DMSS App

User's Manual

V1.3.0

Foreword

General

This manual introduces the functions and operations of DMSS App (hereinafter referred to as "the App").

Software Version

V1.90.000.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
⚠️ **DANGER**	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠️ **WARNING**	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠️ **CAUTION**	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
⚠️ **TIPS**	Provides methods to help you solve a problem or save you time.
📖 **NOTE**	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.3.0	Added illumination settings function. Upgraded "5 Video Call". Added function of entrusting device in batches. Added account upgrading function. Upgraded "2.3.11.1 Sharing Devices". Added IPC external alarm in "10.1 Subscribing Alarm Messages".	April 2021
V1.2.0	Updated "1 Overview", "2.3.10 Sharing and Entrusting Devices", "3 Live View", "5 Video Call", "7 Access", "8 Alarm Control", ,"10.2 Viewing Messages", "11System Configuration and Account Management". Updated images. Deleted cloud storage, and FAQ.	January 2021

V1.1.0	Reorganized manual structure. Updated and optimized descriptions for all chapters. Updated images.	January 2020
V1.0.0	First release.	July 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Night Light Inc.

Table of Contents

1 Overview

1.1 Introduction

DMSS App is a mobile monitoring software that is designed for professional security surveillance. It has functions such as live view, video playback, alarm notification push, and alarm control. Various devices can be added and used with cellular data or Wi-Fi, such as cameras, video recorders, video intercoms, doorbells, access control devices, and alarm devices.

1.2 Applicable Smartphone

- Android 9.0 or later.
- iOS 5.0 or later.

2 Basic Operations

You can do the operations such as live view, video playback, remote configuration, push notifications, video talk, and more.

You can use the App after logging in or use it without logging in, and the functions and types of added devices (divided as account devices and local devices) might vary. For example, cloud storage and cloud upgrade are available only after login. This manual takes operations after login as an example.

Interfaces might vary with different added devices.

Account Device

Account devices have following features:

- Added after login.
- Have "From ***" below the device name.

Figure 2-1 Account device

- Bound to the account, cannot be used after logout, and cannot be added by other accounts, but can be shared with other users.

Local Devices

Local devices have following features:

- Added without login, or added after login but does not have "From ***" below the device name.
- Can only be used on the current mobile phone, cannot be shared, but can be added on multiple mobile phones.

2.1 Login

2.1.1 Logging in to the App

Step 1 Search for DMSS in Google play or Apple store, download, and then install the App.

<u>Step 2</u> On your mobile phone, tap 🔵.

<u>Step 3</u> Select your region, and then tap **Done**.

⊙━━

You can change your region in **Me > Change Region**.

<u>Step 4</u>   Read **User Service Agreement and Privacy Policy**.

<u>Step 5</u>   Tap **Sign up**, enter email address and password, select **I have read and agree to**, and then tap **Get verification code**.

📖

Support Thailand phone number registration.

<u>Step 6</u>   Enter verification code and then tap **Log in**.

<u>Step 7</u>   Tap **Home**.

Figure 2-2 Home
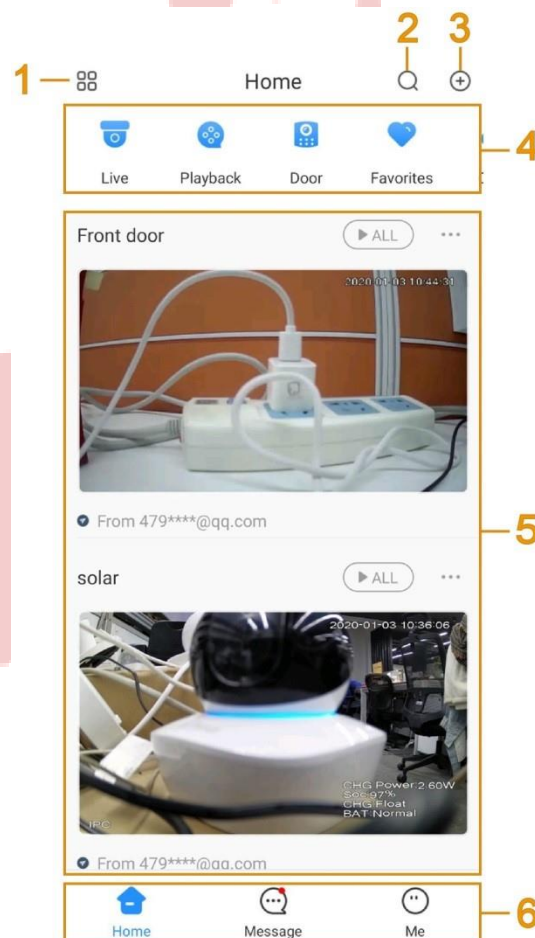
Table 2-1 Home interface descriptions

No.	Function	Description
1	Display mode	Tap 🔲 to switch between displaying devices in list mode or picture mode.
2	Search	Tap 🔍 to search devices or channels with keywords.
3	Add devices	Tap ⊕ to add devices.

No.	Function	Description
4	Function modules	Display the main function modules. Tap and drag the icon to change its place.
5	Devices	Display the added devices. Tap a thumbnail under the device name to play a single channel. If a device has several channels, slide thumbnails to the left to view more. Tap ▶ALL to play all channels under this device. Tap ••• to view device details and top the device or move down.
6	Navigation bar	Three tabs: **Home**, **Message**, and **Me**.

2.1.2 Upgrading Account

When the system prompts a note on the **Home** interface for account upgrading after you logging in to the App, you need to upgrade the account; otherwise you cannot enjoy all functions.

After upgrading the account, the original device sharing link will become invalid. If you want to enjoy this service again, establish the sharing again.

Step 1   Click **To Upgrade** to go to the upgrading interface.

Step 2   Click **Upgrade** on the upgrading interface.

Step 3   Enter the password to start upgrading.

2.2 Adding Devices

Before operating on the App, you need to add devices such as cameras, video recorders, video intercoms, alarm devices, and access control devices.

Before adding devices, make sure that the device is connected to power and network.

- Wi-Fi connection: Connect the device to the same Wi-Fi as the mobile phone.
- Wired connection: Connect the device to the same network as the mobile phone.
- AP configuration: Turn on device hotspot, and connect the mobile phone to the hotspot.

2.2.1 Adding Uninitialized Devices

You need to initialize the device for the first-time use or after it is reset.

- Uninitialized devices can only be added through scanning device QR code, or manually entering device SN.
- The on-screen instructions might vary depending on the device that you add, and might differ from the actual interface.

2.2.1.1 Adding through Wi-Fi

You can add uninitialized wireless camera through Wi-Fi.

Step 1 On the **Home** interface, tap ⊕, and then select **SN/Scan**.

Step 2 Scan device QR code, or manually enter device SN, and then the system will identify the device type automatically.

📖

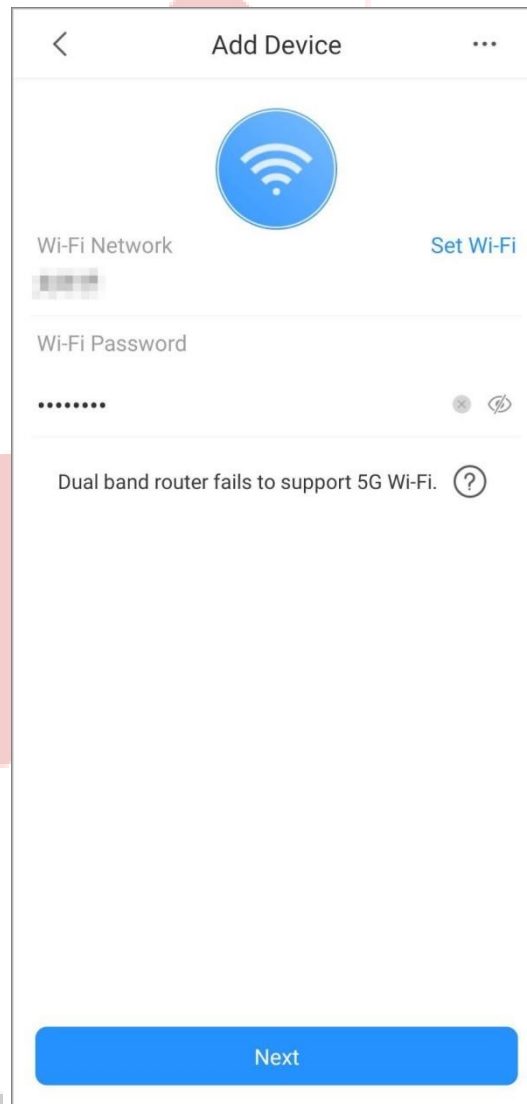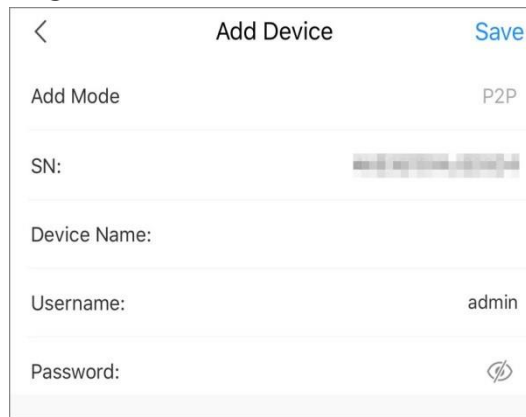If the device type cannot be identified by the system, you need to select the device type.

Step 3 Follow on-screen instructions to connect the device, and then tap **Next**.

Step 4 Enter the Wi-Fi password connected by the mobile phone, and then tap **Next**.

🔑

Tap ••• at the upper-right corner to switch network configuration by Wi-Fi, wire, or AP.

Figure 2-3 Enter Wi-Fi password

Step 5 Set device username, device password, enter email address as needed, and then tap **OK**.

Step 6 On the **Cloud Update Configuration** interface, read **Cloud Access** and **Auto-check items**, select them as needed, and then tap **OK**. The device is initialized.

📖

The **Cloud Update Configuration** only displays when you add uninitialized devices.

Step 7 Enter device name, and then save settings.

Step 8 Configure time zone as needed, and then tap **Completed**.

📖

Time zone configuration is available on account devices.

2.2.1.2 Adding through Wired Network

You can add uninitialized wired camera through wired network.

Step 1　Connect the Ethernet cables to the appropriate sockets.

Step 2　Go through step 1 to step 2 in "2.2.1.1 Adding through Wi-Fi ".

Step 3　Tap ●●● at the upper-right corner and select Switch to wired network configuration to connect to the wired network.

Step 4 Follow on-screen instructions to initialize and add the device. For details, see step 5 to step 8 in "2.2.1.1 Adding through Wi-Fi ".

2.2.1.3 Adding through AP Configuration

You can add uninitialized wireless device through AP configuration. This section takes a wireless alarm hub as an example.

Step 1　Go through step 1 to step 2 in "2.2.1.1 Adding through Wi-Fi ". Flip

Step 2　the DIP switch of the hub from STA to AP to configure AP.

　　　📖

　　　The indicator flashes blue.

Step 3　Search for the hub hotspot, tap **Join** to connect to the hub hotspot.

Step 4　Set device username, device password, enter email address as needed, and then tap **OK**.

Step 5　Go through step 5 to step 6 in "2.2.1.1 Adding through Wi-Fi " to complete initialization.

Step 6　Search for nearby Wi-Fi available, and then enter Wi-Fi password. Turn

Step 7　off AP on the hub, and then wait for network configuration.

Step 8　Follow on-screen instructions to add the device. For details, see step 7 to step 8 in "2.2.1.1 Adding through Wi-Fi ".

2.2.2 Adding Initialized Devices

You can add initialized devices through scanning device QR code, manually enter device SN, entering IP/domain, or searching online devices. This section takes adding an initialized wireless camera as an example.

2.2.2.1 Adding by SN/QR Code

You can add device by scanning device QR code or manually entering device SN.

Step 1 On the **Home** interface, tap ⊕, and then select **SN/Scan**.

Step 2 Scan device QR code, or manually enter device SN, and then the system will identify the device type automatically.

　　　📖

　　　If the device type cannot be automatically identified by the system, you need to select the device type.

Step 3 Enter device name, device password, and save settings.

Figure 2-4 Add initialized device (SN/scan)

2.2.2.2 Adding by IP/Domain
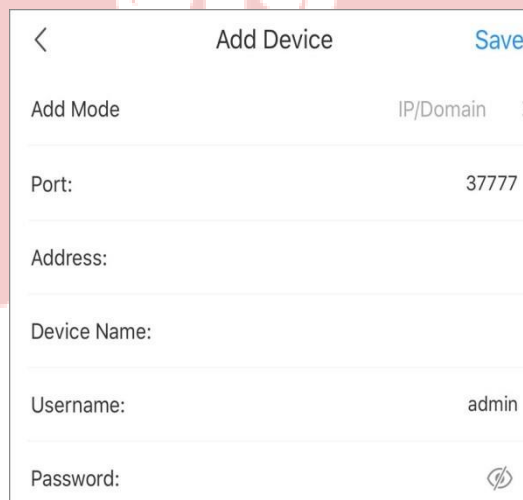
You can add devices by entering IP of the device or specific domain. This section takes entering device IP as an example.

Step 1 On the **Home** interface, tap ⊕, and then select **IP/Domain**.

Step 2   Select the device type.

Step 3   Enter information as needed, and then save settings.
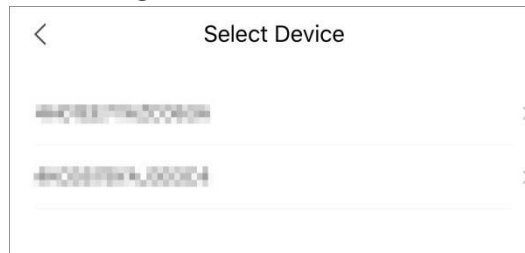
Figure 2-5 Add initialized device (IP/domain)

2.2.2.3 Adding by Search

You can search online devices and add them.

Step 1 On the **Home** interface, tap ⊕, and then select **Search online**.

Figure 2-6 Select device SN

Step 2   Tap the device SN as needed.

Step 3   Select the device type.

Figure 2-7 Add initialized device (search online)
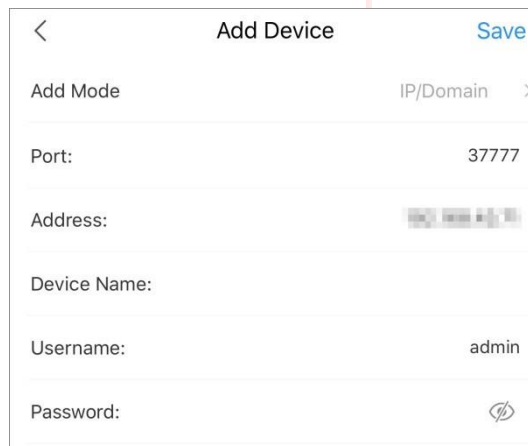
Step 4 Enter information as needed, and then save settings.

2.3 Managing Devices

You can configure devices, subscribe alarm messages, configure devices remotely, set video streams, configure alarm output, and more.

Configurations of different devices might vary, and the actual interface shall prevail.

2.3.1 Device Configuration

You can view device information such as adding mode and SN, modify device information such as device name, device password, and username.

Step 1   On the **Home** interface, tap   , and then tap **Device Details**.

You can also tap the device or channel, and then tap   on the interface to go to device management interface.

Step 2   Tap **Device Configuration**, and then you can view and modify device information. Tap

Step 3 **Save**.

2.3.2 Alarm Subscription

You need to subscribe alarm messages, and then the alarm notification can be pushed to App when an alarm is triggered. For details, see "10.1 Subscribing Alarm Messages."

2.3.3 Device Channel

If a device has more than one channel (such as a network video recorder), you can view the names of those channels under the device.

2.3.4 Stream Setting

Select video streams from **Sub** or **Main** for live view or video playback.

2.3.5 Illumination Settings

Set illumination mode for the devices that support illuminator.

Step 1   On the **Home** interface, tap ●●●, and then tap **Device Details**.

Step 2   Tap **Illumination Settings**.
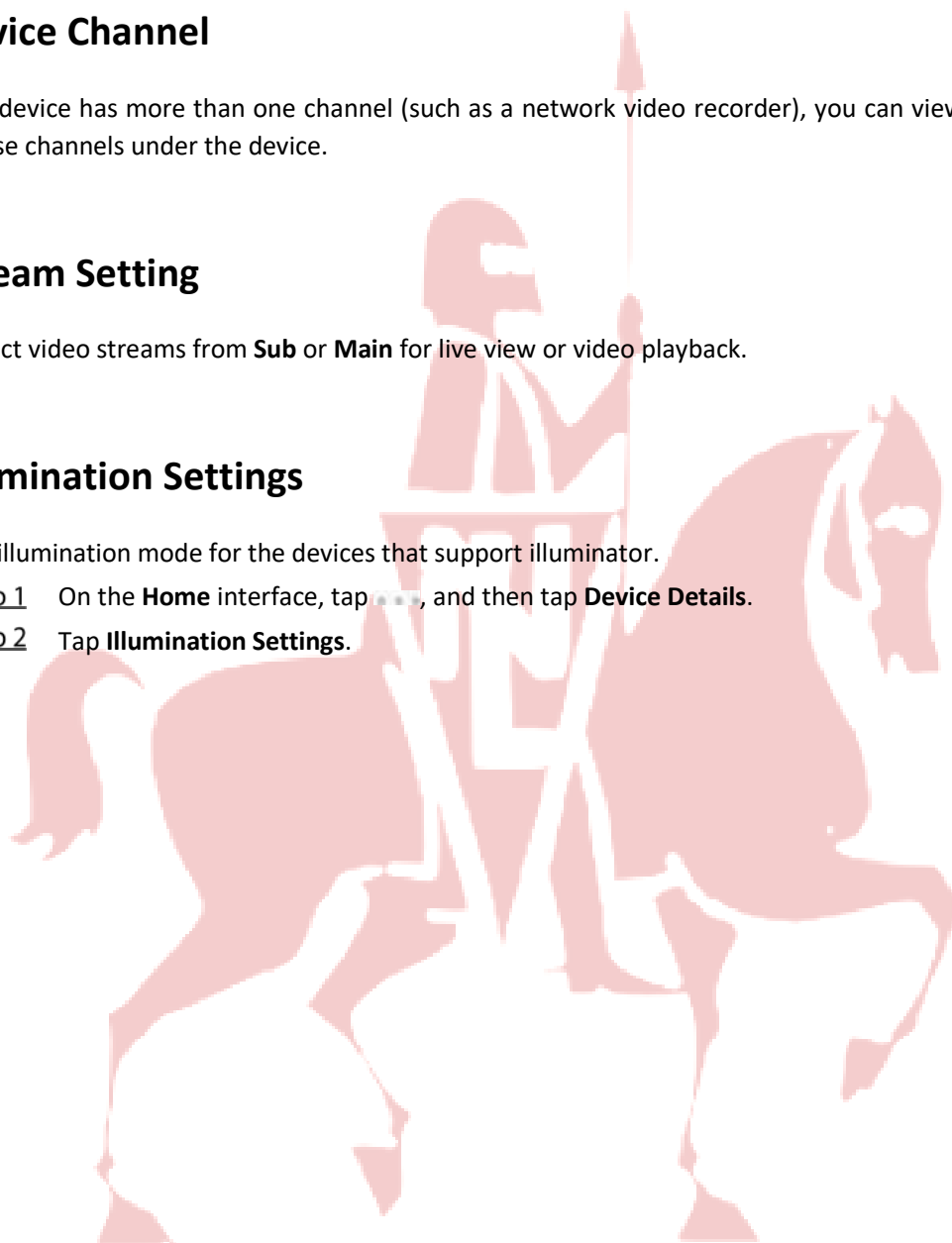
Figure 2-8 Illumination settings
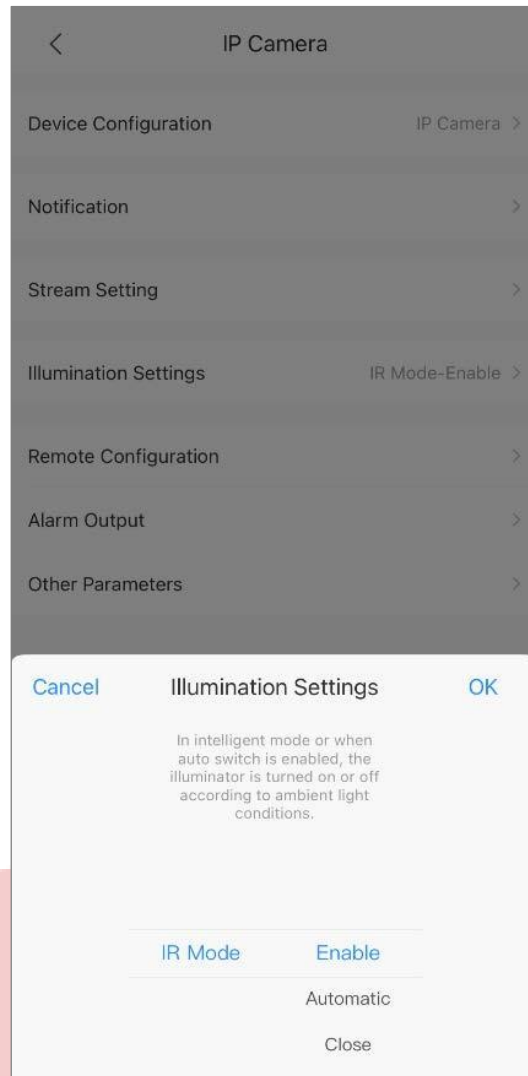
Step 3 Set the illumination mode.
- Smart illumination: When smart illumination is enabled, the system will switch the illuminators according to the actual condition. When the ambient light reaches the threshold of IR illuminator, the IR illuminator is enabled. The white light is enabled when an alarm (such as motion detection or human detection) is triggered, disabled when the target is out of the surveillance area; the IR illuminator is enabled according to the ambient light. It is set to **Automatic** by default, and the illuminator delay is 60 s.
- IR Mode:
  ◇ **Enable**: Enable the IR illuminator, and the white light is disabled.
  ◇ **Automatic:** The system enables the IR illuminator according to the ambient lighting condition.
  ◇ **Close**: Disable the IR illuminator.
- White Light:
  ◇ **Enable**: Enable the white light, and the IR illuminator is disabled.
  ◇ **Automatic**: The system enables the white light according to the ambient lighting condition. Set the sensitivity to **Middle**, and the upper limit of brightness is 100.
  ◇ **Close**: Disable the white light.

2.3.6 Remote Configuration

You can remotely configure the device including video detection, alarm setting, camera setting, storage management, and image adjustment.

2.3.6.1 Video Detection

In case of detection of moving object within defined conditions and shielded video image, the system performs alarm linkage actions.

Motion Detection

Alarm linkage action is performed when a moving object appears on the image and its moving speed reaches the preset sensitivity.

<u>Step 1</u>　On the **Home** interface, tap ，and then tap **Device Details**.

<u>Step 2</u>　Tap **Remote Configuration > Video Detection > Motion Detection**.

<u>Step 3</u>　Select the device channel that you want to configure.

<u>Step 4</u>　Enable **Advanced Configuration** to configure other parameters.

Advanced　Figure 2-9　　　　　　　　　　　　configuration (motion detection)
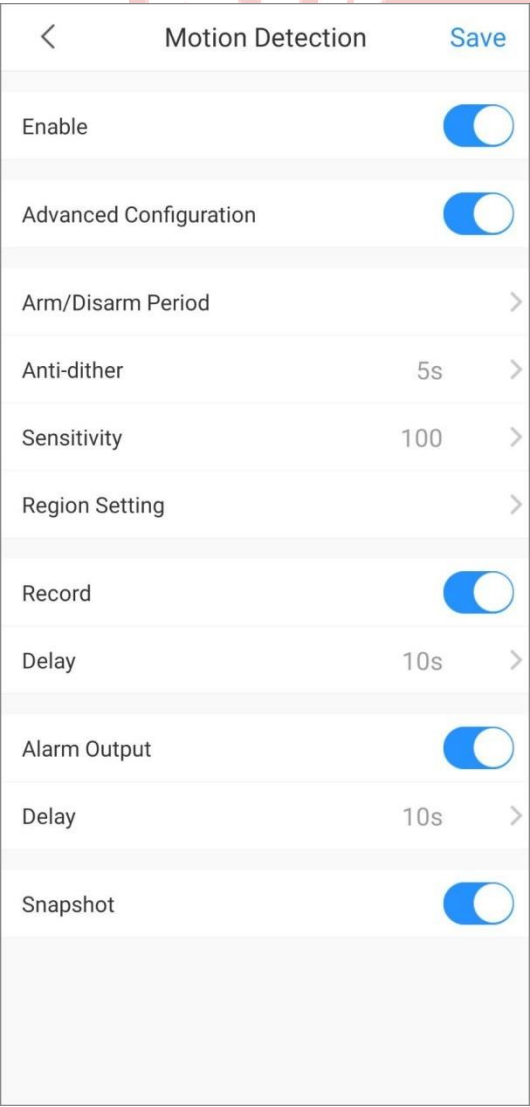
Table 2-2 Advanced configuration (motion detection)

Function	Description
Arm/Disarm Period	Set arming periods, and the alarm can only be triggered when it occurs during the defined period. Tap ✎, select the date, and then set the start time and end time of the period (up to 6 periods can be set each date). See Figure 2-10. ◎━┙ Tap **Copy**, select other days as needed, and then the defined arming period will apply to the selected days.
Anti-dither	Set anti-dither period from 0 s to 600 s. Only one motion detection event is recorded during the period.
Sensitivity	Set sensitivity value from 0 to 100. It is more easier to trigger the alarm with higher sensitivity.
Region Setting	Set motion detection region. The whole video image is the effective area for motion detection by default. See Figure 2-11. Tap ✎ to set motion detection region. Tap ✎ to clear the zone you have set. Tap ✋, and then pinch or stretch out with fingers to zoom out or zoom in the image.
Record	Enable **Record**, and then the system records automatically when an alarm is triggered.
Delay	The alarm record keeps for the defined time after the alarm is ended.
Alarm Output	Enable **Alarm Output**, and then the connected alarm output device will be linked when the alarm is triggered.
Delay	The alarm keeps output for the defined time after the alarm is ended.
Snapshot	Enable **Snapshot**, and then the system automatically captures pictures when the alarm is triggered.

Figure 2-10 Arm/Disarm period

Figure 2-11 Region setting
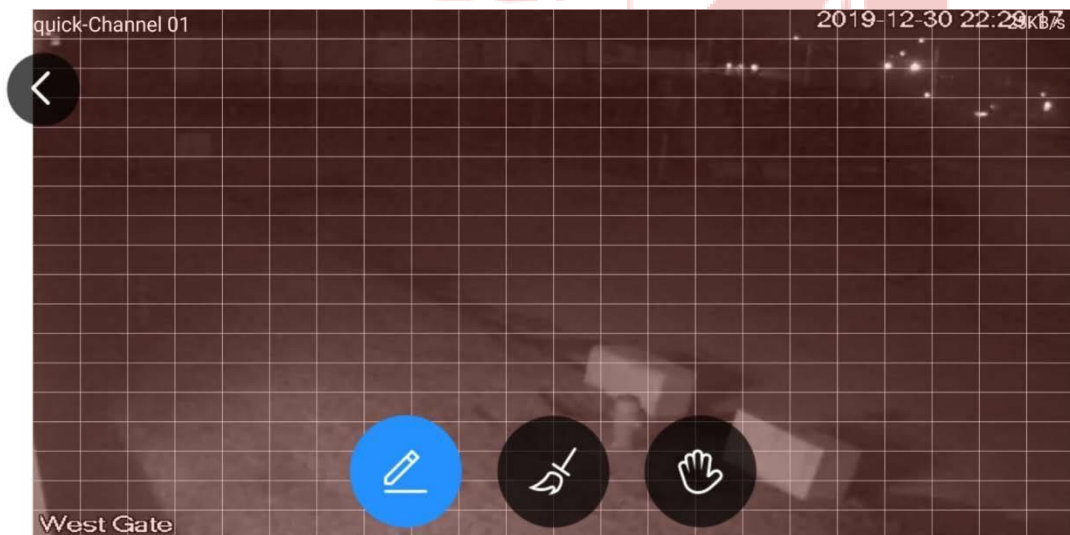
Step 5   Tap **Save**.

Video Mask

Alarm is triggered when the monitoring image is shielded and the output video is in single color.

Step 1   On the **Home** interface, tap   , and then tap **Device Details**. Tap

Step 2   **Remote Configuration > Video Detection > Video Mask**.

Step 3   Select the device channel that you want to configure.

Enable   Step 4   **Advanced Configuration** to configure other parameters. For details, see Table 2-2.

Step 5   Tap **Save**.

Figure 2-12 Advanced configuration (video mask)
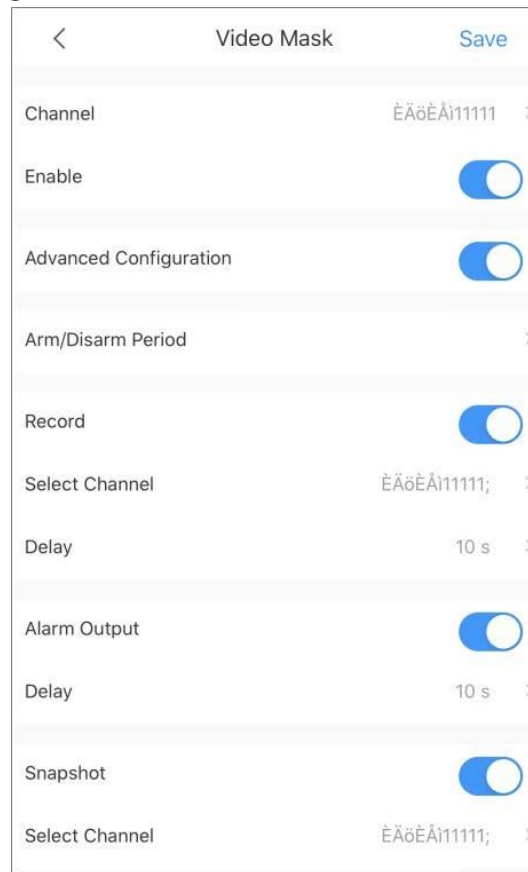
2.3.6.2 Alarm Setting

When the alarm is triggered, alarm action is linked such as recording, snapshot, and alarm output.

Alarm types (mainly for network video recorders) include local alarm, network alarm, IPC external alarm, IPC offline alarm, and PIR alarm.

Table 2-3 Alarm setting

Alarm Type	Description
Local Alarm	Connect the alarm device to the alarm input port of the added device. When the alarm is triggered, alarm linkage action performs.
Network Alarm	Alarm linkage action performs when alarm signal is transmitted to the device through network.
IPC External Alarm	Connect the IPC to the alarm input device. When the alarm is triggered, alarm linkage action performs.
IPC Offline Alarm	Alarm linkage action performs when the added device and IPC are disconnected.
PIR Alarm	The alarm is triggered when an object is detected by a PIR-based motion detector.

This section takes setting local alarm as an example.

Step 1 On the **Home** interface, tap , and then tap **Device Details**.

Step 2 Tap **Remote Configuration > Alarm Setting > Local Alarm**.

Step 3 Select the device channel that you want to configure.

Step 4 Enable **Advanced Configuration** to configure other parameters. For details, see Table 2-2. Tap

Step 5 **Save**.

Figure 2-13 Advance configuration (local alarm)

2.3.6.3 Camera Settings

You can set video stream parameters such as encoding mode, resolution, frame rate, bit rate type, and bitrate.

Step 1 On the **Home** interface, tap ...., and then tap **Device Details**.

Step 2 Tap **Remote Configuration > Camera Setting > Video Stream**.

Step 3 Select the device channel you want to configure. (Optional)

Step 4 Set channel name.

     We recommend setting a channel name that is easy to be recognized. You can set according to device installation place.

Step 5 Select main stream or sub stream.

Figure 2-14 Video stream (main)

Table 2-4 Video stream parameters

Function	Description
Main/Sub	Main stream: Large bit stream, small compression image, and high resolution, but also requires large bandwidth. Sub stream: Smaller bit steam, smoother video, and requires smaller bandwidth. Used to replace main stream when the bandwidth is insufficient.
Encode Mode	**MJPEG**: The image requires high bit rate to ensure clarity. It is recommended to set the **Bitrate** value to the biggest for a better image. **H.264**: Main Profile encode mode. **H.264H**: High Profile encode mode; use smaller bandwidth than H.264 with the same image quality.
Video	This parameter can be set only when you select sub stream. Enable **Video**, and then the video stream type is sub stream.
Audio	Set the audio stream type as main stream or sub stream.
Function	Description
Resolution	Set video stream resolution. The higher the resolution is, the better the video quality, but the bigger the bandwidth will be. Resolutions supported by the device might vary, and the actual interface shall prevail.
Frame rate	Set frame rate from 1 to 25. The higher the frame rate is, the more vivid and fluent the video, but the bigger the bandwidth will be.
Bitrate Type	CBR (Constant Bit Rate): The bit rate changes little and keeps close to the defined bit rate value. When the scene is complicated, the image might not be clear; when the scene is simple, the bandwidth might be wasted. VBR (Variable Bit Rate): The bit rate changes along with monitoring scene, so as to make image clear under complicated scene and the bandwidth is small under simple scene.

Quality	This parameter can be configured only when the **Bitrate Type** is set as **VBR**. The better the quality is, the larger the bandwidth will be.
Bitrate	Set video bitrate. The higher the bitrate is, the faster the data is transmitted.

Step 6 Tap **Save**.

2.3.6.4 Storage Manager

Configure the device recording period and recording type.

Step 1   On the **Home** interface, tap , and then tap **Device Details**.

Step 2   Tap **Remote Configuration > Storage Manager > Schedule**. Select the

Step 3   device channel you want to configure.

Different recording types have different colors.

- Green: Normal video recordings.
- Orange: Record when motion detection alarm is triggered.
- Red: Alarm recording. Record when alarm is triggered.

Figure 2-15 Schedule
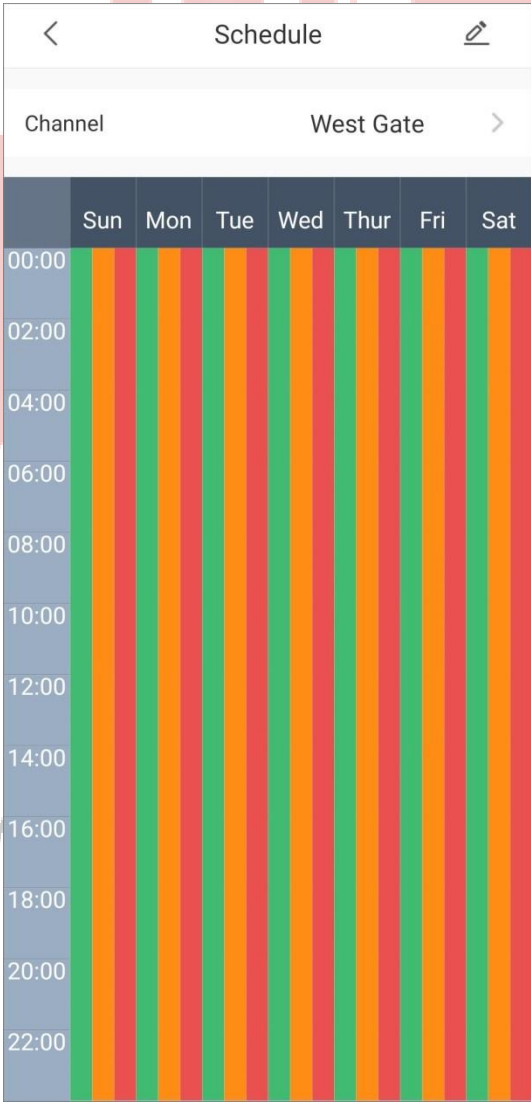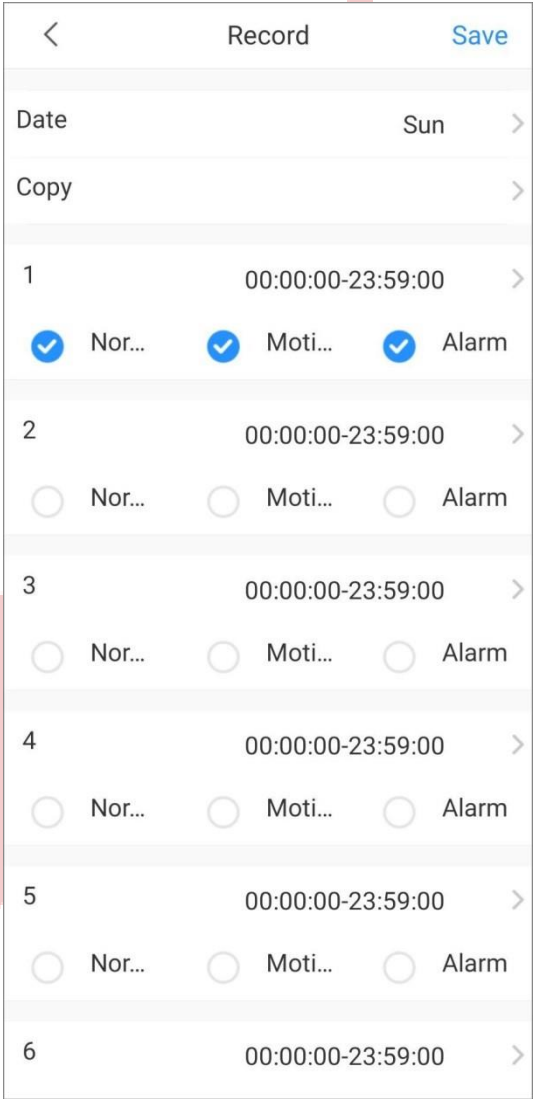
Step 4   Tap ✎, select the date, and then set the start time and end time of the period (up to 6 periods can be set for each day).

🔑
Tap **Copy**, select other days as needed, and then the set arming period will apply to the selected days.

Figure 2-16 Set recording

Step 5 Tap **Save**.

2.3.6.5 Image Adjustment

Adjust live video image such as focus, zoom, brightness, contrast, and image quality.

Step 1   On the **Home** interface, tap ..., and then tap **Device Details**.

Step 2   Tap **Remote Configuration > Image Adjustment**.

Step 3   Select the device channel you want to configure, and then the system goes to live interface.

Step 4   Operate on the app.

Figure 2-17 Image adjustment
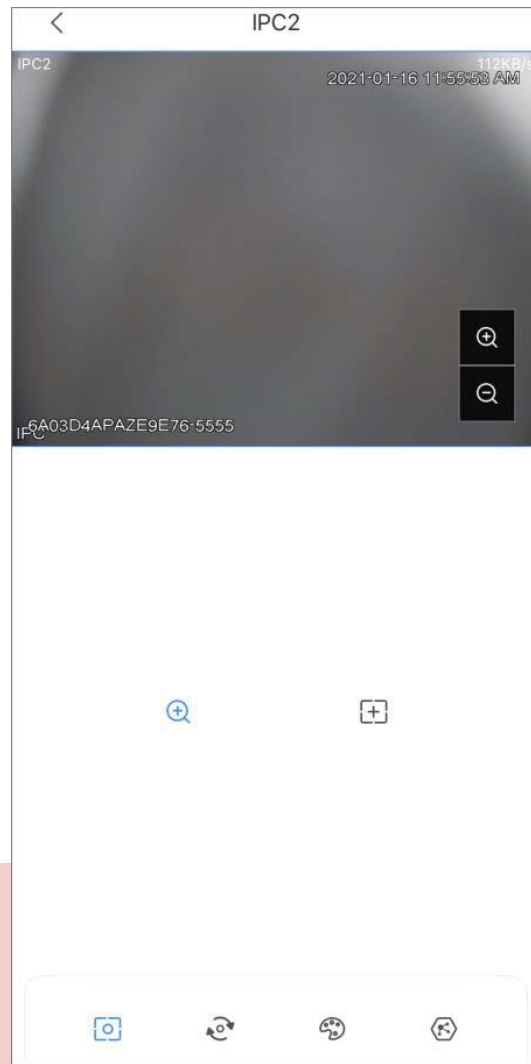
Table 2-5 Function icon descriptions

Function	Description
Focus/Zoom	Tap ⬚, and then you can: Tap ⊕ to zoom out or zoom in the image. Tap ⊞ to adjust focus to make the image clearer 📖 Tap + or – on the image to adjust focus or zoom effect.
Rotate/Flip	Tap ↻ to rotate or flip the image. ◿: Flip horizontally. ◁: Flip vertically. ⟲₉₀: Rotate 90° anticlockwise. ⟳₉₀: Rotate 90° clockwise.

Function	Description
	(180): Rotate 180°.
Image effect	Tap 🎨 to adjust image effect. ☼: Brightness. ◑: Contrast. 🎨: Hue. 📐: Saturation. ↻: Restore to default.
Video quality	Tap 🔶 to adjust live video quality. ⌁: Real-time mode. ⊜: Fluent mode. (AUTO): Auto mode.

2.3.7 Alarm Output

You can set alarm output mode as close, manual, or automatic. When the added device has connected to alarm output device, and **Alarm Output** is enabled in **Video Detection** or **Alarm Setting**, you need to set alarm output mode to make alarm linkage actions work.

Step 1 On the **Home** interface, tap ▪▪▪, and then tap **Device Details**.

Step 2 Tap **Alarm Output**.

Step 3 Set alarm output mode.

- **Automatic**: Alarm is triggered only when the alarm event occurs.
- **Manual**: Alarm is always on.
- **Close**: Alarm is disabled.

Figure 2-18 Alarm output
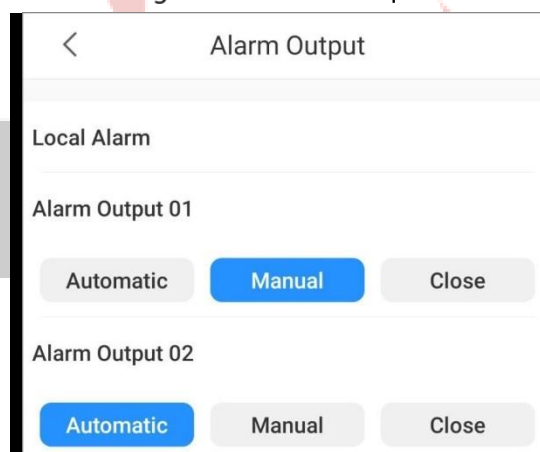
2.3.8 Storage Manager

You can view storage capacity of the SD card or HDD, and format the SD card or HDD.

<u>Step 1</u>   On the **Home** interface, tap [icon], and then tap **Device Details**

<u>Step 2</u>   Tap **Storage Manager**

Figure 2-19 Hardware
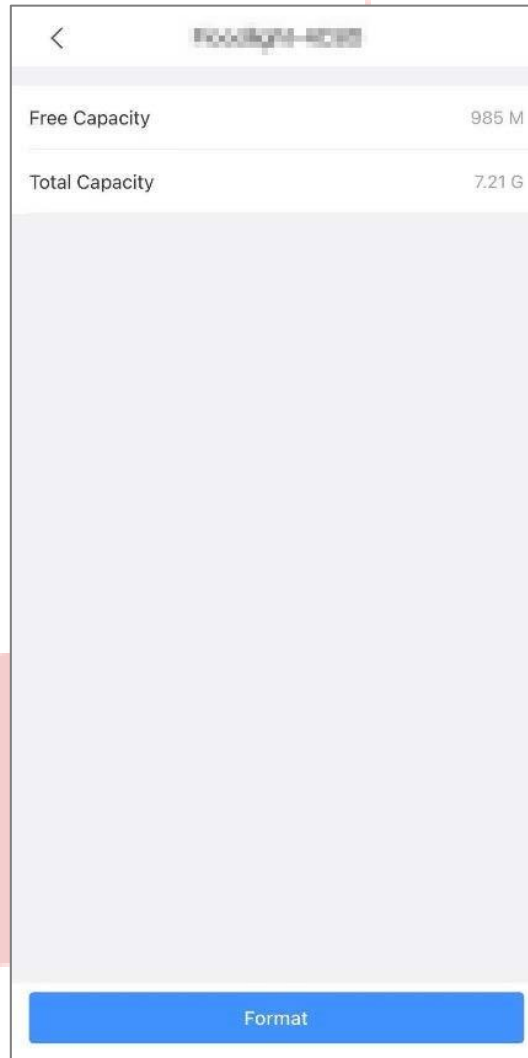
<u>Step 3</u> (Optional) Tap **Format** to format the SD card or HDD.

2.3.9 Time Zone

When your region has Daylight Saving Time (DST), you can select the time zone and set DST.

[icon]

The function is available on account devices.

<u>Step 1</u>   On the **Home** interface, tap [icon], and then tap **Device Details**.

<u>Step 2</u>   Tap **Time Zone**.

<u>Step 3</u>   Select the time zone that the device is at.

<u>Step 4</u>   (Optional) Enable DST, and then set start time and end time of the DST.

Figure 2-20 Time zone
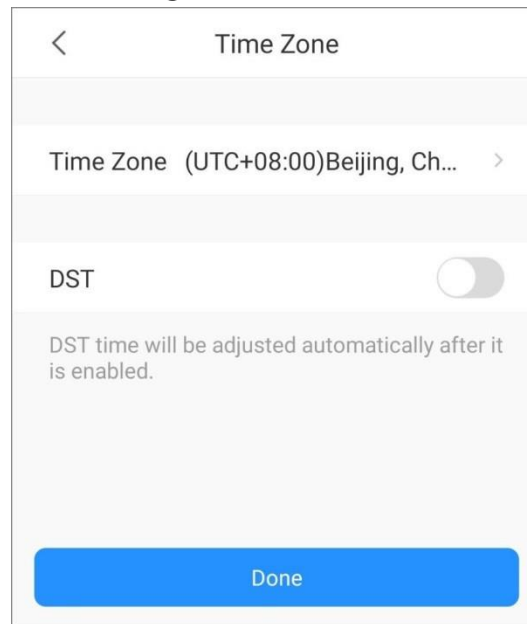
2.3.10 Custom Audio and Video Encryption

After enabling **Custom Audio and Video Encryption**, you need to enter password for live view and playback (cloud videos included).

The function is available on account devices.

Step 1 On the **Home** interface, tap •••, and then tap **Device Details**.

Step 2 Tap **Custom Audio and Video Encryption**.

Step 3 Enable the function and set password.

2.3.11 Device Sharing

You can share devices with up to 6 DMSS users and entrust them to one enterprise.

The function is available on account devices.

2.3.11.1 Sharing Devices

Step 1 On the **Home** interface, tap •••, and then tap **Device Details**. Tap

Step 2 **Device Sharing**.

Step 3 Tap ⊕ **> Sharing to User**, enter DMSS account to share the device to users, and then select permissions as needed. All permissions are selected by default.

- For devices that do not support entrusting service, Tap ⊕ to enter DMSS account and select permissions as needed.

● You can decide whether to select **Playback**, **Alarm Push Notification**, or **Device Control** as needed. **Live View** is selected by default, and you cannot cancel the selection.

Figure 2-21 Device sharing
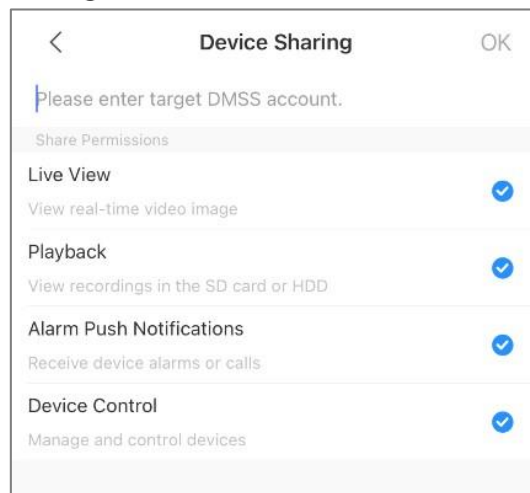
Step 4 Click **OK** to share the device.

2.3.11.2 Entrusting Devices

2.3.11.2.1 Entrusting Device One by One

Step 1 On the **Home** interface, tap ···, and then tap **Device Details**. Tap
Step 2 **Device Sharing**.

Step 3 Tap ⊕ > **Entrust to Company**, and then scan the corresponding QR code of the installer, or tap

🖼 on the upper-right corner of the interface to upload QR code.

Figure 2-22 Entrust to company (1)
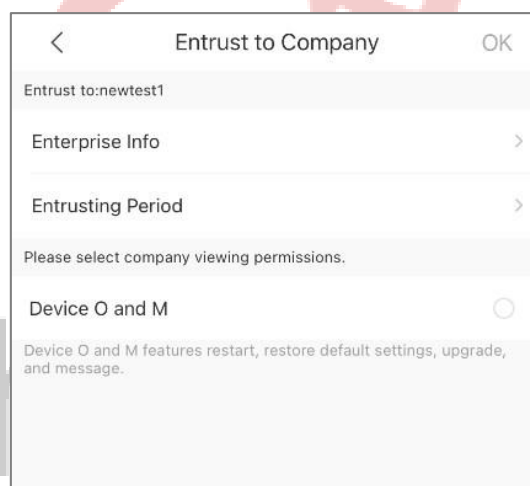
Step 4 Enter the enterprise information (logo, name, contact information and address), entrusting period, and then select company viewing permissions.
Step 5 Click **OK**.

2.3.11.2.2 Entrusting Device in Batches

Step 1 On the **Home** interface, tap ⊞ to display devices in list mode.

Step 2 Tap 🔗 , select devices (up to 20), and then tap **Batch Entrust**.

Figure 2-23 Batch entrust (1)
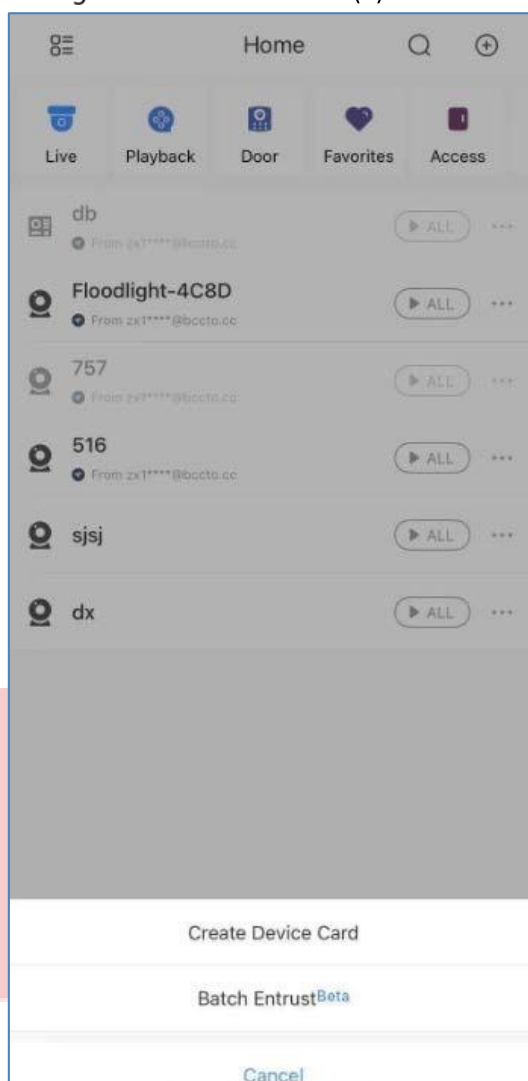
Step 3 Select the devices to be entrusted, and then click **Scan Entrusting QR Code**.

Figure 2-24 Batch entrust (2)
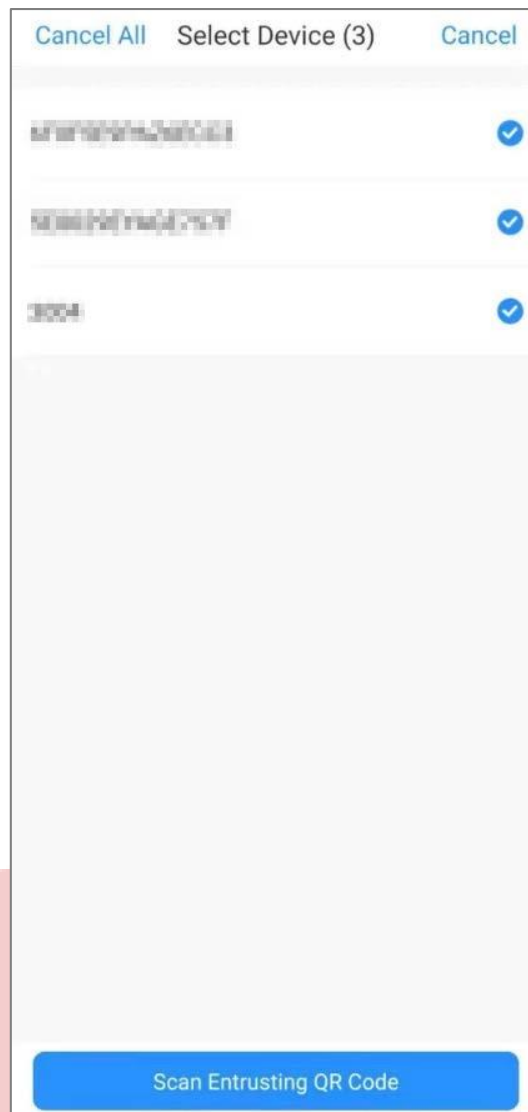
Step 4 Scan the corresponding QR code of the installer to or tap on the upper-right corner of the interface to upload QR code.

Figure 2-25 Batch entrust (3)
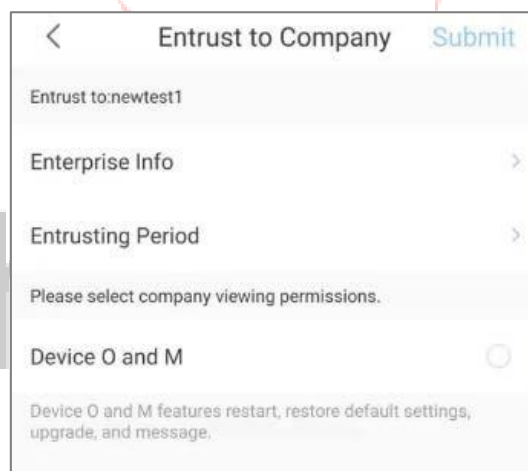
Step 5 Enter the enterprise information (logo, name, contact information and address), entrusting period, and then select company viewing permissions.

Step 6 Click **Submit**.

2.3.12 Cloud Update

You can view the current device version and upgrade the device when a new version is discovered by the system.

The function is available on account devices.

Step 1   On the **Home** interface, tap ..., and then tap **Device Details**.

Step 2   Tap **Cloud Update**, and then follow on-screen instructions to upgrade the device.

2.3.13 Other Parameters

You can view the information of the connected solar power system, such as its electricity generation power, status of the solar power panel, the battery, the load, and the controller.

Step 1   On the **Home** interface, tap ..., and then tap **Device Details**.

Step 2   Tap **Other Parameters**.

Step 3   Tap the solar power system you want to view.

Step 4   Tap **Real-time** or **Analysis** to view real-time or history data of the solar power system.

Figure 2-26 Solar power system
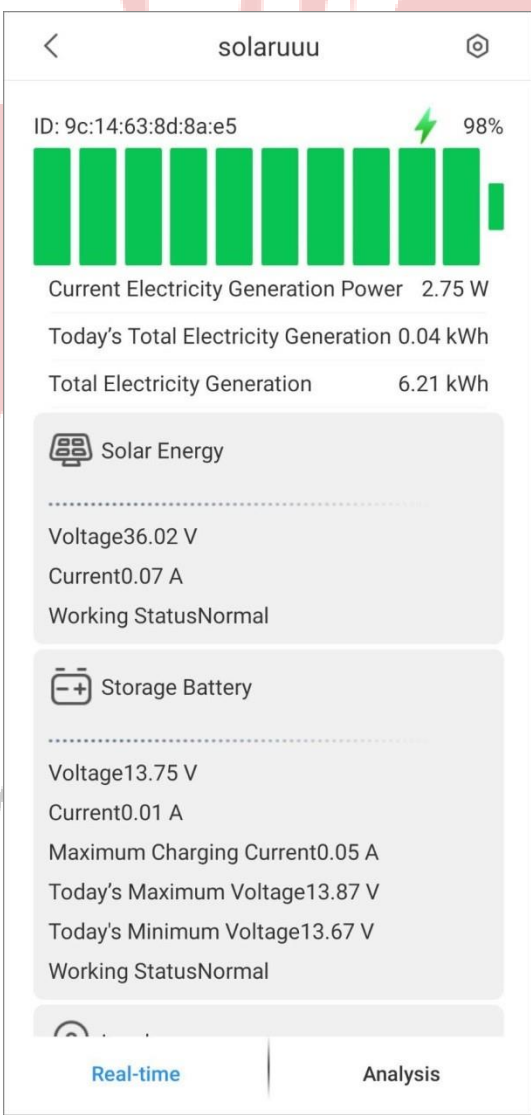
2.3.14 Creating Device Card

You can quickly add devices by scanning the device card.

Step 1 On the **Home** interface, tap 🔲 to display devices in list mode.

Step 2 Tap 🔗 , select devices (up to 10), and then tap **Create Device Card**.

You cannot create device card for account devices.

Figure 2-27 Create device card
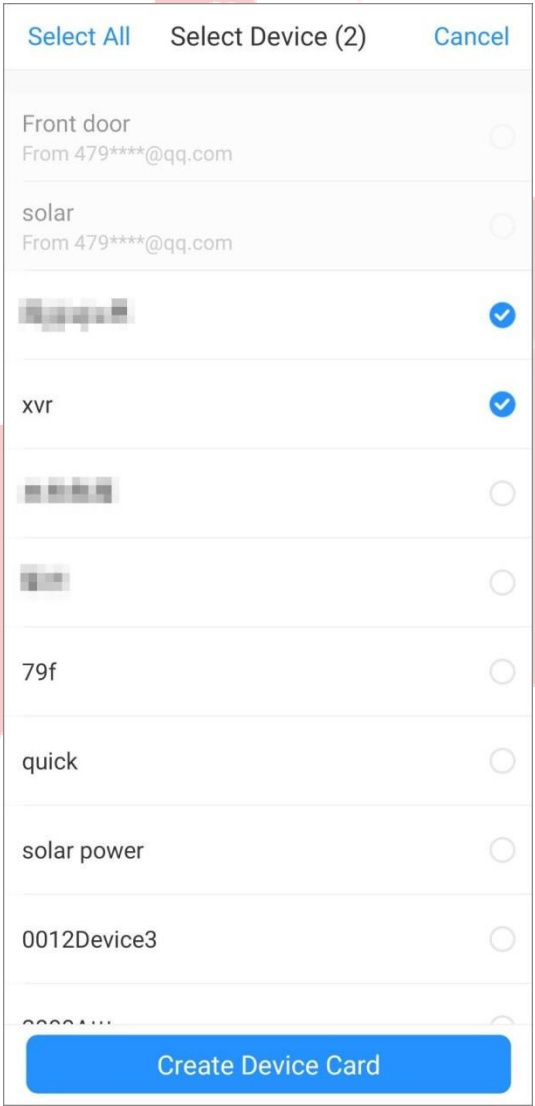
Step 3 (Optional) Enter the password, and then tap OK.

You need to enter the password when you import devices by scanning the device card. Step 4 Save the QR code of the device card to your album.

2.3.15 Deleting Device

You can delete added devices as needed.

Step 1   On the **Home** interface, tap ⋯, and then tap **Device Details**.

Step 2   Tap **Delete**.

3 Live View

You can view the monitoring channels and do the operations such as taking snapshots, recording videos, and adding channels to favorites.

Step 1 On the **Home** interface, tap [icon] .

Step 2 Play a channel or multiple channels.

- Play a channel: Tap [icon] in the window, and then select a channel in the device list to be played.

- Play multiple channels: Tap [icon], select channels in the device list as needed.

[icon]

When displayed channels exceed the maximum number of displaying window you set, swipe left or right to view other live videos.

Step 3 Operate on the live videos.

Figure 3-1 Live view of a single channel

Table 3-1 Live view function icons

Function	Description

Device details	Tap ⬡ to go to the device details interface, and then you can configure your device. For details, see "2.3 Managing Devices." You can also tap ⬡⟶ of a device on the **Home** to view its details.
Play/Pause	Tap ‖ to pause playing and tap ▷ to play.
Video stream	Tap 𝐇𝐃 to swich between SD and HD video quality.
Mute/Unmute	Tap ◁× to mute the video. Tap ◁⍩ to unmute.
Window split	Tap ④ to change window split modes. You can display in 1, 4, 9, or 16 windows.
Landscape	Tap ⬓ to change image orientation to landscape.
Recording playback	Tap ⊙ to go to video playback interface and today's recording will be automatically played if it exists.
Snapshot	Select a video, and then tap 📷 to take snapshot. 📖 ● You can configure the capture mode in **Me > Setting**. For more details, see "12 System Configuration and Account Management." ● Snapshots are saved in the **File**. You can also tap the captured image at the lower-left corner on **Live** interface to go to **File**. For more details, see "10 File."
Video recording	Select a video, and then tap 📹 to start recording. Tap the icon again to stop recording. 📖 Recorded videos are saved in the **File**. You can also tap the video at the lower-left corner on **Live** interface to go to **File**. For more details, see "10 File."
Voice chat	Select a video, and then tap 🎤 to enable two-way voice call if the function is supported. Tap and hold the icon till the **Voice Call** interface is displayed. Tap the device to which the channel belongs to enable device talk if the function is supported. 📖 If a device has many channels, tap 🎤 on **Live** interface is talking to the played channel, and device talk means directly talking to the device.
Memory play/Close videos	Memory play: Tap ⊙ (a tick in the center) to play the channels that have been played last time. Close videos: Tap ⊗ (a cross in the center) to close all the played videos.

Function	Description
PTZ control	Select a video, tap ⌄ , and then tap ⊙ to control PTZ. Tap ⊕ to zoom in or zoom out the image. Tap ⚙ to adjust the brightness of the video. Tap ⚑ , select the preset point, and then tap ✓ to turn the PTZ to the monitoring target. Use ◉ to control PTZ directions: Left, right, up, down, upper-left, upper-right, lower-left, and lower-right are supported. ⊙━ᴅ You can also use gestures to control PTZ. ● Swipe on the screen to control the PTZ direction. ● Pinch or stretch out with fingers on the screen to zoom out or zoom in. 📖 ● Only one window is displayed during PTZ control. ● PTZ function is available on select models.
Fisheye	Select a video, tap ⌄ , and then tap ⓠ to enable fisheye. Swipe on the screen to adjust the display effect of video image. 📖 The function is is available on select models.
Wiper	Select a video, tap ⌄ , tap ▽ , and then the wiper control interface is displayed. Tap **Single**, the wiper works one time, and then stop. Tap **Enable**, then configure time interval, the wiper works after each time interval. Tap **Stop**, the wiper stops working. 📖 The function is available on select models.
Spotlight/Buzzer	Tap ☀, and then select ♀ to enable white light; select ⌂ to enable buzzer. 📖 The function is available on select models.
Change video place	Tap and hold a video, and then you can move it to the target window.
Enlarge window	Double tap the window to enlarge it. Double tap again to restore.
Help	If the video is not properly played, tap **Help** in the window to solve the problem.

Delete video	Tap and hold a video till the trash bin appears at the top of the interface. Drag the video to the trash bin, and then release.

Step 4 Click 🗐 to select the date to view the corresponding video as needed.
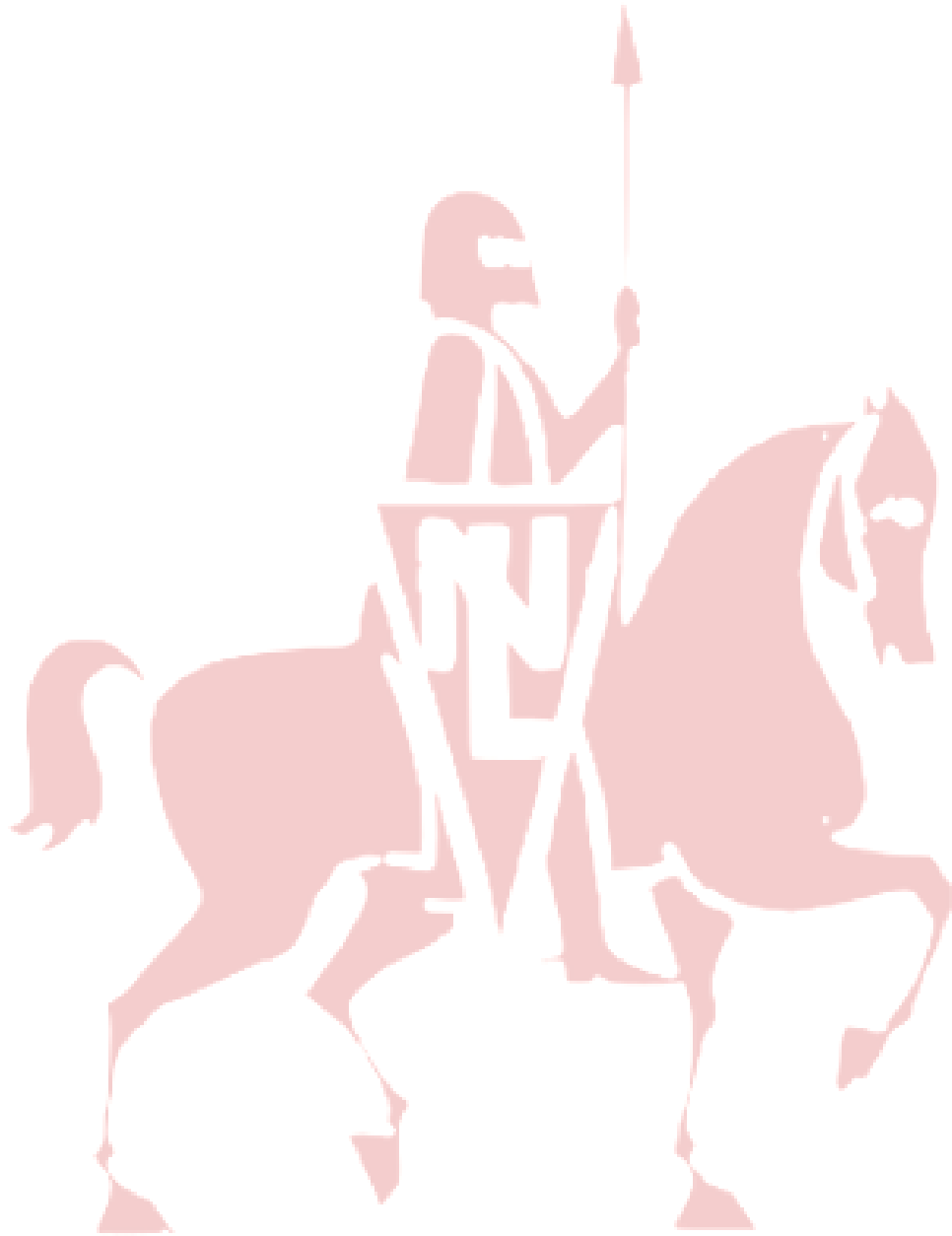
4 Video Playback

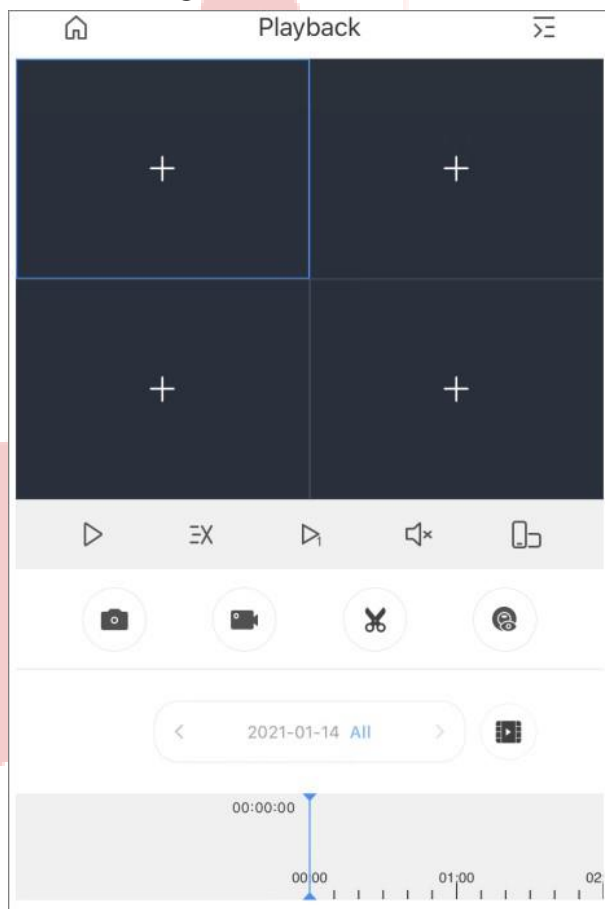You can search and play back videos according to time, video type, and channels.

Before playing back videos, you need to set alarm rules and record plan of the channel.

Step 1 On **Home** interface, tap .

Step 2 Tap or to select a channel or multiple channels.

Figure 4-1 Video playback

Step 3 Tap 2020-01-03   All   to change date and record type. The date with a blue dot means it has videos.

Figure 4-2 Playback conditions

Record types are as follows.

- **All (grey)**: Play all types of records by default.
- **Regular (green)**: Normal recordings.
- **Alarm (red)**: Record when alarm is triggered, such as audio alarm and local alarm.
- **Motion Detection (orange)**: Record when motion detection alarm is triggered.
- **Smart Recording (yellow)**: Record when smart event alarm is triggered such as face detection and recognition, IVS, video metadata, and more.

Table 4-1 Video playback function icons

Function	Description
Play back videos	Select a video, and then you can: ⏸ : Pause playing; ▷ : Continue playing ◁◁ : Play slowly; ▷▷ : Play fast; ▷⏐ : Play by frame 🔇ˣ : Mute the video; 🔊 : Unmute the video. ⬛ : Changes image orientation to landscape.

Function	Description
Clip	Select a video, and then tap ⬚ to clip the video. Drag time bar, tap ▶ to set a start point, and then tap ■ to set a stop point.
Snapshot	See "Table 3-1 Live view function icons."
Video recording	
Fisheye	
Time bar	The color block indicates recorded videos with different types. Grey means all videos; green means regular videos; red means alarm videos; orange means motion detection videos; yellow means smart videos. Drag the time bar to view the record of any time frame. Pinch or stretch out to zoom the bar.

5 Video Call

You can view the live video of the added video intercoms, realize video call between the device and App, lock/unlock the door, and more.

<u>Step 1</u> On the **Home** interface, tap .

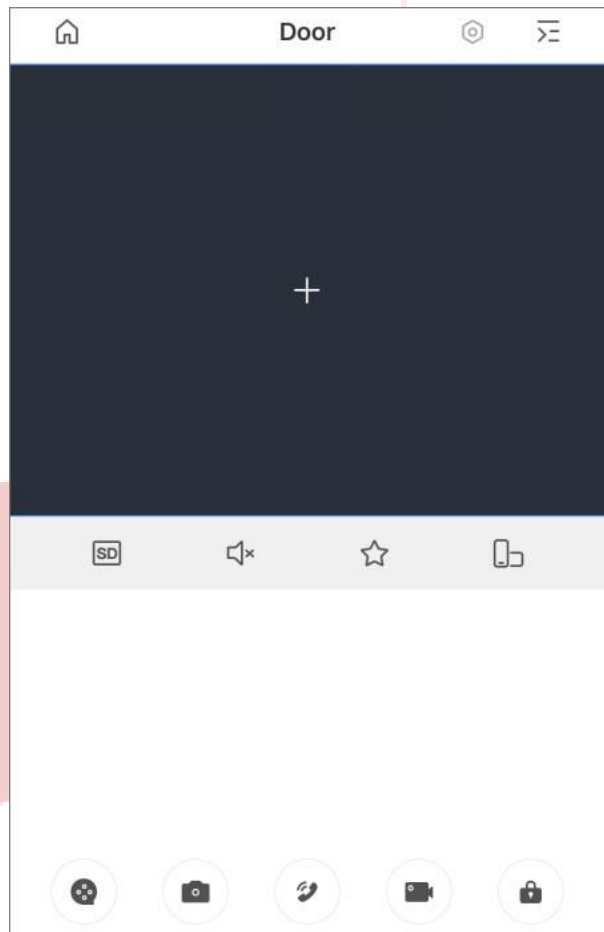<u>Step 2</u> Tap or to select a channel.

Figure 5-1 Door

Table 5-1 Video call function icons

Function	Description
Video stream	Tap ![SD] to swich between SD and HD video quality.
Mute/Unmute	Tap ![mute]/![unmute] to mute/unmute the video.
Favorites	Tap ☆ to create a favorites group and add the selected channel to the **Favorites** or to the existing favorites group. See "9 Favorites."
Landscape	Tap ![landscape] to change image orientation to landscape.
Recording playback	Tap ![recording] to go to video playback interface and today's recording will be automatically played if it exists.

Function	Description
Snapshot	Tap 📷 to take snapshot during video call.
Answer/End the call	App answers the call from VTO: Tap ✅ to answer the call; tap to ❌ decline or hang up the call. 📖 Enable **Alarm Subscription** of the VTO, and then you can answer the call on App when VTO is calling.
Recording	Tap 🎥 to start recording during video call.
Unlock	Tap 🔒 to unlock the door. 📖 VTO that has two locks can be added to the App. Tap 🔒, and then select ① or ② to unlock the door.

Step 3 View the call history of VTO between app. Tap
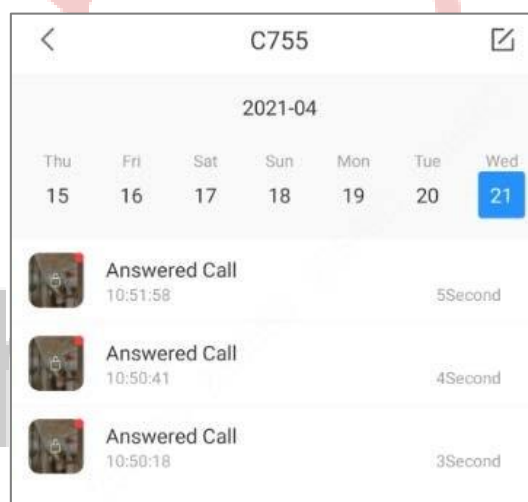**Message** at the bottom of the interface.
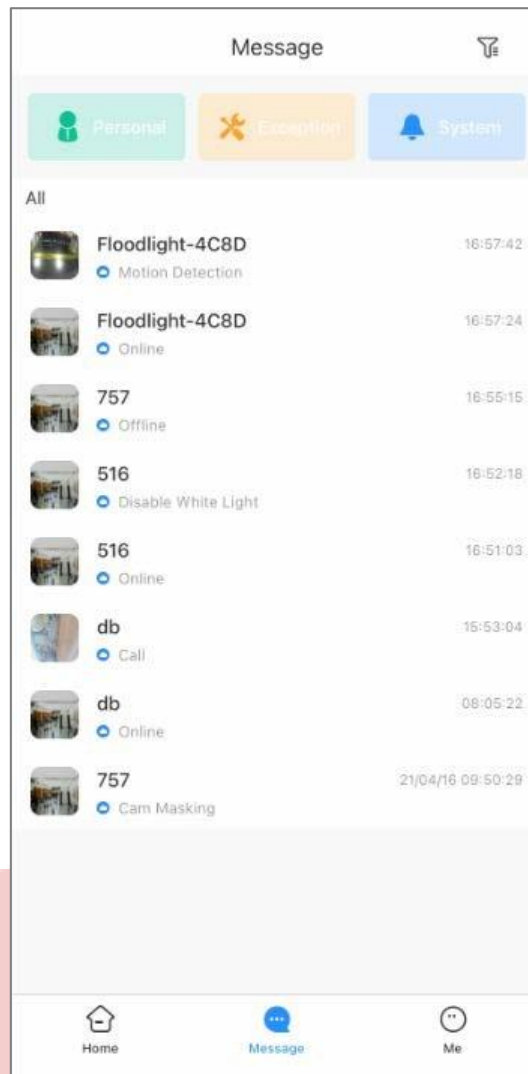
Figure 5-2 Message

Tap a VTO as needed, and then you can view the call history (such as time, duration), and play back the recorded video.
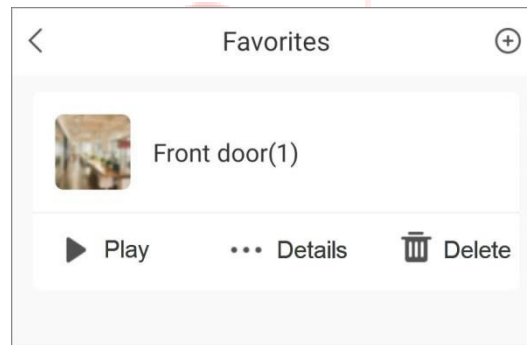
Figure 5-3 Message

6 Favorites

You can save channels to **Favorites** so as to find them and go to live view quickly when needed.

<u>Step 1</u> On the **Home** interface, tap 💙 .

<u>Step 2</u> Tap ⊕ , select one or multiple channels from the same device type, and then tap **Next**.

<u>Step 3</u> Enter favorites name to create the favorites.

Figure 6-1 Favorites created

- Tap ▶ to play channels in this favorites group simultaneously.

- Tap ••• to view details of the channels, delete channels, or rename the favorites.

- Tap 🗑 to delete the favorites.

7 Access

You can view door status, unlock records, remotely unlock the door, watch live video of the access control device, and more.

On the **Home** interface, tap .

Figure 7-1 Access control device
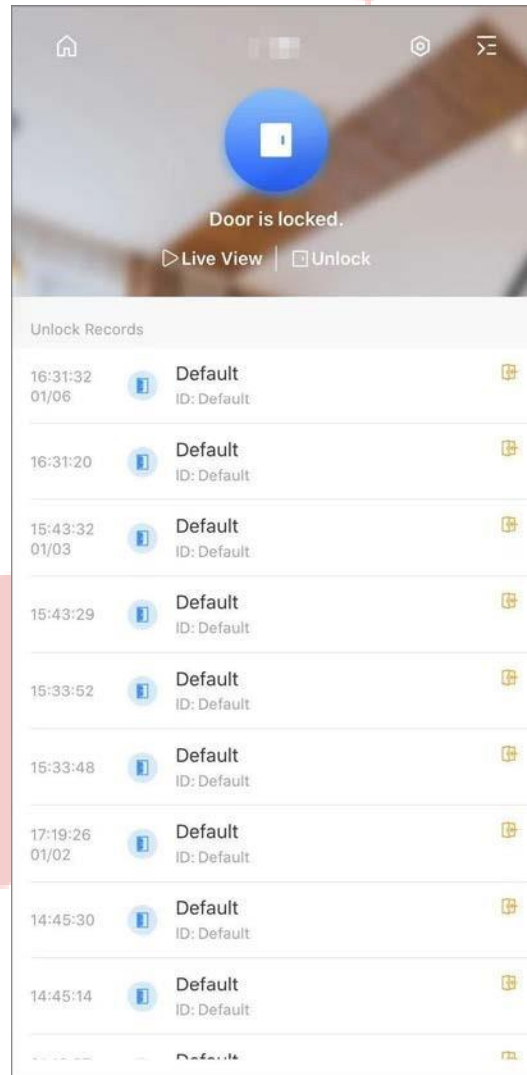
Table 7-1 Function icon description

Function	Description
Switch device	Tap to select another access control device.
Device details	Tap to go to device details interface, and then you can view device configuration, and view unlock records within 7 days. You can also tap of the access control device on the **Home** interface, and then tap **Device Details**.

Function	Description

Door status	: The door is locked. : The door is unlocked.
Unlock	Tap **Unlock** to unlock the door.
Unlock records	Display person name, ID, unlocking time, and unlocking methods. : Remotely unlock the door on App. : Unlock by card. : Unlock by fingerprint. : Unlock by password. : Unlock by key. : Unlock by face. : Duress unlock. : Unlock methods combination. : Unlock by group combination. : Failed to unlock the door.
More	Tap **More** at the bottom of the interface to view unlock records within 7 days.
Live view	Tap **Live View** to go to live view of the device. See Figure 7-2. Tap for snapshot. Tap to switch between SD and HD video quality. Tap to mute the video; tap unmute the video. Tap to unlock the door. Tap to record videos.

Figure 7-2 Access (live)
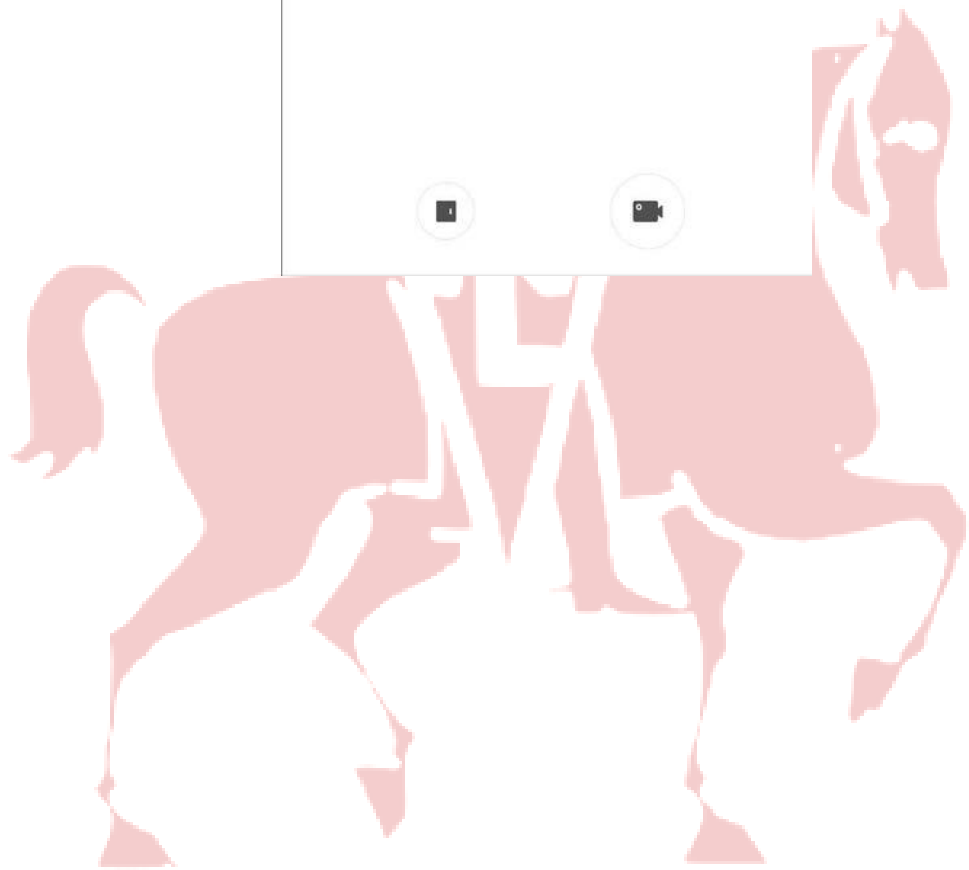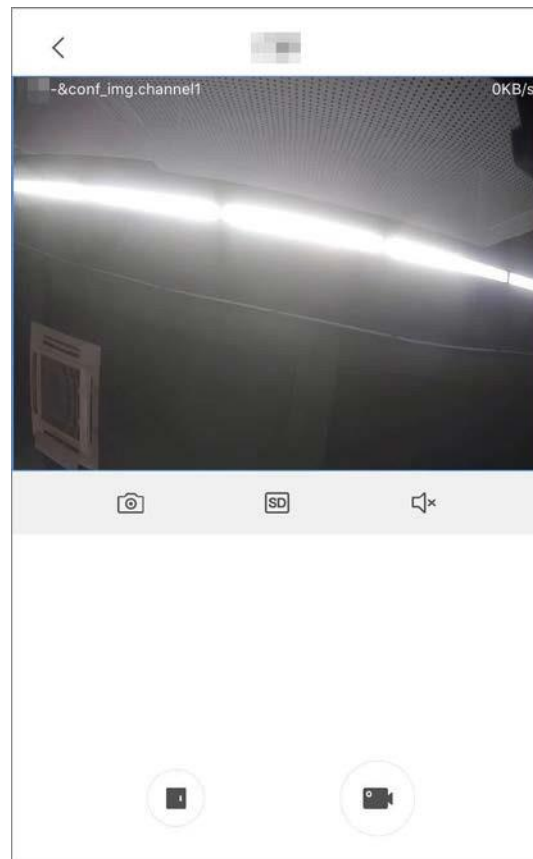
8 Alarm Control

You can manage the added alarm hub and its accessories such as switching arming mode, and configuring accessories.

On the **Home** interface, tap ⚪.

8.1 Configuring Alarm Devices

Configuring the Alarm Hub

You can view and modify device configuration.
- Tap **Device Details** > **Hub Setting** to configure the hub.

Figure 8-1 Configure the hub parameters
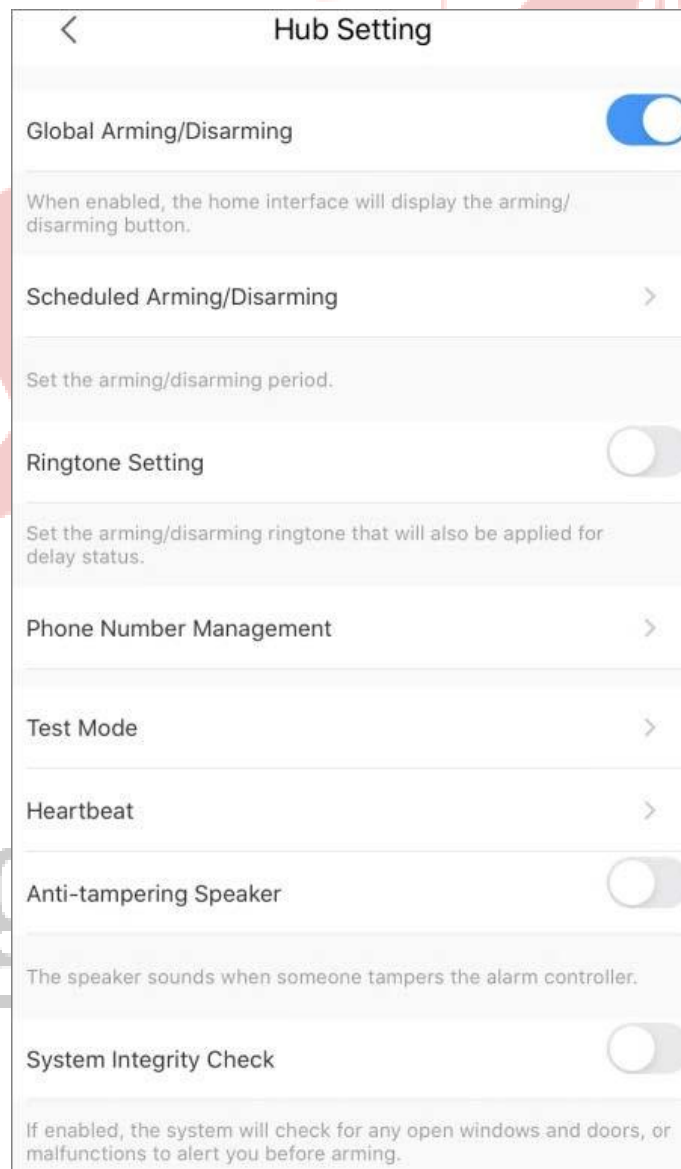
Figure 8-2 Configure the alarm hub

Parameter	Description
Global Arming/Disarming	If enabled, arm or disarm all areas with one tap.
Schedule Arming/Disarming	Arm or disarm the areas by the schedule. ● Area: Select the area in which the hub operates. ● Command setting: Select an armed mode as needed by tapping **Home Arm**, **Out Arm**, or **Disarm**. ● Time: Select the time period in which the hub operates. ● Repeat: Copy the arming or disarming schedule.
Ringtone Setting	The ringtone when entering or exiting arming and disarming mode.
Phone Number Management	● Add and manage the phone number. ● You can be notified of all events (alarm, fault, operation) through push notifications, SMS messages and calls (if activated).
Test Mode	Tap **Start** to check the status of the detectors connecting to the hub in different areas, and then tap **Stop** to complete detection.
Heartbeat	Configuring the hub-detector ping interval. The settings determine how frequently the hub communicates with devices and how quickly the loss of connection is detected. ● **Detector Ping Interval**: The frequency of connected detectors operated by the hub is configured in the range of 12 s to 300 s (60 s 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. (3 packets by default). The smaller the number, the more frequently the device offline status is detected and reported.
Anti-tampering Speaker	Alert with a siren if the lid of accessories and hub is open.

System Integrity Check	● The function is off by default. ● If enabled, the hub checks the status of all detectors before arming. If problems are detected, warnings will be displayed.

● Tap **Device Details** > **Hub Status** to view hub parameters.

Table 8-1 Hub parameter description

Parameter	Description
GSM 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 2-3 bars. ● : Ultra low. ● : Low. ● : Moderate. ● : High. ● : No.
Storage Battery	Show remaining electricity of the battery. ● : Fully charged. ● : Sufficient electricity. ● : Moderate electricity. ● : Insufficient electricity. ● : Charging.
Anti-tampering	The tamper mode of the detector, which reacts to the detachment of a damage of the body.
Main Power Status	Show main power status.
GSM Connection Status	Internet connection status of the hub via SIM card. ● : Connected. ● : Disconnected.

	Internet connection status of the hub via WI-FI.
WI-FI Connection Status	● ⊖: Connected.
	● ⊂▷: Disconnected.
	Internet connection status of the hub via Ethernet.
Network Cable Connection Status	● ⊖: Connected.
	● ⊂▷: Disconnected.
Parameter	**Description**
	Connection status of the SIM card.
	● 🔵S1: SIM card 1 is active.
SIM Card Status	● 🔵S2: SIM card 2 is active.
	● 🔴no: No SIM card.
Program Version	The program version of the hub.

Configuring Alarm Detectors

View and modify settings of the detectors. This section takes wireless door detector as an example.

● Tap 🖉 to configure door detector.

Figure 8-3 Configure the door detector

Table 8-2 Configure the door detector

Parameter	Description
Device Configuration	● View device name, type, SN and device model. ● Edit device name, and then tap **Save** to save configuration.
Area	Select the area to which the door detector is assigned.

Parameter	Description
24 H protection Zone	The zone in which the door detector enters into armed state. If enabled, alarm will be triggered when event is detected.
Home Mode	Arming mode at home.
Delay Mode Under Home Mode	Enter into delay arming mode at home.
Delay Time	● The period of time that you can leave through or enter the protection zone without alarm. ● Select from 0 s to 120 s. The arming mode will be ineffective after the delay time.
External Detector Access	Connect the wired peripheral with alarm cable.
Alarm-speaker Linkage	When an alarm is triggered, the selected device channel will alert with siren.
Alarm-video Linkage	When an alarm is triggered, the live video of the selected device channel will be displayed on the DMSS app.
Video Channel	After selecting video channel, the linked video channel will store alarm recordings.
Signal Strength Detection	Check the current signal strength. Install the detector in an area with great signal strength.
Detector Test	Tap **Start Detection** to check the status of the detector.
Transit Power	● The higher the transmission power, the farther the transmission and the higher power consuming. ● Select from high, low, and automatic.
Cloud Update	Update online.

● Tap the alarm detector under an alarm hub to view the settings of alarm detector.

Figure 8-4 Parameters
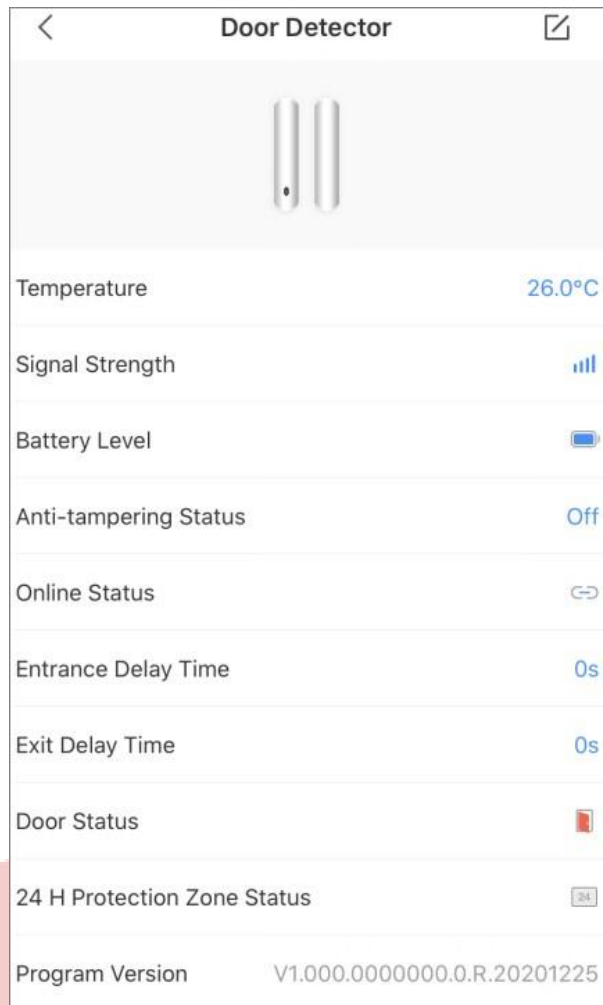
Table 8-3 Parameter description

Parameters	Value
Temperature	The temperature of the environment. The temperature is measured on processor and changes gradually.
Signal Strength	The signal strength between the hub and the door detector. For details, see Figure 8-1.
Battery Level	The battery level of the detector. For details, see Figure 8-1.
Anti-tampering Status	The tamper mode of the detector, which reacts to the detachment of a damage of the body.
Online Status	Online and offline status of the detector. For details, see Figure 8-1.
Entrance Delay Time	The period of time that you can leave through or enter the protection
Parameters	**Value**

	zone without alarm.
Exit Delay Time	● Entrance delay time: If entrance delay time is configured for the delayed zone, when you enter an armed delayed zone, the zone alarm will not be triggered until the end of entry delay. ● Exit Delay Time: If exit delay time is configured for the delayed zone, after you arm the zone on the indoor unit, you can exit the zone without triggering alarm until the end of exit delay.
Door Status	Open or close status of the door. ● Open: . ● Close: .
24 H Protection Zone Status	If enabled, the door detector will enter into armed state for 24 hours. ● Enable: . ● Disable: .
Program Version	The program version of the door detector.
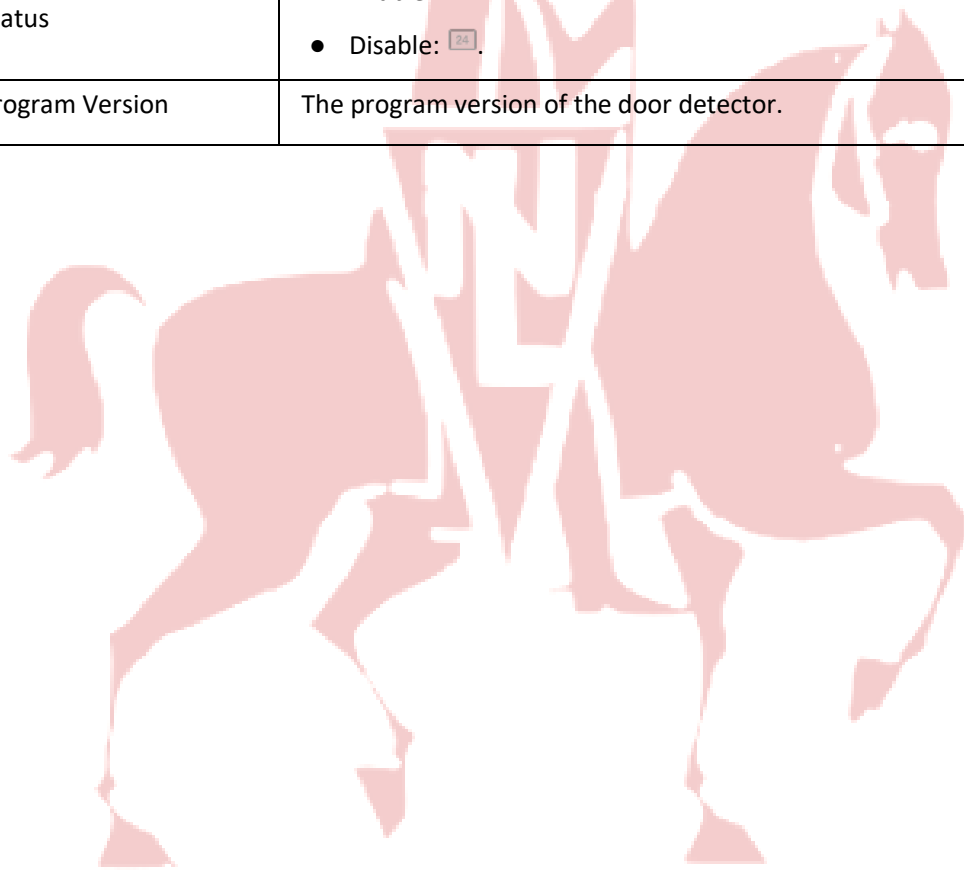
8.2 Arming and Disarming

After the accessory is added to arming mode, an alarm will be trigged only in armed status. It supports two types of arming and disarming modes: Manual, and scheduled arming and disarming.

Figure 8-5 Alarm hub
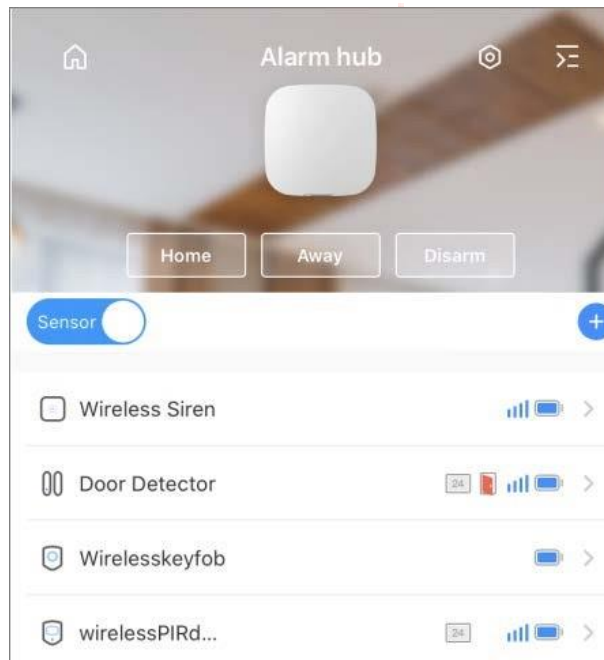
8.2.2 Manual Arming and Disarming

You can manually arm and disarm a single area or all the areas.

Arming and Disarming a Single Area

Step 1   Go to **Hub** interface.

Step 2 Tap (Area), and then select from **Home**, **Away**, **Disarm** , and **Disable** in the white box, to switch arming modes.

Figure 4-20 Switch arming mode
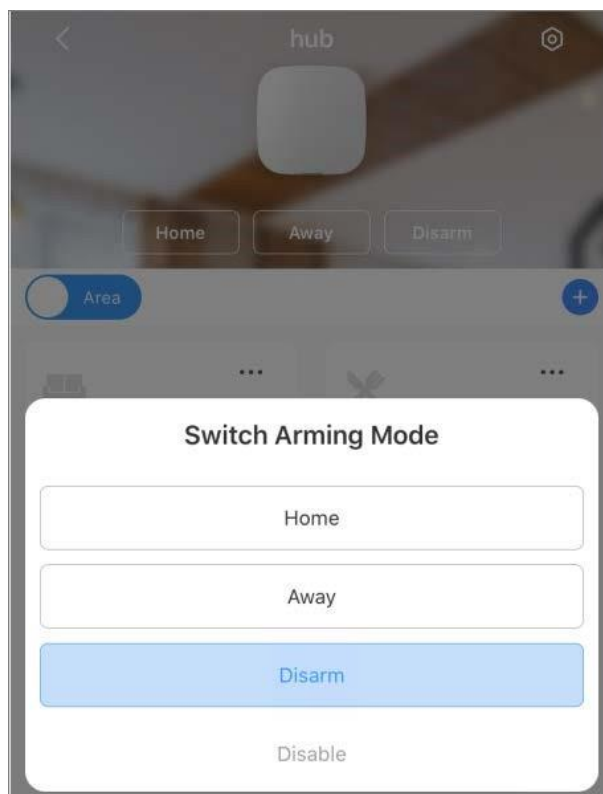
Arming and Disarming All the Areas

Step 1   On the **Hub** interface, tap ⊙, and then tap **Hub Setting**.

Step 2   Enable **Global Arming and Disarming**.

Step 3 Go back to the **Hub** interface, and then select from **Home**, **Away**, and **Disarm** at upper of the box.

Figure 4-21 Select mode

8.2.3 Scheduled Arming and Disarming

You can arm and disarm the selected areas by schedule.

Step 1   On the **Hub** interface, tap ⊙, and then tap **Hub Setting**.

Step 2   Enable **Schedule Arming and Disarming**.

9 File

You can view, manage, share, and export the recorded videos and snapshots in **File**.

Step 1 On the **Home** interface, tap ![folder icon] . Step 2

Operate on the interface.

- To share files, tap ![share icon], select one or multiple files, and then tap ![export icon].

- To save files on your album, tap ![save icon].

- To delete files, tap ![delete icon].

Figure 9-1 Files
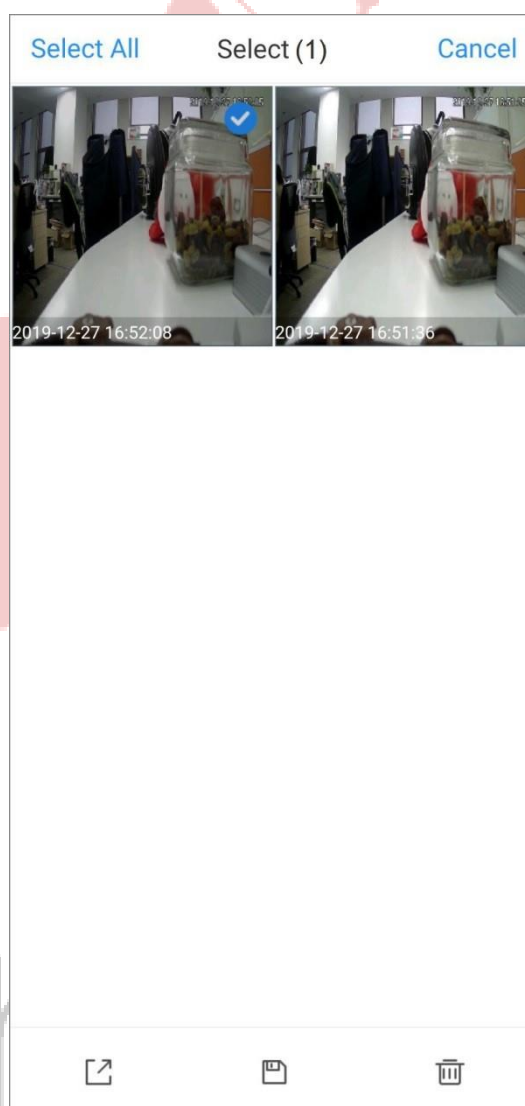
Step 3 Tap a video or a snapshot to view details, and for detailed function icon descriptions on video playback interface, see Table 4-1.

Figure 9-2 Recorded videos
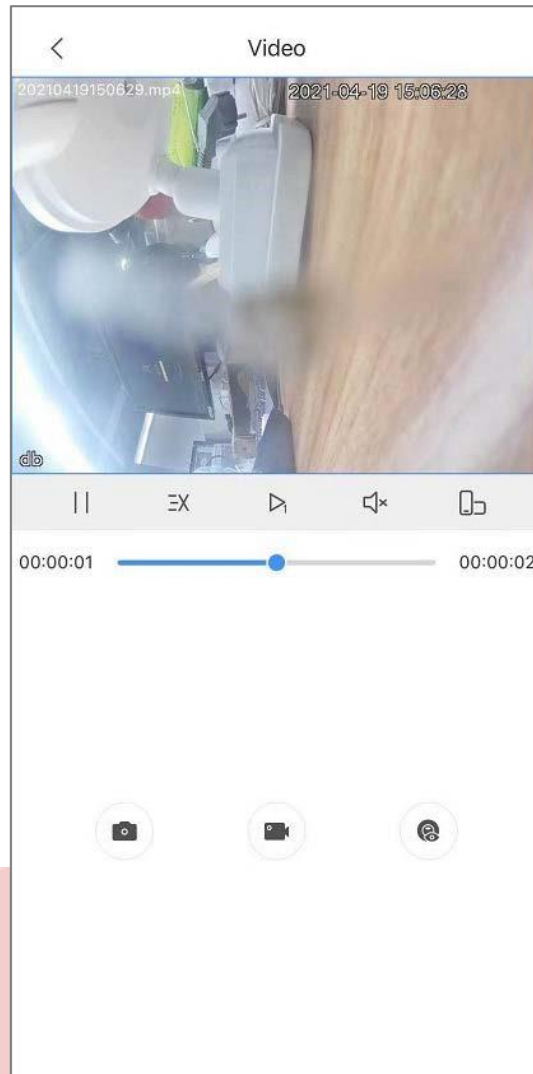
Related Operations

- $||$: Pause playing; $\triangleright$: Continue playing ● $\equiv X$: Change video speed, speed up or slow down video.

- $\triangleright$: Play by frame.

- $\triangleleft^{\times}$: Mute the video; $\triangleleft^{\gg}$: Unmute the video.

- $\square\square$: Changes image orientation to landscape.

10 Message

Alarm messages generated by added devices can be pushed to the App. You can view recorded videos, live video, and picture playback of alarm events.

$\square$

You need to set alarm rules and enable alarm function of the device or channel.

10.1 Subscribing Alarm Messages

You need to subscribe alarm messages, and then the alarm notification can be pushed to the App when the alarm is triggered. Here take local devices as an example.

Step 1   On the **Home** interface, tap ▪▪▪, and then tap **Device Details**.

Step 2   Tap **Notification**, enable the alarm subscription, and then set the period.

⌇

Tap **Others** to display more alarm types.

Figure 10-1 Enable alarm subscription
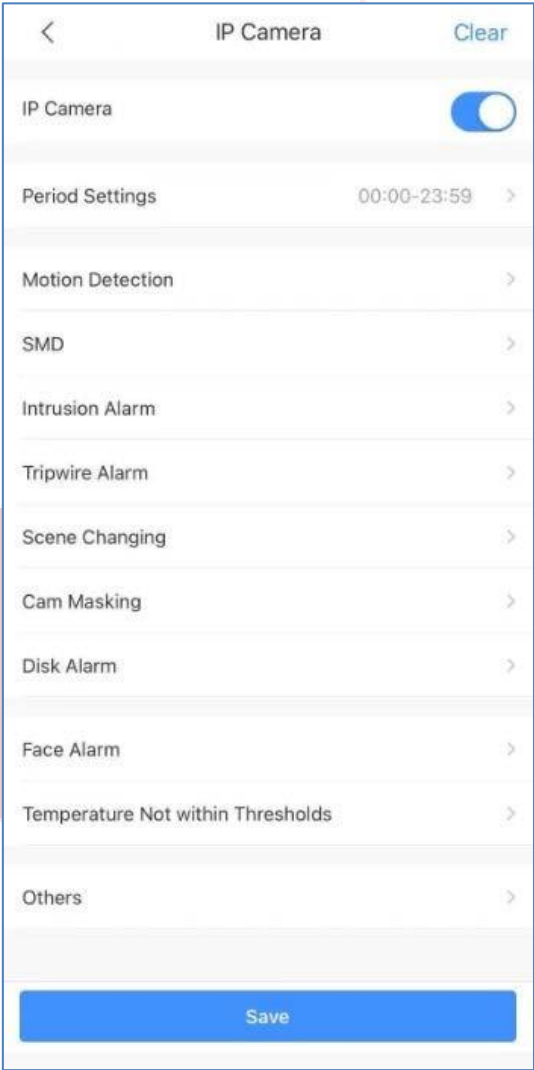
Step 3   Set alarm types as needed. Multiple alarm types can be selected simultaneously.

Table 10-1 Configure alarm subscription

Name	Description
Prompt type	**Live**: Live video is pushed when the alarm is triggered. **Video**: The recorded alarm video will be pushed when the alarm is triggered. ⌇ You need to install storage device and configure video plan of the device first.

Alarm type	Select alarm types and its specific alarm event, and then alarm notification will be pushed when the alarm events happened. **AI analysis**: The alarm is triggered when the defined rules are broken such as **Tripwire**, **Intrusion**, **Abandoned Object**, and **Scene Changing**. **Stereo Vision**: Defined behaviors will be detected and alarmed such as **Fall Detection**, **People Approaching**, and **People Stay**. **Thermal Alarm**: The alarm is triggered when there is abnormal temperature change in the image such as **Fire Alarm**, **Temperature Contrast Alarm**, **Hot Spot Alarm**, and **Smoking Alarm**. Thermal imaging alarm is supported by thermal cameras. **Motion Detection**: The alarm is triggered when there is abnormal moving object in the image. **Cam Masking**: The alarm is triggered when the camera is covered abnormally. **Defocus**: The alarm is triggered when the camera cannot focus on the target or has softened or blurred image. **Face Alarm**: The alarm is triggered when human faces are detected in the image and alarm is triggered under defined conditions including face detection and face recognition. **Audio Alarm**: Sound in the video is detected and alarm is triggered under conditions such as abnormal audio output and intensity change. **HDD Alarm**: The alarm is triggered when no disk, low space or disk error occur. **Voltage Test**: The alarm is triggered when the device voltage is too low or too high. **Network Alarm Type**: Notification is pushed when network alarm, and IPC offline alarm occur. **Sensor Alarm**: The alarm is triggered when there is alarm information from the connected sensors such as **IPC External Alarm**, and **Accessory Alarm**. **Battery Alarm**: The alarm is triggered with low battery or low solar energy. **License Plate Recognition**: The alarm is triggered when detecting a blocklist vehicle. **IPC External Alarm**: When a device connecting to an IPC, such as NVR, is added to the App, notification will be pushed when an alarm is generated on the IPC.

Step 4   Save settings.

$\square$

For account devices, you can also arm and disarm the zone.

10.2 Viewing Messages

Tap **Message** at the bottom of the interface.

Figure 10-2 Message
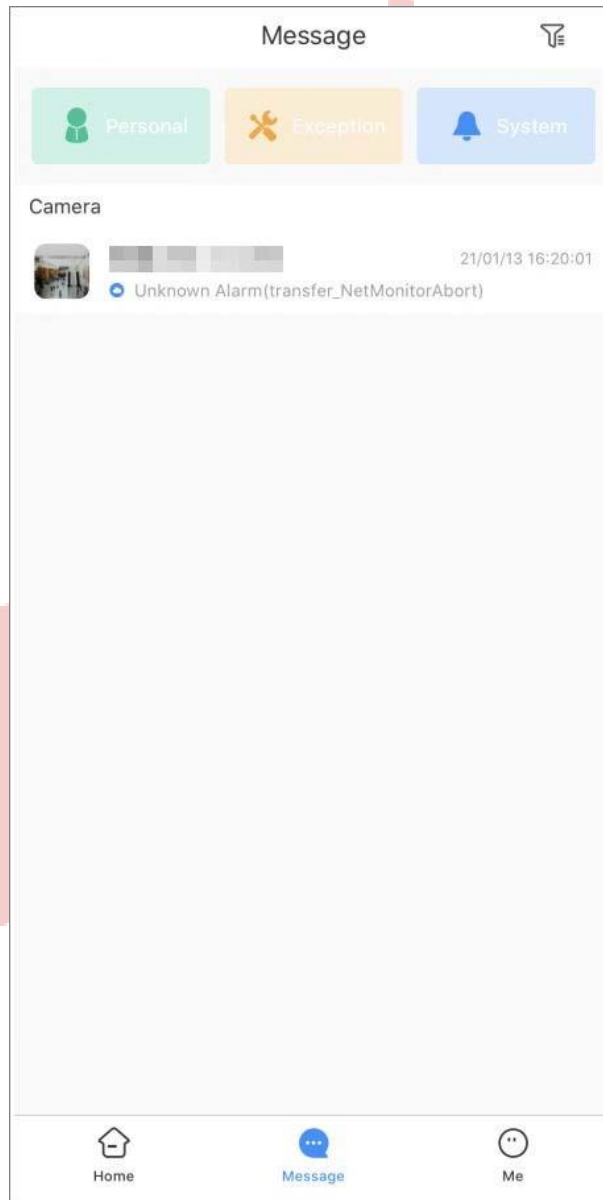
Table 10-2 Message description

Function	Description	
Personal message	Display messages such as sharing devices, and deleting devices.	$\square$ Personal, exception and system messages can only be viewed after login.
Exception message	Display messages such as exception type, occurrence and resoluton time, and rating of the service.	
System message	Display messages such as system maintenance and declaration.	

Function	Description
Alarm message	Display messages when alarm events happened. ◎━⊓ Tap ▽≡ at the upper-right corner to filter alarm message sources from cameras, video intercoms, alarm devices, all devices, and more.

Step 1   On the **Message** interface, tap an alarm event to view its alarm messages.

◎━⊓

Tap 🔔 to stop the alarm sound from detectors.

Figure 10-3 Alarm messages
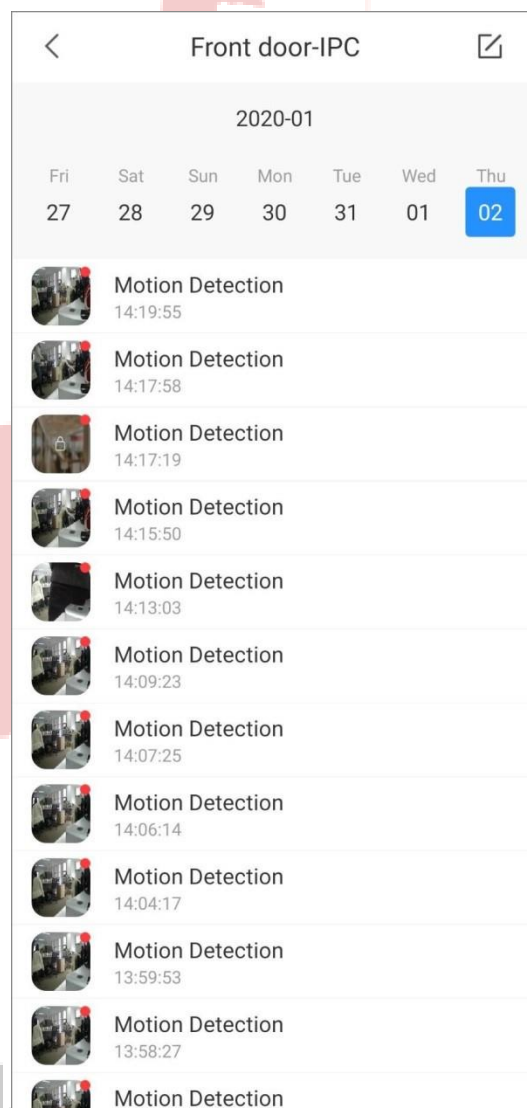
The message with red point is unprocessed.

Step 2 Tap the alarm message as needed, and then the message is displayed as the prompt type you set. For detailed function icon descriptions, see Table 3-1 and Table 4-1.

Step 3 (Optional) Click **Live view** to go to the live view interface.

Figure 10-4 Display the alarm message
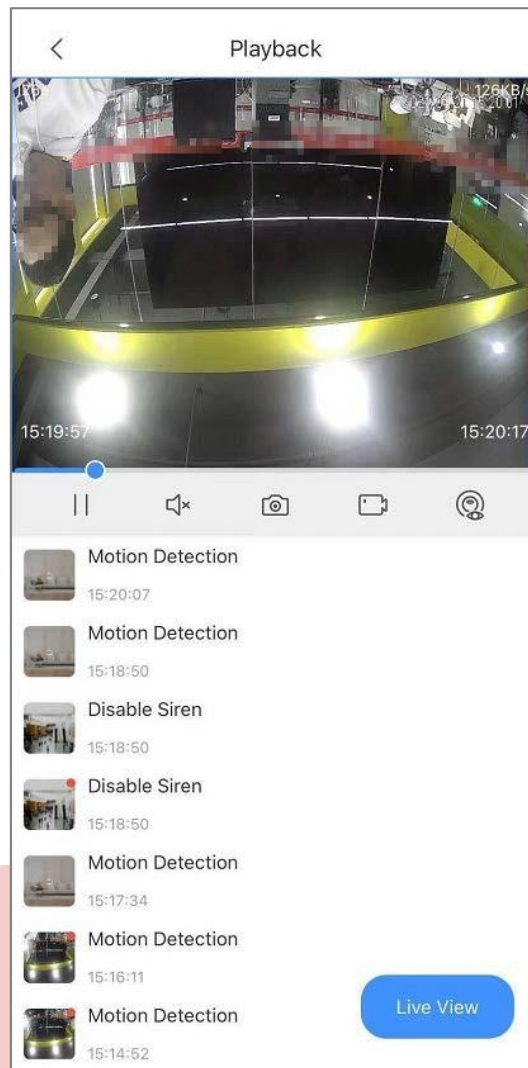
10.3 Marking Alarm Messages

Step 1   Tap **Message** at the bottom of the interface.

Step 2   Tap an alarm event to view its alarm messages.

Step 3   Tap ⬚, select one or multiple messages with red dot, and then tap **Mark as read** to mark the

selected messages as read.

10.4 Deleting Alarm Messages

Step 1   Tap **Message** at the bottom of the interface.

Step 2   Tap an alarm event to view its alarm messages.

Step 3   Tap ⬚, select one or multiple messages, and then tap **Delete**.

11 System Configuration and Account Management

On **Me** interface, you can manage account information and configure system parameters.

Figure 11-1 Me
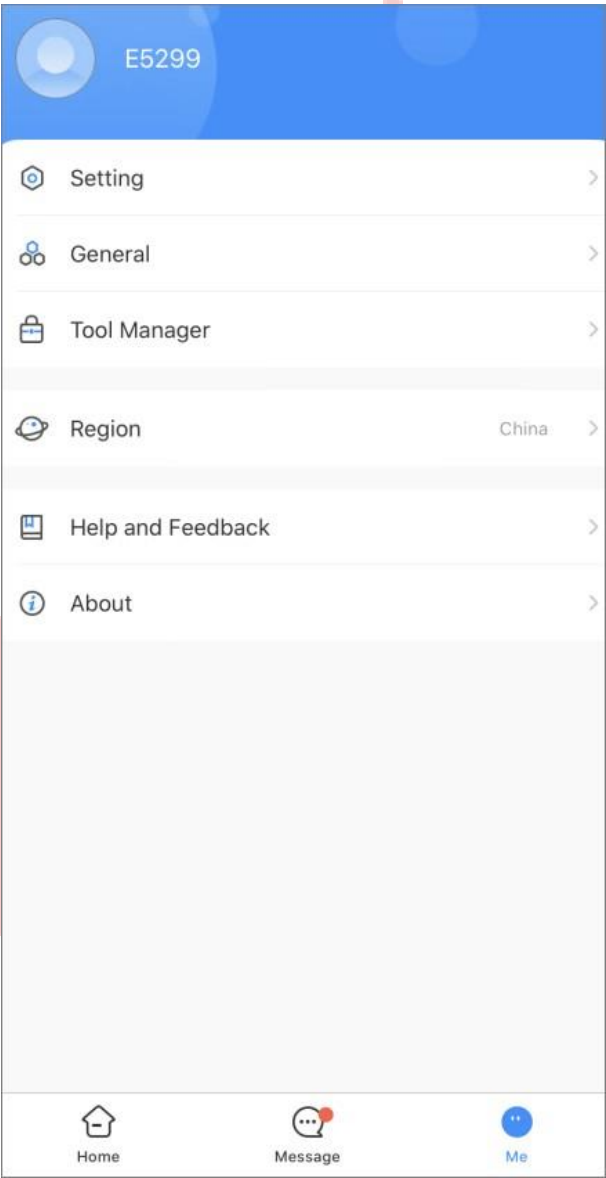
Table 11-1 Me

Name	Description
Account management	Tap ![icon] to go to the **Account Management** interface. You can change the account password, delete account, export account information, and log out.
Setting	PTZ speed: Select the speed for PTZ camera from 1 to 8. The higher the value is, the faster the PTZ moves. 📖 The function is available on cameras supporting PTZ.

Name	Description
	Capture mode: Set quantity of manual snapshot for a single time.
	NR setting: The higher the NR level is, the better the noise reduction will be.
	Hard decoding: Enable **Hard Decoding**, and then the performance of video stream is improved.
	Pushed video delay: Set delay of pushed recordings. Total pushed video duration=10 s before recording started + recording duration + delay time you set. Default page: Select page interface as needed.
	Password protection: Enable **Password Protection**, set password, and then you need to enter password every time you log in to the App or return to App from any interruption.
General	Auto Play When Not in a Wi-Fi Network: Enable **Auto Play When Not in a Wi-Fi Network**, and then videos can be automatically played with other network such as cellular data.
	Notification and Period: Enable **Notification** and set push period, and then notifications can only be pushed within the defined period. Period setting is only supported by account devices.
	Appearance Mode: Select from dark mode and light mode.
	Picture-in-Picture: Enable **Picture-in-Picture** mode, and then live video can be viewed on the small floating windows simultaneously.
	Clear Cache: Clear browsing data.
Tool Manager	Test Wi-Fi status and notification pushing status of VTO, and reset device password.
Region	Reselect your region.
Help and Feedback	View brief function introduction of each module. 📖 Tap 🔍 to search specific functions with keywords.
About	View information about the App

Appendix 1 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 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.