

DMSS App

User's Manual



V1.6.0

Foreword

General

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

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	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.6.0	Updated the home page, alarm hub functions and tool for transferring local devices.	July 2023
V1.5.0	Added Configuring DDNS and UPnP.	November 2022
V1.4.0	• Updated methods for adding devices. • Optimized the function for entrusting and sharing devices, and added countries that support device entrusting services. • Optimized device details. • Updated the descriptions of all the chapters. • Updated images.	January 2022
V1.3.0	• Added illumination settings function. • Added function of entrusting device in batches. • Updated device sharing functions. • Added IPC external alarm	April 2021
V1.2.0	• Optimized language. • Updated images • Deleted cloud storage, and FAQ.	January 2021

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

Foreword	I
1 Overview	1
1.1 Introduction	1
1.2 Applicable OS	1
2 Login	2
2.1 Signing Up	2
2.2 Resetting the Password	4
3 Home	7
4 Adding Devices	9
4.1 Adding by SN/QR Code	9
4.2 Adding by IP/Domain searching	9
4.3 Adding through Online Searching	10
5 Configuring DDNS and UPnP	11
5.1 Configuring DDNS	11
5.2 Configuring UPnP	12
6 Basic Operations	15
6.1 Configuring Devices	15
6.1.1 Alarm Settings	16
6.1.1.1 Notification	16
6.1.1.2 Multi-channel Alarm Subscription	18
6.1.1.3 Alarm Ringtone Settings	18
6.1.1.4 Disabling Alarm Linkage	19
6.1.2 Video Play Settings	19
6.1.2.1 Stream Settings	19
6.1.2.2 Customizing Audio and Video Encryption	20
6.1.3 Device Configuration	20
6.1.3.1 Audio Recording	20
6.1.3.2 White Light	21
6.1.3.3 LED Indicator	22
6.1.4 General Configuration	22
6.1.4.1 Time Zone	22
6.1.4.2 Device Sharing	22
6.1.4.3 Cloud Update	22
6.1.5 Others	22
6.1.5.1 Remote Configuration	22

6.1.5.1.1 Video Detection	23
6.1.5.1.2 Alarm Settings.....	26
6.1.5.1.3 Camera Settings	27
6.1.5.1.4 Record Plans	29
6.1.5.1.5 Image Adjustment.....	31
6.1.5.1.6 Storage Manager.....	33
6.1.5.1.7 Arm/Disarm Period	34
6.1.5.2 Alarm Output.....	34
6.2 Sharing Devices.....	34
6.3 Applying for Security Services.....	35
6.4 Entrusting Devices	36
6.4.1 Entrusting Devices One by One	36
6.4.2 Entrusting Devices in Batches	37
6.5 Creating Device Cards.....	38
6.6 Resetting and Modifying the Device Password.....	39
7 Live View	41
8 Video Playback	45
9 Video Call.....	48
10 Access.....	50
11 Alarm.....	53
11.1 Single Arming and Disarming	53
11.2 Global Arming and Disarming.....	54
11.3 Manual Arming and Disarming.....	55
11.4 Scheduled Arming and Disarming	55
12 Message.....	56
12.1 Subscribing for Alarm Messages.....	56
12.2 Viewing Messages	56
13 Favorites.....	58
14 Me	59
Appendix 1 Cybersecurity Recommendations.....	63

1 Overview

1.1 Introduction

DMSS is a mobile surveillance app with functions such as remote monitoring, video playback, push notifications, remote configuration, device sharing and entrusting. Devices such as IPC, NVR, XVR, VTO, door bells, alarm hubs, and access controllers can be added.

1.2 Applicable OS

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

2 Login

For first-time use, you need to create an account. This user manual uses the operations for iOS as an example.

2.1 Signing Up

Procedure

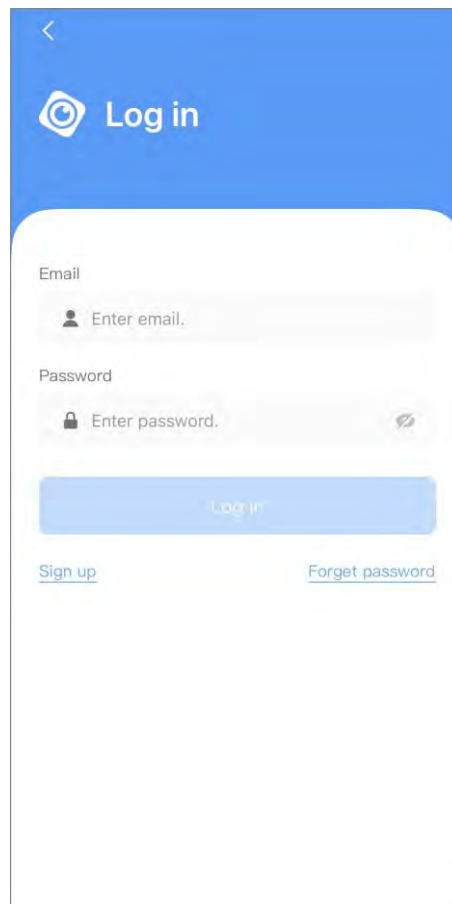
Step 1 Search for DMSS in the App store, and then download the app.



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

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

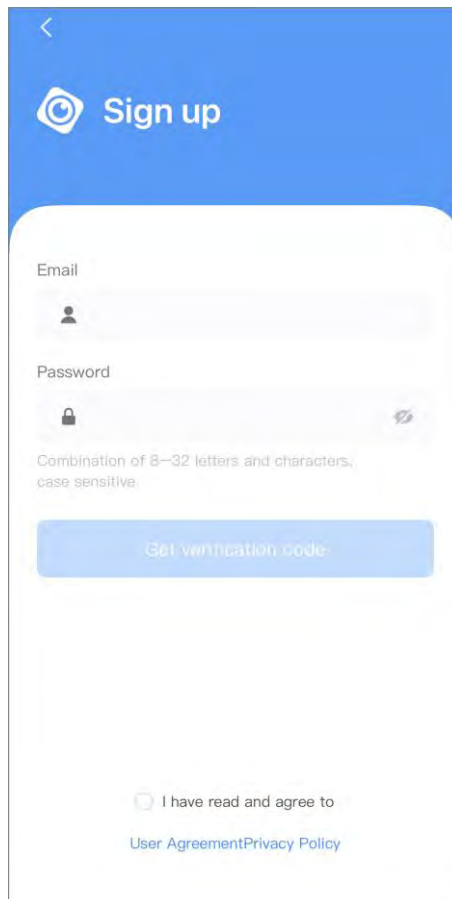
Figure 2-1 Login



Step 3 Create an account.

1) On the **Log in** screen, tap **Sign up**.

Figure 2-2 Sign up



The image shows a mobile application's sign-up screen. At the top, there is a blue header with a back arrow and the text 'Sign up' next to a logo. Below the header, there are two input fields: 'Email' with a person icon and 'Password' with a lock icon. A small text note below the password field states: 'Combination of 8–32 letters and characters, case sensitive.' Below these fields is a blue button labeled 'Get verification code'. At the bottom, there is a checkbox labeled 'I have read and agree to' followed by links for 'User Agreement' and 'Privacy Policy'.

- 2) Enter your email address and password.



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

- 3) Read the **User Agreement** and **Privacy Policy**, and then select the **I have read and agree to** checkbox.
- 4) Tap **Get verification code**, check your email box for the verification code, and then enter the code.



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

Figure 2-3 Enter verification code



5) Tap **OK**.

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



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

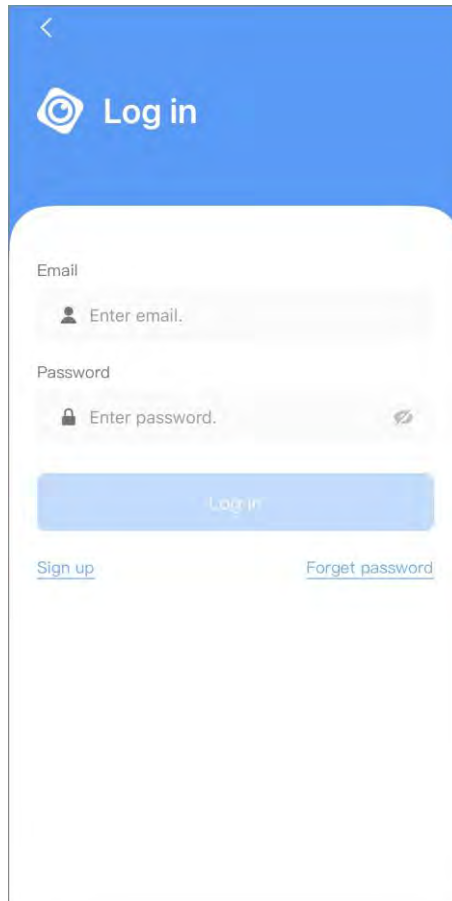
2.2 Resetting the Password

On the **Login** screen, you can reset your password.

Procedure

Step 1 Tap **Forget password**.

Figure 2-4 Login

The image shows a mobile application login screen. At the top, there is a blue header bar with a white back arrow icon on the left and the text "Log in" in white. Below the header, the main content area is white. It features two input fields: "Email" with a placeholder "Enter email." and a person icon, and "Password" with a placeholder "Enter password." and a lock icon. To the right of the password field is a small eye icon for toggling visibility. Below these fields is a blue "Log in" button. At the bottom, there are two links: "Sign up" on the left and "Forget password" on the right.

Step 2 On the **Forget password** screen, enter the email address that you set during registration, set a new password, confirm it, and then tap **Get verification code**.

Figure 2-5 Forget password

< Forget password

Email

New Password

Confirm Password

Combination of 8–32 letters and characters, case sensitive.

Get verification code

Step 3 On the **Forget password** screen, enter the verification code obtained from the email, and then tap **OK**.



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

Step 4 On the **Log in** screen, tap **Log in**.

3 Home

Figure 3-1 Home

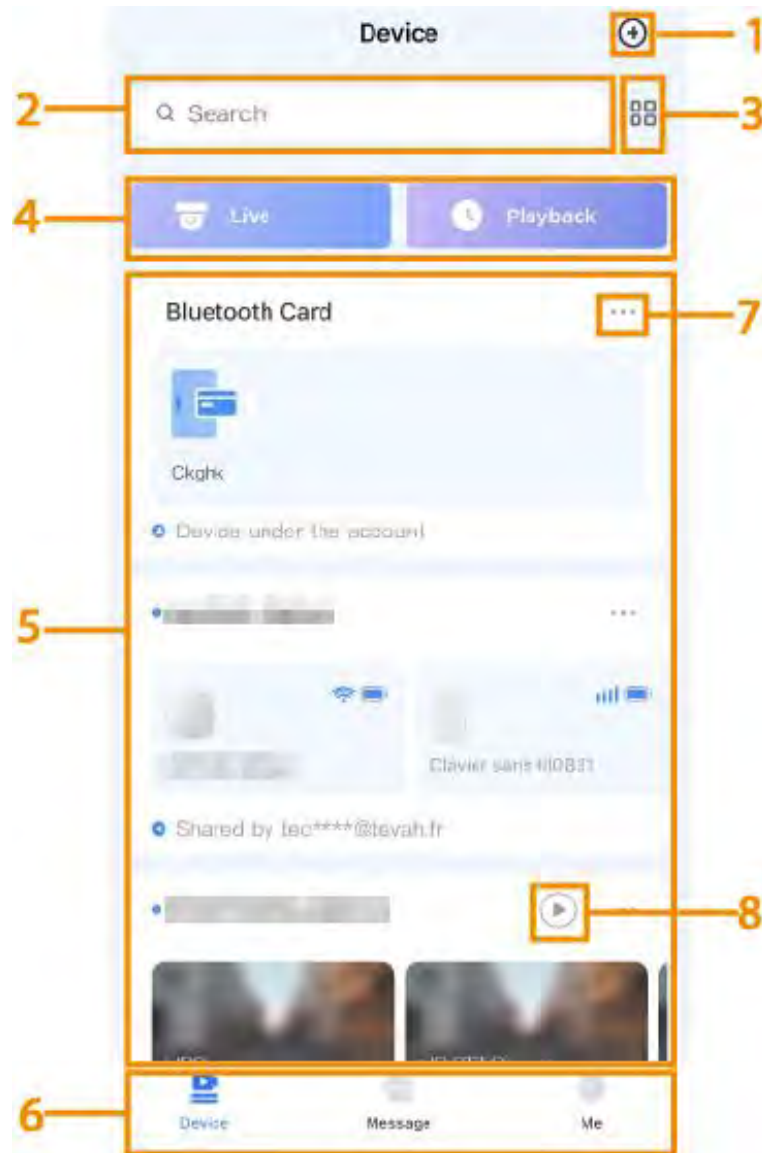


Table 3-1 Description of the home page

No.	Name/Icon	Description
1		Tap to add devices. For details, see "4 Adding Devices".
2	Search	Tap it and then enter the keywords to search for a device.
3		Tap to switch displaying mode of devices.
4	Functions	- Tap Live to go to live view page. - Tap Playback to go to the playback page.
5	Devices	Displays the information of added devices.
6	Navigation bar	Tap Device , Message or Me to go to the corresponding modules.

No.	Name/Icon	Description
7	...	Tap to view the details on the device. If the device is not on the top, you can tap this icon, and then select Move to the Top to move the device to the top of the list.
8		Tap to go to the live view page.

4 Adding Devices

You can add devices by manually entering the device SN, scanning the QR code, entering the IP of the device or specific domain, or by performing an online searching.

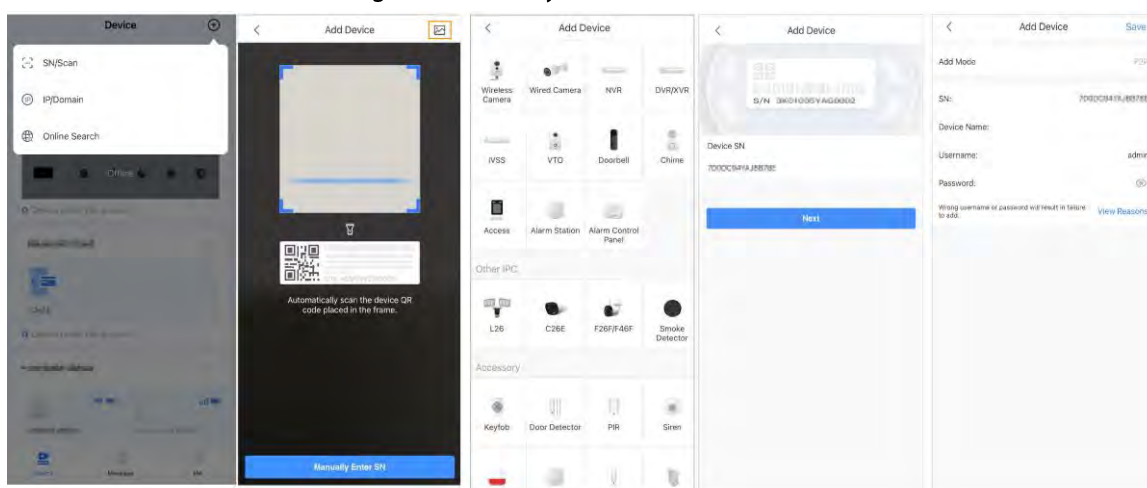
4.1 Adding by SN/QR Code

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

Procedure

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

Figure 4-1 Add by SN/QR code



Step 2 Add a device.

- Scan the device QR code directly, or tap  and import the QR code picture to add a device.
- Tap **Manually Enter SN**, and then enter the device SN to manually add a device.

Step 3 Select the device type, and then tap **Next**.



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

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

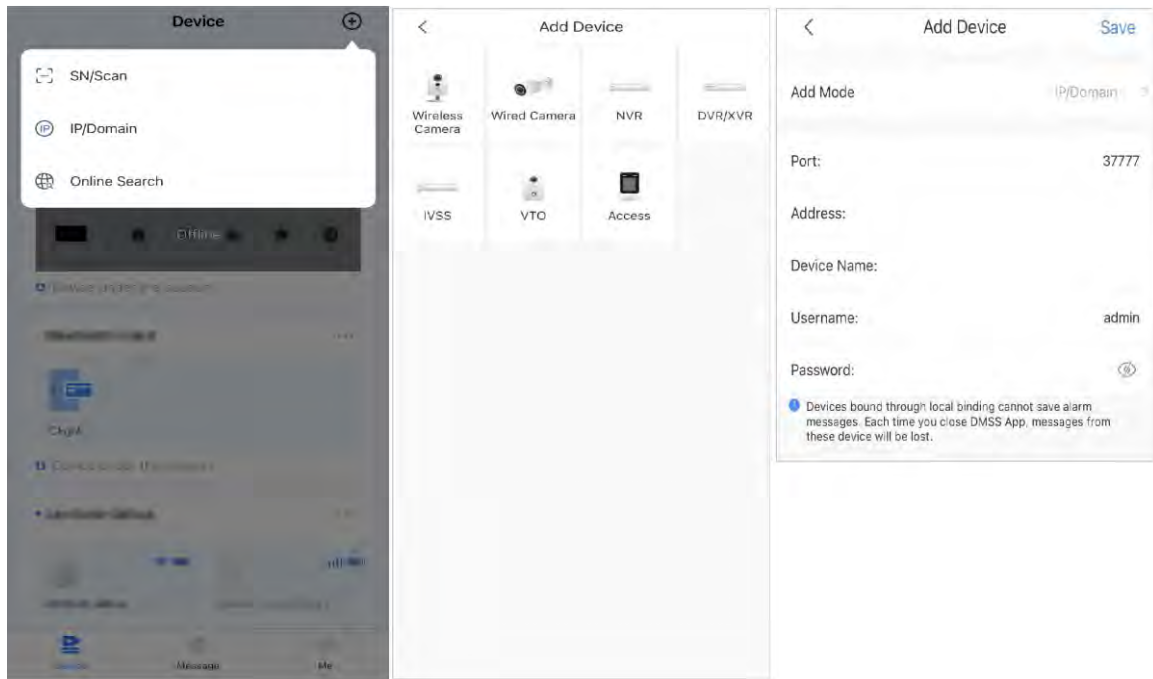
4.2 Adding by IP/Domain searching

You can add devices by entering the IP of the device or specific domain.

Procedure

Step 1 On the **Device** screen, tap , and then select **IP/Domain**.

Figure 4-2 Add by IP/domain searching



Step 2 Select the device type, and then tap **Next**.

Step 3 Enter information as needed, and then tap **Save**.

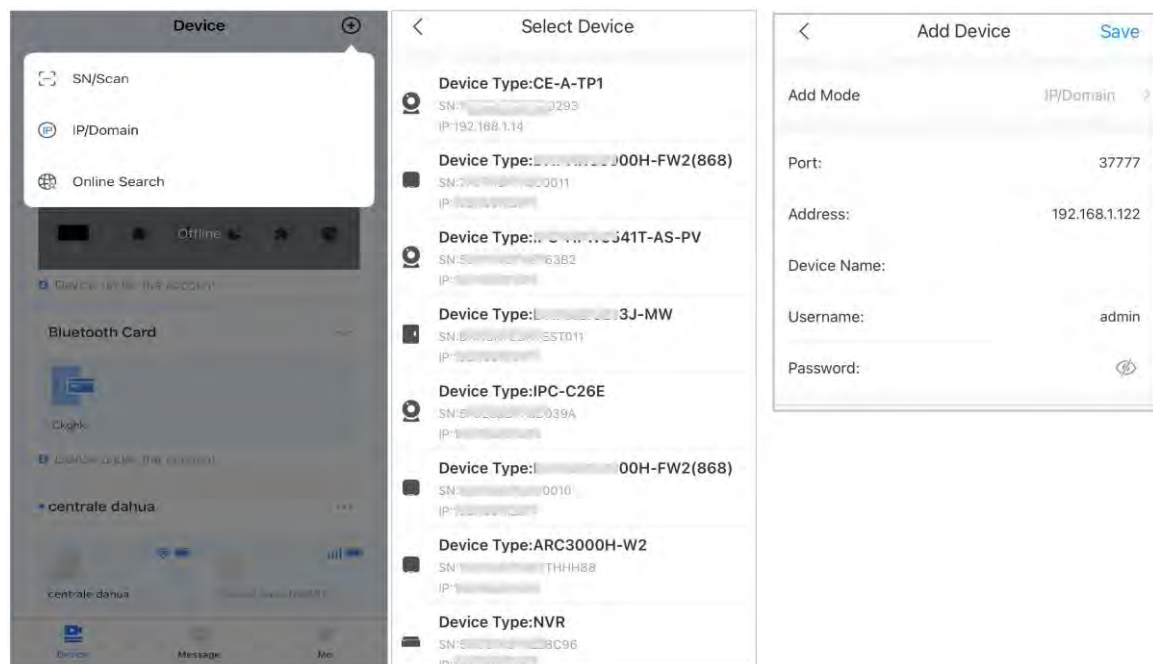
4.3 Adding through Online Searching

You can search for online devices and add them.

Procedure

Step 1 On the **Device** screen, tap **+**, and then select **Online Search**.

Figure 4-3 Add through online search



Step 2 On the **Select Device** screen, select the device as needed.

Step 3 On the **Add Device** screen, enter information as needed, and then tap **Save**.

5 Configuring DDNS and UPnP

5.1 Configuring DDNS

Configure DDNS (Dynamic Domain Name System) parameters to bind the domain of the DNS server to the Extranet IP of the device to directly access the device.

Prerequisites

- Make sure that the device supports the server that can achieve domain name resolution.
- Make sure you have the account registered by third-party DDNS. Here uses NO-IP registration as an example: Go to the website to fill in information for registration.
 - ◇ Signing up address: <https://www.noip.com/sign-up>.
 - ◇ Getting started guide: <https://www.noip.com/support/knowledgebase/getting-started-with-no-ip-com/>

Figure 5-1 Free sign up

Create Your No-IP Account

Indicates required fields

Email *

Password *

Minimum of 8 characters

Choose a hostname for your account. You can change your hostname or add more later.

Hostname: noip.org

Choose a hostname for your account. You can change your hostname or add more later.

If you have chosen an Enhanced domain, but want to sign up for a No-IP Free account, please choose the appropriate domain option.

Why not upgrade?

Upgrade to Enhanced Dynamic DNS Today! Learn more about the benefits of upgrading below:

	Enhanced DDNS	Free DDNS
Domain Choices	50+	1
Hostnames	1	1
No Ads	✓	✗
No 30-Day Hostname Confirmation	✓	✗
Phone Support	✓	✗
Includes 1 TrustCor Standard DV SSL Certificate	✓	✗
	\$1.99/mo	\$0

Terms of Service and Privacy Policy *

☒ I agree to the Terms of Service and Privacy Policy. I also agree that I will only create one free account.

Email Opt-In

☒ Send me newsletters & special offers

Get Enhanced Free Sign Up



After enabling DDNS, the third-party server might collect your device information.

Procedure

- Step 1** After adding devices, go to the **Add Device** screen, and then click **Third-party DDNS** to configure.
- You can also select **Device Details** > **Third-party DDNS** to configure.
- Step 2** Click **Type**, and then configure parameters as required.
- Step 3** Click **Save**.

Figure 5-2 DDNS parameters



Table 5-1 DDNS parameter description

Parameter	Description
Type	The name and address of the DDNS server supplier, with the following connection: • CN99 DDNS: The server address is <i>www.3322.org</i>. • NO-IP DDNS: The server address is <i>dynupdate.no-ip.com</i>. • Dyn dns DDNS: The server address is <i>members.dyndns.org</i>.
Address	
IP/Domain	
Username	Enter the username and password from the DDNS server supplier. You need to register first at the website (including username and password).
Password	
Update interval	The interval of connection update between the device and the server.

5.2 Configuring UPnP

Establish mapping between Intranet and Extranet through UPnP (Universal Plug and Play) protocol to improve the transmission speed to quickly display live videos.

Prerequisites

- Log in to the router to connect the IP of the WAN port to Extranet.
- The router enabled UPnP.
- Connect the device to the router LAN port to Intranet.
- At the left-upper corner of the web page, click , select **Network settings** > **TCP/IP** to configure the router IP or enable **DHCP** to automatically acquire IP address.

Procedure

- Step 1 After adding devices, go to the **Add Device** screen, and then enable **UPnP** to configure it. You can also select **Device Details** > **UPnP** to configure it.
- Step 2 Click  to enable all.

Figure 5-3 Configure UPnP (1)

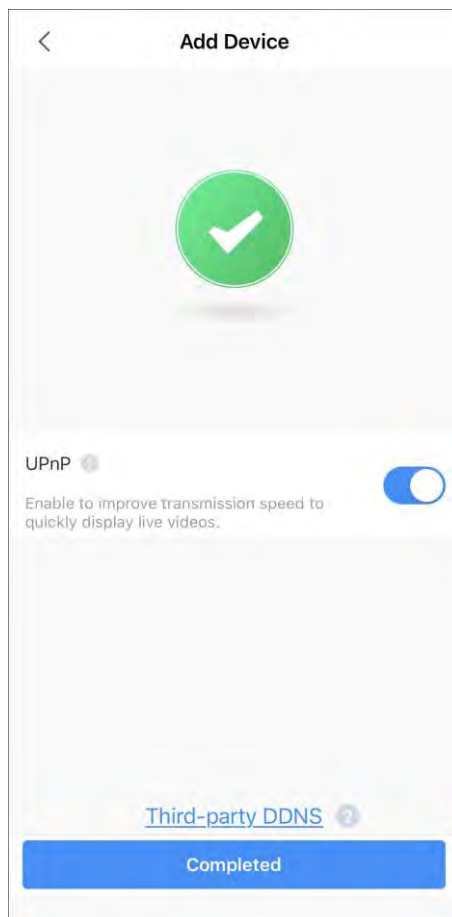
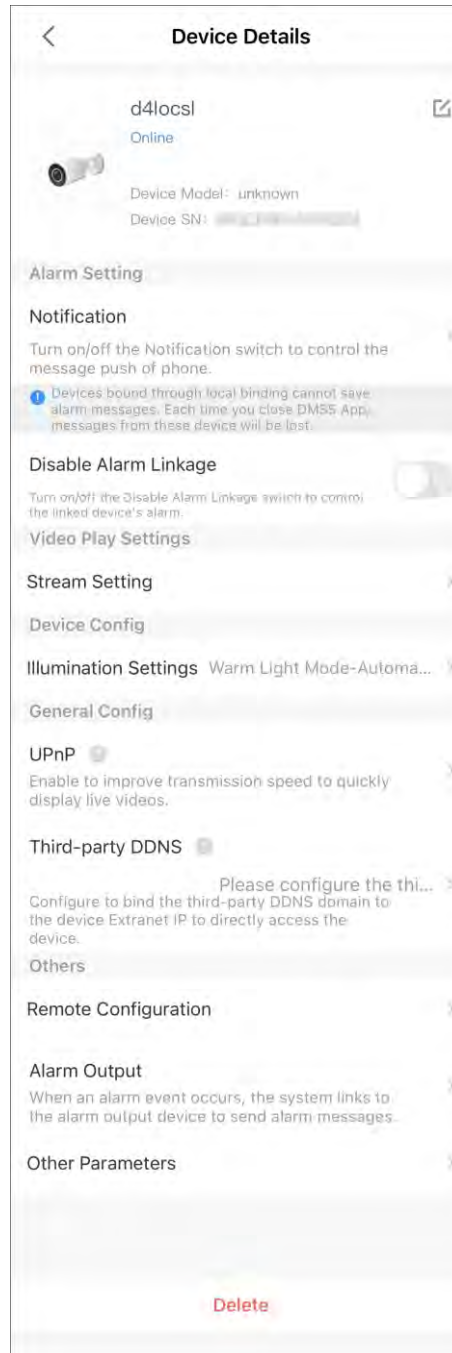


Figure 5-4 Configure UPnP (2)



6 Basic Operations

After adding devices, you can perform basic operations, such as configuring the parameters of devices, restarting and deleting devices on the **Device Details** screen, sharing and entrusting devices, creating device cards, and setting and changing the password of the device.



The interface might vary depending on the device.

6.1 Configuring Devices

Procedure

- Step 1 On the **Device** screen, tap **...** next to a device, and then tap **Device Details**.
- Step 2 Configure parameters on the **Device Details** screen.

Figure 6-1 Device details

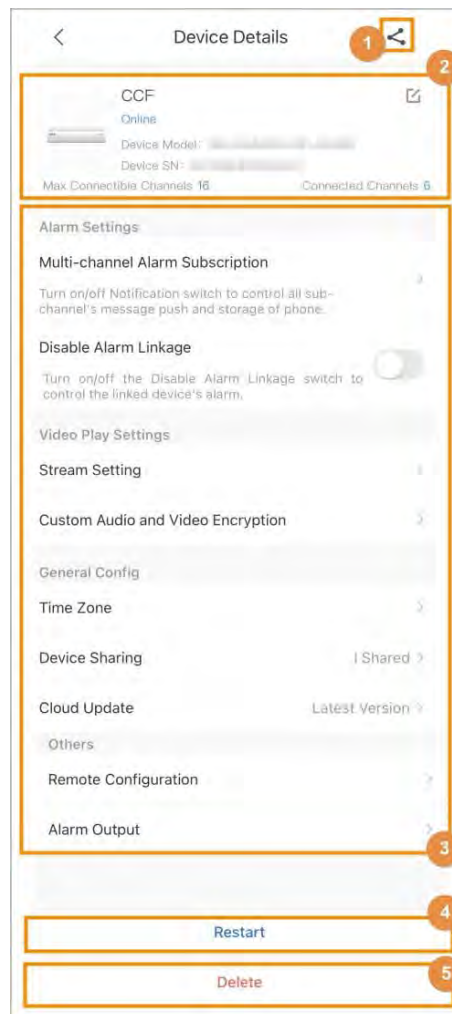


Table 6-1 Device details

No.	Description
1	Tap  to share the device. For details on sharing the devices, see "6.2 Sharing Devices".
2	- View basic information on the device, including device model, SN, and the maximum and current number of connectible channels. - Tap  to open the Device Configuration screen, and then modify the device name and password, and view linked channels and the SN. For details on modifying the device password, see "6.6 Resetting and Modifying the Device Password". On the Device Configuration screen, you can tap  to copy the device SN.
3	Configure devices. Device configuration can be divided into five categories: alarm settings, video play settings, device config, general config, and other basic configurations.  Some devices do not have the above 5 categories in the device configuration section. Please configure the device based on your actual situation. - For details on performing operations in Alarm Settings, see "6.1.5.1.2 Alarm Settings". - For details on performing operations in Video Play Settings, see "6.1.2 Video Play Settings". - For details on performing operations in Device Config, see "6.1.3 Device Configuration". - For details on performing operations in General Config, see "6.1.4 General Configuration". - For details on performing operations in Others, see "6.1.5 Others".
4	Tap Restart to restart the device.
5	Tap Delete to delete the device.

6.1.1 Alarm Settings

You can subscribe for alarm messages, disable alarm linkage, set push notifications, and more.

6.1.1.1 Notification

Background Information

You can subscribe for alarm messages to have notifications sent to DMSS when an alarm is triggered. You can set the type of notification to be sent. Multiple types of notifications can be selected simultaneously. This section uses configuring the IP camera as an example.

Procedure

- Step 1 On the **Device** screen, tap  next to a device, and then tap **Device Details**.
- Step 2 On the **Alarm Setting** section, tap **Notification**, and then configure the parameters.



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

Figure 6-2 Notification

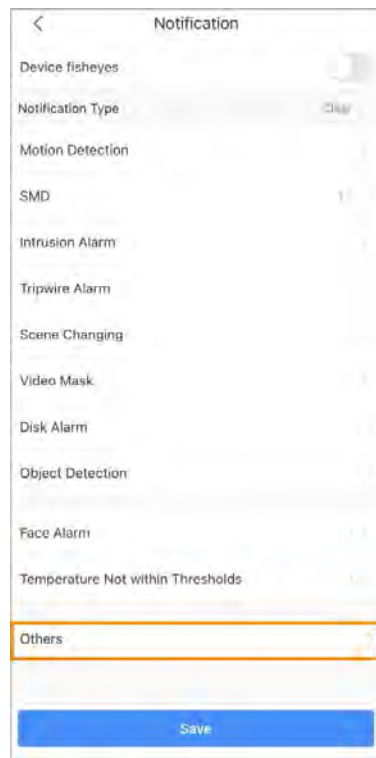


Table 6-2 Configure notification push

Notification Type	Description
Motion Detection	The alarm is triggered when a target is moving abnormally in the picture.
SMD	Select Motion: Human or Motion: Vehicle .
Intrusion Alarm	The alarm is triggered when the defined rules for functions are broken such as for Tripwire , Intrusion , Abandoned Object , and Scene Changing .
Tripwire Alarm	
Scene Changing	
Abandoned Object	
Video Mask	Alarm is triggered when the monitoring image is shielded and the output video is in single color.
Disk Alarm	Alarm is triggered when there is no disk, or disk error occurs.
Face Alarm	The alarm is triggered when human faces are detected in the image.
Temperature Not Within Thresholds	The alarm is triggered when the temperature is not within the thresholds.
IPC Offline Alarm	The alarm is triggered when the IPC is offline.
License Plate Recognition	The alarm is triggered when recognized the license plate.
Defocus	The alarm is triggered when the camera cannot focus on the target or the image has softened or become blurred.
Missing Object	The alarm is triggered when an object is missing from the image.

Notification Type	Description
Fast Moving	The alarm is triggered when there is a fast moving target in the image.
Loitering Detection	The alarm is triggered when people are loitering in the image.
People Stranding	The alarm is triggered when people remain in a location for longer than the defined time.
Fire Alarm	An alarm is triggered by the presence of fire.
Smoking Alarm	An alarm is triggered by the presence of smoke.
Phone Call Alarm	The alarm is triggered when people are making a phone call.
IPC External Alarm	When a device that is connected to an IPC, such as an NVR, is added to DMSS, notifications will be sent when an alarm is generated on the IPC.
Local Alarm	Connect the alarm device to the alarm input port of the added device. When an alarm is triggered, alarm linkage actions will be performed.
Network Alarm	Notifications are sent when a network alarm occurs.
Solar Energy Alarm	An alarm is triggered when solar energy levels are low.
Crowd Alarm	The alarm is triggered when there are a lot of people in the area, and crowd density reaches the limit.

6.1.1.2 Multi-channel Alarm Subscription

On the **Alarm Setting** section, tap **Multi-channel Alarm Subscription**, you can subscribe alarm messages for several channels of the device simultaneously, after which alarm notification can be pushed to the DMSS when the alarm is triggered.

The configuration for the multi-channels are the same as that of the device. For details on the notification type description, see "6.1.1.1 Notification".

6.1.1.3 Alarm Ringtone Settings

You can configure alarm ringtone.

Procedure

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

Step 2 In the **Alarm Setting** section, tap **Alarm Ringtone Setting**.

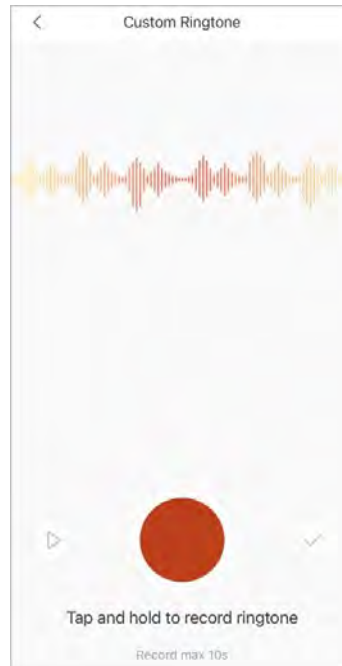
Step 3 On the **Alarm Ringtone Setting** screen, tap  next to **Alarm and Siren Linkage** to enable the function.

A prompt window will appear to alert you that the siren is very loud. If you are sure that you want to enable this function, tap **OK**, and then  will become .

Step 4 Set an alarm ringtone.

- Select an existing alarm ringtone.
- Tap , and then hold  to create your own custom ringtone.
Tap  when you finish recording. Tap  if you want to pause recording.

Figure 6-3 Custom a ringtone



6.1.1.4 Disabling Alarm Linkage

On the **Alarm Setting** section, tap  next to **Disable Alarm Linkage** to disable the function of alarm linkage.

6.1.2 Video Play Settings

You can set video stream parameters, create your own custom audio and perform video encryption.

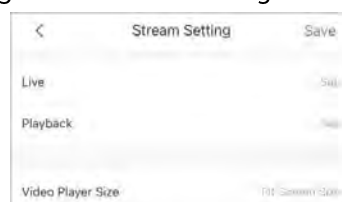
6.1.2.1 Stream Settings

You can set video streams and the size of the video player.

Procedure

- Step 1** On the **Device** screen, tap  next to a device, and then tap **Device Details**.
- Step 2** In the **Video Play Settings** section, tap **Stream Setting**, and then configure parameters.
- Select video streams from **Sub** or **Main** for live view or video playback.
 - ◇ **Main**: Has a large bit stream, small image compression size, and high resolution, but also requires large bandwidth.
 - ◇ **Sub**: Has a smaller bit stream, smooth video, and requires less bandwidth. It is used to replace main stream when the available bandwidth is insufficient.
 - Select **Fit Screen Size** or **Original Screen** for the size of the video player.

Figure 6-4 Stream setting



6.1.2.2 Customizing Audio and Video Encryption

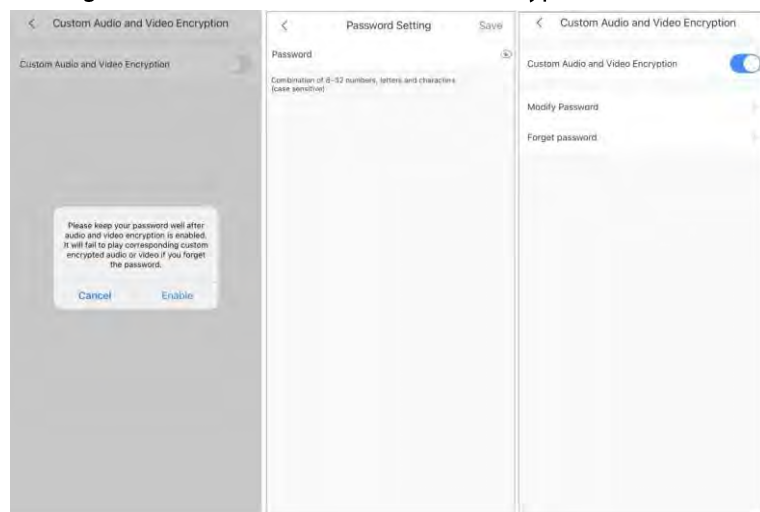
Background Information

You can create your own custom audio and perform video encryption. After enabling **Custom Audio and Video Encryption**, you need to enter the password for live view and playback (cloud videos included).

Procedure

- Step 1 On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2 In the **Video Play Settings** section, tap **Custom Audio and Video Encryption**, and then configure parameters.
- Step 3 On the **Custom Audio and Video Encryption** screen, tap ☐ next to **Custom Audio and Video Encryption** to enable the function.

Figure 6-5 Custom audio and video encryption



- Step 4 After a prompt appears, tap **Enable**.
- Step 5 On the **Password Setting** screen, set a password, and then tap **Save**.
After setting the password, **Modify Password** and **Forget password** will appear on the **Custom Audio and Video Encryption** screen, and ☐ will become ☒.

Related Operations

- To modify the password, tap **Modify Password** on the **Custom Audio and Video Encryption** screen, and then enter the old and new password.
- To change the password if you forget the old one, tap **Forget Password** on the **Custom Audio and Video Encryption** screen, and a verification email will be sent to your linked email. Enter the verification code from the email and then create a new password.

6.1.3 Device Configuration

You can set an audio recording, white light and LED indicator.

6.1.3.1 Audio Recording

In the **Device Config** section, tap ☐ next to **Audio Recording** to enable audio recording

function.

6.1.3.2 White Light

You can set white light.

Background Information

White light is activated when an alarm (such as motion detection or human detection) is triggered, and switches off when targets are not in the surveillance area.

Procedure

- Step 1 On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2 In the **Device Config** section, tap **White Light**.
- Step 3 On the **White Light** screen, tap ☐ next to **Alarm and White Light Linkage** to enable the function.

Figure 6-6 Alarm and White Light Linkage



- Step 4 Tap **Brightness**, and then select from 1, 2, 3, and 4 for brightness.

Figure 6-7 Brightness



- Step 5 Tap **Save**.

6.1.3.3 LED Indicator

On the **Device Config** section, tap **LED Indicator** to set LED indicator.

6.1.4 General Configuration

You can set the time zone, share devices and view device updating information.

6.1.4.1 Time Zone

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

Procedure

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

Step 2 On the **Device Details** screen, tap **Time Zone** of the **General Config** section.

Figure 6-8 Time zone



Step 3 Select the time zone that the device is in.

Step 4 (Optional) Tap ☐ next to **DST** to enable the function, and then set the start time and end time of the DST.

6.1.4.2 Device Sharing

On the **Device Sharing** screen of the **Device Config** section, you can share devices. For details on sharing devices, see "6.2 Sharing Devices".

6.1.4.3 Cloud Update

On the **Cloud Update** screen of the **General Config** section, you can view the current device version and upgrade the device when a new version is discovered by the system.

6.1.5 Others

You can remotely configure devices and set alarm output in the **Others** section.

6.1.5.1 Remote Configuration

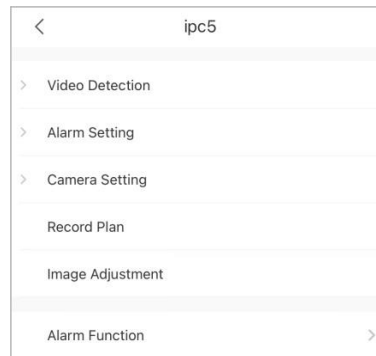
You can remotely configure the device including video detection, alarm settings, camera settings,

storage management, and image adjustment.

Procedure

- Step 1 On the **Home** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2 On the **Device Details** screen, tap **Remote Configuration** in the **Others** section, and then perform operations.

Figure 6-9 Remote configuration



6.1.5.1.1 Video Detection

When a target is detected as moving within the defined conditions, or the video image is shielded, the system will perform alarm linkage actions.

Motion Detection

An alarm linkage action is performed when a moving target appears in the image, and its speed reaches the sensitivity level.

1. On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
2. On the **Others** section, select **Remote Configuration > Video Detection > Motion Detection**.
3. Select the device channel that you want to configure.
4. Tap ☐ next to **Enable** to enable the function.
5. Tap ☐ next to **Advanced Configuration** to enable the function, and then configure other parameters.

Figure 6-10 Advanced configuration (motion detection)

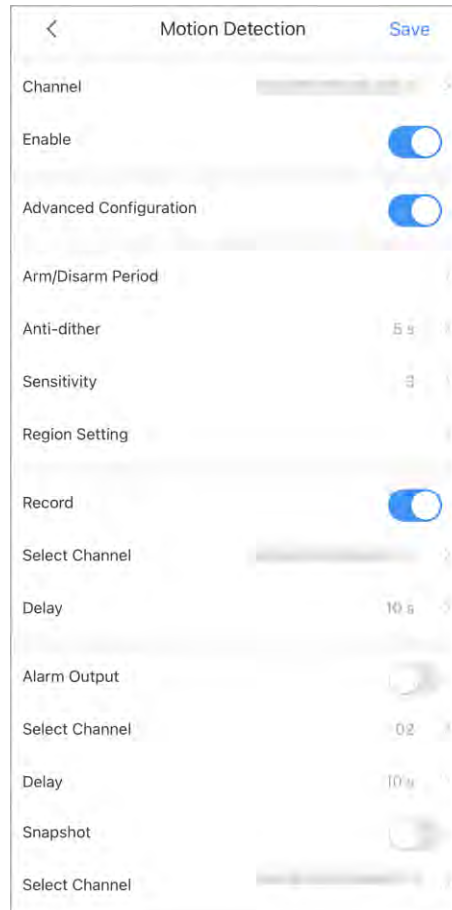


Table 6-3 Advanced configuration (motion detection)

Function	Description
Arm/Disarm Period	Set arming periods. The alarm can only be triggered when it occurs during the defined period. Select dates, tap  next to defined arming period, and then tap Save .
Anti-dither	Set the anti-dither period from 0 s to 600 s. Only one motion detection event is recorded during the period.
Sensitivity	Set the sensitivity value from 0 to 100. It is easier to trigger an alarm when the sensitivity level is higher.
Region Setting	Set the motion detection region. The entire video image is the monitoring area by default. - Tap  to set the motion detection region. - Tap  to clear the zone you have set. - Tap , and then pinch or stretch out your fingers to zoom in or out of the image.
Record	Tap  next to Record to enable the function, and then the system records automatically when an alarm is triggered.
Delay	The record will be generated for the alarm at the time that was selected and will be sent after the alarm ends.
Alarm Output	Tap  next to Alarm Output to enable the function, 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.

Function	Description
Snapshot	Tap ☐ next to Snapshot to enable the function, and then the system will automatically capture pictures when the alarm is triggered.

Figure 6-11 Arm/Disarm period

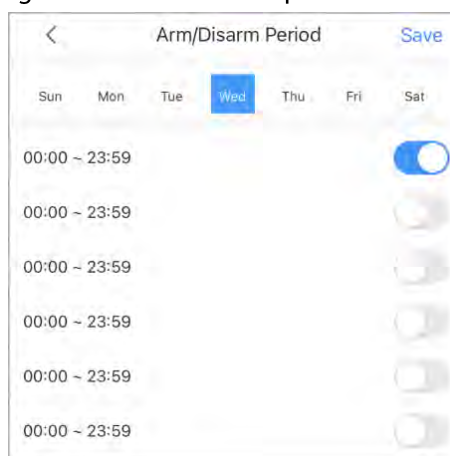
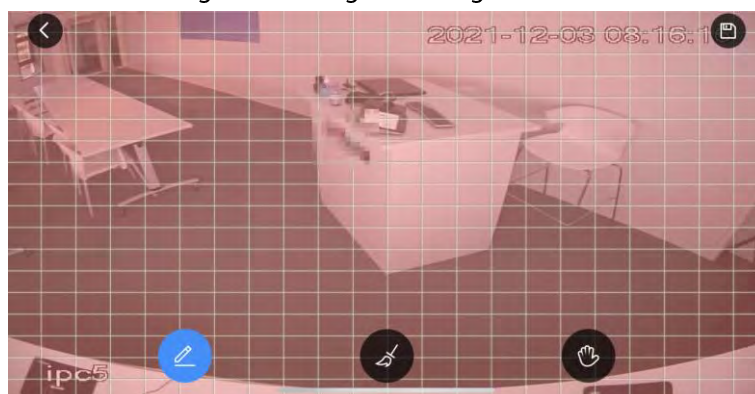


Figure 6-12 Region setting

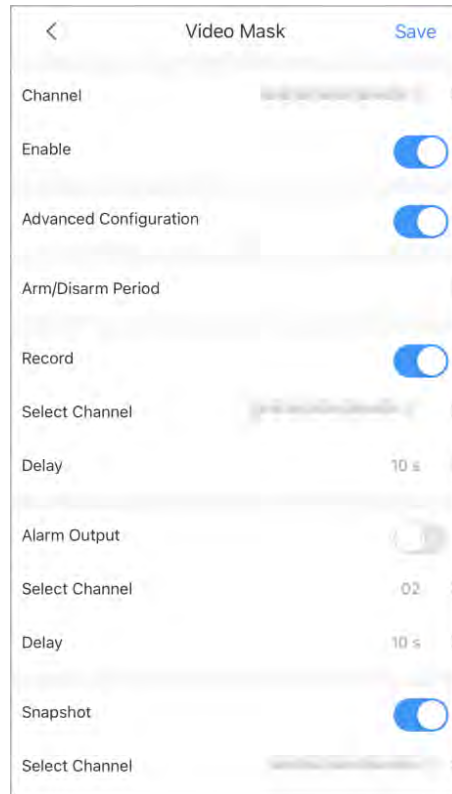


Video Mask

An Alarm is triggered when the monitoring image is shielded or the output video is in a single color.

1. On the **Device** screen, tap **...** next to a device, and then tap **Device Details**.
2. In the **Others** section, select **Remote Configuration** > **Video Detection** > **Motion Detection**.
3. Select the device channel that you want to configure.
4. Tap ☐ next to **Enable** to enable the function.
5. Tap ☐ next to **Advanced Configuration** to enable the function, and then configure other parameters.

Figure 6-13 Advanced configuration (video mask)



6. Tap **Save**.

6.1.5.1.2 Alarm Settings

Background Information

When an alarm is triggered, alarm actions are 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.

This section uses setting local alarm as an example.

Table 6-4 Alarm setting

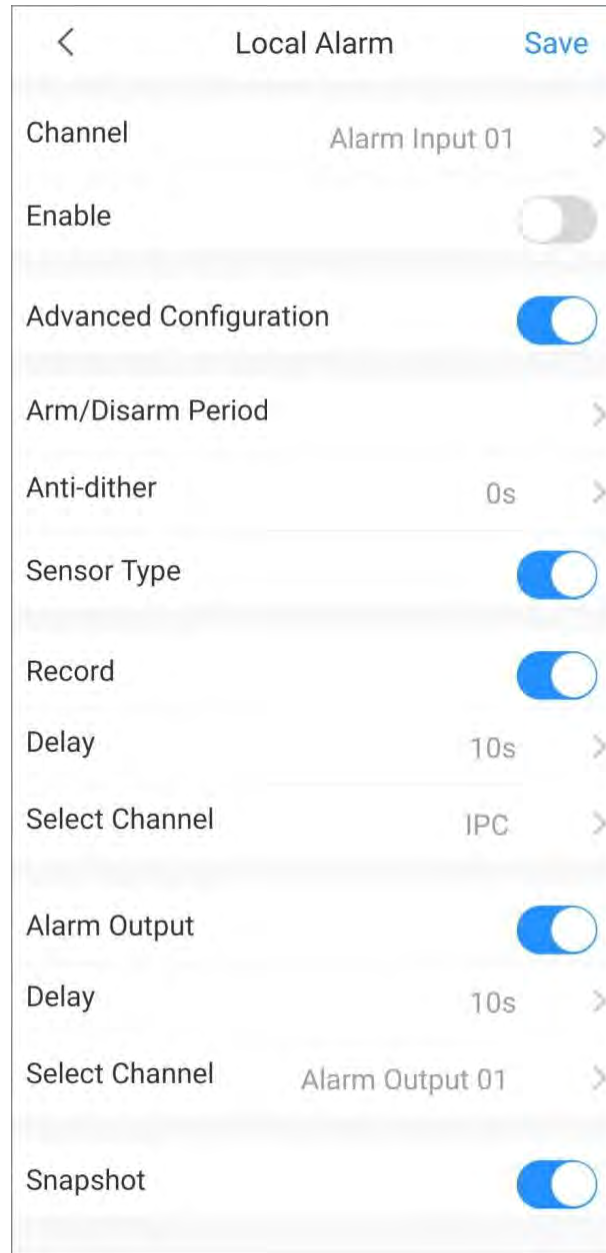
Alarm Type	Description
Local Alarm	Connect the alarm device to the alarm input port of the added device. When the alarm is triggered, alarm linkage actions will be performed.
Network Alarm	An alarm linkage action is performed when an alarm signal is transmitted to the device through network.
IPC External Alarm	Connect the IPC to the alarm input device. When the alarm is triggered, alarm linkage actions will be performed.
IPC Offline Alarm	Alarm linkage actions will be performed 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.

Procedure

- Step 1 On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2 In the **Others** section, select **Remote Configuration > Alarm Setting > Local Alarm**.
- Step 3 Select the device channel that you want to configure.

- Step 4** Tap ☐ next to **Enable** to enable the function.
- Step 5** Tap ☐ next to **Advanced Configuration** to enable the function, and then configure other parameters.
- Step 6** Tap **Save**.

Figure 6-14 Advance configuration (local alarm)



6.1.5.1.3 Camera Settings

Background Information

You can set the parameters for video stream.

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

Procedure

- Step 1** On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2** In the **Others** section, select **Remote Configuration > Camera Setting > Video Stream**.

Step 3 Select the device channel you want to configure.

Step 4 (Optional) Set channel name.



We recommend setting a channel name that is easy to be recognized. You can set this according to the installation location of the device.

Step 5 Select main stream or sub stream.

Figure 6-15 Video stream (main)

The screenshot shows a configuration window titled 'simuipc'. At the top left is a back arrow, and at the top right is a 'Save' button. The settings are as follows:

- Channel Name: IPC3
- Main/Sub: Two radio buttons, 'Main' is selected.
- Encode Mode: H.264H
- Video: A toggle switch that is turned on (blue).
- Audio: A toggle switch that is turned off (grey).
- Resolution: D1 (704*576)
- Frame rate: 25
- Bitrate Type: CBR
- Bitrate: 1024

Table 6-5 Video stream parameters

Function	Description
Main/Sub	• Main stream: Has a large bit stream, small image compression size, and high resolution, but also requires large bandwidth. • Sub stream: Has a smaller bit stream, smooth video, and requires less bandwidth. It is used to replace main stream when the available 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 highest value for better image quality. • H.264: Main Profile encode mode. • H.264H: High Profile encode mode. It uses a smaller bandwidth than H.264, while maintaining the same image quality.
Video	This parameter can be set only when you select sub stream. Enable Video , and then the video stream type will become sub stream.
Audio	Set the audio stream type as main stream or sub stream.

Function	Description
Resolution	Set the resolution for video stream. The higher the resolution, the better the video quality, but the larger the bandwidth needs to be.  The supported resolutions vary depending on the device. Please be advised.
Frame rate	Set the frame rate from 1 to 25. The higher the frame rate, the smoother and more vivid the video is, but the larger the bandwidth needs to be.
Bitrate Type	• CBR (Constant Bit Rate): There is very little change in the bitrate. It remains close to the defined bitrate value. When the scene is complicated, the image might not be clear. But when the scene is simple, the bandwidth might be wasted. • VBR (Variable Bit Rate): The bitrate changes with the monitoring scene to make the image clear when the scene is complicated. Very little bandwidth is needed for these types of simple scenes.
Quality	This parameter can be configured only when the Bitrate Type is set as VBR . The higher the quality is, the larger the bandwidth needs to be.
Bitrate	Set the video bitrate. The higher the bitrate is, the faster the data is transmitted.

Step 6 Tap **Save**.

6.1.5.1.4 Record Plans

You can configure the device recording period and recording type.

Procedure

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

Step 2 In the **Others** section, select **Remote Configuration** > **Record Plan**.

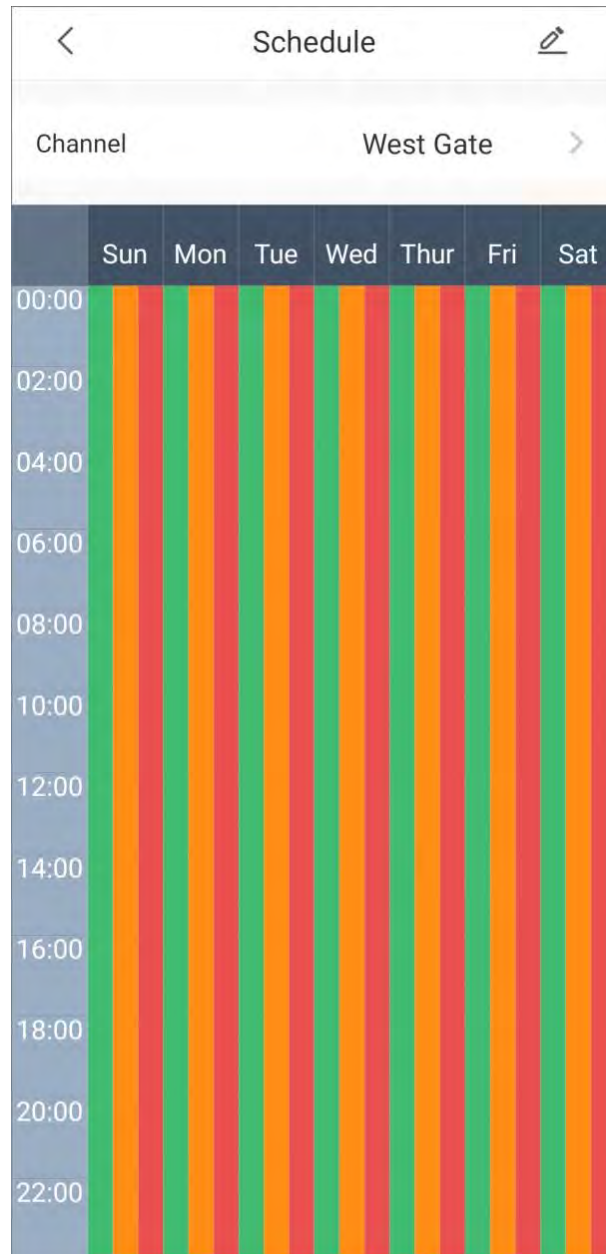
Step 3 Select the device channel you want to configure.



Different recording types have different colors.

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

Figure 6-16 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, and then the defined arming period will be applied to the selected days.

Figure 6-17 Set recording

Period	Time Range	Nor...	Moti...	Alarm
1	00:00:00-23:59:00	☒	☒	☒
2	00:00:00-23:59:00	☐	☐	☐
3	00:00:00-23:59:00	☐	☐	☐
4	00:00:00-23:59:00	☐	☐	☐
5	00:00:00-23:59:00	☐	☐	☐
6	00:00:00-23:59:00	☐	☐	☐

Step 5 Tap **Save**.

6.1.5.1.5 Image Adjustment

You can adjust settings for the live view image such as focus, zoom, brightness, contrast, and image quality.

Procedure

- Step 1 On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2 In the **Others** section, select **Remote Configuration > Image Adjustment**.
- Step 3 Select the device channel you want to configure, and then the system goes to the **Live** screen.

Step 4 Perform operations on the app.

Figure 6-18 Image adjustment

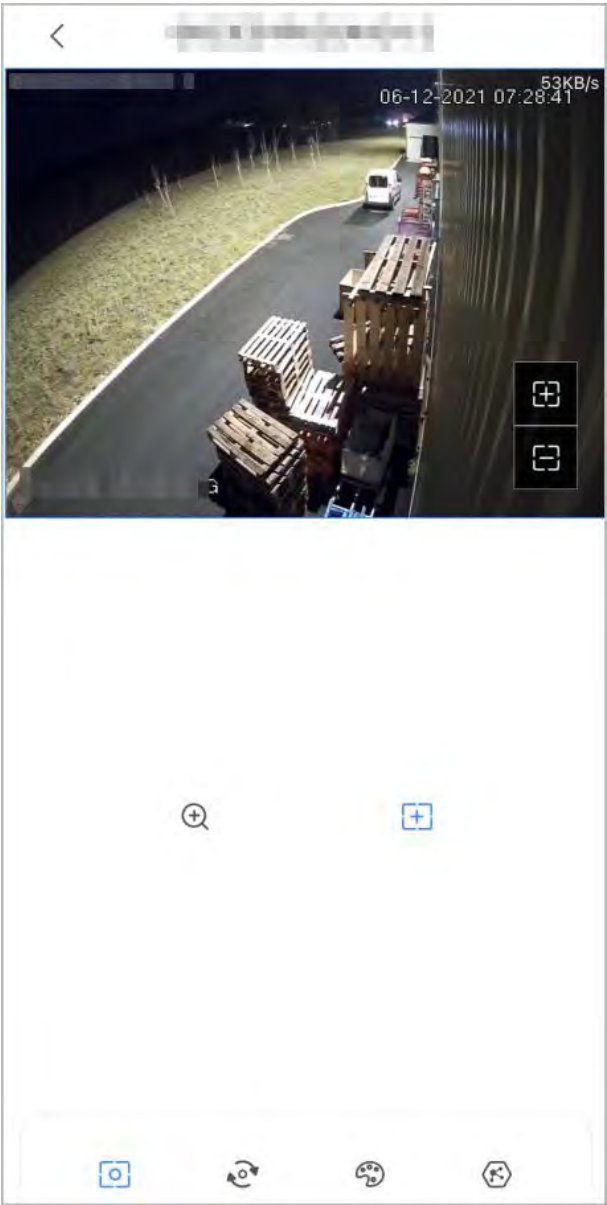


Table 6-6 Function icon descriptions

Function	Description
Focus/Zoom	• Tap  to zoom in or out of the image. • Tap  to adjust the focus to make the image clearer  Tap + or- on the image to adjust the focus or zoom effect.
Rotate/Flip	Tap  to rotate or flip the image. •  : Flip horizontally. •  : Flip vertically. •  : Rotate 90° anticlockwise. •  : Rotate 90° clockwise. •  : Rotate 180°.

Function	Description
Image effect	Tap  to adjust image effects. •  : Brightness. •  : Contrast. •  : Hue. •  : Saturation. •  : Restore to default.
Video quality	Tap  to adjust the quality of the live video. •  : Real-time mode. •  : Fluent mode. •  : Auto mode.

6.1.5.1.6 Storage Manager

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

Procedure

- Step 1 On the **Device** screen, tap  next to a device, and then tap **Device Details**.
- Step 2 In the **Others** section, select **Remote Configuration** > **Storage Manager**.
- Step 3 View the storage capacity of the SD card or HDD. You can also tap **Format the Disk** to format the SD card or HDD if you need to.

Figure 6-19 Storage



6.1.5.1.7 Arm/Disarm Period

You can set arming periods. The alarm can only be triggered when it occurs during the defined period.

Procedure

- Step 1 On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2 In the **Others** section, select **Remote Configuration > Arm/Disarm Period**.
- Step 3 Set arming periods. For details on setting arming periods, see "6.1.5.1.1 Video Detection".

6.1.5.2 Alarm Output

You can set the alarm output mode as close, manual, or automatic. When the added device has connected to an alarm output device, and **Alarm Output** is enabled in **Video Detection** or **Alarm Setting**, you need to set the alarm output mode for alarm linkages to take effect.

Procedure

- Step 1 On the **Device** screen, tap **•••** next to a device, and then tap **Device Details**.
- Step 2 In the **Others** section, tap **Alarm Output**.

Figure 6-20 Alarm output



- Step 3 Set the alarm output mode.
- **Close:** Alarm is disabled.
 - **Manual:** Alarm is always on.
 - **Automatic:** Alarm is triggered only when the alarm event occurs.

6.2 Sharing Devices

You can share devices with up to 6 DMSS users.

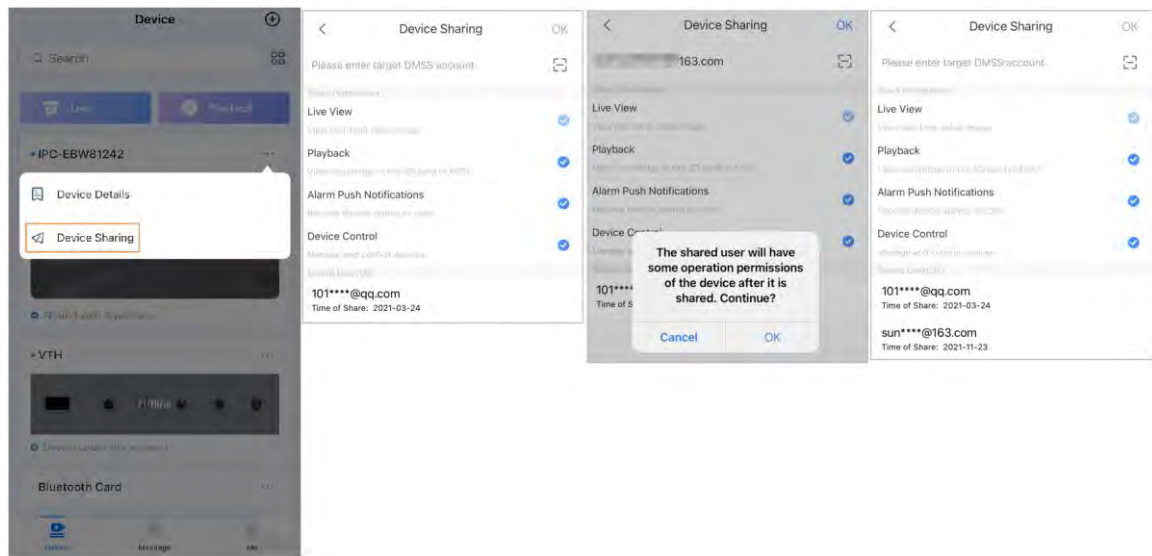
Background Information

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

Procedure

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

Figure 6-21 Share device



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

Step 3 Select permissions as needed.

You can select **Playback**, **Alarm Push Notifications**, or **Device Control**. **Live View** is selected by default, and cannot be disabled.



Permissions for alarm devices are different to other devices. Select device permissions for users based on your actual need.

Step 4 Tap **OK**.

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

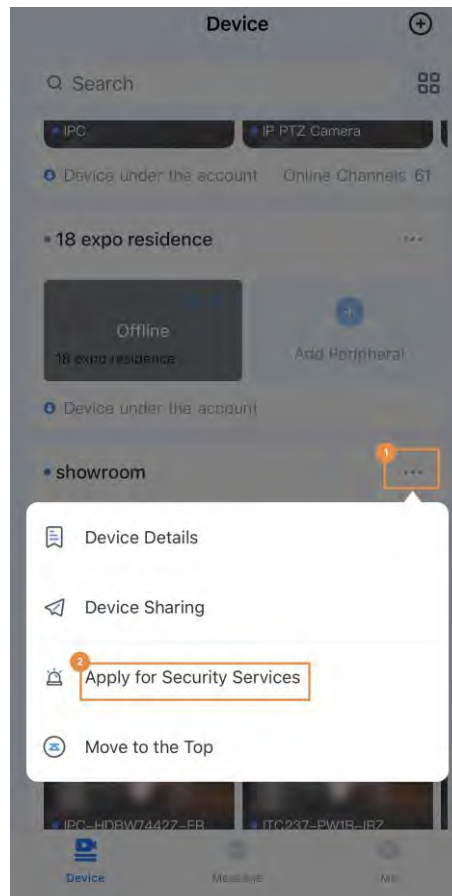
6.3 Applying for Security Services

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

Procedure

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

Figure 6-22 Apply for security services



Step 2 Tap **Apply for Company**.

Step 3 Tap  to select the country and region.

The system displays the available security companies in the region automatically. You can select a company or you can enter the keyword to search for the company.

Step 4 Tap **OK**.

6.4 Entrusting Devices

You can entrust devices one by one or in batches.



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

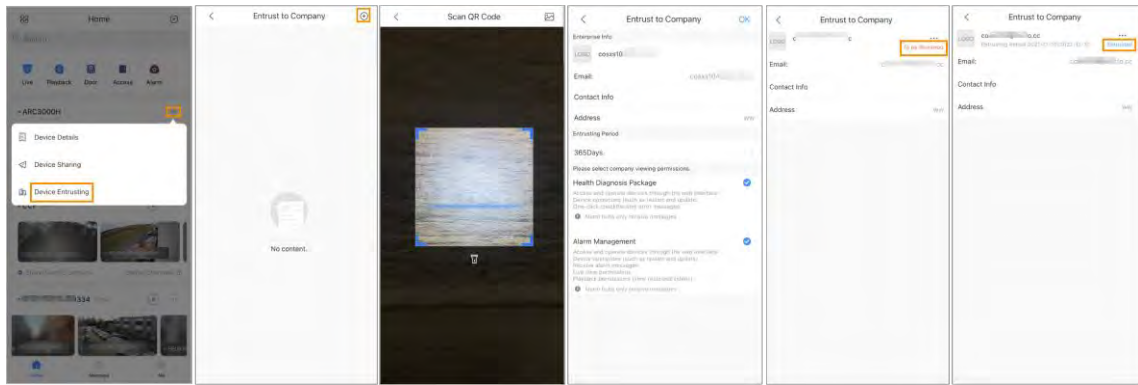
6.4.1 Entrusting Devices One by One

You can entrust a device to one enterprise.

Procedure

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

Figure 6-23 Entrust a device



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



You can ask installers for their QR codes.

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



- You must select at least one viewing permission from **Health Diagnosis Package** and **Alarm Management**.
- Enterprise information will be automatically recognized after you scan the QR code of the installer.

Step 4 View entrusting details on the **Entrust to Company** screen.
When successfully entrusted, **To be Reviewed** will change to **Delivered**.



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

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**.

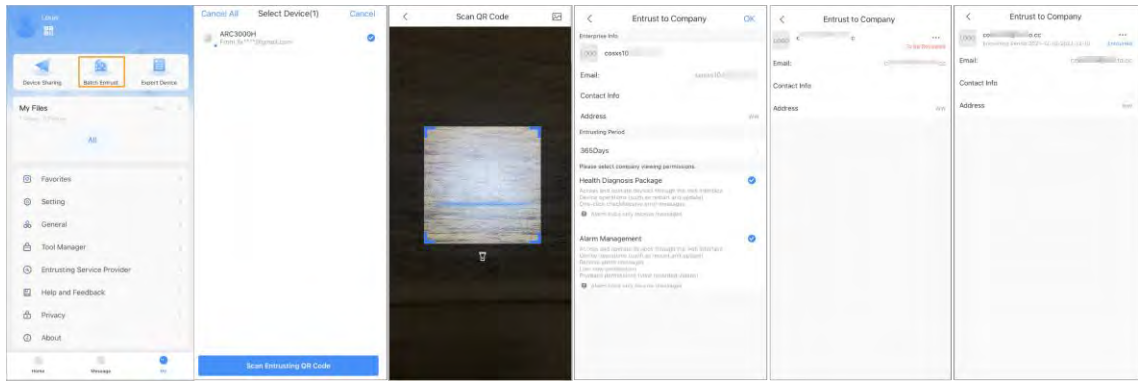
6.4.2 Entrusting Devices in Batches

You can entrust devices to one enterprise in batches.

Procedure

Step 1 On the **Device** screen, select **Me > Batch Entrust**.

Figure 6-24 Entrust devices in batches



Step 2 On the **Select Device** screen, select the devices to be entrusted, and then entrust those to the enterprise. The process for entrusting multiple devices is the same as entrusting a single device. For details, see "6.4.1 Entrusting Devices One by One".

6.5 Creating Device Cards

You can quickly add devices by scanning the device card.

Background Information

Procedure

- Step 1** On the **Me** screen, tap **Export Device**.
- Step 2** Select devices (10 at most), and then tap **Create Device Card**.

Figure 6-25 Create device card

Device Name	Source	Status
Front door	From 479****@qq.com	
solar	From 479****@qq.com	
[Blurred]		✓
xvr		✓
[Blurred]		☐
[Blurred]		☐
79f		☐
quick		☐
solar power		☐
0012Device3		☐
0000****		☐

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.

6.6 Resetting and Modifying the Device Password

Background Information

You can go to **...** > **Device Details** > **...** > **Modify Device Password** to modify the device password. If you forget the device password, you can go to **Me** > **Tool Manager** > **Device Password Management** to reset the device password. The methods for these two processes are similar. This section uses resetting the device password as an example.

Procedure

- Step 1 On the **Me** screen, tap **Setting**.
- Step 2 Tap  next to **Password Protection**.
- Step 3 On the **Password Protection** screen, enter the new and confirmed password.
- Step 4 Tap **OK**.
After successfully resetting the device password,  will become , and **Modify Password** will appear on the **Setting** screen.

7 Live View

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

Procedure

Step 1 On the **Device** screen, tap **Live**.

Step 2 Play a channel or multiple channels.

- Play a channel: Tap  in the window, and then select a channel from the device list to be played.
- Play multiple channels: Tap , and select channels from the device list as needed.



When the number of displayed channels exceeds the maximum number of available windows, you can swipe left or right to view the other live videos.

Step 3 View and perform operations for the live videos.

Figure 7-1 Live view of a single channel

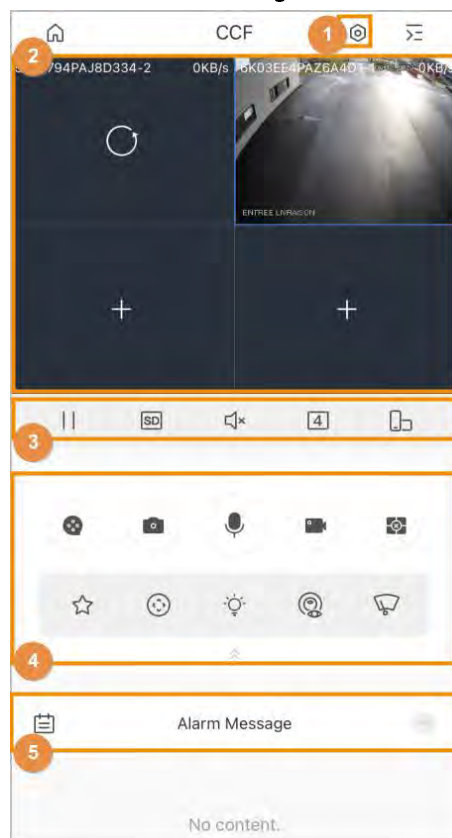


Table 7-1 Live view function icons

No.	Icon/Function	Description
1		Device details. Tap  to go to the Device Details screen, and then you can configure your device. For details, see "6.1 Configuring Devices".

No.	Icon/Function	Description
2	Other functions	- To change the position of a video, tap and hold the video, and then move it to the target window. - Double tap to enlarge a window, and then double tap again to restore it to its original size. - To delete a video, tap and hold the video until the trash bin appears on the top of the screen, and then drag the video to the trash bin, and release it. - If the video is not playing properly, tap Help in the window to find solutions to solve the problem.
3		Play/Pause.
		Video stream. Tap  to switch between SD and HD video quality.
		Mute/Unmute.
		Split view. You can display in 1, 4, 9, or 16 views.  To focus on a single window, double-tap the video in the window to zoom in.
		Change the image orientation to landscape.
4		Video playback. For details on performing operations on the Playback screen, see "8 Video Playback".
		Take snapshot.  - You can configure the capture mode in Me > Setting. For details, see "14 Me". - Snapshots are saved in the My Files. For details, see "14 Me".
		Two-way audio. - Channel talk: Talk to a person through a channel that is playing. - Device talk: Talk to a person through the device.  - Two-way audio is available on select models. - If device talk is available, the system will prompt you to select between device talk and channel talk. Otherwise, only channel talk is available.
		Video recording.  Recorded videos are saved in the My Files . For details, see "14 Me"

No.	Icon/Function	Description
		Memory play/Close videos. - Memory play: To play the last channels that were played, tap  and a tick will appear in the center. - Close videos: To close all the channels that are being played, tap  and a cross will appear in the center.
		Favorites. Select a video, tap , and then select an existing file that you want to save the video to.  If you want to create a new folder, select  > , and then enter the name of the folder.
		PTZ control. Select a video, tap , and then tap  to control the PTZ. - Tap  to zoom in or out of the image. - Tap  to adjust the brightness of the video. - Tap , select the preset point, and then tap  to turn the PTZ to the monitored target. - Use  to control PTZ directions: Left, right, up, down, upper-left, upper-right, lower-left, and lower-right are all supported.  You can also use gestures to control the PTZ. - Swipe on the screen to control the PTZ direction. - Pinch or stretch out your fingers on the screen to zoom in or out.  - Only one window is displayed during PTZ control. - The PTZ function is available on select models.
		Tap , and then select  to enable white light. Select  to enable buzzer.  The 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 available on select models.

No.	Icon/Function	Description
		Wiper. Select a video, tap , tap , and then the wiper control screen is displayed. • Tap Single, and the wiper wipes once, and then stops. • Tap Enable, and then configure the time interval for the wiper to work within. • Tap Stop, the wiper stops working.  The function is available on select models.
5		Alarm messages. Tap , and then select the date to view videos from that time.

8 Video Playback

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

Prerequisites

Before you can play back a video, you need to set alarm rules and record plans for the channel.

Procedure

Step 1 On the **Device** screen, tap **Playback**.

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

Figure 8-1 Video playback



Table 8-1 Video playback function icons

Function	Description
	For details on icons, see Table 7-1.
	
	
	
	
	
	Play slowly/Play fast/Play by frame.

Function	Description
	Clip videos.
	Select a video, and then tap  to clip the video. Drag the time bar, tap  to set a start point, and then tap  to set a stop point.
Time bar	The color block indicates the different types of recorded videos. • Grey: All videos. • Green: Regular videos. • Red: Alarm videos. • Orange: Motion detection videos. • Yellow: Smart videos. Drag the time bar to view recordings linked to the different time frames. Pinch or stretch out your fingers to zoom into the bar.

Step 3 Tap  to change the date and type of recording.

Dates with a blue dot have videos.

The recording types are as follows:

- **All:** Play all the recording types.
- **Regular:** Normal recordings.
- **Alarm:** Recordings of when alarms were triggered, such as audio alarm and local alarm.
- **Motion:** Recordings of when motion detection alarms were triggered.
- **Smart:** Recordings of when smart event alarms were triggered such as face detection and recognition, IVS, video metadata, and more.
- **Motion: Vehicle:** Recordings of when vehicles were detected and motion detection alarms were triggered.
- **Motion: Human:** Recordings of when humans were detected and motion detection alarms were triggered.

Figure 8-2 Playback conditions

Select search conditions

Cancel

2021/12

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Record Type

All

Regular

Alarm

Motion

Smart

Motion: Vehicle

Motion: Human

OK

9 Video Call

You can watch the live view, access video intercoms, make video calls between the device and the app, lock and unlock doors, and more.

Procedure

- Step 1 On the **Device** screen, tap a VTO or VTH.
- Step 2 Tap  or  to select a channel.

Figure 9-1 Door

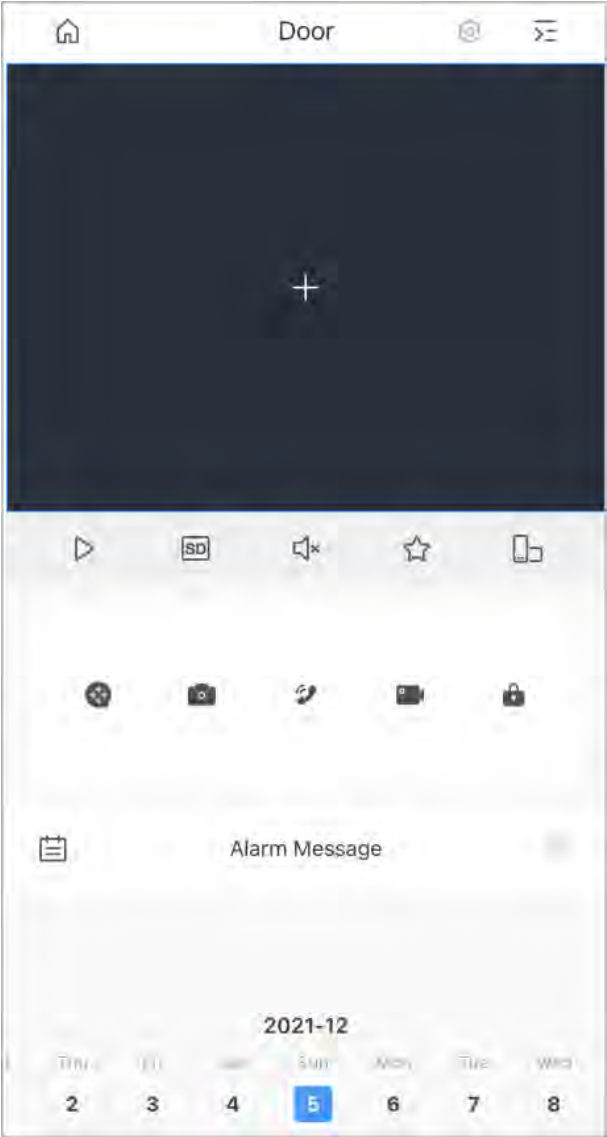


Table 9-1 Video call function icons

Function	Description
	For details on icons, see Table 7-1.
	
	
	

Function	Description
   	
	Answer/End the call. Receive calls from the VTO on the app: Tap  to answer the call; tap  to decline or hang up the call.  Enable Alarm Subscription for the VTO to receive calls from the VTO on DMSS.
	Unlock the door.  VTO that have two locks can be added to DMSS. Tap , and then select  or  to unlock the door.

Step 3 View the call history between the VTO and the app.
Tap **Alarm Message** on the bottom of the screen.

10 Access

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

On the **Device** screen, tap a access control device.

Figure 10-1 Access control device

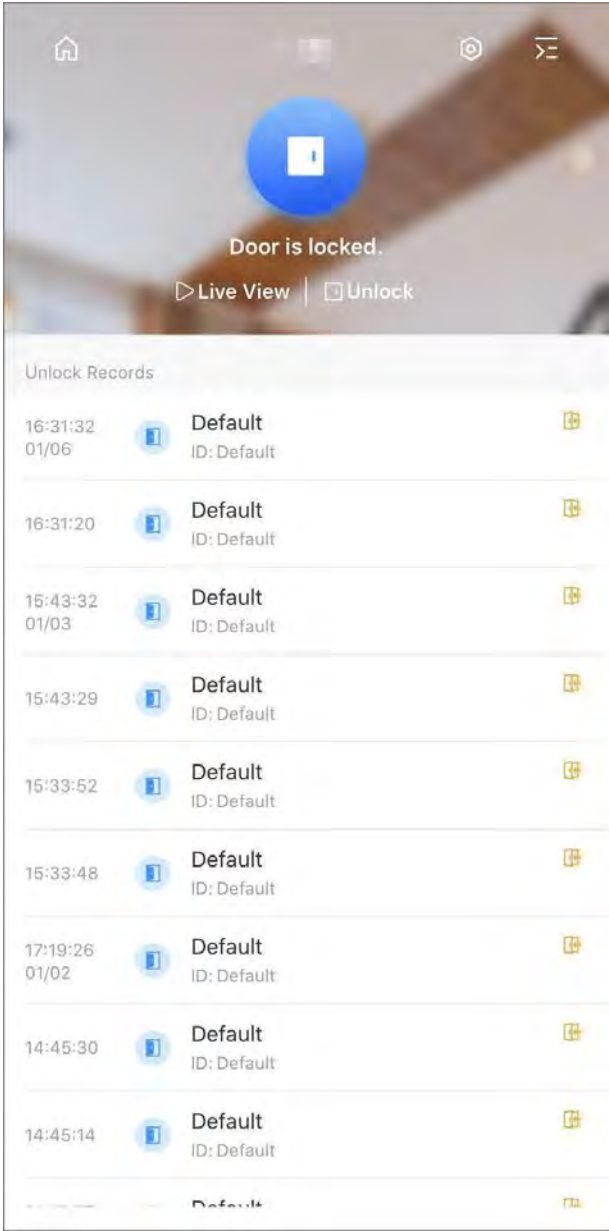
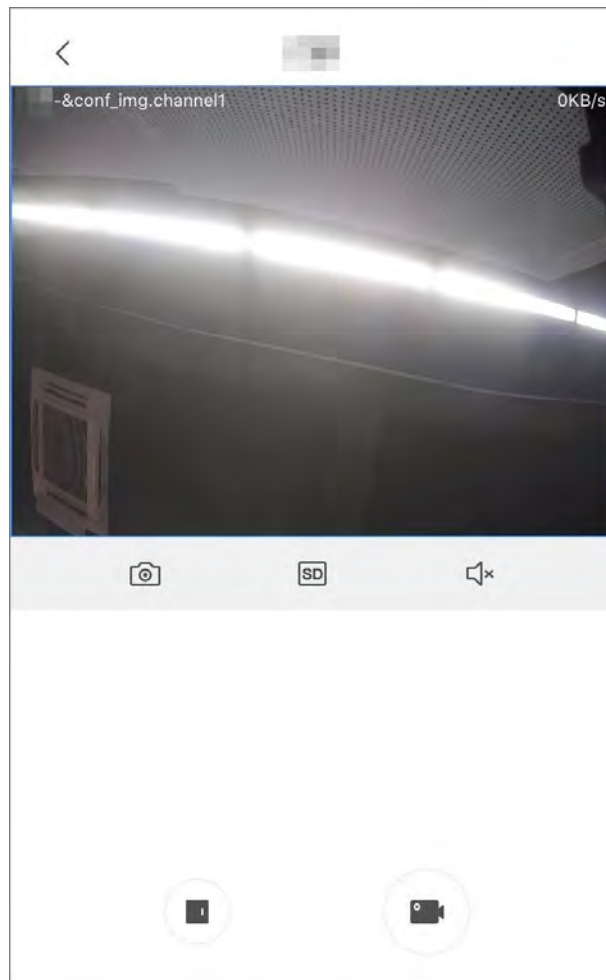


Table 10-1 Function icon description

Function	Description
Switch device	Tap  to select another access control device.

Function	Description
Device details	Tap  to go to the Device Details screen, and then you can view unlock records from the last 7 days.  You can also tap  of the access control device on the Home screen, and then tap Device Details.
Door status	: The door is locked. : The door is unlocked.
Unlock	Tap Unlock to unlock the door.
Unlock records	Display person name, ID, unlock time, and unlock methods. • : Remotely unlock the door through the 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 screen to view unlock records from the last 7 days.
Live view	• Tap Live View to go to live view of the device. See Figure 10-2. • Tap  for snapshot. • Tap  to switch between SD and HD video quality. • Tap  to mute the video, and tap  to unmute the video. • Tap  to unlock the door. • Tap  to record videos.

Figure 10-2 Access (live)



11 Alarm

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

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.

Procedure

- Step 1 On the **Device** screen, tap an alarm hub.
- Step 2 Tap  to add the accessories. For details on adding the accessories, see the user's manual of the corresponding device.
- Step 3 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. For details, see "11.1 Single Arming and Disarming".
 - **Global Arming and Disarming:** Arm and disarm the detectors in all the areas. For details, see "11.2 Global Arming and Disarming".
 - **Manual Arming and Disarming:** Arm the security system through the DMSS app or keyfob.
 - **Schedule Arming and Disarming:** Arm and disarm the detectors by schedule. For details, see "11.4 Scheduled Arming and Disarming".

Related Operations

To view and edit the parameters of the hub, go to the hub screen, and then tap . For information on configuring parameters for the **General Config** section, see "6.1.4 General Configuration".

- To view the status of the hub, tap **Hub Status** on the **Device Config** section. For details on icons, see the user's manual of the corresponding hub.
- To edit the parameters of the hub, tap **Hub Setting**. For details on the parameters, see the user's manual of the corresponding hub.

11.1 Single Arming and Disarming

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

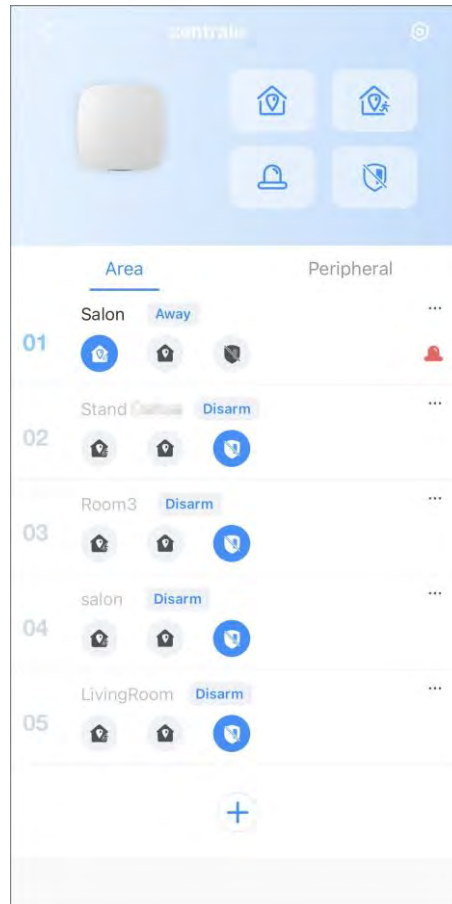
Procedure

- Step 1 On the **Device** screen, tap an alarm hub device.
- Step 2 Select an area and then tap ,  or  to set as **Away**, **Home** or **Disarm** respectively.



- **Home:** An arming mode that allows you to 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 11-1 Arm a single area



11.2 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. On the hub screen, select

 > **Hub Setting**, and then enable **Global Arming/Disarming**.

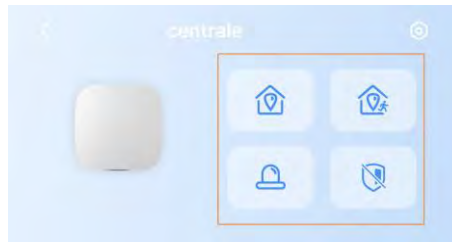
Procedure

Step 1 On the **Device** screen, tap an alarm hub.

Step 2 On the hub screen, tap , , or  on the upper screen.

- : Home.
- : Away.
- : Disarm.
- : Panic button.

Figure 11-2 Global arming and disarming



11.3 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 "11.1 Single Arming and Disarming", and "11.2 Global Arming and Disarming".
- To operate through the keyfob, you need to assign the control permissions of the areas to the keyfob first. For details, see the user's manual of the corresponding keyfob.

11.4 Scheduled Arming and Disarming

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

Procedure

Step 1 On the **Device** screen, tap an alarm hub.

Step 2 On the hub screen, select  > **Hub Setting** > **Scheduled Arming/Disarming**.

Step 3 On the **Scheduled Arming/Disarming** screen, tap **Add**, and then configure arming plans.

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



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

- Forced Arming: Tap ☐ to enable the function as needed.
After the function is enabled, the command for the scheduled arming/disarming is invalid. In the system integrity check scenario, even if the system detects an error, the scheduled arming can be carried out successfully.



Only up to 8 arming/disarming schedules can be added. To delete a schedule, swipe left and then tap **Delete**.

12 Message

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



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

12.1 Subscribing for Alarm Messages

You can subscribe for alarm messages, and then alarm notifications will be pushed to DMSS when an alarm is triggered. For details on subscribing for alarm messages, see "6.1.1.1 Notification".

12.2 Viewing Messages

Background Information

On the **Message** screen, you can view messages for alarms, errors, the system and your personal messages.

Figure 12-1 Message

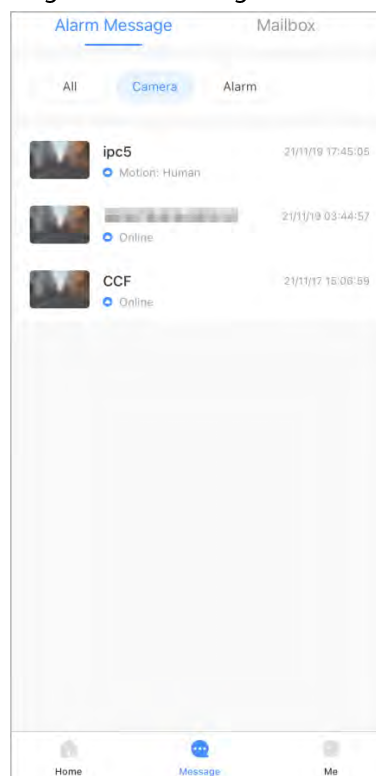


Table 12-1 Message

Type	Messages	Description
Alarm Message	All Messages	Displays all the alarm messages related to the cameras and alarm devices.

Type	Messages	Description
Mailbox	Camera Message	Displays messages about the cameras.
	Alarm Message	Display messages about the alarm devices.
	Personal message	Displays personal messages such as notifications of shared devices and deleted devices.
	Exception message	Displays messages on errors, showing the type of error, when it occurred, when it was resolved and the service rating.
	System message	Display messages such as system maintenance and declaration.

Procedure

- Step 1** On the **Device** screen, select **Message > Alarm Message**.
- Step 2** On the **Alarm Message** screen, tap an alarm event to view its alarm messages.

Figure 12-2 Alarm messages



Messages with red dots have not been viewed as yet.



- To mark messages as read, tap , select one or multiple messages with red dots, and then tap **Mark as read**.
- To delete alarm messages, tap , select one or multiple messages, and then tap **Delete**.

Step 3 Tap the alarm message and then its prompt type will be displayed.

Step 4 Tap the alarm message, and then the **Playback** screen opens. For details on performing operations on the **Playback** screen, see "8 Video Playback".

Tap **Live View** on the lower right corner, and then the **Live** screen opens. For details on performing operations on the **Live** screen, see "7 Live View".

13 Favorites

You can save channels to **Favorites** to find them easily and go to the **Live View** when needed.



For details on saving the played video in **Favorites**, see "7 Live View".

Procedure

- Step 1 On the Device screen, tap **Favorites**.
- Step 2 Tap , select one or multiple channels from the same device type, and then tap **Next**.
- Step 3 Enter the folder name.

Related Operations

- Tap  to play channels in this folder simultaneously.
- Tap  to view details on the channels, add more channels, delete existing channels, or rename the folder.
- Tap **Delete** to delete the folder.

14 Me

You can manage your account, configure the app and use the tools. You can also view the user manual of the app in help center.

Figure 14-1 Me

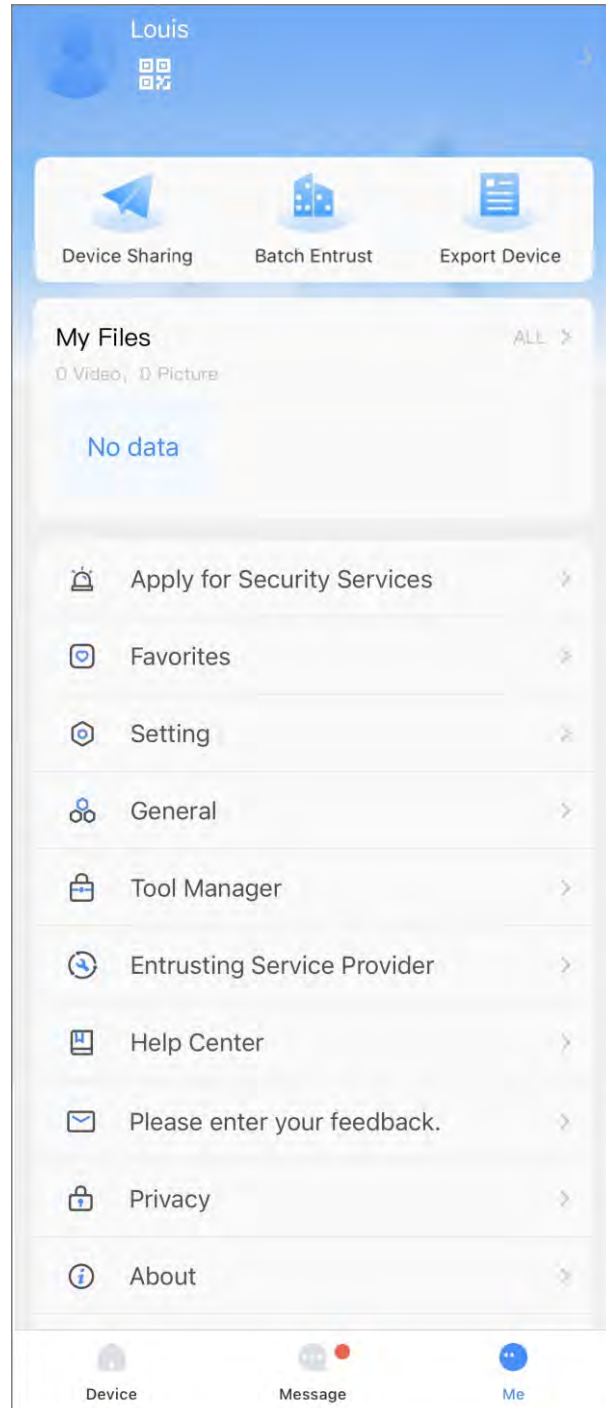


Table 14-1 Me

Name	Description
Account management	Tap  to open the Account Management screen. - View personal information. - Change the password of the user. Tap Modify Password, enter the old and the new password, and then tap Done. - Delete the account. Select Delete Account > Apply for Deletion to delete the account. - Export your account information. - Select Export Account Information > Export. - Enter your email address, and then tap Next. - Check your email box to receive a verification code, and then enter the code.  Use the verification code within 60 seconds of receiving it. Otherwise, the verification code will become invalid. - Check your email box to view the exported account information. - Exit DMSS. Tap Log out to exit DMSS.
Device Sharing, Batch Entrust, Export Device	- For details on sharing and entrusting devices, see "6.2 Sharing Devices" and "6.4.2 Entrusting Devices in Batches". - For details on exporting devices, see "6.5 Creating Device Cards".  Only part of the countries/regions support the batch entrusting function.
My Files	Snapshots and recorded videos are saved in Files .
Apply for Security Services	You can apply security servicer for the alarm hub. For details, see "6.3 Applying for Security Services".
Favorites	For details, see "13 Favorites".
Setting	PTZ Speed: Select the speed for the PTZ camera from 1 to 8. The higher the value is, the faster the PTZ moves. 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: Tap  next to Hard Decoding to enable the function, and then the performance of video stream will be improved. Pushed Video Delay: Set the delay for pushed recordings. You can select from 10 s, 30 s, 1 min, 2 min, and 5 min. Default Page: Select the display type. Password Protection: You can set the password of the device. For details on changing the device password, see "6.6 Resetting and Modifying the Device Password".

Name	Description
General	• Region: Select your region. • Auto Play When Not in a Wi-Fi Network: Tap  to enable the function, and then videos can be automatically played with other networks, such as cellular data. • Notification and Period: Tap  to enable the alarm notifications function, and then you can set the period for receiving notifications.  ◇ Notifications can only be sent during the defined period. ◇ The period setting is only supported by devices registered to the account. • Appearance Mode: ◇ Keep Match System Settings as default. ◇ If you want to personalize appearance mode, select General > Appearance Mode, tap  next to Match System Settings, and then select from Dark or Light. • Picture-in-Picture: Tap  to enable the function, and then the live video can be simultaneously viewed in the small, floating window. • Clear Cache.
Tool Manager	• To test the Wi-Fi status, tap . • To reset the password of linked devices, tap .  You can tap Learn more on the top of the page to learn how to reset device password. • To test the notification pushing, tap . • To configure the mobile carrier domain name, tap . Enter the DNS and then tap Test. • To transfer local devices, tap . You can select one or multiple devices. You can view the results after transferring completed.  Up to 10 devices can be selected to transfer at a time.
Entrusting Service Provider	View information on the entrusting service provider.
Help Center	View a brief introduction of the functions and user manual.  Tap  to search for specific functions with keywords.
Please enter your feedback	You can enter the feedback about the product. Tap Report Issue , and then enter your opinions and information on products.
Privacy	• View the DMSS privacy policy. • Tap System Permission Settings to assign permissions to the app on your phone.

Name	Description
About	View information on DMSS, including the version, user agreement and more.

Appendix 1 Cybersecurity Recommendations

The necessary measures to ensure the basic cyber security of the platform:

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. Customize the Answer to the Security Question

The security question setting should ensure the difference of answers, choose different questions and customize different answers (all questions are prohibited from being set to the same answer) to reduce the risk of security question being guessed or cracked.

Recommendation measures to enhance platform cyber security:

1. Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism, and configure the IP/MAC of the terminal where the commonly used client is located as an allowlist to further improve access security.

2. Change Passwords Regularly

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

3. Turn On Account Lock Mechanism

The account lock function is enabled by default at the factory, and it is recommended to keep it on to protect the security of your account. After the attacker has failed multiple password attempts, the corresponding account and source IP will be locked.

4. Reasonable Allocation of Accounts and Permissions

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

5. Close Non-essential Services and Restrict the Open Form of Essential Services

If not needed, it is recommended to turn off NetBIOS (port 137, 138, 139), SMB (port 445), remote desktop (port 3389) and other services under Windows, and Telnet (port 23) and SSH (port 22) under Linux. At the same time, close the database port to the outside or only open to a specific IP address, such as MySQL (port 3306), to reduce the risks faced by the platform.

6. Patch the Operating System/Third Party Components

It is recommended to regularly detect security vulnerabilities in the operating system and third-party components, and apply official patches in time.

7. Security Audit

- Check online users: It is recommended to check online users irregularly to identify whether there are illegal users logging in.
- View the platform log: By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

8. The Establishment of a Secure Network Environment

In order to better protect the security of the platform and reduce cyber security risks, it is

recommended that:

- Follow the principle of minimization, restrict the ports that the platform maps externally by firewalls or routers, and only map ports that are necessary for services.
- Based on actual network requirements, separate networks: if there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.