Alarm Hub 2

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO.LTD. V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the alarm hub 2 (hereinafter referred to as the "hub"). 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.	December 2023

Privacy Protection Notice

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

About the Manual

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

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

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

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

- 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

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

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

Table of Contents

1 Introduction

1.1 Overview

Alarm Hub is a central device in the security system, which controls the operation of all connected peripherals. If the security system detects the presence, entry, or attempted entry of an intruder into the armed area, the hub will receive the alarm signals from the detectors, and then alert users.

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	Wireless Zone	150 channels wireless peripherals (6 sirens, 64 PIR cameras, 64 keyfobs, 8 keypads and 4 repeaters)
	Network Mode	Europe: Supports installation of dual SIM cards. Only one card can be enabled at a time. Also, multiple frequency bands are supported for the SIM cards (GSM: 900/1, 800 MHz, WCDMA: B1/B5/B8, LTE-FDD: B1/B3/B5/B7/B8/B20/B28A, LTE-TDD:B38/B40/B41). USA: Supports installation of dual SIM cards. Only one card can be enabled at a time. Also, multiple frequency bands are supported for the SIM cards (GSM: 850/900/1800/1900 MHz, WCDMA:B1/B2/B4/B5/B8, LTE-FDD:B1/B2/B3/B4/B5/B7/B8/B28, LTE-TDD: B40) Only available on 4G models.
	Network Port	1 RJ-45, 10 Mbps/100 Mbps Ethernet port.
	Storage Battery	One built-in 4,750 mah rechargeable lithium battery.
Audio & Video	Video Input	8-ch IPC, which only supports the upload of alarm videos.
	Audio Output	1 channel
	Volume Control	Yes
	Voice Broadcast	• 4G: Telephone and local speaker • Wi-Fi: Local speaker
Function	Indicator Light	The indicator indicates the status of alarms, arming and disarming, the network connection and device failure.
	Button	Includes a reset button, voltage button and AP switch button.

Type	Parameter	Description	
	SMS	Yes (up to 5 phone numbers) Only available on 4G models.	
	Phone Call	Yes (up to 5 phone numbers) Only available on 4G models.	
	Video Linkage	Yes	
	Offline Cache	Stores up to 50 alarm messages.	
	Arm and Disarm Method	App, keyboard, remote control, card, scheduled arming and disarming.	
	Remote Update	Cloud update	
	Low Battery Detection	Yes	
	User Management	Functions can be shared by the app users. These include 1 installer, 1 administrator and 31 general users.	
	Power Failure Protection for Configured Parameters	Yes	
	Logs	Up to 5, 000 entries	
	Transmission Protocol	SIA, SoftGuard	
RF	Carrier Frequency	DHI-ARC3800H-FW2(868)/ DHI-ARC3800H-FW2: 868.0 MHz–868.6 MHz	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: 433.1 MHz–434.6 MHz
	Transmitter Power (EIRP)	DHI-ARC3800H-FW2(868)/ DHI-ARC3800H-FW2: Limit 25 mW	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: Limit 10 mW
	Communication Mechanism	Two-way	
	Communication Distance	DHI-ARC3800H-FW2(868)/ DHI-ARC3800H-FW2: Up to 2,000 m (6,561.68 ft) in an open space.	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: Up to 1,200 m (3,937.01 ft) in an open space
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
	Wi-Fi	2.4 G	

Type	Parameter	Description
Basic	Language	• 4G models: Up to 7 languages are supported for SMS: English, Spanish (Latin America), French, Italian, Arabic, Turkish, and Danish. It is set as English by default. The alarm voice message feature and local speaker only support English. • Wi-Fi models: English
	Power Supply	100–240 VAC, 50/60 Hz
	Standby Time	The battery lasts up to 12 hours when it is fully charged and is within the following conditions: It is connected to the Wi-Fi, its ID is connected to the alarm receiving center, the heartbeat interval is 1,800 seconds, and it is connected to 8 peripherals and the cloud.
	Power Consumption	≤12 W
	Operating Temperature	–10 °C to +55 °C (+14 °F to +131 °F)
	Operating Humidity	10%–90% (RH)
	Product Dimensions	174.8 mm × 174.8 mm × 38.3 mm (6.88" × 6.88" × 1.51") (L × W × H)
	Net Weight	510 g (1.12 lb)
	Gross Weight	860 g (1.90 lb)
	Installation	Supports wall mount and desktop mount installation.
	Casing Material	PC + ABS
	Certifications	CE
	Anti-corrosion Level	Basic Protection
	Storage Temperature	–10 °C to +55 °C (+14 °F to +131 °F)
	Storage Humidity	10%–90% (RH)
	Packaging Dimensions	254 mm × 211 mm × 61 mm (10.00" × 8.31" × 2.40") (L × W × H), standalone in the inner box 524 mm × 508 mm × 442 mm (20.63" × 20.00" × 17.40") (L × W × H), protective case
Power Supply	PS Type	Type A
	Main Power	100–240 VAC, 0.4A
	Battery Capacity	3.7 V/4750 mAh

Type	Parameter	Description
	Battery Standby	Up to 12 h When following conditions are met, the standby time can reach 12 h: ● Connects with Wi-Fi, GPRS/3G/4G. ● Connects to ARC and heartbeat interval is 1800 seconds. ● Connects to 8 inputs and 1 siren. ● Connects to the cloud.
	Battery Type	Battery type: Built-in rechargeable Lithium-ion polymer; battery model: 01DQ0023-69
	Max. current available	1.3A
	Power Consumption	Max. 12 W
	Current Consumption	Normal: 370 mA; alarm: 440 mA
	Battery Low Battery Threshold	3.675 VDC
	Battery Restore Threshold	3.675 VDC
	Release Voltage	< 3V
	Battery Recharge Time	80% approx. 11 h
ARC Signaling	ATS Category	DP2/SP2 (LAN/Wi-Fi and GPRS/4G)
	Acknowledgment Operation	Pass through
	Protocols	SIA-DC09
	Primary Transmission Path	LAN /Wi-Fi (NO 50136-2)
	Secondary Transmission Path	GPRS/4G
	Notification Equipment	C/E/F

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

ATE Category	Reporting Time	Protocols	Communication Devices			Communication Device to be Used
			PSTN	2G/3G	IP	
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
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: Al-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. Al-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.

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

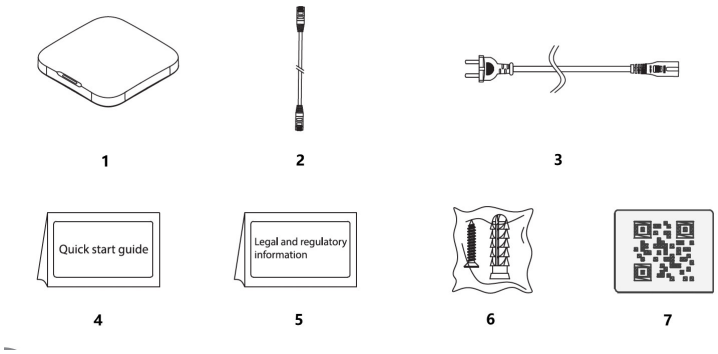


Table 1-3 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Alarm Hub 2	1	5	Legal and regulatory information	1
2	Cable	1	6	Package of screws	2
3	Adapter	1	7	QR code	1
4	Quick start guide	1	—	—	—

2 Design

2.1 Appearance

Figure 2-1 Appearance

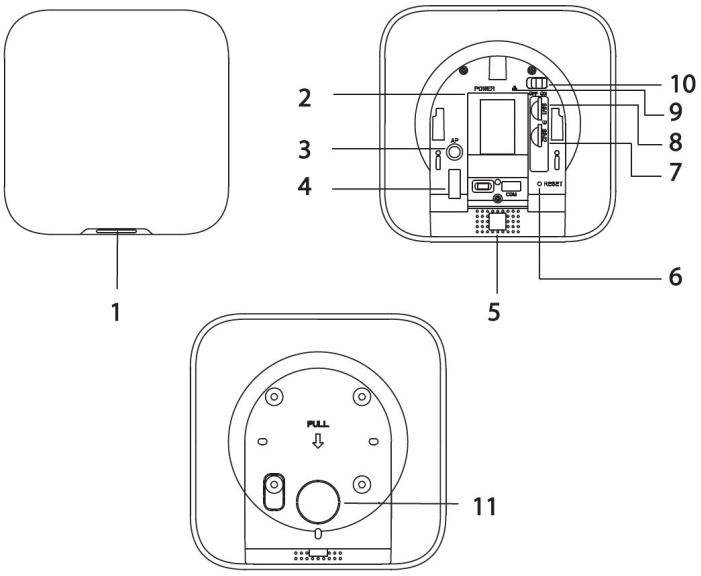


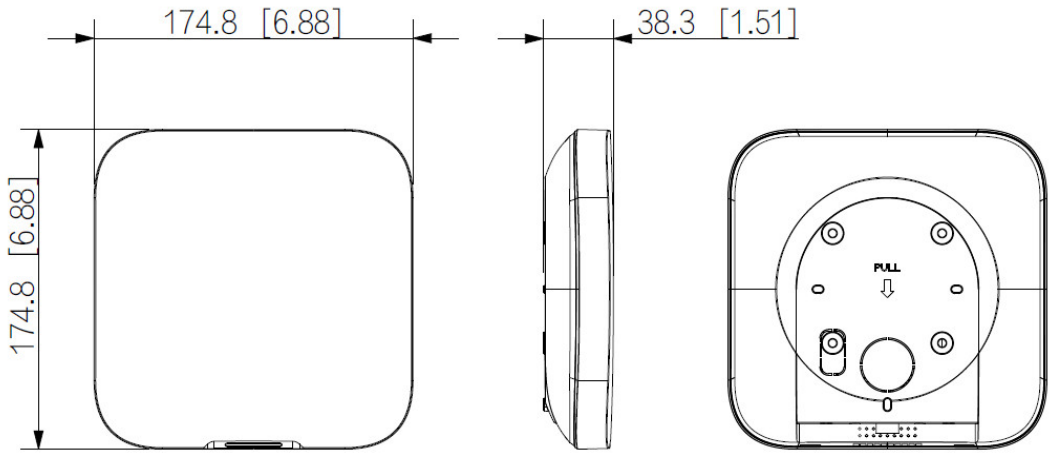
Table 2-1 Structure

No.	Name	Description
1	Indicator	• Flashes green slowly: Reduced sensitivity mode. • Flashes green: The hub starts working. • Solid yellow: Failed to connect to the cloud. • Solid green: Disarming mode. • Solid blue: Arming mode. • Flashes red: Alarm event was triggered. • Flashes yellow: Detected a malfunction. • Flashes blue: Running AP configuration or the hub is pairing with peripherals. • Flashes blue quickly: Card issuing mode.
2	Power port	Connect to power supply.
3	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 hub, and then sync Wi-Fi username and password to the hub. You can also turn off the AP through pressing and holding the button for 2 seconds when AP is enabled.
4	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
5	Speaker	Generate sound.
6	Reset button	Press and hold the button for 10 seconds to restart the hub and restore factory default settings.

No.	Name	Description
7	Slot for SIM 2	Install main card to the first slot, and standby card to the second slot. ● Support dual SIM cards and single standby. ● SIM cards allow the hub to use cellular data, and push alarm notifications. ● SIM cards will not work until network configuration has been completed. ● SIM function is only available on select models.
8	Slot for SIM 1	
9	Ethernet cable socket	Connect the hub to the Ethernet.
10	Power switch	Turn on or turn off the hub.
11	Back cover	If the back cover is opened, the tamper alarm will be triggered.

2.2 Dimensions

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



3 Startup

3.1 Users

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.

User Access Level

Table 3-1 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 hub to them, or when they entrust the hub 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 3-1 Business flow (DMSS user)

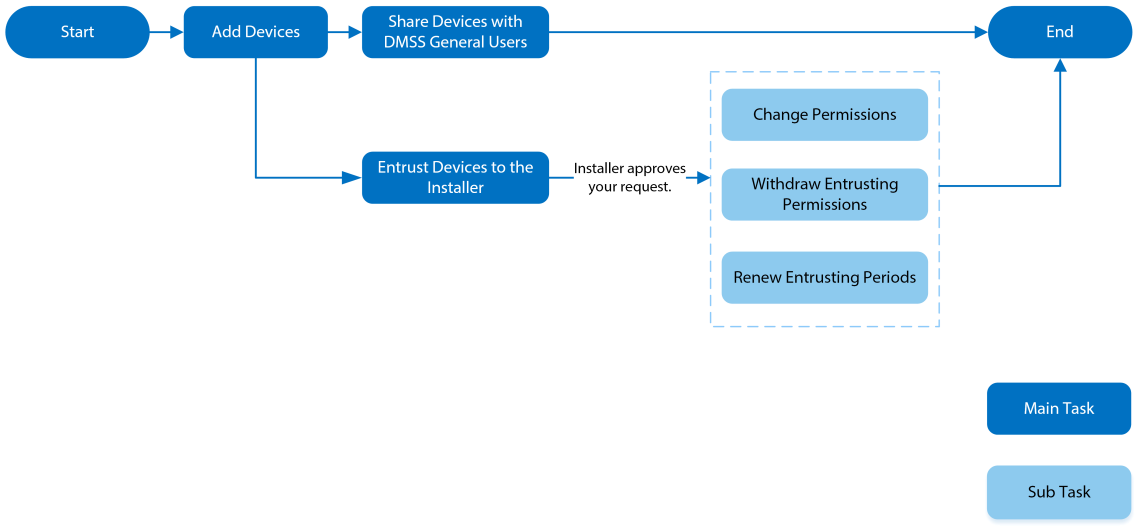
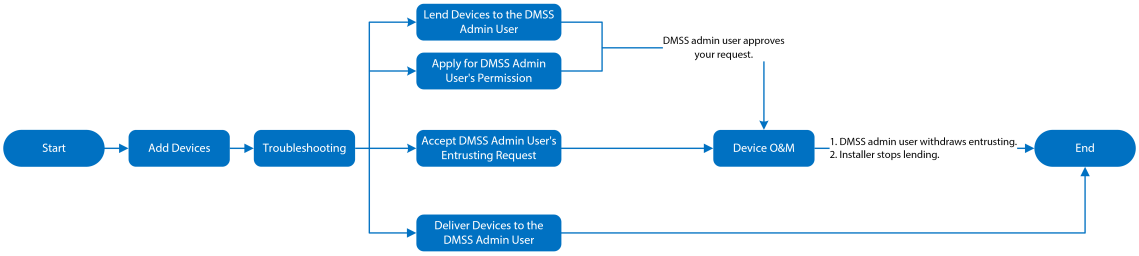


Figure 3-2 Business flow (Installer)



3.2 Operation Process

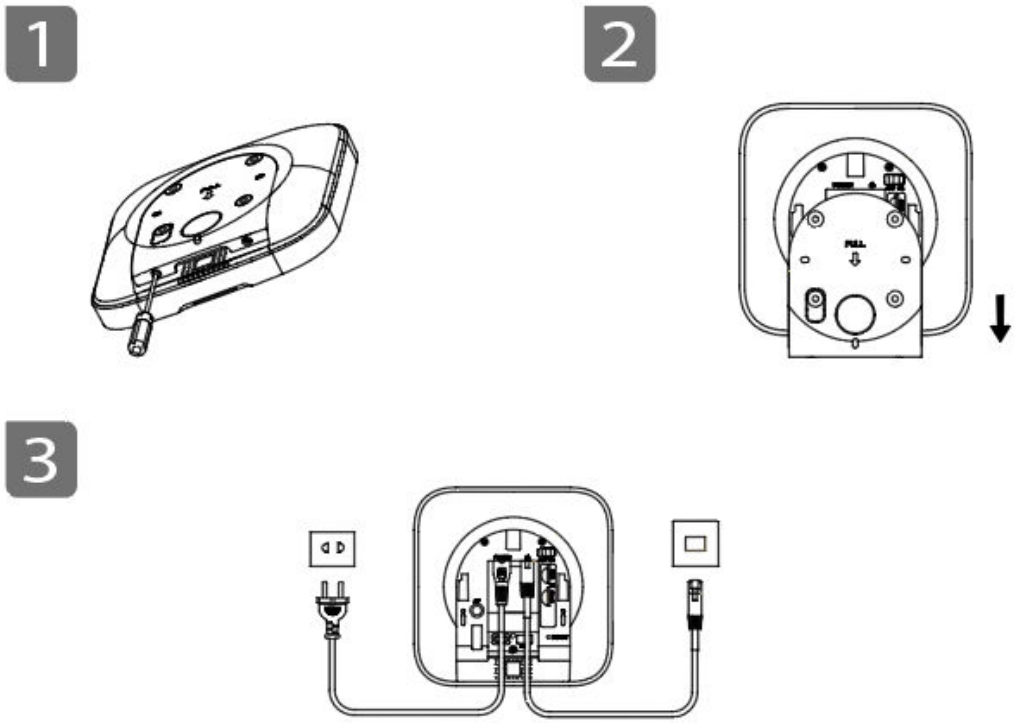
Follow the procedures below to turn on the wireless alarm system.

Figure 3-3 Operation process

Power On

Connect the hub to the Ethernet, and power on the hub.

Figure 3-4 Power on



Adding Devices

1. Add the hub to the DMSS app.

2. Add the peripherals to the hub.

Installing the Hub

We recommend using expansion screws to install the hub. Do not place the hub in the following areas:

- Outdoors.
- Places close to metal objects that cause attenuation and shielding of the radio signal.
- Places with a weak GSM signal.
- Places close to radio interference sources that are less than 1 meter away the router and power cables.
- Places where the temperature and humidity exceed allowed limits.

Figure 3-5 Installation

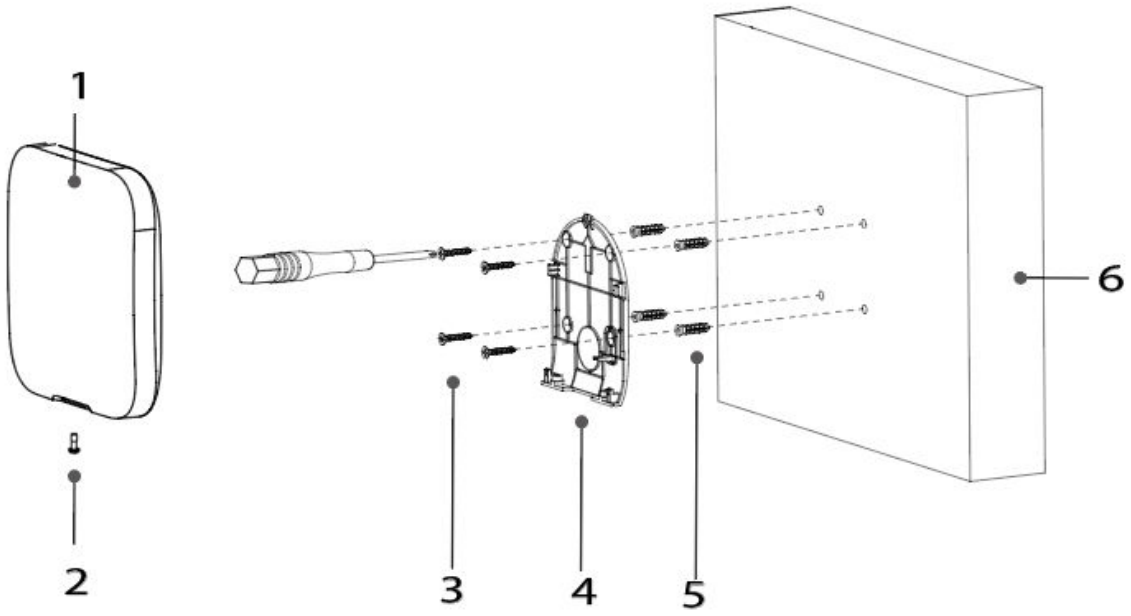


Table 3-2 Installation items

No.	Item Name	No.	Item Name
1	Hub	4	Mounting plate
2	M3 × 8 mm countersunk head screw	5	Expansion bolt
3	ST4 × 25 mm self-tapping screw	6	Wall

1. Confirm the position of the screw holes, and then drill them into the mounting plate.
2. Put the expansion bolts into the holes.
3. Attach the mounting plate into the wall, and then align the screw holes on the plate with the expansion bolts.
4. Fix the mounting plate with ST4 × 25 mm self-tapping screws.
5. Put the alarm hub into the mounting plate from top to bottom.
6. Fix the alarm hub and mounting plate with M3 × 8 mm countersunk head screws.

Configuring the Hub

Configure the hub on the DMSS app.

Arming the Alarm System

You can use the keypad, keyfob and app to arm your system. After an arming command is sent to DMSS app, the system will check the status of the system. If the system has a fault, you will need to choose whether to force arm it. For details on peripherals, see the user's manual of the corresponding device.

4 DMSS Operations for End Users

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

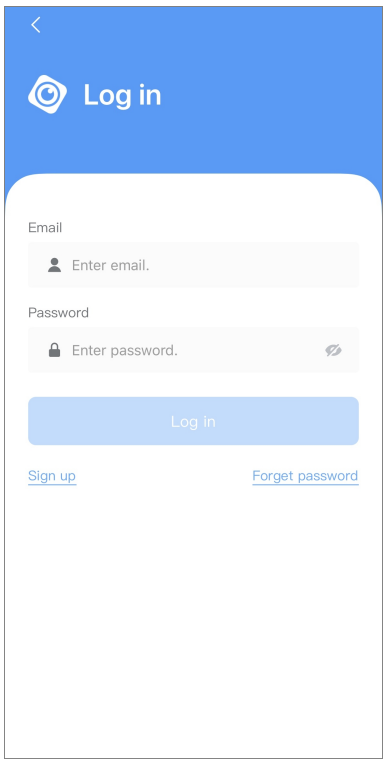
Procedure

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.

Figure 4-1 Login



Step 3 Create an account.

1. On the **Login** screen, tap **Sign up**.

2. Enter your email address and password.

   Tap to show the password, and the icon will become .
3. Read the **User Agreement** and **Privacy Policy**, and then select the **I have read and agree to** checkbox.
4. 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.
5. Tap **OK**.

Step 4 On the **Login** screen, enter your email and password, and then tap **Log in**.

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

4.2 Adding Devices

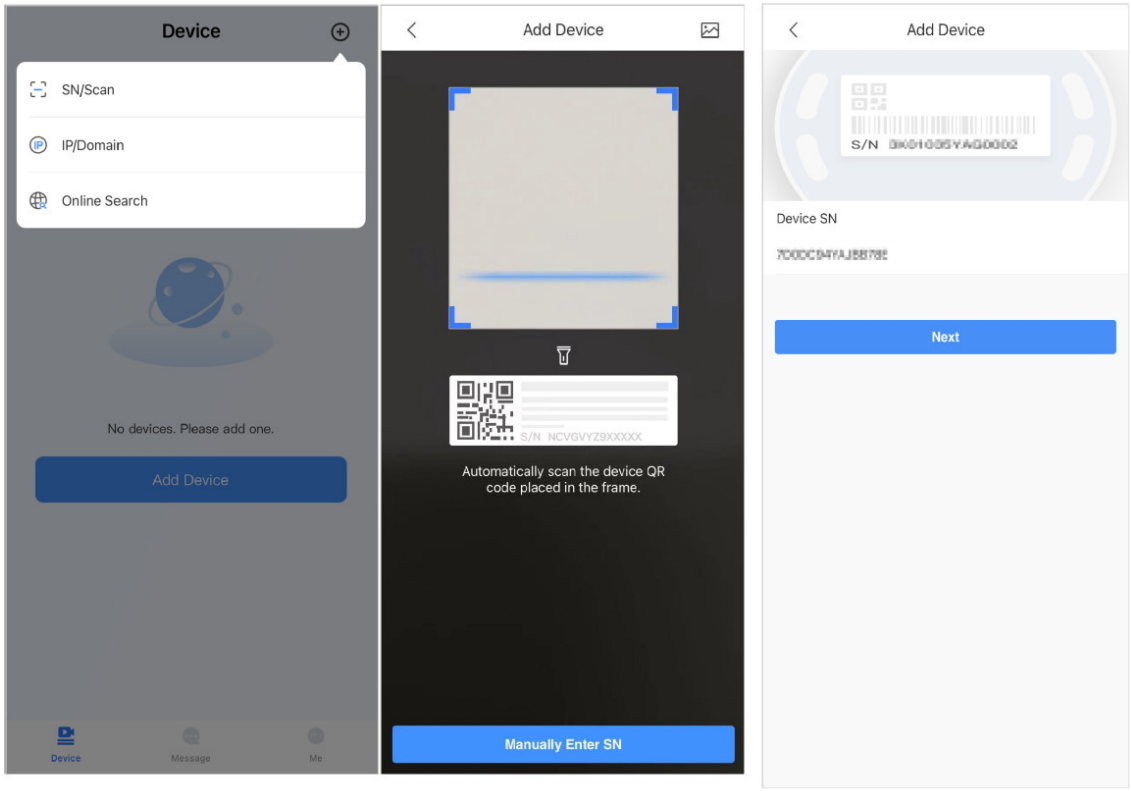
For end users, you can add alarm devices to DMSS app.

4.2.1 Adding the Hub

Procedure

Step 1 On the **Device** screen, tap , and then select **SN/Scan**.

Figure 4-2 Add by SN/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 the device type, and then tap **Next**.

Tap **Next** if the system identifies the device type automatically.

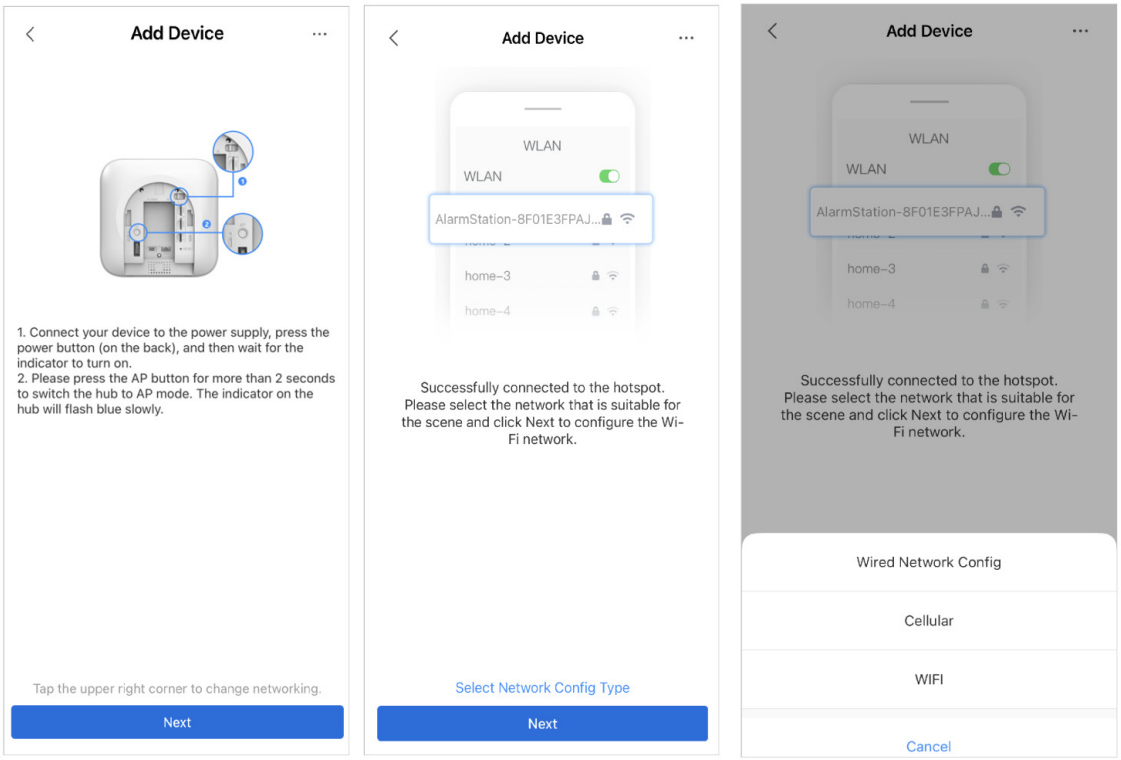
Step 4 On the **Add Device** screen, customize the device name, enter the username and the device password, and then tap **Save**.

Step 5 Configure network settings.

1. On the **Add Device** , tap **Next** to join the hotspot of the hub.
2. When the connection is established successful, tap **Select Network Config Type**.
3. Select the network types you want to configure.

- Wired network: Enable DHCP function, or manually enter the IP address, subnet mask, gateway, DNS and MAC address.
- Cellular: Configure the APN, Autho mode, username, password, dial number, roaming data for the SIM card.
- Wi-Fi: Select a Wi-Fi network, and then enter the password to connect to it.

Figure 4-3 Configure network types



4.2.2 Adding Peripheral

You can add multiple peripherals into the hub. For details on adding peripherals, see user's manuals of respective peripherals.

Procedure

Step 1 Go to the hub screen, and then tap **Peripheral** to add the peripheral

Step 2 Tap **+** to scan the QR code at the bottom of the device, and then tap **Next**.

Step 3 Tap **Next** after the device has been found.

Step 4 Follow the on-screen instructions and switch the device to on, and then tap **Next**.

Step 5 Wait for the pairing.

Step 6 Customize the name of the device, and select the area, and then tap **Completed**.

4.2.3 Adding IPC

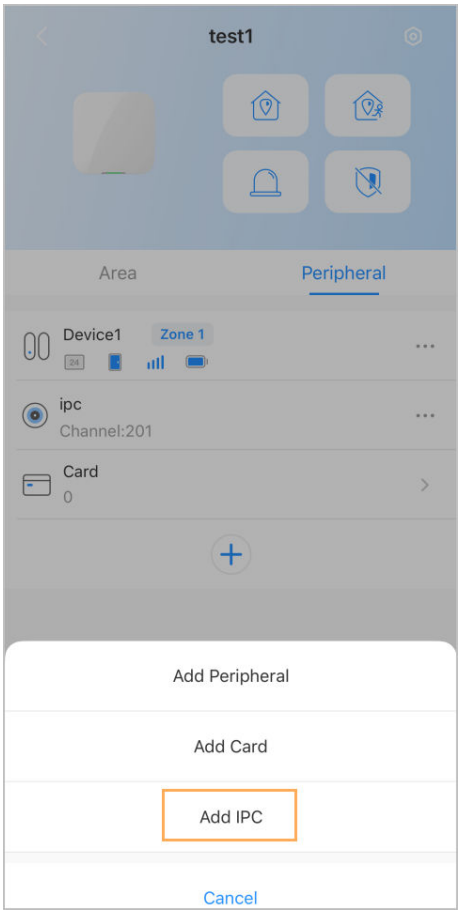
Add IPCs to the hub.

Procedure

Step 1 On the hub screen, tap **Peripheral** , and then tap **+**.

Step 2 Select **Add IPC**.

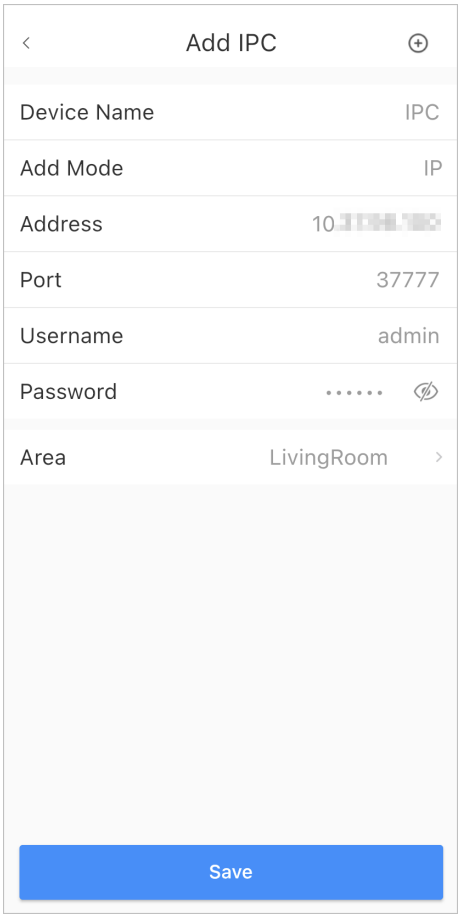
Figure 4-4 Add IPC



Step 3 Add an IPC to the hub.

- 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.
  2. Tap **Save**.

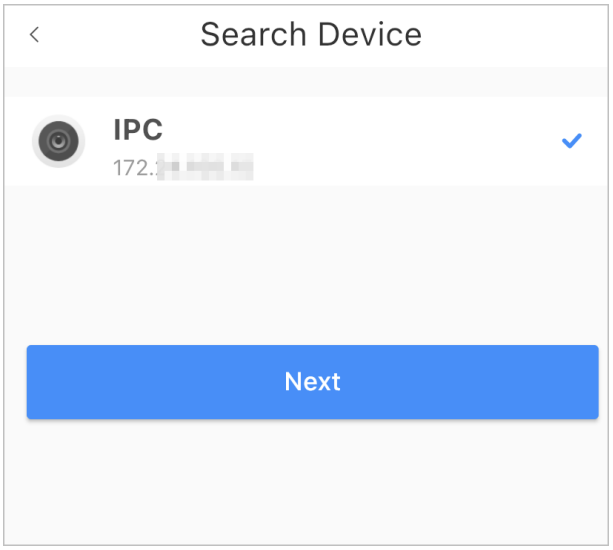
Figure 4-5 Manually add



- Online search:

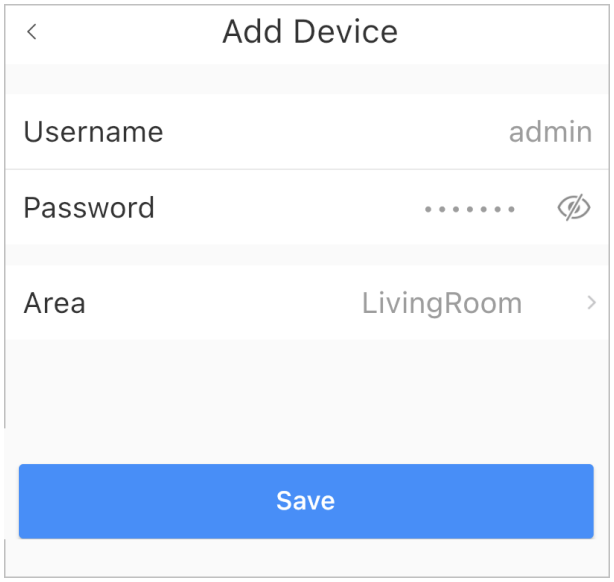
1. Tap ⊕ to search for the IPC in the same network segment.

Figure 4-6 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 **Save**.

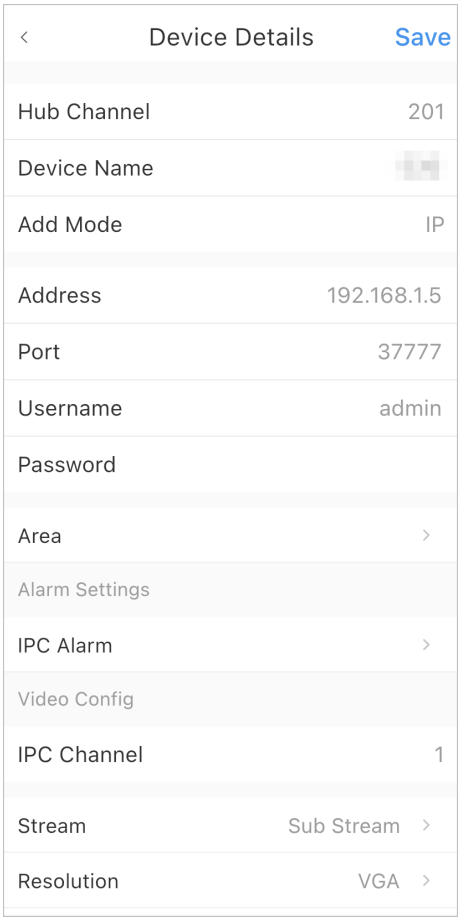
Figure 4-7 Enter password



Related Operations

On the **Device Details** screen, configure the parameters of the IPC.

Figure 4-8 Configuring IPC



4.3 Configuring Alarm Linkage Video

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

Prerequisites

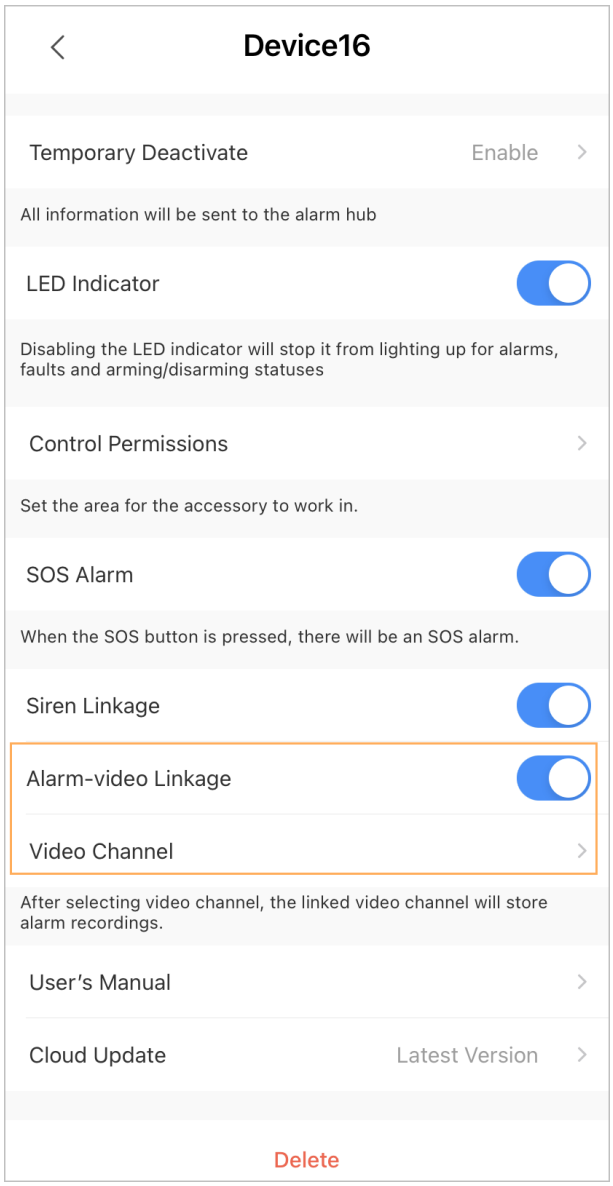
- Make sure that the hub is armed before you configure the alarm-video linkage.
- Make sure that you have added peripherals to the hub.

Procedure

Step 1 On the hub screen, select a peripheral in the **Peripheral** list, and then tap on the **Device Details** screen to configure the parameters.

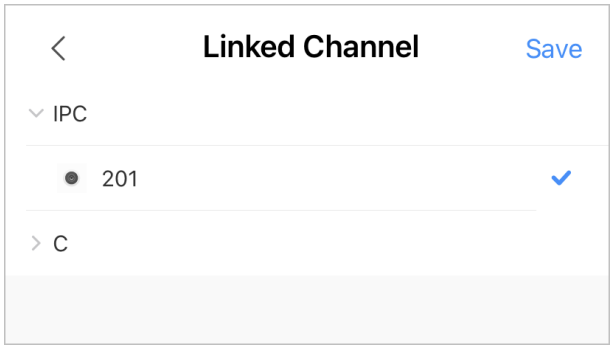
Step 2 Enable **Alarm-video Linkage** , and then select **Video Channel**.

Figure 4-9 Configuration screen



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

Figure 4-10 Linked channel



4.4 Hub General Settings

You can view and edit basic device information.

Procedure

Step 1 On hub screen, tap to go to **Device Details** screen.

Table 4-1 Parameter description

Parameter	Description
Hub Status	View status of the hub.
Hub Setting	Configure parameters of the hub.
Network Configuration	Tap **Network Configuration** 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 hub operates. • **DST** : Select date or week, and then select start time and end time.
Device Sharing	Tap **Device Sharing** to share the status of the hub with the other users.
Device Languages	Select the language for the hub. You can choose from English, Spanish, Arabic, Dansk, French, Italian and Türkçe.
Device Entrusting	Entrust devices to service providers for them to perform alarm operation services for you.
User's Manual	Tap **User's Manual** to obtain the user's manual of the alarm hub.
Cloud Update	Update online. Update is not allowed when the hub is in armed status or the battery level is low.

Parameter	Description
Logs	Device and app logs. ● Device log: Select **Log** > **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 **Log** > **App log** to view alarm logs. You can also tap on the **App log** screen to send alarm logs to the linked email.

4.4.1 Viewing Hub Status

On the **Hub** screen, select > **Hub Status** to view the status of the hub.

Table 4-2 Status

Parameter	Description
GMS/LTE Signal Strength	The signal strength of the mobile network for the active SIM card. ● : Ultra low. ● : Low. ● : Moderate. ● : High. ● : No.
Wi-Fi Signal Strength	Internet connection status of the hub via Wi-Fi. For greater reliability, we recommend installing the hub in places with the signal strength of at least 2 bars. ● : Ultra low. ● : Low. ● : Moderate. ● : High. ● : No.
Battery Level	Show remaining electricity of the battery. ● : Fully charged. ● : Sufficient. ● : Moderate. ● : Insufficient.
Anti-tampering	This is the anti-tamper function for the peripheral. The hub reacts when a peripheral is disassembled.
Main Power Status	Show main power status.

Parameter	Description
GSM/LTE Connection Status	Internet connection status of the hub via SIM card, Wi-Fi, and Ethernet. ● : Connected. ● : Disconnected.
Wi-Fi Connection Status	
Network Cable Connection Status	
SIM Card	Connection status of the SIM card. ● : SIM card 1 is active. ● : SIM card 2 is active. ● : No SIM card.
SIM Card Status	This status bar is only supported when there is a SIM card inserted into the hub. ● : The SIM card is unlocked. ● : The SIM card is locked.
Program Version	The program version of the hub.

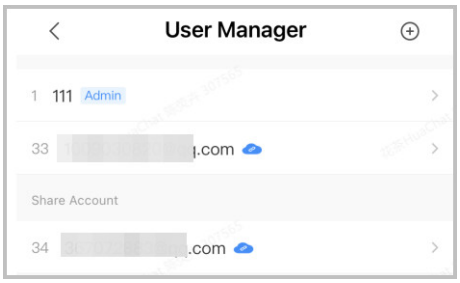
4.4.2 Configuring the Hub

Procedure

Step 1 On the **Hub** screen, tap .

Step 2 View and edit general information of the hub.

Table 4-3 Hub parameter description

Parameter	Description
User Manager	You can add, modify, or delete keypad users when it is disarmed. ● **Adding Users** : Tap ⊕ to add a user. Enter your username, keypad code (4 to 6 digits), and duress passcode (optional), and then select arming and disarming 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. Figure 4-11 Add keypad user  ● **Deleting User** : Select the user, and then swipe left to delete the user. The admin user must be the last to be deleted. ● **Modifying User's Information** : Tap the user you need to edit, and then you can modify user's information, including username, passcode, duress code, arming and disarming permission on the user information page. ● **Adding Card** : Tap ⊕ on the upper-right corner of the user information page to add card for the user. Press any key to wake up the keypad, and then place the card near the card swiping area of the keypad to enter to the linking process within 30 seconds. If the card information is successfully recognized, the card ID will be displayed on the user information page, and then the keypad will beep once. After you save the configurations, the card will have the user's permissions. Up to 8 cards can be linked to a user. ● **Deleting Card** : Select the card, and then swipe left to delete the card.
Global Arming/ Disarming	Arm or disarm all the detectors in all the areas with one tap.

Parameter	Description
Schedule Arming/ Disarming	Arm or disarm the areas by schedule. • **Area** : Select the area in which the hub operates. • **Command setting** : Select an armed mode as needed by tapping **Home**, **Away**, or **Disarm**. • **Time** : Select the time period in which the hub operates. • **Repeat** : Copy the arming or disarming schedule. • **Force Armed** : You can arm the system when errors happen in zones.
Ringtone Setting	Set the arming, disarming ringtone that will also be applied or delay status. Select **Speak** to configure the ringtones.
LED Indicator	**LED Indicator** is enabled by default. If **LED Indicator** is disabled, the LED indicator will remain off regardless of whether the hub is functioning normally or not.
Phone Number Management	Tap **Add** on the upper-right corner of the page to add a phone number to receive the event, and then select the event type that needs to send SMS. The event types include alarm, fault, operation, and whether the alarm is linked to the phone. After adding, you can swipe left to test phone calls and SMS messages to verify whether the current phone number is valid. You can also swipe left to delete the mobile phone number. Tap the phone number to enter the phone number editing page, and then you can edit the number and select the event type that needs to send SMS. Only 2G/4G devices support this function.
Test Mode	Tap **Start** to test the status of the peripherals connecting to the hub in different areas, and then tap **Stop** to complete detection.
Reduced Sensitivity Mode	Enable **Reduced Sensitivity Mode**, and then the hub's transmit power will be reduced.
Cloud Service Connection	Set the server-hub ping interval with the range from 150 to 900 seconds (150 seconds by default). If the D-cloud detects that the hub's offline duration exceeds 150 seconds, it will report the hub status to the user through app.

Parameter	Description
Heartbeat	Configure the hub-detector ping interval. The settings determine how frequently the hub communicates with the peripherals and how quickly the loss of connection is detected. • **Detector Ping Interval** : The frequency of connected peripherals operated by the hub 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 undelivered packets to determine connection failure** : 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 hub 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 state, when the **Link Siren for Tamper** is enabled, the hub will link the alarm sound. The siren will alert when the lids of the hub and peripherals are open. • **Always Active** : Configure whether to link the alarm sound in the disarming state. It is disabled by default. After enabling **Always Active**, when the **Link Siren for Tamper** is enabled, the hub will link the alarm sound in both arming and disarming state. This is not according to EN50131-1 certifications.
System Integrity Check	When enabled, the hub checks the status of all detectors before arming, such as battery charge level, tamper incidents, and connectivity. If errors are detected, warnings will be displayed. • 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.
CMS	Enter IP address, port and device ID, and then you can register the hub to the DSS Pro or Converter.

Parameter	Description
Alarm Receive Central	Enable the function, and then set the SIA protocol parameters for the alarm receiving center (ARC). • **Protocol** : Select from **SIA-DC09**AND **Private**. **Private** is enabled by default. • **Preferred IP/Domain Name** : Enter the IP/domain address and port number of the ARC. • **Communication Test** : **Scheduled Test**is disabled by fault. After enabling and configuring the **Auto Report Period**, the hub reports periodic test event regularly.
Fault Check	• **Main Power Failure** : It is enabled by default. After disabling, when the main power of the hub fails, the hub will not indicate and notify. • **Alarm Hub Tamper** : It is enabled by default. After disabling, when the lid of the hub is open, the hub will not indicate and notify. • **Connections to Cloud Platform** : It is enabled by default. After disabling, when the connection between the hub and cloud platform is abnormal, the hub will not indicate and notify. • **Wired Network and Wi-Fi Errors** : It is enabled by default. After disabling, when the wired network and Wi-Fi of the hub fails, the hub will not indicate and notify. • **Cellular Network Errors** : It is enabled by default. After disabling, when the cellular network of the hub fails, the hub will not indicate and notify. • **RF Jamming** : It is enabled by default. After disabling, when the hub detects RF jamming, the hub will not indicate and notify, but the event can be viewed in the log. Disabling any of these functions will cause the system to not comply with EN50131-1, and the error messages will not be sent related to the disabled function.

4.5 Network Configuration

On the **General Config** of the **Device Details** screen, tap **Network Configuration**, and then you can select network for the hub: wired network, wireless network, or cellular network.

4.5.1 Wired Network Configuration

Procedure

Step 1 Select **Network Settings** > **Wired Network Config**.

Step 2 Configure wired network connection parameters.

Table 4-4 Description of wired network parameters

Parameter	Description
DHCP	When there is a DHCP server on the network, you can enable **DHCP**, and then the hub gets a dynamic IP address automatically.

Parameter	Description
IP Address	Set the IP address manually: Set IP address, subnet mask, default gateway, DNS and MAC address manually for the hub.
Subnet Mask	
Gateway	
DNS	
DNS 2	
MAC Address	

4.5.2 Wi-Fi Network Configuration

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.

4.5.3 Cellular Configuration

Procedure

Step 1 Select **Network Settings** > **Cellular**.

Step 2 Configure cellular parameters.

Table 4-5 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 1	• Supports dual SIM cards and single standby. • SIM cards allow the hub to use cellular data, and push alarm notifications.
SIM 2	
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 username and password of the cellular network.
Password	
Dial Number	The number that the hub 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	Enter the PIN of SIM cards 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.

4.6 Managing Users

4.6.1 Adding User

For DMSS admin users, you can add both installers and DMSS general users.

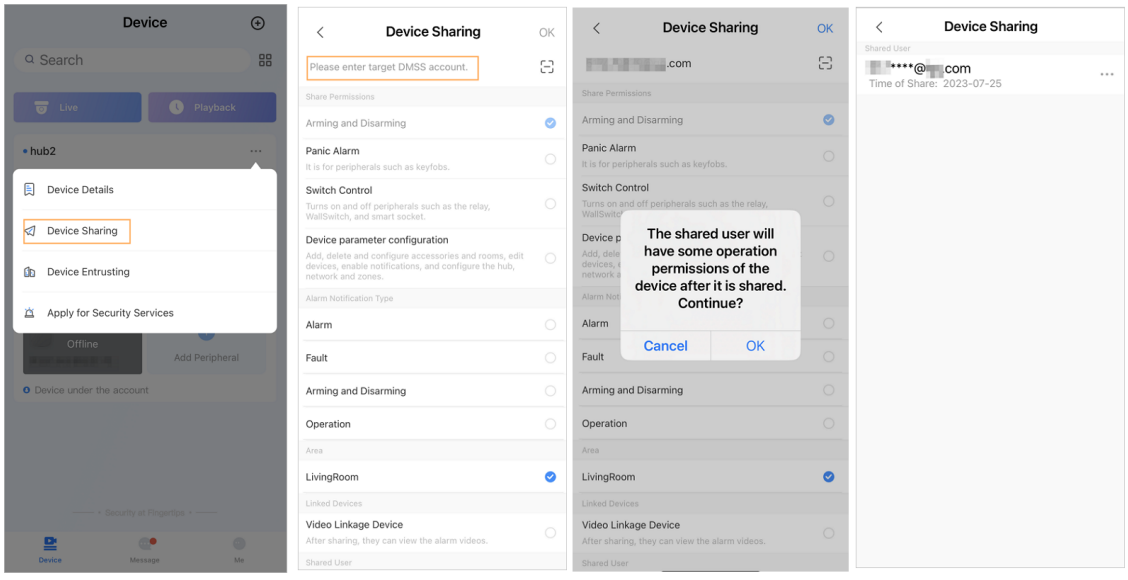
4.6.1.1 Adding DMSS General User

You can go to ••• > **Device Details** > <, or ••• > **Device Details** > **Device Sharing** to share the device. These methods are similar. This section uses sharing devices on ••• > **Device Sharing** as an example.

Procedure

Step 1 On the **Device** screen, tap ••• next to a device, and then tap **Device Sharing**.

Figure 4-12 Share device



Step 2 On the **Device Sharing** screen, share the device with the user by entering their DMSS account or scanning their QR code.

Step 3 Select device permissions for users based on your actual need.

Step 4 Tap **OK**.

The account that you shared the device with will appear on the **Shared User** section of the **Device Sharing** screen.

4.6.1.2 Adding Installer

For DMSS admin users, you can add installers by entrusting devices to them. You can entrust devices to the installer one by one or in batches.

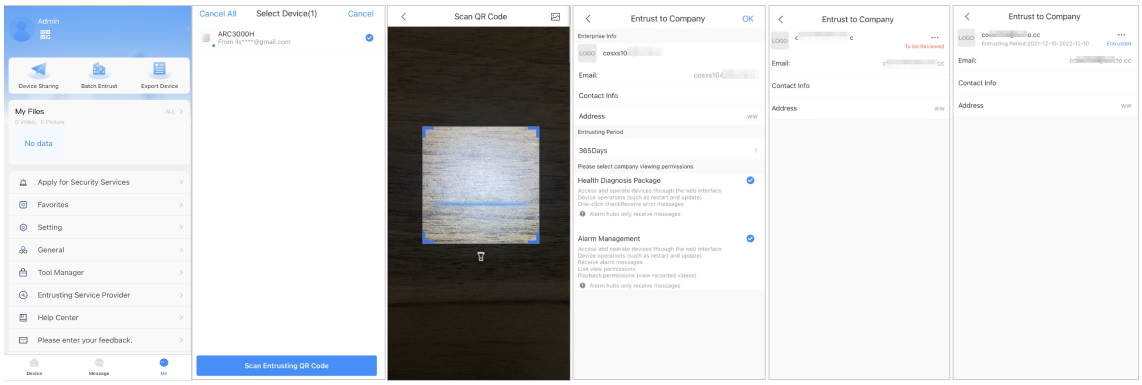
4.6.1.2.1 Entrusting Devices in Batches

You can entrust devices to one enterprise in batches.

Procedure

Step 1 Select **Me** > **Batch Entrust**.

Figure 4-13 Entrust devices in batches



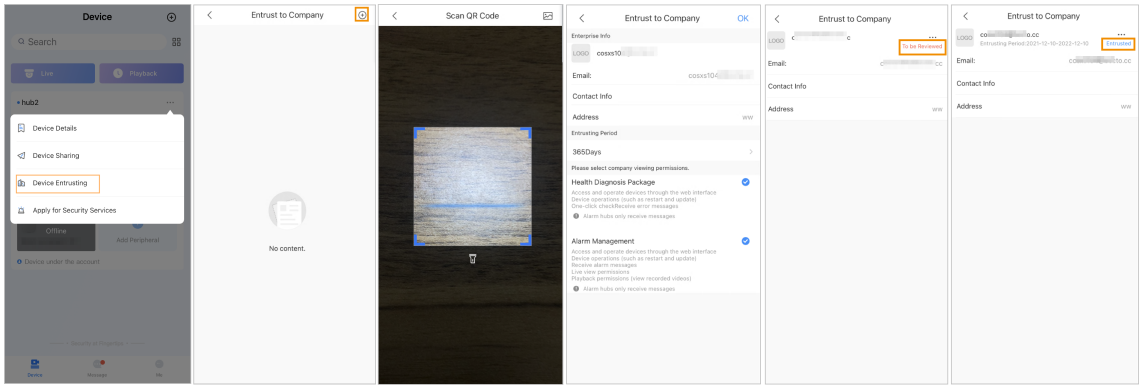
Step 2 On the **Select Device** screen, select the devices to be entrusted, and then entrust those to the enterprise. The process for entrusting multiple devices is the same as entrusting a single device.

4.6.1.2.2 Entrusting Device One by One

Procedure

Step 1 On the **Device** screen, tap ••• next to a device, and then tap **Device Entrusting**.

Figure 4-14 Entrust a device



Step 2 On the **Entrust to Company** screen, tap ⊕, and then scan the corresponding QR code of the installer, or tap 🖼 and import the QR code picture to entrust the device to the installer.

You can ask installers for their QR codes.

Step 3 On the **Entrust to Company** screen, select entrusting periods, and company viewing permissions, and then tap **OK**.

- You must select **Health Diagnosis Package** or **Alarm Management** for viewing the permissions.
- Enterprise information will be automatically recognized after you scan the QR code of the installer.

Step 4 View entrusting details on the **Entrust to Company** screen.

When successfully entrusted, **To be Reviewed** will change to **Delivered**.

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 **Personal** screen. To visit this location, go to **Me** > **Mailbox** > **Personal**.

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**.

4.6.2 Deleting User

For DMSS admin users, you can delete both installers and DMSS general users.

4.6.2.1 Canceling Device Sharing

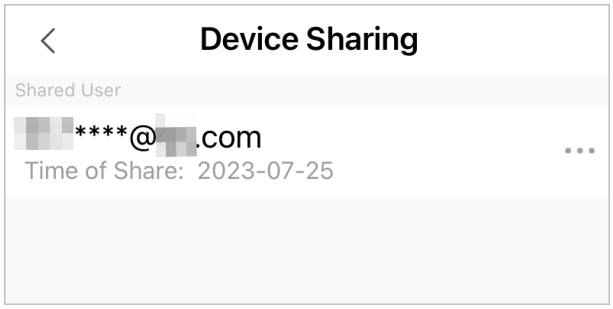
DMSS admin users can delete DMSS general users when they stop sharing devices with them on the **Device Sharing** screen. This process is illustrated in this section using the path of ••• > **Device Sharing**.

Procedure

Step 1 On the **Device** screen, tap ••• next to a device, and then tap **Device Sharing**.

Step 2 In the account list of the **Device Sharing** screen, select an account, and tap ••• .

Figure 4-15 Shared user



Step 3 Select **Cancel Sharing** , and then tap **OK** to cancel sharing.

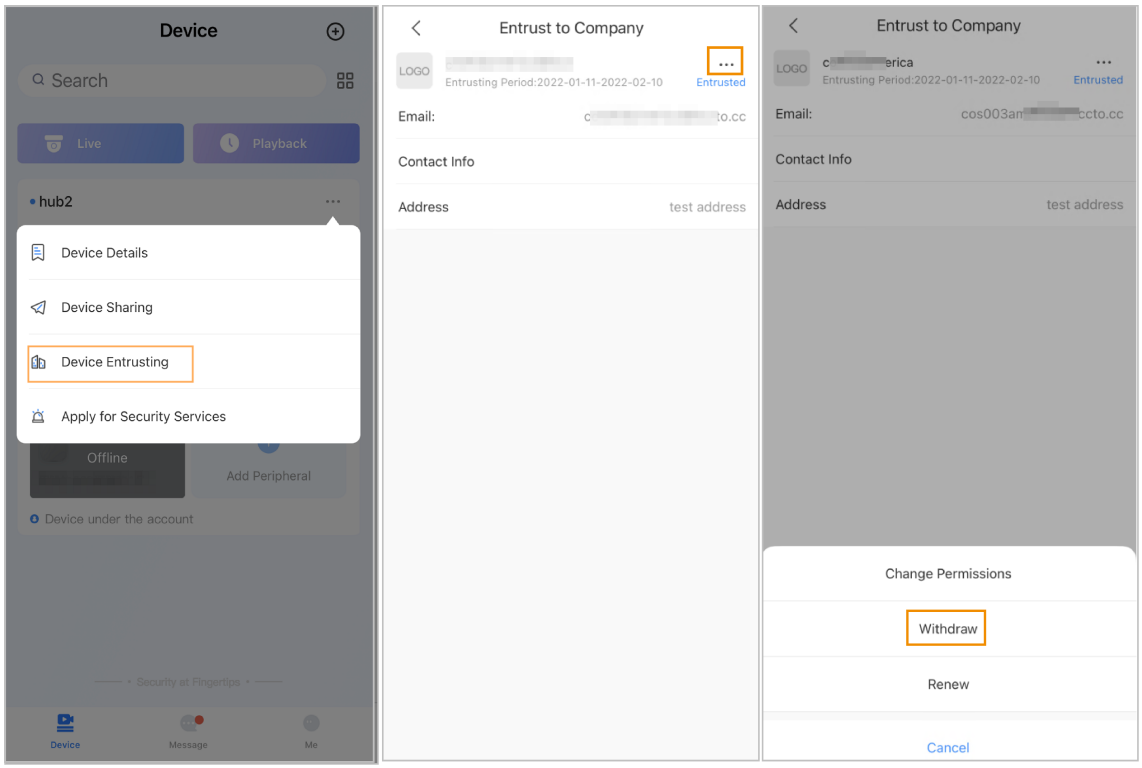
4.6.2.2 Canceling Entrusting the Application

For DMSS admin users, you can delete an installer by canceling the entrusting application.

Procedure

Step 1 On the **Device** screen, tap ••• next to a device, and then tap **Device Entrusting**.

Figure 4-16 Withdraw entrusting application



Step 2 On the **Device Entrusting** screen, select ••• > **Withdraw**, and then tap **OK**.

A message will be sent to the account of the installer. After the installer reads the message and approves your request to cancel the entrusting application in DoLynk Care, your application will be canceled.

4.6.2.3 Deleting Device

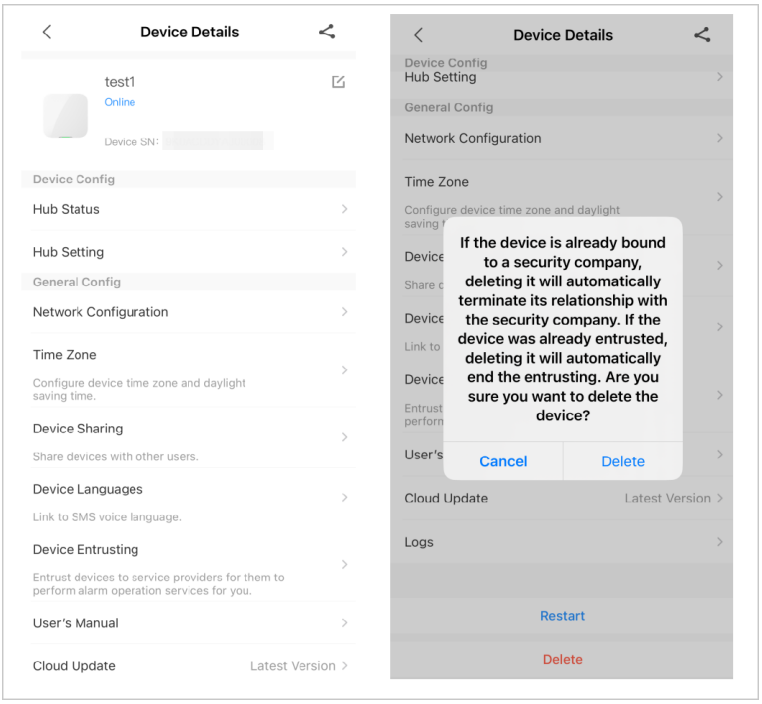
For DMSS admin user, you can delete both installers and DMSS general users by deleting devices.

DMSS admin user cannot delete an installer if the devices are shared by the installer.

Procedure

Step 1 On the **Device** screen, select ••• > **Device Details**.

Figure 4-17 Delete the device



Step 2 On the **Device Details** screen, tap **Delete**.

Step 3 Tap **Delete** to delete the devices.

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 hub before performing configurations.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Background Information

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

Procedure

Step 1 On the hub screen, tap **Peripheral** to add the peripherals. For details on adding the peripherals, see the user's 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 hub screen, tap **Area**.

Step 2 Tap an area, and then select from **Home** , **Away**, **Disarm**, and **disable** in the pop-up window.

- **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.
- **disable** : Close the current screen.

5.2 Global Arming and Disarming

Prerequisites

Make sure that you have enabled the **Global Arming/Disarming** function. On the hub screen, select > **Hub Setting**, and then enable **Global Arming/Disarming**.

Background Information

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

Procedure

Step 1 Go to the hub screen.

Step 2 Select from **Home** , **Away**, and **Disarm** on the upper screen.

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's 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 hub screen, select > **Hub Setting** > **Scheduled Arming/Disarming**.

Step 2 On the **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.

Appendix 1 Arming Failure Events and Description

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

No.	Reason	Description
1	ModuleLoss	The peripheral was offline.
2	HeartError	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	exOpen	The back cover of the external device was open.
6	Tamper	Peripheral tamper alarm was triggered.
7	LowBattery	Low battery of the device was detected.
8	PriPowerLoss	Peripheral main power failure was detected.
9	BatteryLoss	Battery failure was detected.
10	OverVoltage	Overvoltage was detected.
11	OverCurrent	Overcurrent was detected.
12	OverHeat	Overheat was detected.
13	FireAlarm	Fire alarm was triggered.
14	MedicalAlarm	Medical alarm was triggered.
15	SOS Alarm	SOS alarm was triggered.
16	PanicAlarm	Panic alarm was triggered.
17	Gas Alarm	Gas leak alarm was triggered.
18	IntrusionAlarm	Intrusion alarm was triggered.
19	HoldUpAlarm	Panic alarm was triggered.

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

No.	Reason	Description
1	SOSAlert	Panic alarm can be triggered through the DMSS app.
2	Tamper	Alarm hub tamper alarm was triggered.
3	Server Connect Error	The hub was offline.
4	SIAServer Connect Error	There is an error with the connection between the hub and the SIA alarm receiving center.
5	LowBattery	Low battery was detected.
6	MainLoss	Main power failure was detected.
7	BatteryLoss	Battery failure was detected.

No.	Reason	Description
8	NoGSM	2G/4G module errors was detected.
9	ATS Fault	Alarm transmission system fault was detected.
10	Cellular Network ATP Fault	Alarm transmission path fault (Cellular network failure) was detected.
11	Wired Network/Wi-Fi ATP Fault	Alarm transmission path fault (Wireless or Wi-Fi network failure) was detected.
12	AP Mode	AP mode fault was detected.

Appendix 2 SIA Event Codes and Description

Appendix Table 2-1SIA event codes and description

No.	Event	CID Code	Description
1	Motion Detected	130	Burglary Alarm.
		133	24 Hour (Safe) Alarm.
		134	Entry/Exit Alarm.
2	Opening Action Detected/Closing Action Detected	130	Burglary Alarm.
		133	24 Hour (Safe) Alarm.
		134	Entry/Exit Alarm.
3	External Contact was Opened/External Contact was Closed	130	Burglary Alarm.
		133	24 Hour (Safe) Alarm.
		134	Entry/Exit Alarm.
4	Duress Alarm	121	Duress Alarm.
5	Panic Button was Pressed	122	Panic Alarm (Silent).
		123	Panic Alarm (Udible).
6	Intrusion Alarm	130	Burglary Alarm.
		133	24 Hour (Safe) Alarm.
		134	Entry/Exit Alarm.
7	Fire Alarm	110	Fire Alarm.
8	Gas Leak Detected	151	Gas Detected Alarm.
9	Medical Alarm Button was Pressed	100	Medical Alarm.
10	Hold-up Button was Pressed	122	Panic Alarm (Silent).
		123	Panic Alarm (Udible).
11	Glass Break Detected	130	Burglary Alarm.
		133	24 Hour (Safe) Alarm.
		134	Entry/Exit Alarm.
12	Tilt Detected	130	Burglary Alarm.
		133	24 Hour (Safe) Alarm.
		134	Entry/Exit Alarm.
13	Shock Detected	130	Burglary Alarm.
		133	24 Hour (Safe) Alarm.
		134	Entry/Exit Alarm.
14	Tripwire Alarm/ Tripwire Alarm Stopped	131	Perimeter Alarm

No.	Event	CID Code	Description
15	Control Panel Lid was Opened/Control Panel Lid was Closed	137	Tamper.
16	Peripheral Lid was Opened/Peripheral Lid was Closed	137	Sensor tamper.
17	External Lid was Opened/External Lid was Closed	137	Sensor tamper.
18	Water Leak Detected / Water Leak Stopped	154	Water leakage.
19	Low Battery/Battery Level Restored	302	Low system battery.
20	Battery Fault/Battery Restored	311	Battery missing/dead.
21	Main Power Failure/ Main Power Restored	301	AC loss.
22	RF Jamming	344	RF Receiver jam detect.
23	Alarm Transmission System Fault/Restored	350	Communication trouble.
24	Alarm Transmission Path:Wire Network/Wi-Fi Fault/Restored	350	Communication trouble.
25	Alarm Transmission Path: Cellular Network Fault/Restored	350	Communication trouble.
26	Peripheral Connection Lost/Peripheral Connection Restored	355	Loss of supervision - RF.
27	Hub is Offline/ Hub is Online	356	Loss of central polling
28	Peripheral Low Battery/ Peripheral Battery Level Restored	302	Low system battery.
29	Peripheral Battery Fault/Peripheral Battery Restored	311	Battery missing/dead.
30	Peripheral Main Power Failure/Peripheral Main Power Restored	301	AC Loss.
31	RF-HD Connection Failed/RF-HD Connection Restored	354	Failure to communicate event.

No.	Event	CID Code	Description
32	Device Locked and Unlocked	501	Access reader disable.
33	Overvoltage Protection Triggered /Overvoltage Protection Restored	319	Power supply overvoltage.
34	Overcurrent Protection Triggered Overcurrent Protection Restored	312	Power supply overcurrent.
35	Overheat Protection Triggered/Overheat Protection Restored	318	Power supply overheat.
36	High Temperature/ Normal Temperature	158	High temp.
37	Low Temperature/ Normal Temperature	159	Low temp.
38	Armed	400 (App)	Open/Close.
		401 (Keypad)	O/C by user.
		403 (Scheduled arming)	Automatic O/C.
		407 (Keyfob)	Remote arm/disarm.
		408	Quick arm.
		409	Keyswitch O/C
39	Disarmed	400 (App)	Open/Close.
		401 (Keypad)	O/C by user.
		403 (Scheduled arming)	Automatic O/C.
		407 (Keyfob)	Remote arm/disarm.
		409	Keyswitch O/C
40	Home Mode Activated	441	Armed STAY.
		442	Keyswitch Armed STAY
41	Unsuccessful Arming	454 (Arming failure)	Failed to close.
		455 (Scheduled arming failure)	Auto-arm failed.
		457 (Exit delay arming failure)	Exit error (user).
42	Armed with Faults	450	Exception O/C.
43	Temporarily Deactivated/ Reactivated	502	Temporarily deactivated.

No.	Event	CID Code	Description
44	Temporarily Disabled Notifications for the Lid /Enabled Notifications for the Lid	503	Temporarily disabled.
45	Test Report was Manually Triggered	601	Manual trigger test report.
46	Periodic Test Report	602	Periodic test report.

Appendix 3 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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

More information

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

ENABLING A SAFER SOCIETY AND SMARTER LIVING

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