Alarm Hub 2

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO.LTD. V1.1.2

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.
	Class II equipment

Revision History

Version	Revision Content	Release Time
V1.1.2	Add new functions and revised SIA event codes.	December 2024
V1.1.1	Revised technical parameters.	June 2024
V1.1.0	Revised hub configuration.	April 2024
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.
- Risk of fire or explosion if the battery is replaced by an incorrect type.

- 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.
- Connect the control panel near an easily accessible socket.

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	
	Area	32 areas (rooms)	
	User Management	Functions can be shared by the app users. These include 33 app users (31 general users, 1 admin user and 1 installer) and 32 keypad 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	

Type	Parameter	Description	
	Wi-Fi	2.4 G	
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.	
	Operating Temperature	When battery is not charging: –10 °C to +55 °C (+14 °F to +131 °F) When battery is charging: 0 °C to +45 °C (+32°F to +113 °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	DHI-ARC3800H-FW2(868)/ DHI-ARC3800H-W2(868): EN 50131-1:2006+A1:2009+ A2:2017+A3:2020 EN 50131-3:2009 EN 50131-6:2017+A1:2021 EN 50131-5-3:2017 EN 50131-10: 2014 EN 50136-2: 2013+A1:2023 Security Grade 2 (IMQ-SISTEMI DI SICUREZZA) Environmental Class II ATS category: SP2/DP2 CE Certification IMQ-SISTEMI DI SICUREZZA is mandatory manage system with APP DMSS for access level 2, and DoLynK Care for access level 3	DHI-ARC3800H-FW2/ DHI-ARC3800H-W2: CE
	Anti-corrosion Level	Basic Protection	

Type	Parameter	Description
	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, +10% -15%, 50/60 Hz, 0.4A Class II equipment
	Battery Capacity	3.7 V/4750 mAh
	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	1.3 A
	Power Consumption	220 VAC 80 mA(Max) 220 VAC 40 mA(Standby)
	Current Consumption	Normal: 370 mA; alarm: 440 mA
	Battery Low Threshold	3.5 VDC
	Battery Restore Threshold	3.675 VDC
	Release Voltage	< 3 V
	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

Type	Parameter	Description
	Primary Transmission Path	LAN /Wi-Fi (NO 50136-2)
	Secondary Transmission Path	GPRS/4G
	Notification Equipment	C/E/F B/E for DHI-ARC3800H-W2(868)

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
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 Category	Reporting Time	Protocols	Communication Devices			Communication Device to be Used
			PSTN	2G/3G	IP	

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.

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

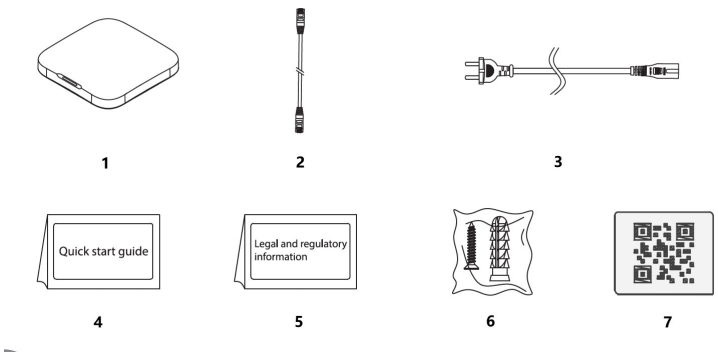


Table 1-3 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Alarm Hub 2	1	5	Legal and regulatory information	1

No.	Item Name	Quantity	No.	Item Name	Quantity
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

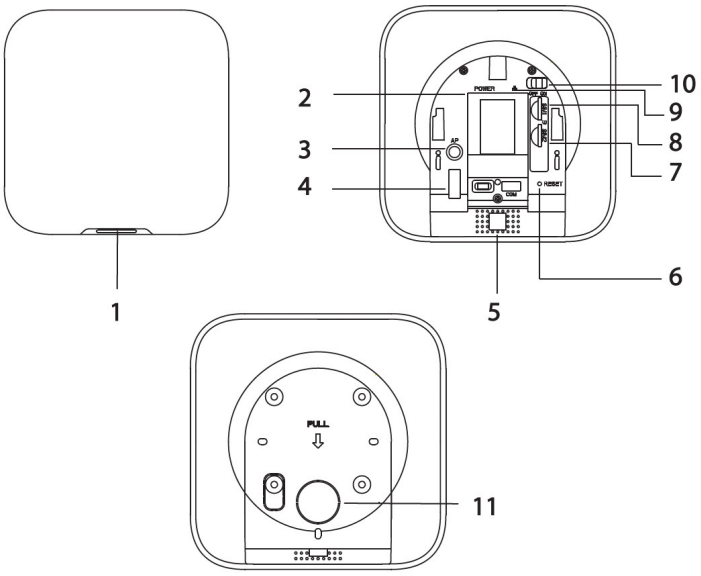


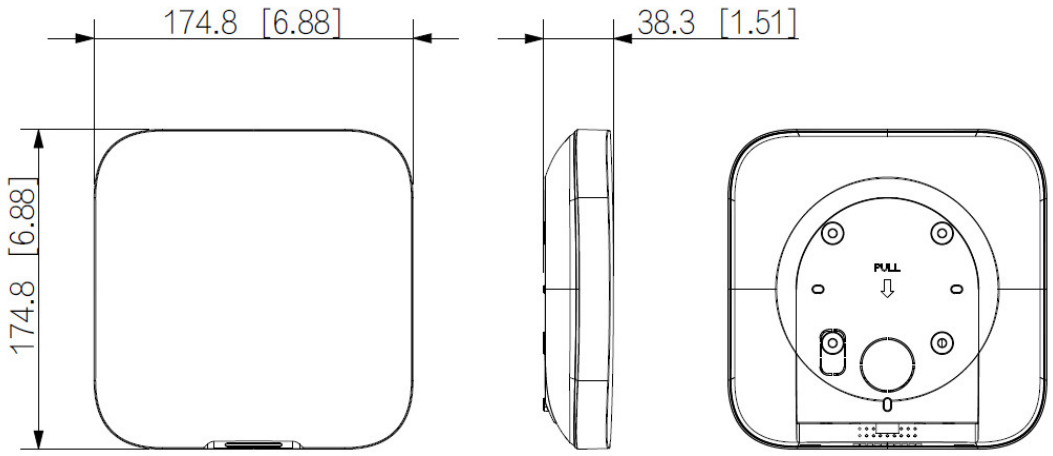
Table 2-1 Structure

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.

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

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)

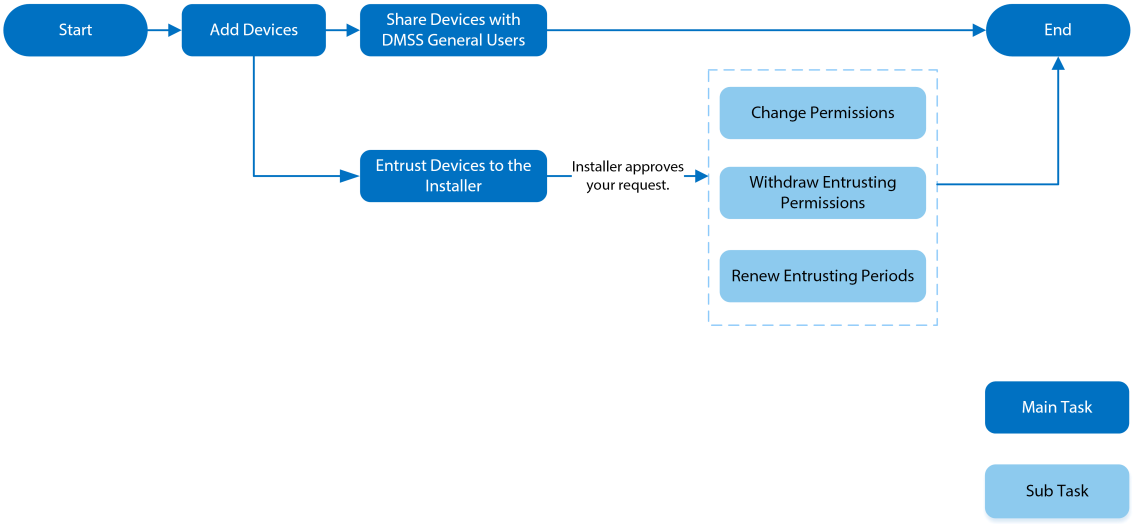
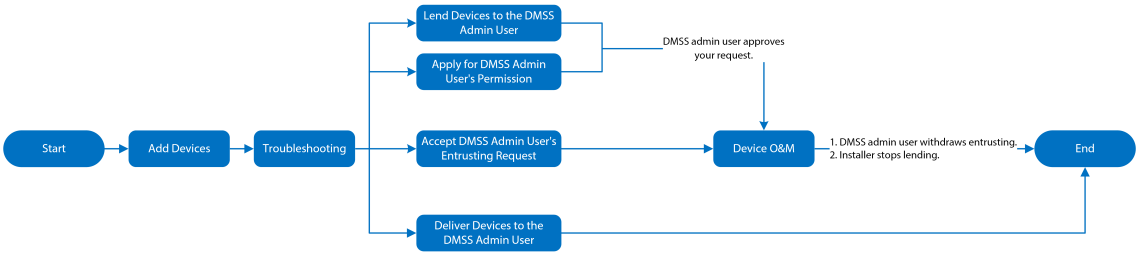


Figure 3-2 Business flow (Installer)



3.2 Operation Process

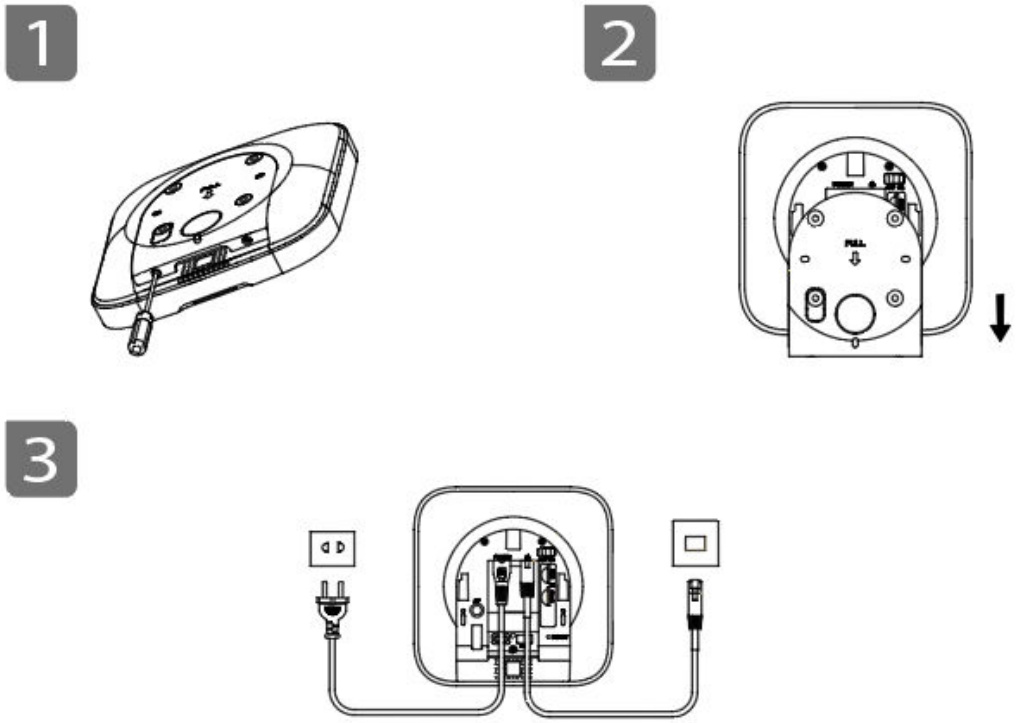
Follow the procedures below to turn on the wireless alarm system.

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

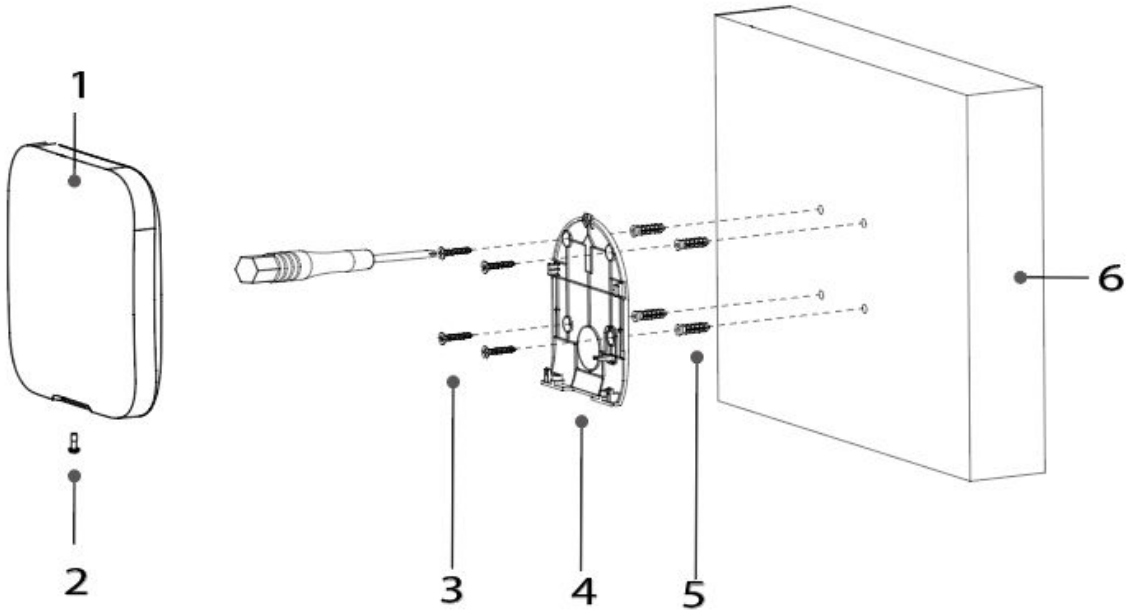


Table 3-2 Installation items

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 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.

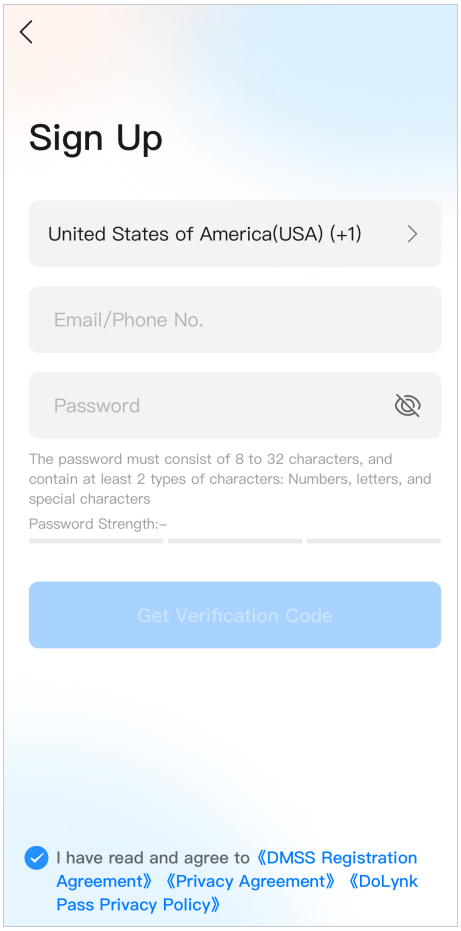
Step 3 Create an account.

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 DoLynk Pass Privacy Policy**.
5. Tap **Get Verification Code**, check your email box for the verification code, and then enter the code.

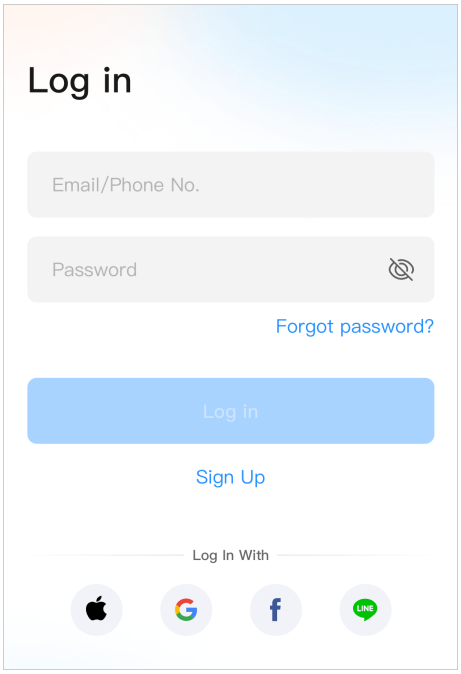
   Use the verification code within 60 seconds of receiving it. Otherwise, the verification code will become invalid.
6. Tap **OK**.

Figure 4-1 Sign up



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

Figure 4-2 Login



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

4.2 Adding Devices

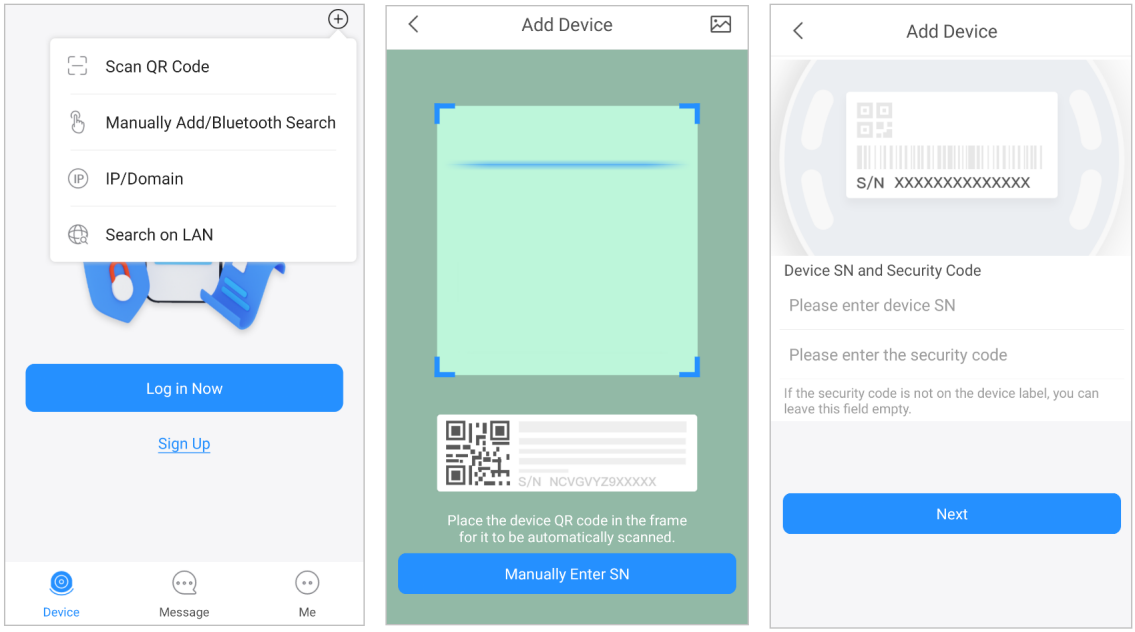
For end users, you can add alarm devices to DMSS app.

4.2.1 Adding the Hub

Procedure

Step 1 On the **Device** screen, tap ⊕, and then select **Scan QR Code**.

Figure 4-3 Add by 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**.

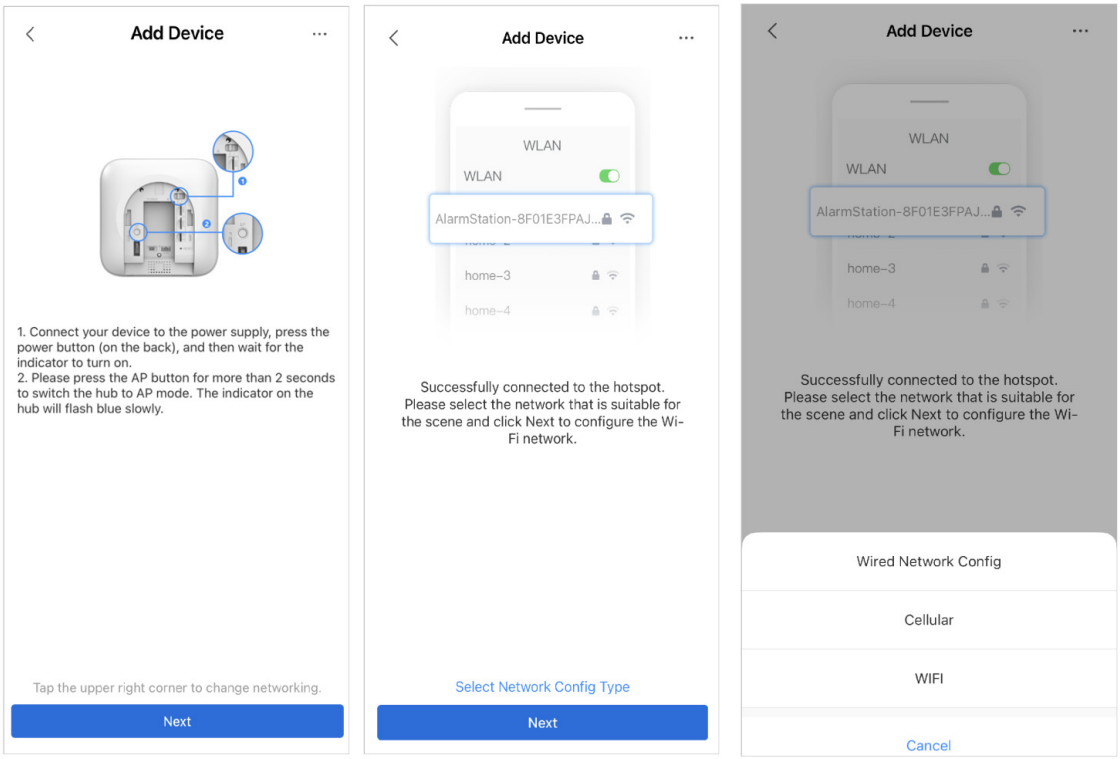
Step 5 Configure network settings.

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 4-4 Configure network types



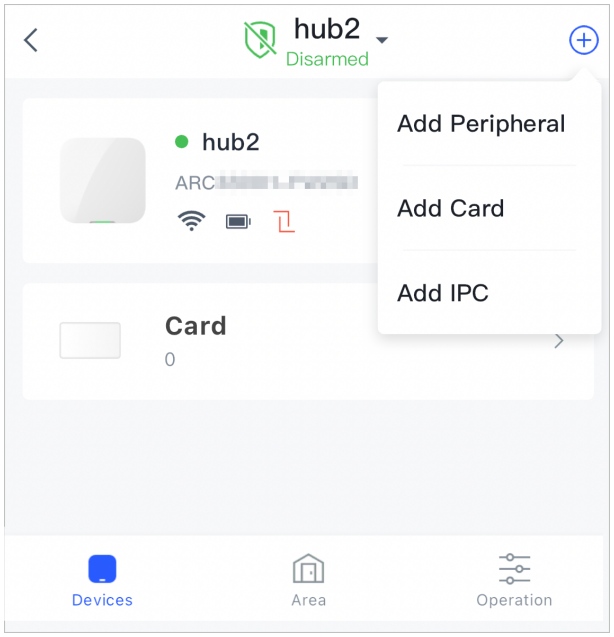
4.2.2 Adding Peripheral

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 **Devices** screen of the hub, and then select ⊕ > **Add Peripheral**.

Figure 4-5 Add peripheral



Step 2 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**.

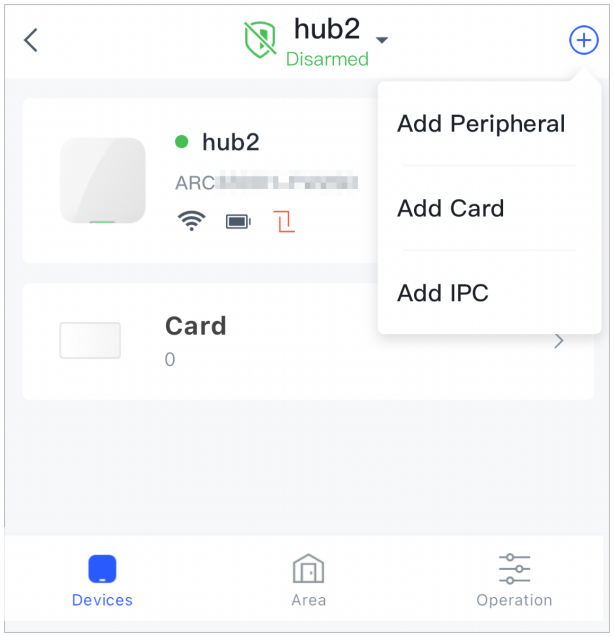
4.2.3 Adding IPC

Add IPCs to the hub.

Procedure

Step 1 Go to the **Devices** screen of the hub, and then select ⊕ > **Add IPC**.

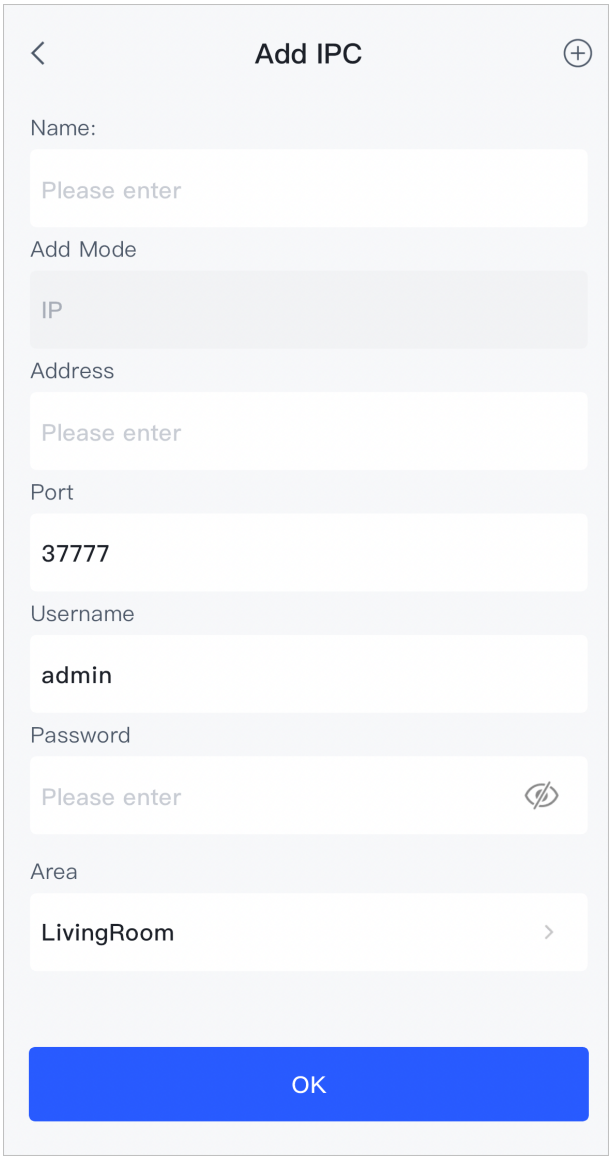
Figure 4-6 Add IPC



Step 2 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, and then tap **OK**.

Figure 4-7 Manually add

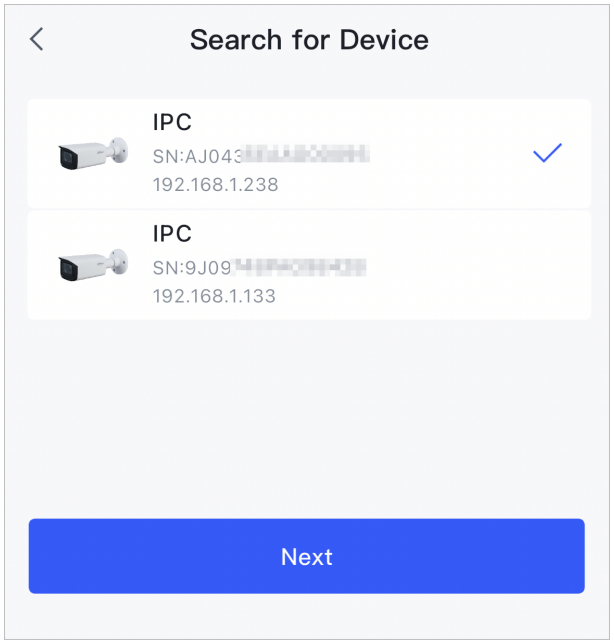


2. Select the channel of the IPC, and then tap **OK**.

- Online search:

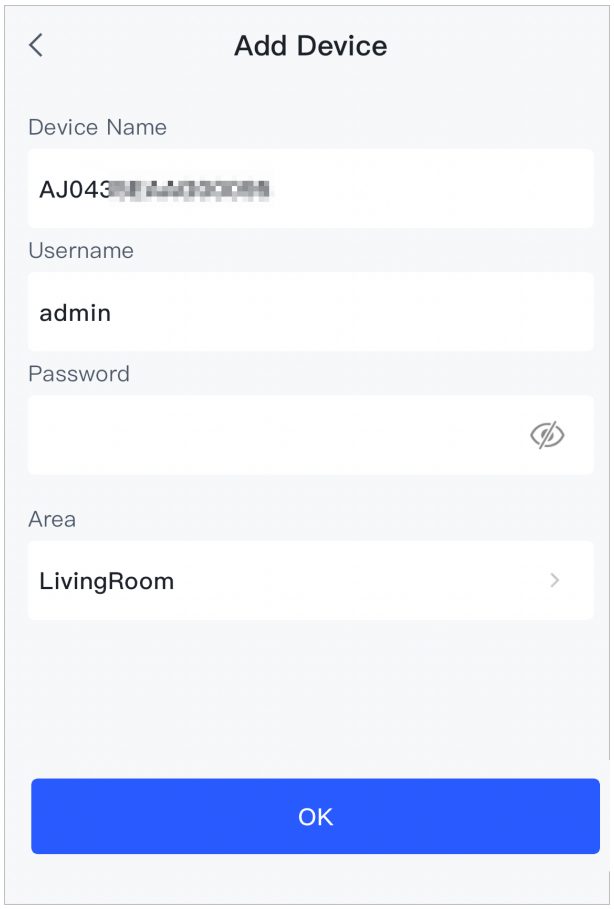
1. Tap ⊕ and select **Search on LAN** to search for the IPC in the same network segment.

Figure 4-8 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 4-9 Enter password



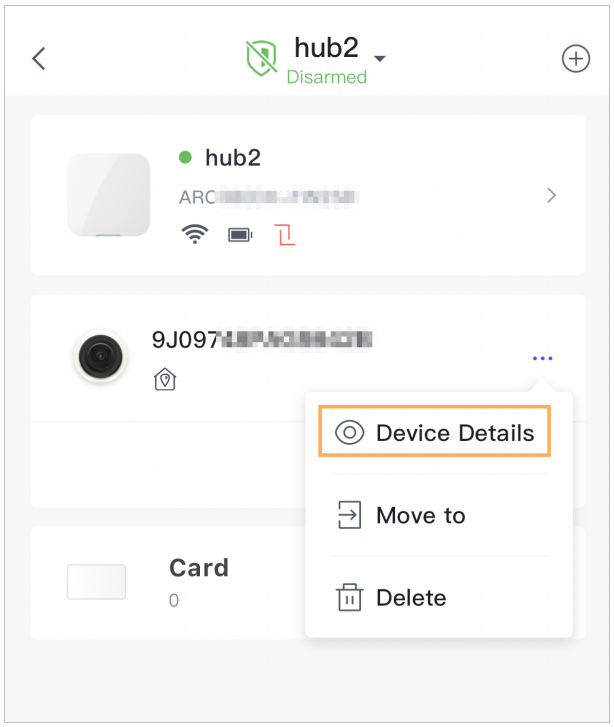
4. Select the channel of the IPC, and then tap **OK**.

Related Operations

You can configure the parameters of the added IPC.

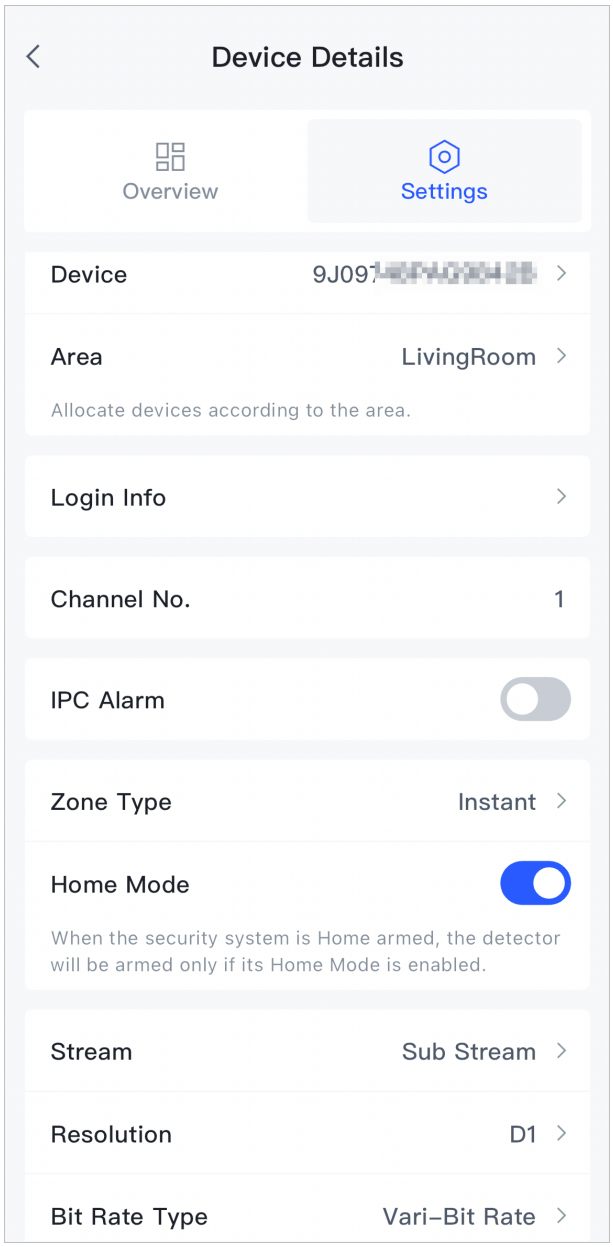
1. Select **Device Details** of the IPC.

Figure 4-10 Device details



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

Figure 4-11 Configure parameters



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.

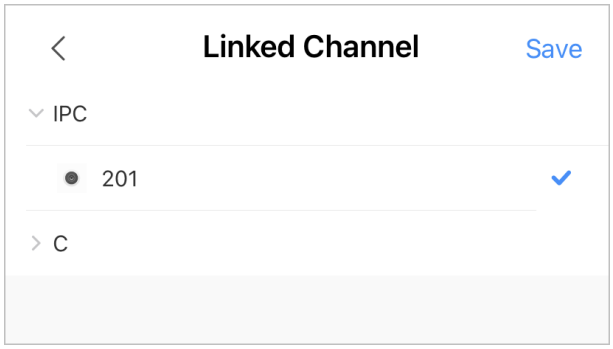
Procedure

Step 1 On the **Device** screen of the hub, select a peripheral, and then go to **Device Details** > **Settings** to configure the parameters.

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

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

Figure 4-12 Linked channel



4.4 Hub General Settings

You can view and edit basic device information.

Procedure

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

Table 4-1 Parameter description

Parameter	Description
Devices	• View name, type, SN and device model of the hub. • Edit device name, and then tap **Save** to save configuration.
Hub Setting	Configure parameters of the hub.
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 hub operates. • **DST** : Select date or week, and then select start time and end time.
Language	Select the language linking to SMS voice. It supports Polish, Greek, and Bulgarian languages. The voice broadcast and phone call broadcast functions support Turkish, Polish, Greek, Spanish (Latin American), Russian, and Bulgarian languages.
User's Manual	Tap **User's Manual** to obtain the user's manual of the alarm hub.
Firmware Update	Update online. Update is not allowed when the hub 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.

4.4.1 Viewing Hub Status

On the **Devices** screen of the hub, select a hub, and then select **Status** to view the hub status.

Table 4-2 Status

Parameter	Description
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 the remaining electricity of the battery in the form of percentage.
Tamper	This is the anti-tamper function for the peripheral. The hub reacts when a peripheral is disassembled.
Main Power Status	Show main power status.
LTE Connection Status	Internet connection status of the hub via SIM card, Wi-Fi, and Ethernet. Displays **Connected** or **Disconnected**.
Wi-Fi Connection Status	
Network Cable Connection Status	

Parameter	Description
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.
Firmware Version	The program version of the hub.

4.4.2 Configuring the Hub

Procedure

Step 1 On the **Devices** screen of the hub, select the hub.

Step 2 Select **Settings** > **Hub Setting** to vie wand edit general information of the hub.

Table 4-3 Hub parameter description

Parameter	Description
Back Up Configuration	After being enabled, the hub configuration will be backed up regularly.
User Manager	You can add, modify, or delete app or keypad users when it is disarmed. ● **Keypad User** : Tap **Add** to add a keypad user. Enter username, 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.

Parameter	Description
SOS Alarm	Configure SOS alarm types, including panic alarm, link to siren, medical alarm, medical alarm and fire alarm. After configuration, tap **SOS** on the **Operation** screen of the hub 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.
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.
Doorbell Sound Config	• 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. • Alarm Sound Duration: Configure the duration for the sound. • Entering/Exiting Delay Time and Arming/Disarming Ringtone: Enable the function so that the ringtone will be applied in these scenarios.
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.

Parameter	Description
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: ◇ App Intercom: Intercom between the siren and DMSS app. Select the siren assigned to different areas, or select **Do Not Link**. ◇ SIP Intercom: Intercom between the siren and third party platform. ○ Select the siren for intercom. Selection filtered by siren and area are both supported. ○ SIP Server Config： ● Username/Password: Subject to configuration in third-party platform. ● SIP Server Address: Enter the IP address of the third party platform. ● SIP Server Port/Local Port: Be consistent with port number of third party platform. ● Registration Status: Displays the status for whether the SIP is configured 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.
Import Configuration	You can transfer the configuration from one hub to another of the same model. After being imported, the existing entrusting, borrowing, or security services relationships will not be retained. Proceed with caution. You must enable **Backup Configuration** before importing configuration.
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. ◇ Masking from detects are manage as Fault conditions, it is not permitted active WD in Unset conditions. ◇ 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/Domain, port and device ID, and then you can register the hub to the DSS Pro or Converter.

Parameter	Description
Alarm Receiving Center	Select Alarm Receiving Center 1 or 2, and go to the respective configuration screen. Enable the function, and then configure parameters. ● **Communication Protocol** : Select from **SIA-DC-09(SIA-DCS)**, **SIA-DC-09(ADM-CID)**,**SIA-DC-09(ADM-CID Mexico)**,**Softguard** and **Private**. ● **Preferred IP Address/Domain Name** : Enter the IP/domain address and port number of the ARC. ● **Alternative IP Address/Domain Name** : Enter the alternative IP/domain address and port number of the ARC. ◇ Messages will be sent to the alternative IP/domain address only when the preferred IP address fails to receive the message. ◇ If **Heartbeat interval** is enabled, the system will judge whether to send the message to the preferred or alternative IP address. ● **IP Protocol** : Select **TCP** by default. ● **Heartbeat Interval** : Set the heartbeat interval with the range from 0 second to 24 hours (60 seconds by default). 0 seconds means **Heartbeat interval** is disabled. ● **Central Account** : Enter the account number that created by the ARC, which is to be used to identify the hub when the hub sends information to the ARC. ● **Reupload Period** : Select the reupload period from the list. ● **Encryption** : The hub uses an encryption format for information security when you configure the ARC. **AES128** is set by default. ● **Upload Events** : Tap next to an event to upload it. ◇ **Alarm** : Alarm message. ◇ **Errors** : Power failure, battery under-voltage, tamper, and offline. ◇ **Events** : Prohibit the use of peripherals, add or delete peripherals, and add or delete users. ◇ **Arming/Disarming** : Message notifications of arming and disarming the system. ● **Communication Test** : Supports **Manual Test** and **Scheduled Test**. ◇ **Manual Test** : Manually test whether the parameters of the preferred and alternative alarm centers are normal. If the test is successful, the center can receive the test event. ◇ **Scheduled Test** : Scheduled test is disabled by fault. After enabling, the hub reports periodic test event regularly. 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).

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.
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.

Parameter	Description
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.
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.

4.6 Managing Devices

4.6.1 Entrusting Devices

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.

4.6.1.1 Entrusting Devices in Batches

You can entrust devices to the service provider in batches.

Prerequisites

You have bound with a service provider.

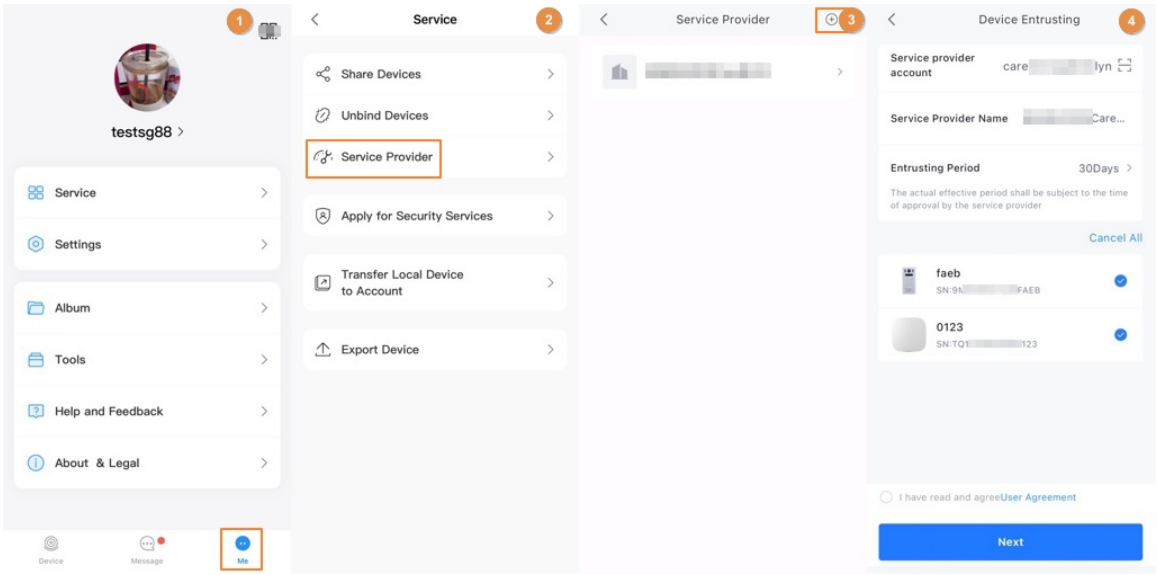
Procedure

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 DoLynk Care. The process for entrusting multiple devices is the same as entrusting a single device.

Figure 4-13 Entrust devices in batches



4.6.1.2 Entrusting Device One by One

You can entrust a device to DoLynk Care users. You can configure the permission 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 Entrusting**.

Step 2 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 3 Select entrusting periods and permissions, and then tap **OK**.

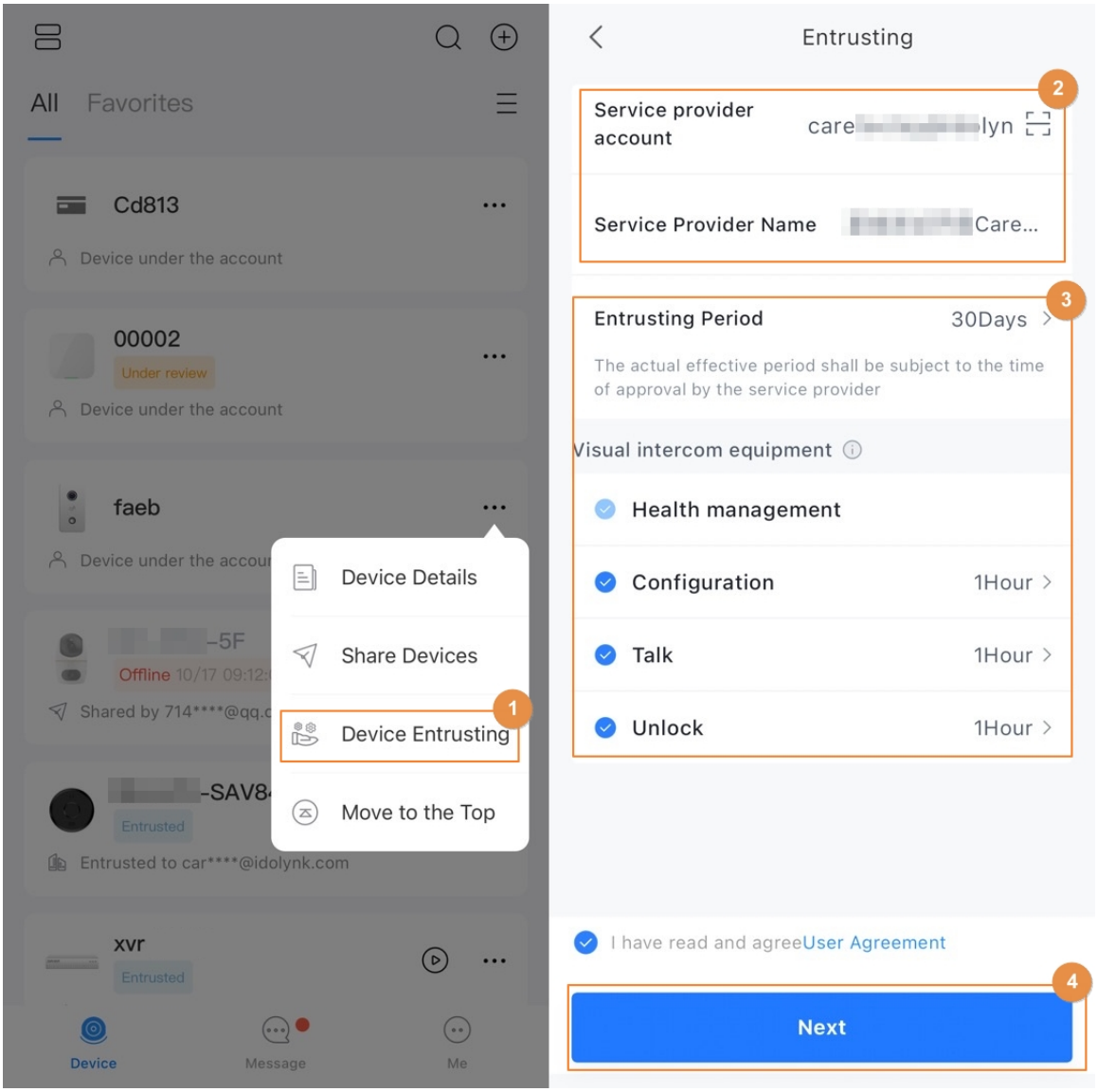
Table 4-6 Instruction of permissions

Permission	Description	Note
Health Management	Select 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 permission: Including restart and upgrade the device, format SD card and configuration plug-in. ● Live video and playback: View the live video, playback the recordings and the 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 permission: 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 permission: 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 4 Read and select **I have read and agree User Agreement** , and then tap **Next**.

Figure 4-14 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

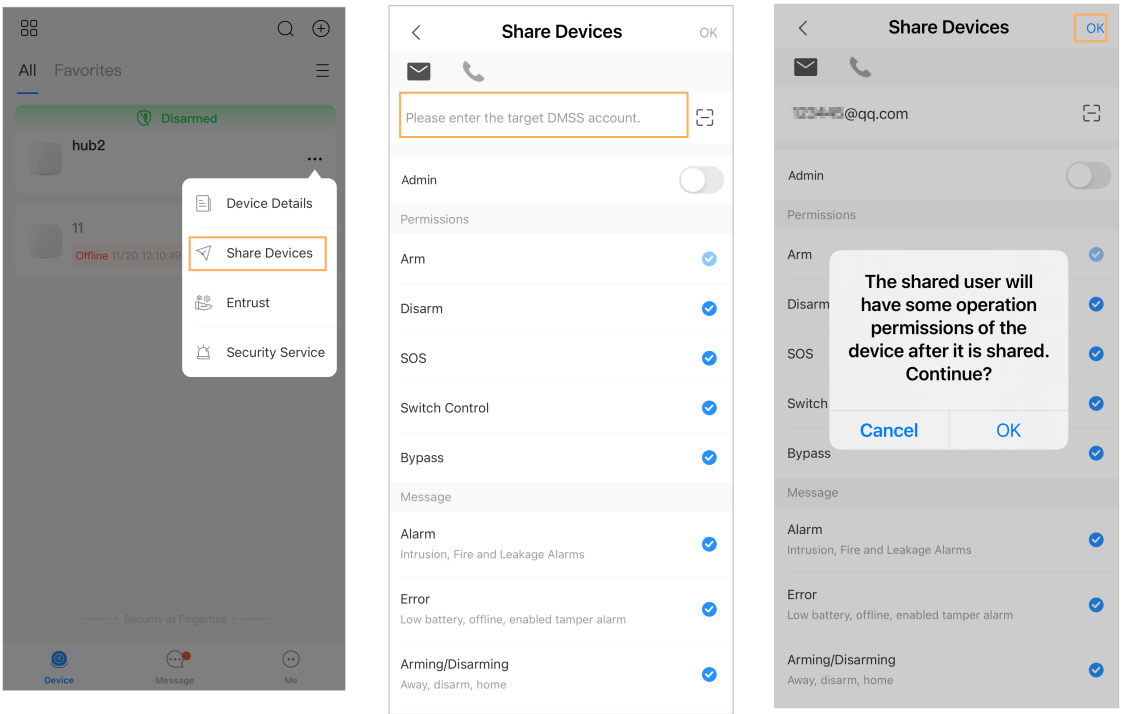
- To change permissions, go to the **Entrust to Company** screen, and then tap **Change Permissions**.
- To withdraw entrusting permissions, go to the **Entrust to Company** screen, and then tap **Withdraw**.
- To renew entrusting periods, go to the **Entrust to Company** screen, and then tap **Renew**.

4.6.2 Sharing Devices

Procedure

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

Figure 4-15 Share device



Step 2 On the **Share Devices** 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 **Share Devices** screen.

4.6.3 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 Select **Me** > **Service** > **Unbine Devices**.

Step 2 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.

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.

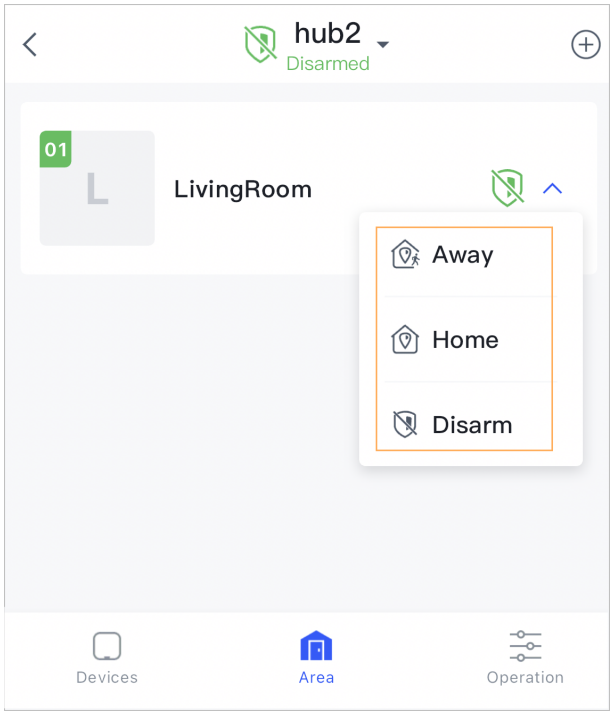
Procedure

Step 1 On the hub screen, tap **Area**.

Step 2 Tap 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.

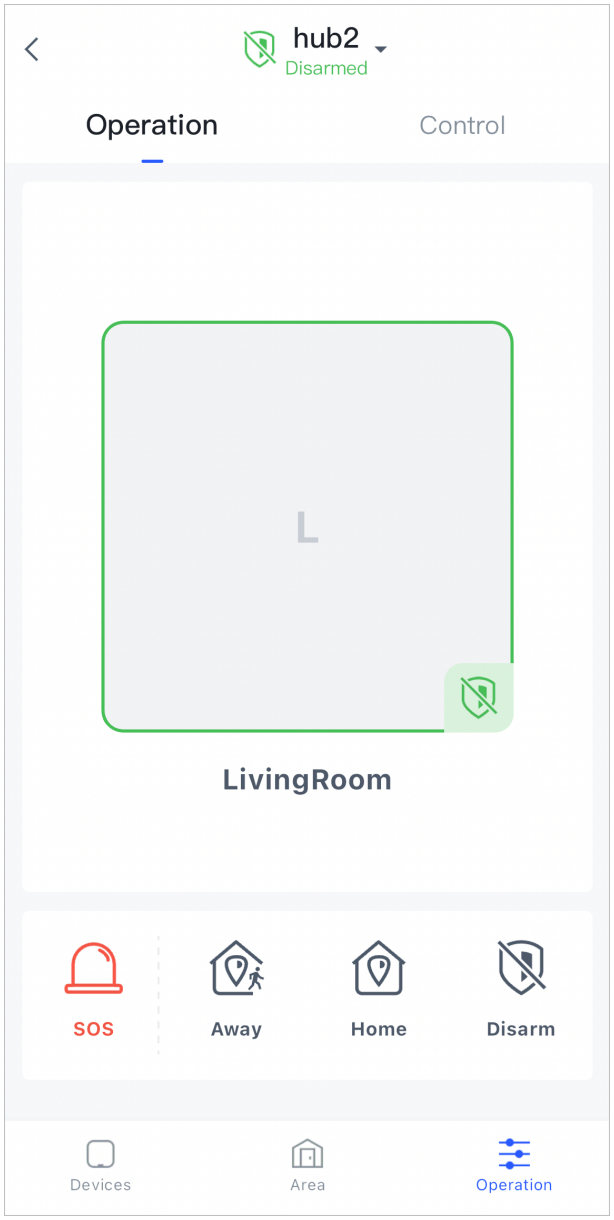
Procedure

Step 1 On the **Operation** screen of the hub, 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'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

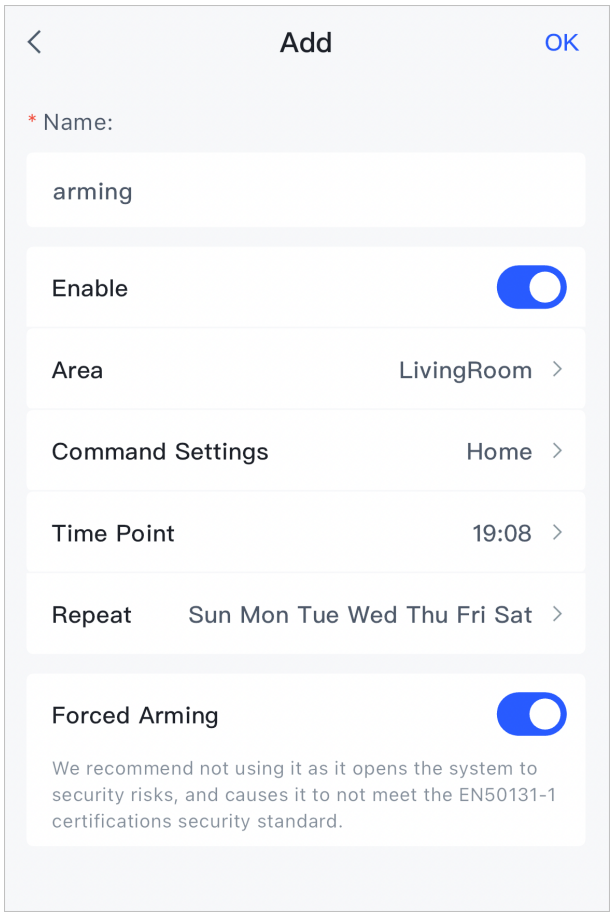
Step 1 On the hub screen, select **Device Details** > **Settings** > **Hub Setting**.

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



Step 3 Tap **OK**.

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	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 Primary ATP Fault Secondary ATP Fault
46	ATS Restored	3350	NR	ATS Restored Primary ATP Restored Secondary ATP 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	Armed
56	Armed By APP	3400	CQ	Disarmed
57	Disarmed By Keypad	1401	OP	Armed
58	Armed By Keypad	3401	CL	Disarmed
59	Disarmed By Schedule	1403	OA	Armed
60	Armed By Schedule	3403	CA	Disarmed
61	Cancel	1406	BC	Cancel
62	Disarmed By Keyfob	1407	OS	Armed
63	Armed By Keyfob	3407	CS	Disarmed
64	Quickly Armed	3408	CS	Armed
65	Disarmed By KeySwtich	1409	OS	Armed
66	Armed By KeySwtich	3409	CS	Disarmed
67	Home Mode Activated	3441	NL	Home Mode Activated
68	Home Mode Activated By KeySwtich	3442	NL	Home Mode Activated
69	Armed With Faults	3450	CF	Armed With Faults
70	Unsuccessful Arming	1454	CI	Unsuccessful Arming
71	Unsuccessful Arming By Schedule	1455	CD	Unsuccessful Arming

No.	Event	Original Code	SIA Code	Description
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

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;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

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

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

2. **Update client software in time**

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

Physical Protection

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

ENABLING A SMARTER SOCIETY AND BETTER LIVING

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