ZH	Normal Temperature
32	Main Power Failure	1301	AT	Main Power Failure
33	Main Power Restored	3301	AR	Main Power Restored
34	Low Battery	1302	YT	Low Battery
35	Battery Level Restored	3302	YR	Battery Level Restored
36	Battery Fault	1311	YM	Battery Fault
37	Battery Restored	3311	YR	Battery Restored
38	Overcurrent Protection Triggered	1312	YI	Overcurrent Protection Triggered
39	Overcurrent Protection Restored	3312	YJ	Overcurrent Protection Restored
40	Overheat Protection Triggered	1318	KA	Overheat Protection Triggered
41	Overheat Protection Restored	3318	KH	Overheat Protection Restored
42	Overvoltage Protection Triggered	1319	YP	Overvoltage Protection Triggered
43	Overvoltage Protection Restored	3319	YQ	Overvoltage Protection Restored
44	RF Jamming	1344	XQ	RF Jamming

No.	Event	Original Code	SIA Code	Description
45	ATS Fault	1350	NT	ATS Fault Wired Network Fault Wi-Fi Fault Cellular Network Fault
46	ATS Restored	3350	NR	ATS Restored Wired Network Restored Wi-Fi Restored Cellular Network Restored
47	Communication Failure	1354	YS	RF-HD Connection Failed
48	Communication Restored	3354	YK	RF-HD Connection Restored
49	Wireless Device Was Disconnected	1355	XL	Connection Lost
50	Wireless Device Was Connected	3355	XC	Connection Restored
51	Protection loop shorted	1372	QT	Protection Loop Shorted
52	Fixed the shorted protection loop	3372	QR	Fixed The Shorted Protection Loop
53	Sensor Fault	1380	AS	Sensor Fault
54	Sensor Restored	3380	AN	Sensor Fault Restored
55	Disarmed By APP	1400	OQ	Disarmed
56	Armed By APP	3400	CQ	Armed
57	Disarmed By Keypad	1401	OP	Disarmed
58	Armed By Keypad	3401	CL	Armed
59	Disarmed By Schedule	1403	OA	Disarmed
60	Armed By Schedule	3403	CA	Armed
61	Cancel	1406	BC	Cancel
62	Disarmed By Keyfob	1407	OS	Disarmed
63	Armed By Keyfob	3407	CS	Armed
64	Quickly Armed	3408	CS	Armed
65	Disarmed By KeySwitich	1409	OS	Disarmed
66	Armed By KeySwitich	3409	CS	Armed
67	Home Mode Activated	3441	NL	Home Mode Activated
68	Home Mode Activated By KeySwitich	3442	NL	Home Mode Activated
69	Armed With Faults	3450	CF	Armed With Faults

No.	Event	Original Code	SIA Code	Description
70	Unsuccessful Arming	1454	CI	Unsuccessful Arming
71	Unsuccessful Arming By Schedule	1455	CD	Unsuccessful Arming
72	Exit Error	1457	EA	Unsuccessful Arming
73	Device Locked	1501	DK	Device Locked
74	Device Unlocked	3501	DO	Device Unlocked
75	Deactivated Device	1502	QB	Permanently Deactivated
76	Reactivated Device	3502	QU	Peripheral Reactivated Peripheral
77	Disabled Tamper	1503	TB	Permanently Deactivated Lid
78	Enabled Tamper	3503	TU	Enabled Lid
79	Bypassed Device	1570	QB	Bypassed
80	Device Bypass Restored	3570	QU	Unbypassed
81	Bypassed Tamper	1578	TB	Bypassed Tamper Signal
82	Tamper Bypass Restored	3578	TU	Unbypassed Tamper Signal
83	Manual Trigger Test Report	1601	RX	Test Report
84	Periodic Test Report	1602	RP	Periodic Test Report
Null	Heartbeat	Null	Null	Heartbeat Reported by Device

Appendix 3 Security Commitment and Recommendation

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

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

Account Management

1. Use complex passwords

Please refer to the following suggestions to set passwords:

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

2. Change passwords periodically

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

3. Allocate accounts and permissions appropriately

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

4. Enable account lockout function

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

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

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

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2. Encrypted transmission of audio and video

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

3. Turn off non-essential services and use safe mode

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

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

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

4. Change HTTP and other default service ports

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

Network Configuration

1. Enable Allowlist

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

2. MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. Build a secure network environment

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

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

Security Auditing

1. Check online users

It is recommended to check online users regularly to identify illegal users.

2. Check device log

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

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

2. **Update client software in time**

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

Physical Protection

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

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188