

Hik-Connect Mobile Client

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE

PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Contents

Chapter 1 Landing Page 1

Chapter 2 About Hik-Connect 3

2.1 Icons Meanings in Hik-Connect 3

Chapter 3 Account 7

3.1 How to register an account? 7

3.2 How to log in? 8

3.3 How to log in as a visitor? 9

3.4 Two-Factor Authentication 9

Chapter 4 Device Management 13

4.1 How to add devices? 13

4.2 How to add groups? 13

4.3 How to switch between large and small card? 17

4.4 How to share devices? 17

Chapter 5 Camera/NVR/DVR/NVS 18

5.1 How to use AI video Q&A? 18

5.2 How to use daily summary? 19

5.3 How to start live view? 20

5.3.1 How to start and stop live view? 20

5.3.2 How to control PTZ? 21

5.3.3 How to set image quality? 22

5.3.4 How to start live view of a fisheye camera? 24

5.3.5 How to open doors during live view? 26

5.4 How to start playback? 26

5.4.1 How to start normal playback? 26

5.4.2 How to capture images and recording videos? 27

5.4.3 How to download a specific video segment? 28

5.4.4 How to view pictures and videos? 29
5.5 How to use the cloud storage service? 29
5.5.1 How to enable/disable cloud storage service for a channel? 29
5.5.2 How to play back and download video footage from the cloud? 30
5.6 How to use intelligence search? 30
5.6.1 How to use AcuSeek? 30
5.6.2 AcuSearch on the Playback Page 33
5.6.3 Smart Search on the Playback Page 36
5.6.4 AcuSeek on the Playback Page 38
5.7 How to use dual-lens cameras? 40
5.8 How to set up cameras? 45
5.8.1 How to manage solar cameras? 45
5.8.2 How to set light for floodlight camera? 45
5.9 How to set motion detection for cameras? 46
5.10 How to manage cameras linked to NVRs/DVRs? 47
5.10.1 How to batch arm/disarm cameras linked to NVRs? 47
5.10.2 How to edit the settings of cameras linked to NVRs/DVRs? 48
5.11 How to reset passwords of NVRs/DVRs? 48
5.11.1 How to reset passwords by Hik-Connect? 48
5.11.2 How to reset passwords by reserved Email address? 49
5.11.3 How to reset passwords by generated QR codes? 49
Chapter 6 Alarm Devices 51
6.1 How to Add Security Control Panels 53
6.1.1 By Wi-Fi 53
6.1.2 By SIM Card 55
6.1.3 By Ethernet 57
6.1.4 Install Devices 59
6.2 How to Unbind Devices 59

6.3 How to Configure Security Control Panels 60
6.3.1 How to Add an Area and Link Devices to it? 61
6.3.2 How to Batch Control Areas? 62
6.3.3 How to Configure Delayed Disarm Alerts? 63
6.3.4 How to Add Areas to Shortcuts on Homepage? 65
6.3.5 How to Quickly Control Automation Devices? 65
6.3.6 How to Add Users? 66
6.3.7 How to Cancel Authorization of Service Provider? 72
6.3.8 How to Configure an ARC? 73
6.3.9 How to Configure Control Panel Services? 77
6.4 How to Add Controls & Automations 78
6.4.1 Entry 81
6.4.2 Group 83
6.4.3 Tap to Run 85
6.4.4 Automation 88
6.4.5 Schedule 90
6.4.6 Arm/Disarm with One Button 92
6.4.7 Alarm Video Verification 93
6.4.8 Chime 94
6.4.9 Alarm Cross Confirm 95
6.4.10 Timeout Alert 96
6.5 How to Add Peripherals 97
6.5.1 Add Bus Devices 97
6.5.2 Add Wired Devices 98
6.5.3 Add Wireless Devices 98
6.6 How to Add Zones for Network Camera Channel 103
6.6.1 Prerequisite 103
6.6.2 Steps 104

6.7 How to Configure Detectors & Peripherals 107
6.7.1 Common Parameters 107
6.7.2 Electric Fence Energizer 108
6.7.3 Keyfob 110
6.7.4 Keypad 111
6.7.5 Tag Reader 116
6.7.6 Sounder 118
6.7.7 Automation (Relay / Smart Plug / Wall Switch) 122
6.7.8 PIR Detector 127
6.8 How to Add an Alarm Widget for Quick Control 127
Chapter 7 Access Control Devices 131
7.1 How to control door status? 131
7.2 How to set door open duration? 131
7.3 How to change super password? 132
7.4 How to view access control logs? 132
7.5 How to manage sliding gate openers? 133
7.5.1 Wired Connection Setup 133
7.5.2 Quick Door Controls 133
7.5.3 Real-Time Event Monitoring 134
7.5.4 Real-time Exception Notifications 135
7.5.5 Keyfob Management 136
7.5.6 Device Sharing 139
Chapter 8 Video Intercom Devices 140
8.1 How to manage indoor stations? 140
8.1.1 How to set indoor station parameters? 140
8.1.2 How to add temporary passes for indoor stations? 141
8.1.3 How to view linked devices of indoor stations? 141
8.1.4 How to control linked devices of indoor stations? 142

8.1.5 How to answer call from indoor stations? 143
8.2 How to manage door bells? 147
8.2.1 How to set motion detection alarm for Wi-Fi doorbells? 147
8.2.2 How to link smart chimes with doorbells? 151
Chapter 9 Network Devices 154
9.1 What are network devices? 154
9.2 What are AC router operations? 154
9.3 What are cloud AP operations? 155
9.4 What are network switch operations? 156
Chapter 10 Notifications 159
10.1 How to enable notifications? 159
10.2 How to set notifications? 164
10.3 How to set AI notifications? 164
10.4 How to view and handle notifications? 165
10.4.1 How to view and handle event notifications? 165
10.4.2 How to view and handle service notifications? 167
10.4.3 How to view and handle other notifications? 168
Chapter 11 Services 170
11.1 View My Services 170
11.2 View Service Market 170
11.3 Invite a Service Provider to Manage Your Devices 171
11.4 Manage 4G SIM Data Service 172
11.4.1 How to get started with the 4G SIM data service? 173
11.4.2 How to renew the service? 181
11.4.3 How to view my order? 187
11.4.4 How to subscribe to / unsubscribe from the service? 189
11.4.5 How to check 4G data notifications? 192
11.4.6 How to use the AI assistant? 193

11.4.7 How to contact the customer service via email? 197
Chapter 12 Top Questions 202
12.1 What to do when my camera turns offline? 202
12.2 How to unbind devices? 202
12.3 My camera time zone, time, or date is incorrect. 203
12.4 How do I set or change the device encryption password? 204
12.5 Why can't I receive alarm notifications? 205
12.6 How to use another email / phone number to manage the account? 206
Chapter 13 More Documents 208
13.1 Personal Mode 208
13.2 Team Mode 208

Chapter 1 Landing Page

- FAQ
  - ***What to do when my camera turns offline?***
  - ***How to unbind devices?***
  - ***My camera time zone, time, or date is incorrect.***
  - ***How do I set or change the device encryption password?***
  - ***Why can't I receive alarm notifications?***
  - ***How to use another email / phone number to manage the account?***
- Camera/NVR/DVR/NVS
  - ***How to use AI video Q&A?***
  - ***How to use daily summary?***
  - ***How to start live view?***
  - ***How to start playback?***
  - ***How to use the cloud storage service?***
  - ***How to use intelligence search?***
  - ***How to use dual-lens cameras?***
  - ***How to set motion detection for cameras?***
  - ***How to manage cameras linked to NVRs/DVRs?***
- Alarm
  - ***How to Add Security Control Panels***
  - ***How to Unbind Devices***
  - ***How to Configure Security Control Panels***
  - ***How to Add Controls & Automations***
  - ***How to Add Peripherals***
  - ***How to Add Zones for Network Camera Channel***
  - ***How to Configure Detectors & Peripherals***
  - ***How to Add an Alarm Widget for Quick Control***
- Access Control
  - ***How to control door status?***
  - ***How to set door open duration?***
  - ***How to change super password?***
  - ***How to view access control logs?***
  - ***How to manage sliding gate openers?***
- Video Intercom
  - ***How to set indoor station parameters?***
  - ***How to add temporary passes for indoor stations?***
  - ***How to view linked devices of indoor stations?***
  - ***How to control linked devices of indoor stations?***
  - ***How to answer call from indoor stations?***

- ***How to set motion detection alarm for Wi-Fi doorbells?***
- ***How to link smart chimes with doorbells?***

- Networking Device
  - ***What are network devices?***
  - ***What are AC router operations?***
  - ***What are cloud AP operations?***
  - ***What are network switch operations?***

Chapter 2 About Hik-Connect

Hik-Connect is a Video Security as a Service (VSaaS) platform with two modes, which are Hik Connect for Teams (HCT), and Hik-Connect for personal (HC). This manual is about the Hik-Connect for personal system. Hik-Connect for personal is used to remotely control devices (NVRs, DVRs, network cameras, indoor stations, doorbells, security control panels, access control devices, etc.) via Wi-Fi or cellular network.

Portal and Mobile Client

Hik-Connect provides easy-to-use clients (a Portal and a Mobile Client) for users to access it.

Table 2-1 Portal and Mobile Client

Client	Description
Portal	For users to log in to Hik-Connect to manage resources and perform related configuration and operations (Portal URL: ***https://www.hik-connect.com/***).
Mobile Client	For users to log in to Hik-Connect to use more lightweight features of the services, such as live view, playback, remote door controls, etc.

Running Environment

Table 2-2 Running Environment

Type	Requirements
System Requirement	For iOS: iOS 11.0 or later versions. For Android: Android 6.0 or later versions.
Memory Requirement	For iOS: 2 GB or above. For Android: 4 GB or above.

2.1 Icons Meanings in Hik-Connect

Here introduces icons in Hik-Connect.

Live View and Playback Icons

Icon	Description
	Start/stop the selected live view window.
	Turn audio on/off.
	Tap to select the window division mode. You can select 1-window, 4-window, 9-window, 12-window, or 16-window.
	Enable digital zoom function.
	Start controlling PTZ.
	Start two-way audio.
	Capture.
	Add a device.
	The resolution in ascending order is Basic < SD < HD < Ultra HD.
	Enable the fisheye mode. **Note** • The function should be supported by the fisheye camera. • The icon displayed on the Live View page varies with the actual fisheye expansion mode.
	Fisheye PTZ.
	Fisheye 360°, 180°.
	Enable the mirror mode. The video will be played in its mirror mode. **Note** The function should be supported by the device.
	Trigger the alarm output function.

Icon	Description
	Note The function should be supported by the device.
	Arm the device.
	Wiper.
	Download the current video.
	Turn on audio alarm.
	Turn on sounder.
	Turn on strobe light.
	Disable noise reduction.
	Noise reduction. 1 means the weakest noise reduction, while 5 is the strongest noise reduction.
	Turn on supplement light (ColorVu camera, Floodlight camera...) or alarm light (panic alarm device).
	Turn on the light of a floodlight camera.

Security Panel Icons

Icon	Meaning
/	Stay Arm / Stay Armed
/	Away Arm / Away Armed
	Disarm
	Silence Alarms
	Online
	Offline
	Uploading Speed
	Downloading Speed
	CPU Usage

Icon	Meaning
	Memory Usage
	Number of Ends
	Normal HDD
	HDD Exception
	Normal Ethernet
	Ethernet Exception
	In Health Monitoring
	Authorized
	Normal Memory
	Memory Exception

Chapter 3 Account

3.1 How to register an account?

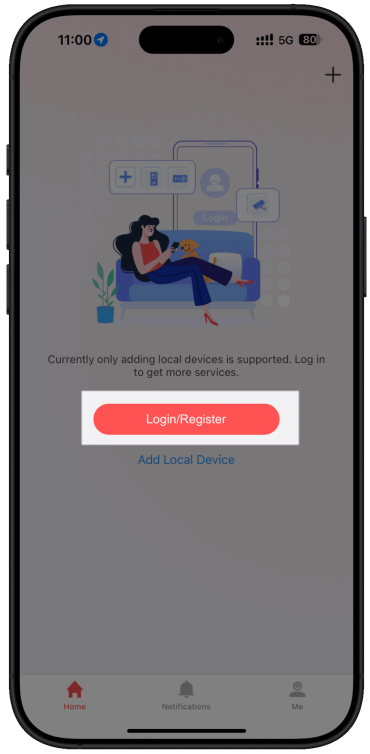


Figure 3-1 Register

3.2 How to log in?

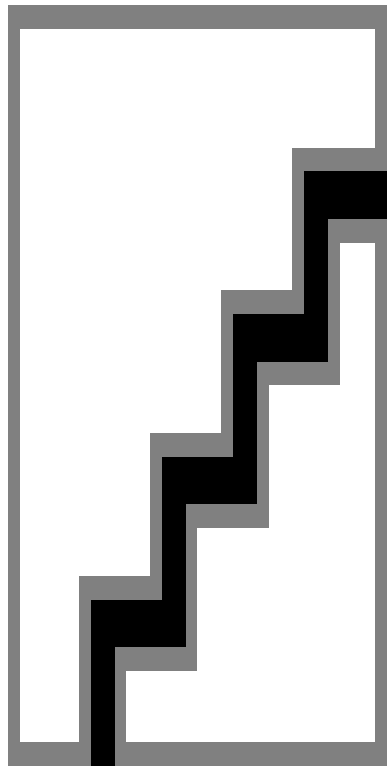


Figure 3-2 Log In

3.3 How to log in as a visitor?

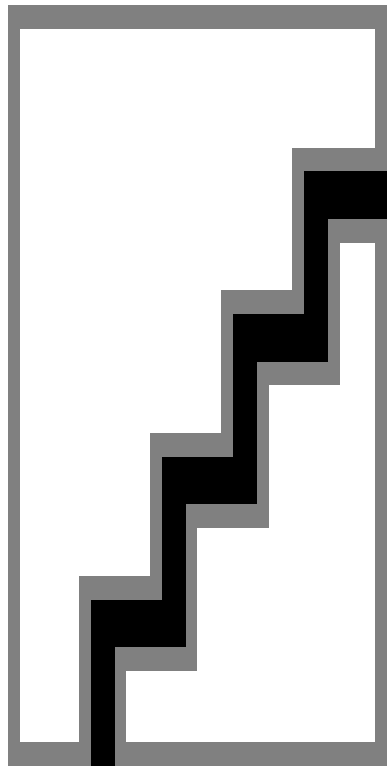
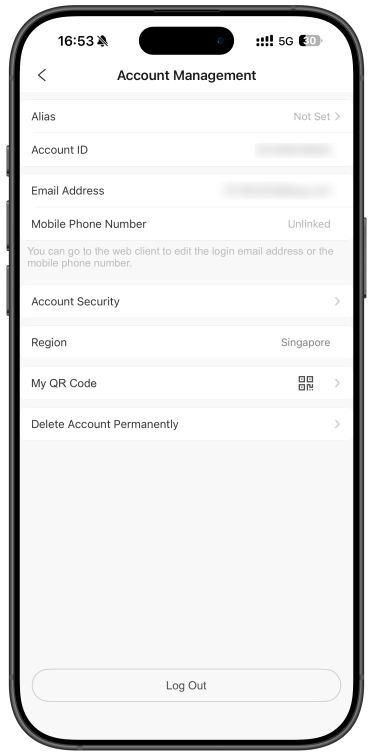


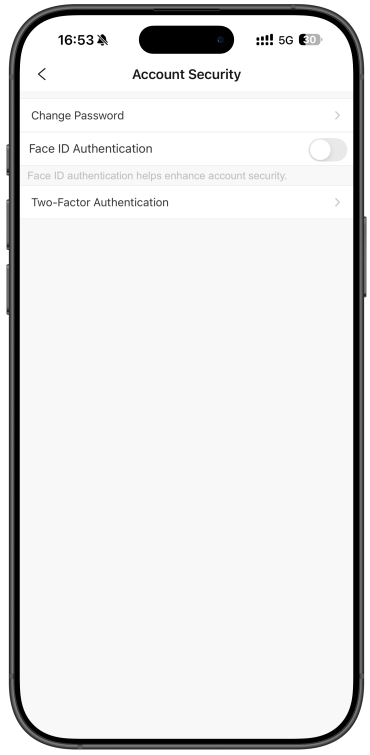
Figure 3-3 Visitor Mode

3.4 Two-Factor Authentication

You can enable Two-Factor Authentication for your account. Once enabled, logging in will require not only your password but also a verification code sent to your email or mobile phone via SMS, or a push notification to a trusted device, adding an extra layer of security.

1. **Enabling Two-Factor Authentication:** Log in to the app and find the option to enable Two-Factor Authentication in the "Me" menu. Enabling it may require a security verification step.


16:53
5G
Account Management
Alias
Not Set
Account ID
Email Address
Mobile Phone Number
Unlinked
You can go to the web client to edit the login email address or the mobile phone number.
Account Security
Region
Singapore
My QR Code
Delete Account Permanently
Log Out


16:53
5G
Account Security
Change Password
Face ID Authentication
Face ID authentication helps enhance account security.
Two-Factor Authentication





2. **Login Process:** When logging into an account with MFA enabled from a new, untrusted device:

a. After entering the correct username and password, the system will require a second verification step.
b. A verification code will be sent by default to your registered email (or phone number). You may also have the option to receive a push notification on another trusted app device.
c. Enter the correct code to log in successfully. You can choose to add the current device to your list of trusted devices, so future logins from this device won't require the second step.

3. **Managing Trusted Devices:** After logging in, you can view and manage your list of trusted devices within the "Me" settings. You can see device info, login location and time, and remove devices you no longer use (you cannot remove the device you are currently using).

Chapter 4 Device Management

4.1 How to add devices?

On the Home page, tap + .

Before you begin:

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- Make sure the device has been activated and connected to Hik-Connect service.

Table 4-1 Methods of Adding Devices

Adding Methods	Application Scenario
Add by IP Address or Domain Name	• You can use the method if you know the IP address or domain name of a device. • Only encoding devices mapped in WAN support this function. • When you need to share devices via QR code. Download or update the Hik-Connect Mobile Client (version 4.5 and later), so you can share the device by sending the QR code generated after the device setup.
Add by Scanning QR Code	You can add a device to a site by scanning the QR code on the device.
Add by Entering Serial No.	If a device is connected to Hik-Connect service, you can manually add it to a site by entering the device serial number and device verification code. Enter the device serial number and device verification code. **Note** The device serial number and the default device verification code are usually on the device label. If no device verification code found, enter the verification code you created when enabling Hik-Connect service.

4.2 How to add groups?

In Hik-Connect, device grouping is used for managing devices by type (e.g., cameras, access control devices), usage (e.g., security, IT), or location (e.g., headquarters, branches). For example, you can add cameras to the same group for batch preview, or group access control devices for batch operations like simultaneous door opening.

- Add a group.

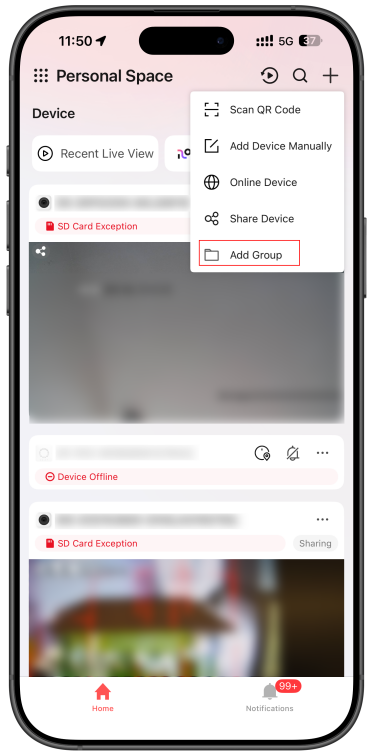
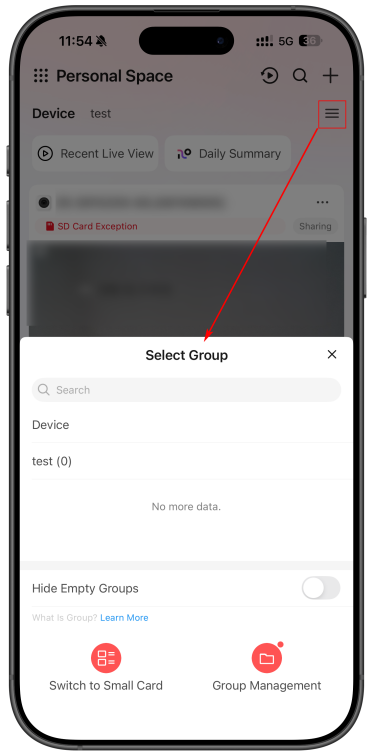
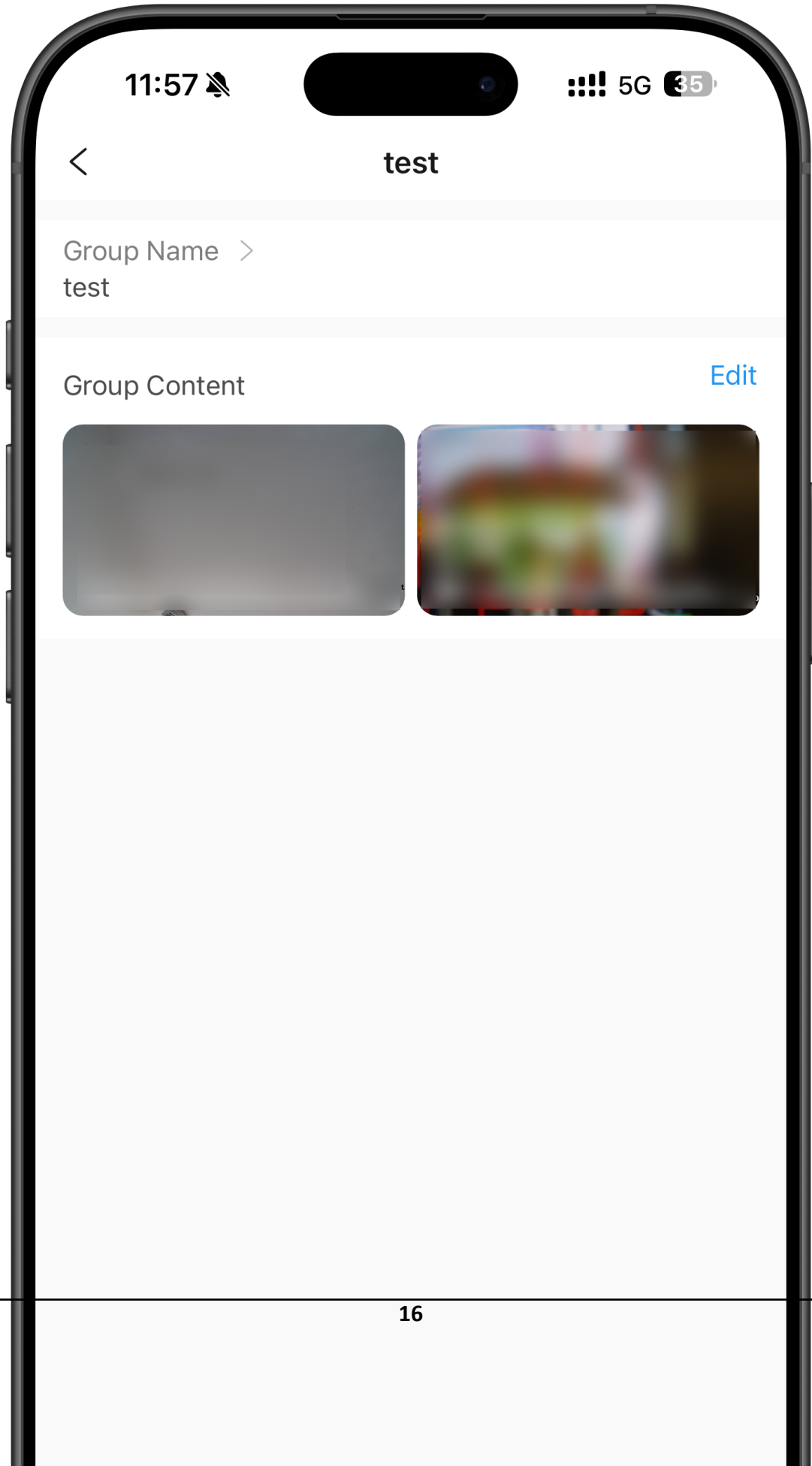


Figure 4-1 Add Group

- You can add, edit, sort, and delete groups. You can also add, edit, sort, and delete devices in a group.


11:54
5G
Personal Space
Device
test
Recent Live View
Daily Summary
SD Card Exception
Sharing
Select Group
Search
Device
test (0)
No more data.
Hide Empty Groups
What Is Group? Learn More
Switch to Small Card
Group Management


11:57
5G
35
test
Group Name
test
Group Content
Edit

4.3 How to switch between large and small card?

You can display devices in large or small device cards.

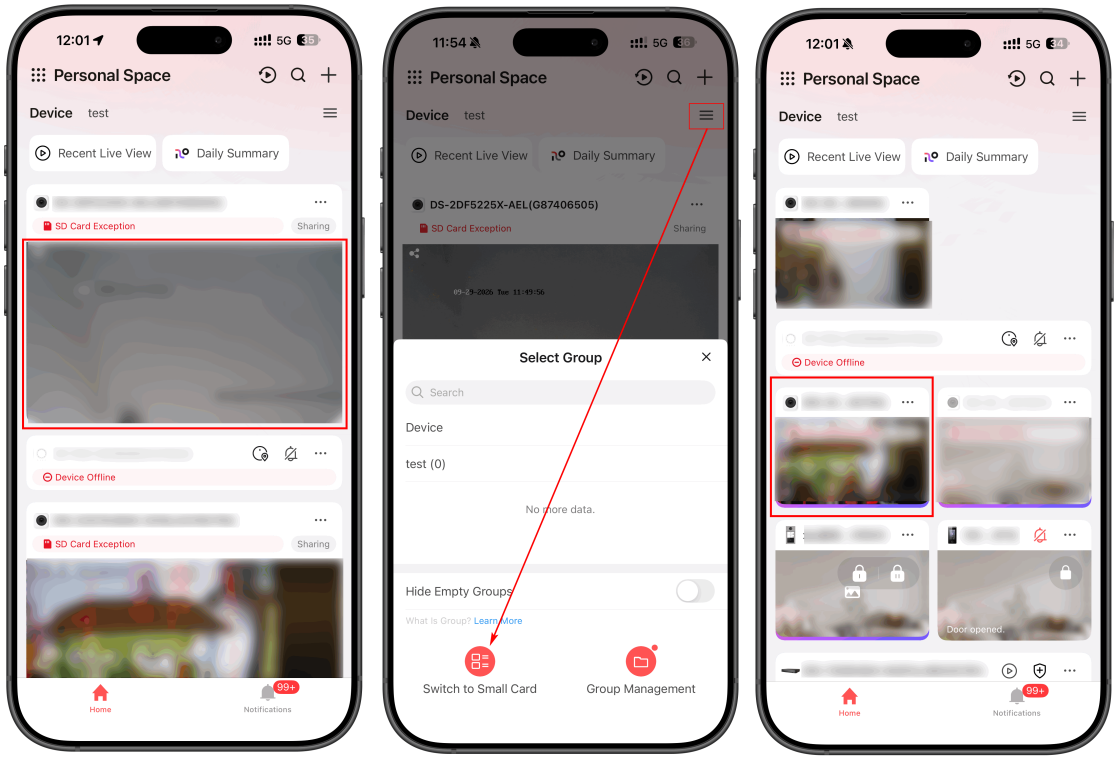


Figure 4-2 Small Card VS Large Card

4.4 How to share devices?

For sharing devices, refer to the video:
http://enpinfodata.hikvision.com/analysisQR/showQR/8bbb8070

Chapter 5 Camera/NVR/DVR/NVS

5.1 How to use AI video Q&A?

To help you quickly find critical information in massive video data and avoid tedious manual searches, The AI Video Q&A unifies video AI capabilities through natural language understanding, making tasks like footage retrieval and video analysis as simple as chatting.

On the Playback page, tap to open the AI Assistant.

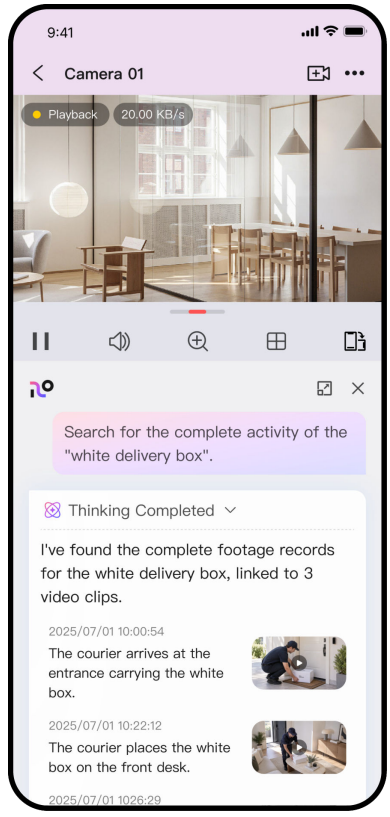


Figure 5-1 AI Video Q&A

1. Ask questions like "Did anyone enter the warehouse last night?" or "How many cars came in today?".
2. The system provides a direct text answer along with relevant video clips. Tap to play and verify instantly.
3. Supports follow-up questions within context. For example, ask "Did John appeared in these clips?", and the system understands the context automatically.

Note

- Supported question types: occurrence (yes/no), count/frequency, time/period, behavior description, and target attributes.
- When no time range is specified, the system defaults to searching the last 24 hours.
- Supports up to 3 turns of contextual conversation.

5.2 How to use daily summary?

The feature analyzes 24 hours of video and events of a camera, automatically generating a daily overview with counts of people, vehicles, animals, suspicious events, and AI alarms—all in one place for quick review.

1. Tap → **Video** → **Camera** → **Daily Summary** .

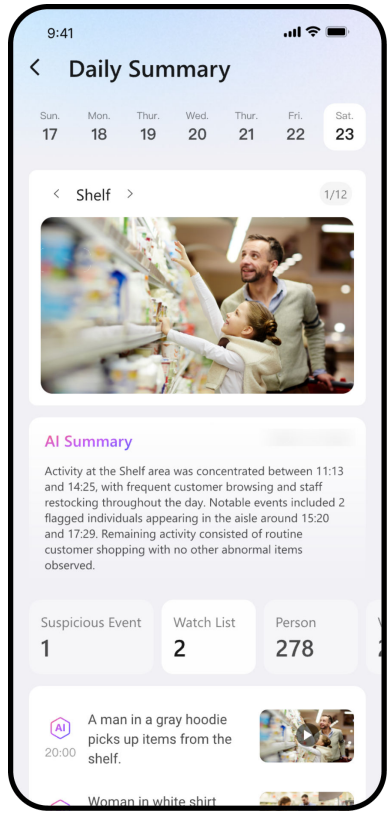


Figure 5-2 Daily Summary

2. Select a date and camera to view the daily summary of the camera.
3. Filter events by tapping **Suspicious Event**, **Person**, **Vehicle**, **Animal**.
4. In the event list, tap to view details.

5.3 How to start live view?

Live view shows you the live video getting from cameras. Perform the following task to start and stop live view.

5.3.1 How to start and stop live view?

1. Tap a camera or tap **Applications → Live View** to enter the Live View page.
   - If the Video and Image Encryption function is disabled, the live video will start playing automatically.
   - If the Video and Image Encryption function is enabled, you should enter the encryption password before live view.

   Note
   - The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling Hik-Connect service.
   - The live video from the video intercom device lasts 5 minutes.
   - Up to 6 users can view the live video of a same door station simultaneously. If the upper-limit is reached, other users can only use the audio function of the door station.
2. Perform the following operations.

View Full Screen Live Video	Rotate the phone to view live video in full screen mode.
Switch Camera	Swipe the live view page to the left or right to switch camera and view its live video.
Reselect Device for Live View	a. Tap to reselect device(s) for live view. b. Reselect cameras and then tap **OK**. **Note** You can select up to 256 cameras.
Switch to Playback	Tap **Playback** to switch to playback.
Toolbar Operations	For details about toolbar operations, see ***Live View and Playback Icons*** .
View Events	If there are any events, they will be displayed in the **Event Messages** section.

3. Stop live view of a camera.
   a. Press and hold a window under live view.
   b. Drag the window upwards to the appearing at the top of the page.

5.3.2 How to control PTZ?

PTZ is an abbreviation for "Pan, Tilt, and Zoom". With the PTZ Control functionality provided by the Mobile Client, you can make the cameras pan and tilt to the required positions, and zoom in or out the live video images.

Start live view of the camera, and tap to pop up the PTZ control panel.

PTZ Control

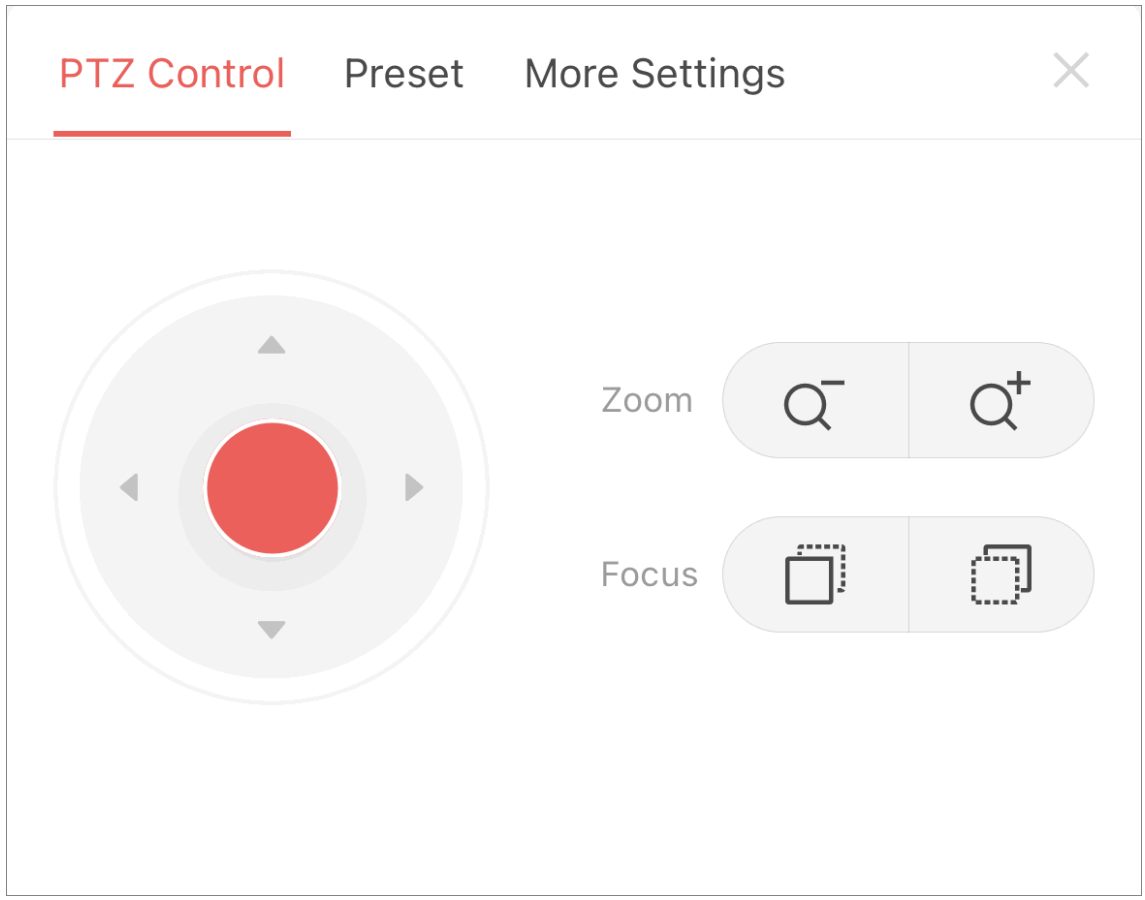


Figure 5-3 PTZ Control

On the PTZ Control panel, the following operations are supported.

- Drag the red circle button to control the camera to the desired direction.
- Tap / to zoom out/in the lens.
- Tap / to make near objects become clear and distant objects become vague, or make distant objects become clear and near objects become vague.

Preset

On the Preset panel, the following operations are supported.

- Edit Name: Tap ··· → **Edit Name** to edit the preset name.
- Set as Preset: Tap ··· → **Set as Preset** to set the current scene as a new preset.

More Settings

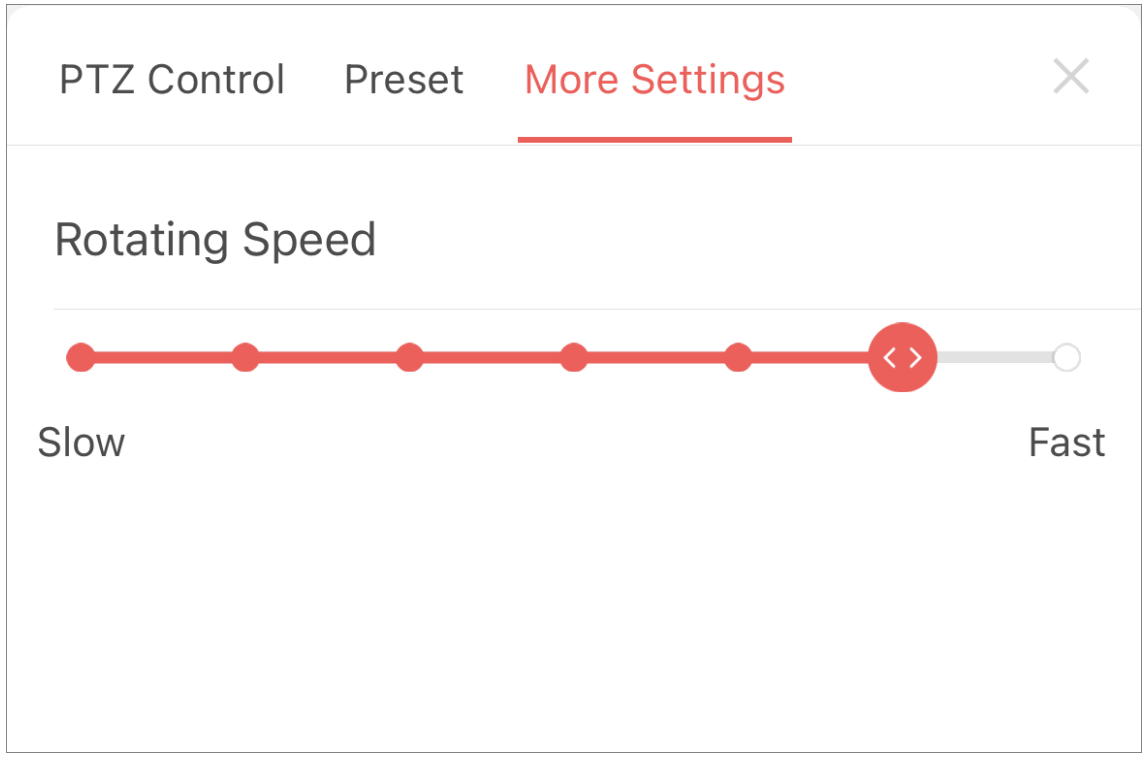


Figure 5-4 More Settings

Drag to the right or left to set the PTZ rotating speed.

5.3.3 How to set image quality?

Note

- If you change the image quality, the live view and recording of the device may be affected due to the new settings.
- In multi-window mode, you can only set the image quality to Fluent, or customize the image quality and the stream type can only be Sub Stream.

1. Start live view of a device added via IP/Domain.
2. Tap on the live view page to enter the quality switching panel.

Note

The icon vary with the actual video quality.

3. Set the image quality as desired.
   - Tap **Clear** to set the image quality as Clear.
   - Tap **Fluent** to set the image quality as Fluent.
   - Tap **Custom** to open the Custom Settings window, and then configure the parameters and tap **Confirm** to confirm the custom settings.

Note

- The live view effect is related to the performance of your network and hardware of your network and phone and tablet. If the live view is not fluent or the image appears blurred, reduce the resolution, frame rate and bitrate of the camera in custom mode, or set the image quality as fluent mode.
- The following table shows the recommended Android and iOS frame rate and bitrate configuration for different resolution at H.264, H.264+ and H.265 video compression by Moto X Pro (CPU: Snapdragon805, Android 5.0.2).

Table 5-1 Android Recommended Configuration

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
H.264 (Software Decoding)				
1080P	√	√		Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264 (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264+ (Software Decoding)				
1080P	√	√		Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
H.264+ (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
H.265 (Software Decoding. Hardware decoding is not supported.)				

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
1080P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 256Mbps

- **Table 5-2 iOS Recommended Configuration**

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
H.264 (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264 (Software Decoding)				
720P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
4CIF	√	√	√	Frame rate: 25fps; Bit rate: 512Kbps
H.264+ (Hardware Decoding)				
1080P	√	√	√	Frame rate: 25fps; Bit rate: 4Mbps
720P	√	√	√	Frame rate: 25fps; Bit rate: 2Mbps
H.264+ (Software Decoding)				
720P	√	√		Frame rate: 25fps; Bit rate: 2Mbps
H.265 (Software Decoding. Hardware decoding is not supported.)				
1080P	√			Frame rate: 25fps; Bit rate: 2Mbps
720P	√	√		Frame rate: 25fps; Bit rate: 1Mbps
4CIF	√	√	√	Frame rate: 25fpc; Bit rate: 256Kbps

5.3.4 How to start live view of a fisheye camera?

In the fisheye view mode, the whole wide-angle view of the fisheye camera is displayed. Fisheye expansion can expand images in five modes: 180° panorama, 360° panorama, 4-PTZ, semisphere, and cylindrical-surface.

Note

The function is only supported by fisheye camera.

1. Start live view of a fisheye camera.
2. Tap to show the fisheye expansion panel.
3. Select mounting type.

Table 5-3 Mounting Type

Icon	Description
	Wall Mounting
	Ceiling Mounting

4. Select fisheye expansion mode.

Table 5-4 Fisheye Expansion Mode

Icon	Description
	Fisheye view for ceiling mounting and wall mounting. In the Fisheye view mode, the whole wide-angle view of the camera is displayed. The mode is the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image. In this mode, you can pinch the fingers together to zoom out the image, and spread them apart to zoom in.
	Dual-180° panorama view for ceiling mounting. The distorted fisheye image is transformed to normal perspective image. In this mode, you can swipe to the left or to the right to adjust the field of view.
	360° panorama view for ceiling mounting and wall mounting. The distorted fisheye image is transformed to normal perspective image. In this mode, you can swipe to the left or to the right to adjust the field of view.
	4 PTZ Views for ceiling mounting and wall mounting. The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view. In this mode, you can pinch the fingers together to zoom out the image, and spread them apart to zoom in. You can also swipe the screen to perform pan and tilt movement.
	Semisphere-shaped view for wall mounting. In this mode, the whole wide-angle view of the camera is displayed. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.

Icon	Description
	In this mode, you can drag the image to adjust the view angle, and pinch the fingers together to zoom out the image, and spread them apart to zoom in.
	Cylindrical-surface-shaped view for wall mounting. In this mode, the whole wide-angle view of the camera is displayed. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image. In this mode, you can drag the image to adjust the view angle, swipe to the left or to the right to adjust the field of view, as well as pinch the fingers together to zoom out the image and spread them apart to zoom in.

5.3.5 How to open doors during live view?

You can open or close the door when viewing the live video of a video intercom device, a face recognition terminal, or a related camera of an access control device. This function allows you to check the visitor or the situation nearby the door before you open it.

Note

- The device should support this function.
- For face recognition terminals, you can enabling opening door by fingerprint authentication or facial authentication.

For the access control device's related cameras, select a live view window and tap **Open Door**, and then enter the device verification code to open the door.

For the video intercom device, select a live view window and tap , and then enter the device verification code to open the door.

Note

The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling Hik-Connect service.

5.4 How to start playback?

5.4.1 How to start normal playback?

Normal playback refers to the playback based on timeline. You can search the camera's recorded video files in a selected time period and then start playback.

1. On the device list page, tap in the upper-right corner or tap **Applications → Playback** to enter the Select Item(s) page.
2. Set the date and time for playback.
   - Select a date.

     Note

     The date during which video files were recorded is marked with a yellow dot.
   - Set the start time point for the playback in the selected date.
3. Select camera(s).

   Note

   You can select up to 4 cameras.
4. Tap **Start Playback** to enter the Playback page.
5. Perform the following operations.

Play Video Footage Stored on Cloud	Tap on the playback page to play back video footage stored on cloud.
Play Video Footage Stored on Local	Tap on the playback page to play back video footage stored locally.
Clip Playback	Tap to switch to clip playback.
Adjust Playback Time	Tap to switch timeline playback. Slide the timeline to adjust the playback time. Spread two fingers apart to scale up the timeline or pinch them together to scale down. **Note** represents continuous recording and represents event-triggered recording. You can determine the recording type (continuous or event-triggered) when setting recording schedule.
Toolbar Operations	For details about toolbar operations, see ***Live View and Playback Icons*** .

5.4.2 How to capture images and recording videos?

1. Start playback.
2. Capture a picture or record video footage.

Capture a Picture	Tap to capture a picture.
Record Video Footage	Tap to start recording video footage, tap again to stop.

The captured pictures and recorded videos will be saved in **Applications → Personal Applications → Personal Album**.

5.4.3 How to download a specific video segment?

During playback of the cameras linked to a DVR or NVR, you can download a specific video segment as an evidence if it contains important information about incidents such as violent crimes in case of the need for settling disputes or legal cases.

Note

The function should be supported by the device.

1. Start playback.
2. Tap if important information occurs on the image.
   By default, the video segment which lasts 130 seconds (from 10 seconds before the tapping, to 120 seconds after that) will be automatically selected for download. For example, if you tap when the video footage is played to 00:00:30, the segment from 00:00:20 to 00:02:30 will be selected.

   Note

   In special occasions when 130-seconds duration is not available to be selected following the above-mentioned rule, the segment will extend afterwards or backwards until the segment duration reaches 130 seconds. For example, if you start downloading from the very beginning of the video footage, the selected segment will be from 00:00:00 to 00:02:10.
3. Drag the slider(s) to lessen the duration of the segment for download.

   Note

   The duration should not be shorter than 10 seconds.
4. Tap the Play icon to preview the selected segment.

   Note

   If the segment is encrypted, you should enter the device verification code before you can preview it. For details about video encryption.
5. Tap **Start Downloading** to start downloading.

   Note

   Downloading at the background is supported. Download task(s) continues if you exit the Download page or the Mobile Client.
6. Go to **Me → Personal Applications → Personal Album** to view the downloaded video segment.

5.4.4 How to view pictures and videos?

After capturing pictures and recording videos during live view, you can view these pictures and videos, and perform more operations such as saving them to the local mobile phone, share them with others, etc.

Go to **Applications → Personal Album** to enter the Pictures and Videos page, and you can perform the following operations.

Table 5-5 Supported Operations

Description	Operation
Batch Share Pictures and/or Videos	Tap **Edit**, select pictures and/or videos, and tap to share the selected ones with others.
Batch Delete Pictures and/or Videos	Tap **Edit**, select pictures and/or videos, and tap to delete the selected ones.
Save to Local Mobile Phone	Tap a picture or video, and tap in the lower-right corner to save it to the local mobile phone.
Play Video	Tap a video, and tap in the lower-right corner to play the video.
Share a Picture or Video	Tap a picture or video, and tap in the lower-right corner to share it with others.
Delete a Picture or Video	Tap a picture or video, and tap in the lower-right corner to delete it.

5.5 How to use the cloud storage service?

5.5.1 How to enable/disable cloud storage service for a channel?

You can enable/disable cloud storage service for a specific channel of a device supporting storing video footage on cloud. You can also view details of the cloud storage service package, including service package type, effective period, and status (activated or expired).

Before You Start

Make sure your Service Provider has activated the cloud storage service for your device. Otherwise, you cannot enable cloud storage.

Steps

1. Enter the settings page of the device.
2. Tap **Cloud Storage** to enter the Cloud Storage page.

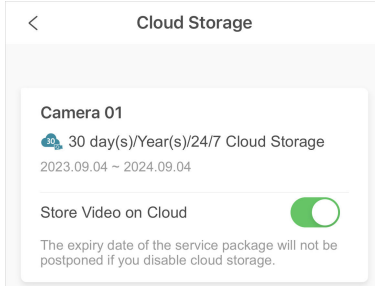


Figure 5-5 Cloud Storage

3. Switch on/off to enable/disable the cloud storage service of a specific channel.

5.5.2 How to play back and download video footage from the cloud?

The Mobile Client allows you to browse through the video footage stored on cloud of each date to quickly locate the footage you need. And you can download the video footage to your phone.

Before You Start

Note

Make sure your Service Provider has activate cloud storage service for your devices and you have enable it.

Steps

1. Start playing back video footage stored on cloud.
2. Tap to play video stored on cloud.
3. Tap to enter the Download Video page.
4. Select a date.

   Note

   The date marked with a blue dot is the date during which video footage is recorded.
5. Tap , and then select the video footage you want to download.
6. Tap to download the selected video footage to your phone.

5.6 How to use intelligence search?

5.6.1 How to use AcuSeek?

AcuSeek helps you quickly find clips or images you are looking for. You can describe a target and their features such as a person wearing a hat, and AcuSeek will find you matching images or clips. Tap **View Devices** on the AcuSeek page to view the devices with the capability.

Note

The feature is only available in certain countries/regions.

1. Tap **AcuSeek** on the top of the Home page.

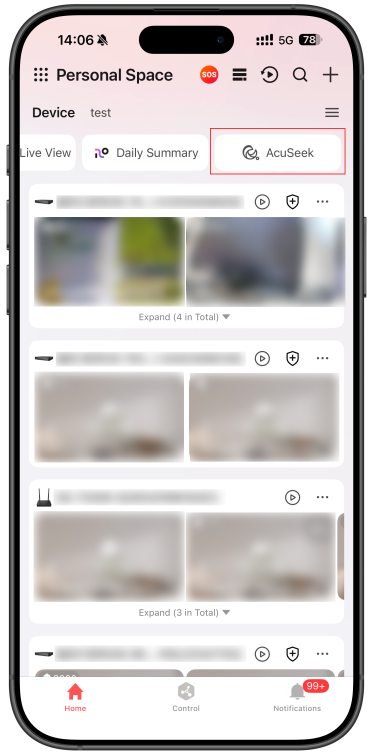


Figure 5-6 AcuSeek Entrance

2. Enter words to search for videos.

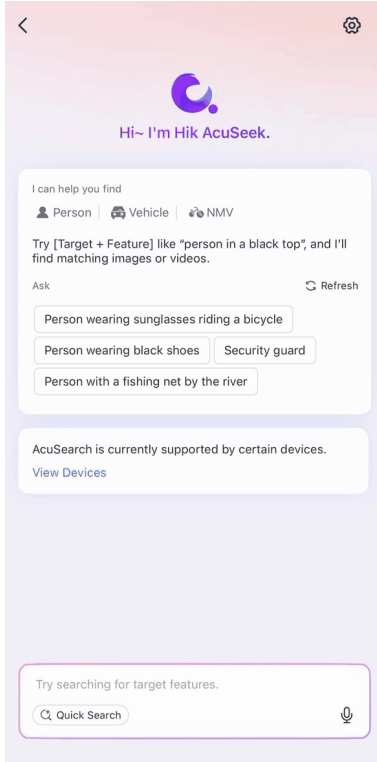


Figure 5-7 AcuSeek

3. You can set the similarity, search range, and devices enabling AcuSeek and AcuSearch.

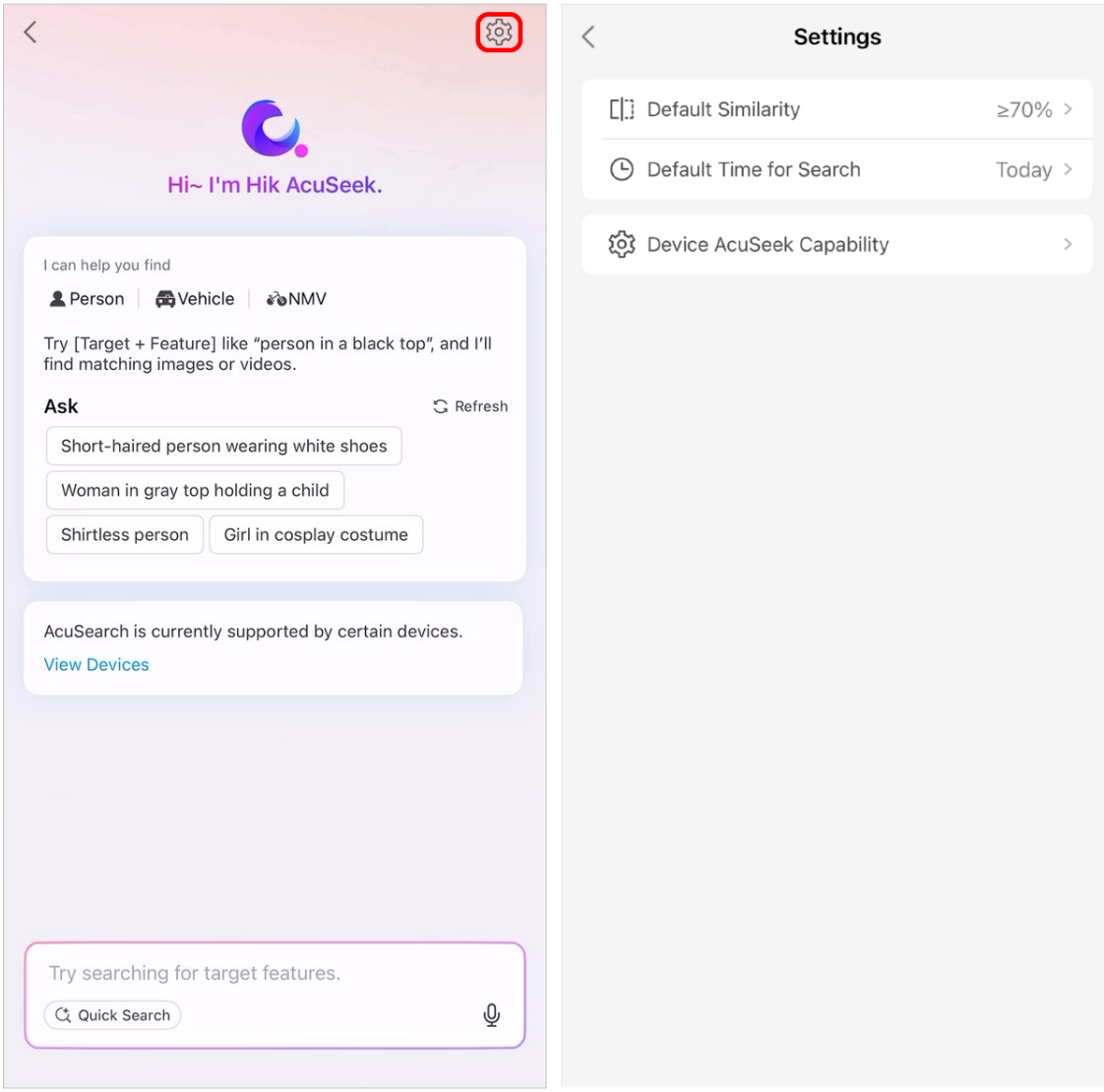
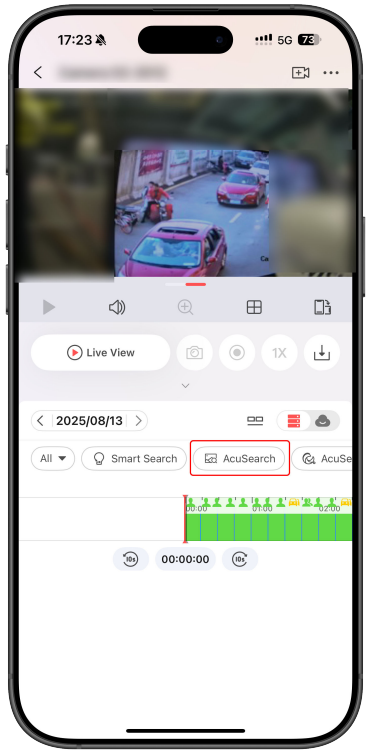
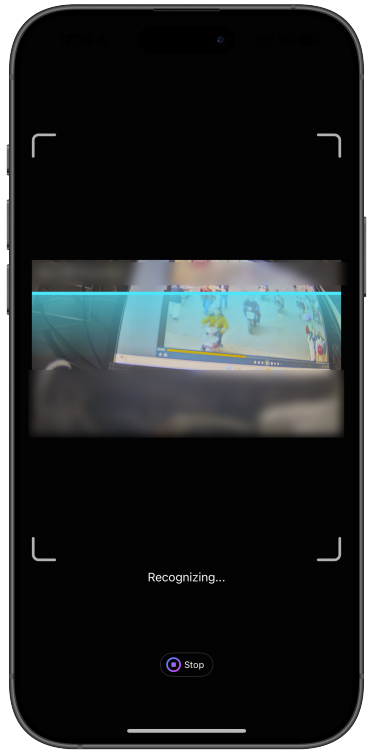


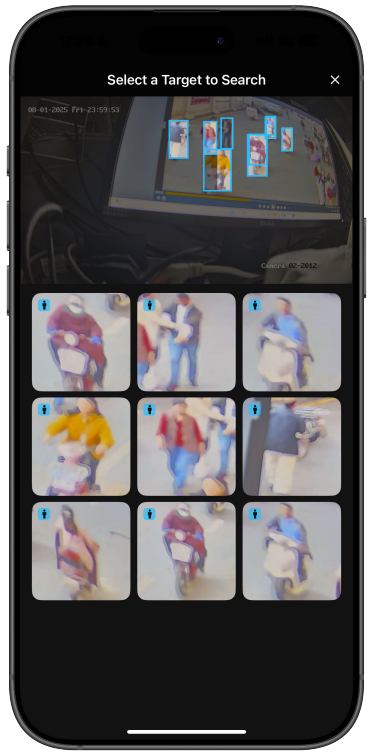
Figure 5-8 Settings

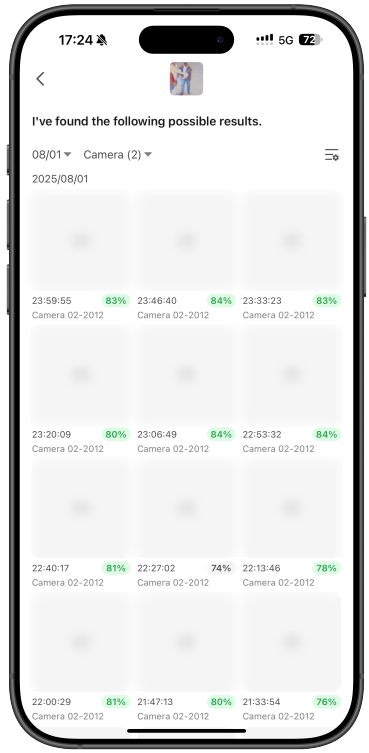
5.6.2 AcuSearch on the Playback Page

- During playback: Use the current frame to search for similar images from your camera's NVR (available on supported devices).


17:23
5G
Live View
1X
2025/08/13
All
Smart Search
AcuSearch
00:00:00


Recognizing...
Stop

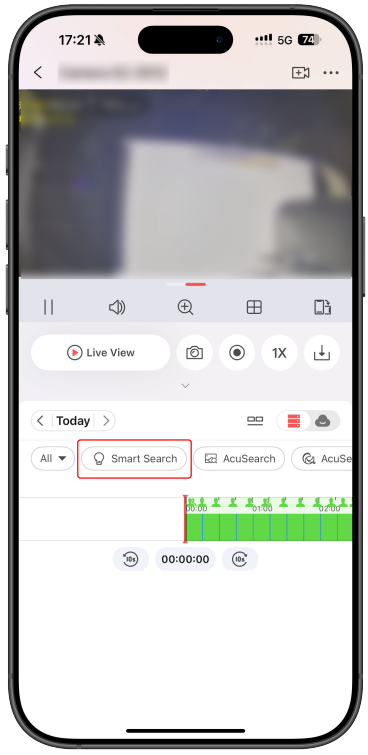

Select a Target to Search

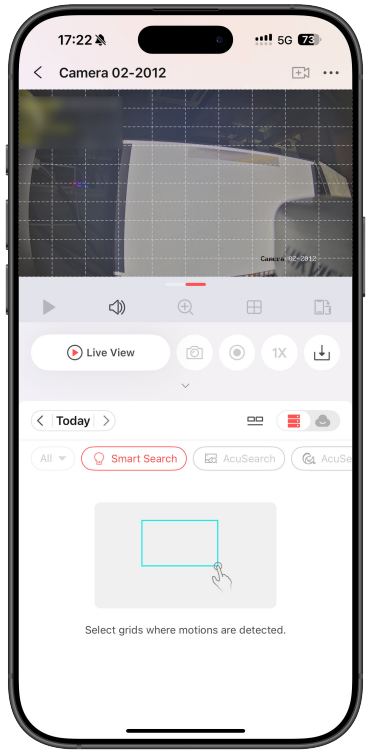

17:24
5G
I've found the following possible results.
08/01
Camera (2)
2025/08/01
23:59:55 83%
Camera 02-2012
23:46:40 84%
Camera 02-2012
23:33:23 83%
Camera 02-2012
23:20:09 80%
Camera 02-2012
23:06:49 84%
Camera 02-2012
22:53:32 84%
Camera 02-2012
22:40:17 81%
Camera 02-2012
22:27:02 74%
Camera 02-2012
22:13:46 78%
Camera 02-2012
22:00:29 81%
Camera 02-2012
21:47:13 80%
Camera 02-2012
21:33:54 76%
Camera 02-2012

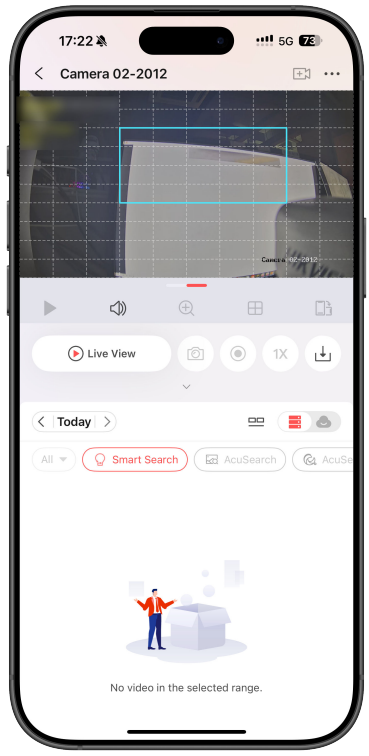


5.6.3 Smart Search on the Playback Page

Now you can use **Smart Search** during playback to search videos of the current channel you're viewing.

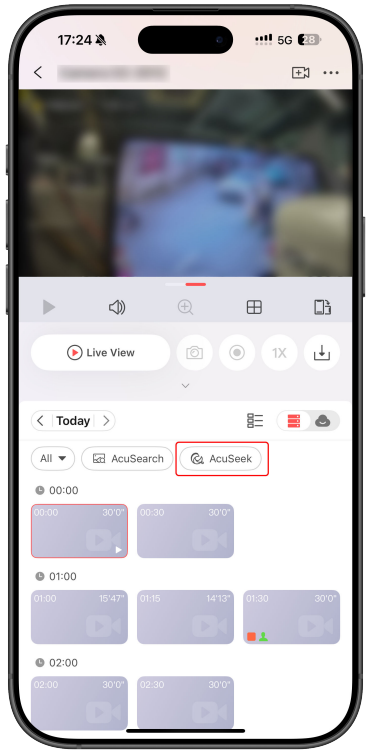

17:21
5G
Live View
1X
Today
All
Smart Search
AcuSearch
00:00:00

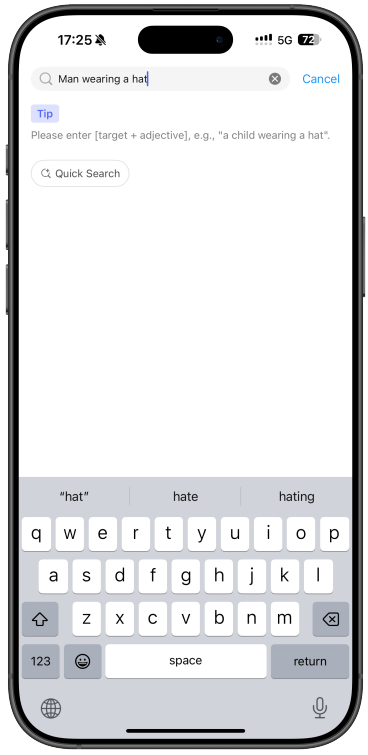

17:22
5G
Camera 02-2012
Live View
1X
Today
All
Smart Search
AcuSearch
Select grids where motions are detected.

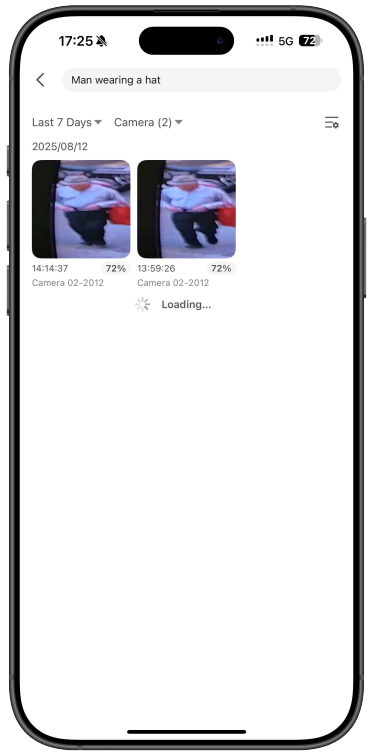


5.6.4 AcuSeek on the Playback Page

Now you can use **AcuSeek** during playback to search videos of the current channel you're viewing.


17:24
5G
Live View
1X
Today
All
AcuSearch
AcuSeek
00:00
01:00
02:00


17:25
5G
Man wearing a hat
Cancel
Tip
Please enter [target + adjective], e.g., "a child wearing a hat".
Quick Search
"hat"
hate
hating
space
return

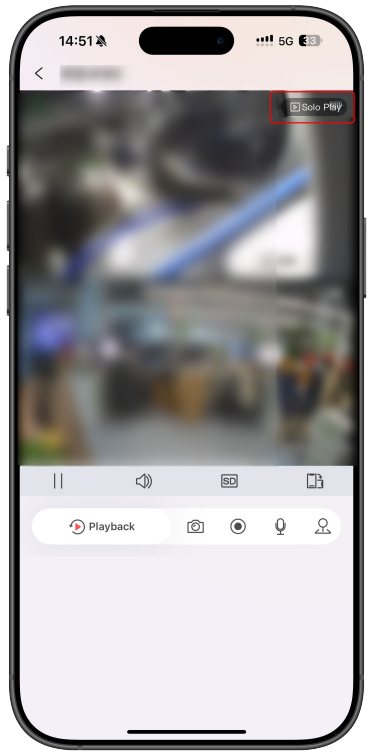


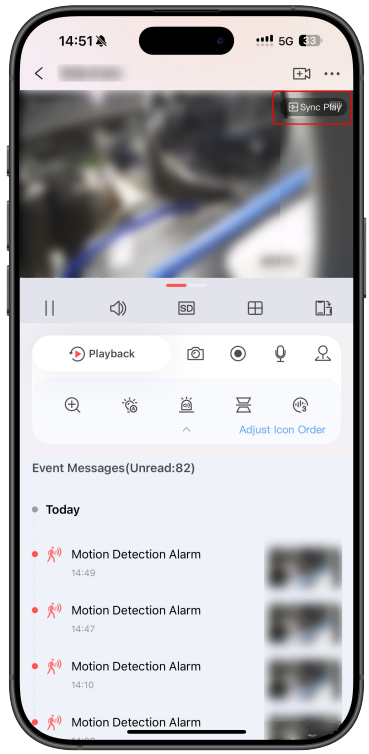
5.7 How to use dual-lens cameras?

Dual-lens cameras combine both a panoramic lens and a close-up lens. The panoramic lens captures a wide-angle view, offering full-scene coverage for broader situational awareness. At the same time, the close-up lens zooms in on specific details within the scene, delivering sharp, high-definition footage of important subjects. Together, these lenses work seamlessly to provide both a comprehensive overview and focused detail—all in one view.

Supported dual-lens camera models (DS-2CFSP8-D/4G/EU(2.8+4mm), DS-2CFSP8-D/4G/LA(2.8+4mm), IPC-CFSP8-D/4G/EU(2.8+4mm), IPC-CFSP8-D/4G/LA(2.8+4mm), IPC-CFWQ6-D(2.8+4mm), DS-2CFWQ6-D(2.8+4mm), IPC-CFSP8-D/W(2.8+4mm)).

- Adaptive Dual-View Display: Switch between single-channel (Solo View) and synchronized dual-channel (Sync View) modes. For Sync View, the image can automatically switch between split-screen (portrait) and picture-in-picture (landscape) for simultaneous panoramic and PTZ viewing.


14:51
5G
Solo Play
SD
Playback



- Tap-to-Zoom During Playback: During playback, tap any area on the panoramic view to automatically reposition the close-up PTZ view.

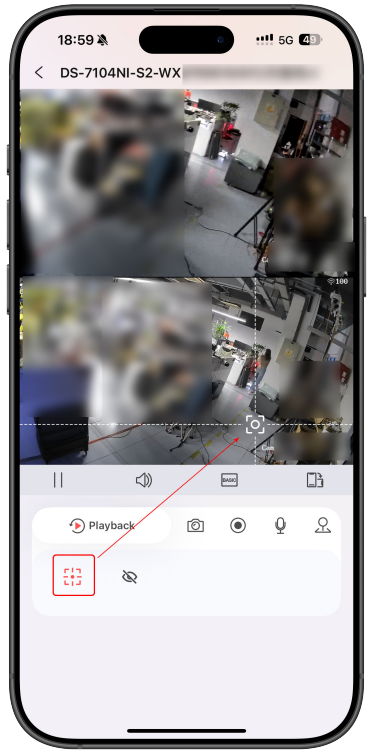


Figure 5-9 Tap to Zoom

- Linked Privacy Masking: Enabling privacy masking on one lens automatically activates it on both lenses.

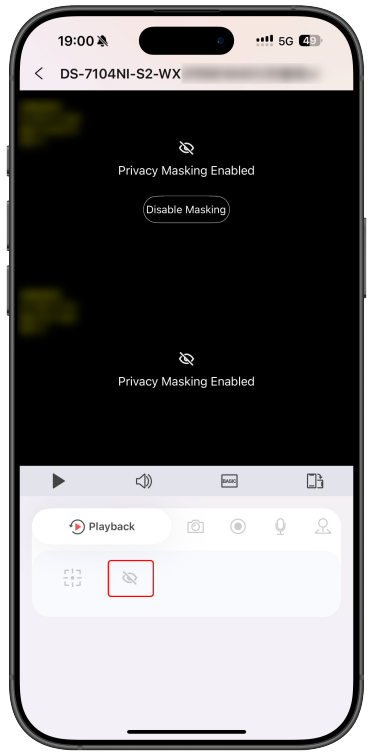


Figure 5-10 Privacy Masking

- Unified Device Management: Both channels appear as a single device card on the home page and share settings such as recording schedules.

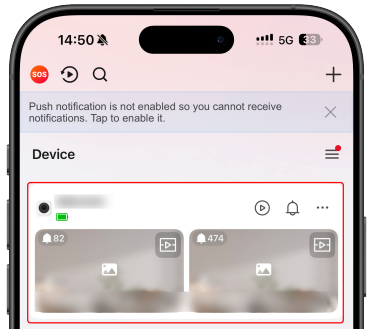


Figure 5-11 Device Card

5.8 How to set up cameras?

5.8.1 How to manage solar cameras?

After adding a solar camera to the Mobile Client, you can control and manage it remotely. The supported functions include waking up the device, viewing its network signal strength, switching power consumption mode, etc.

Wake Up Solar Camera

Unlike using other network cameras, you need to wake up a solar camera before you can control it. You can wake it up in the following two ways:

- On the device list page, tap ··· → **Settings** to enter the device settings page. Once you enter this page, the camera will start waking up.
- On the device list, tap the device to enter its live view page. Once you enter this page, the camera will start waking up.

View Network Signal Strength

Enter the device settings page of the solar camera, and then tap **Network Strength** to view its network strength level.

Switch Power Consumption Mode

Enter the device settings page of the solar camera, tap **Power Consumption Mode** and then select a mode.

Note

After switching power consumption mode, you need to reboot the solar camera to make the new settings take effect on the device.

5.8.2 How to set light for floodlight camera?

You can set light for the Floodlight camera.

Make sure you have added a Floodlight camera to the Mobile Client.

1. On the device list page, tap ··· → **Settings** on a device card to enter the Settings page of a Floodlight camera.
2. Tap **Light Settings** to enter the Light Settings page.
3. Set the parameters.

- **Adjust Brightness**: Adjust the brightness of the camera light.
- **Light Linkage**: If enabled, when activities of human beings or animals are detected at night in the areas specified by you (see **Light Linkage Area Settings**), the camera light will be automatically turned on.
- **Light Linkage Area Settings**: Tap the areas to specify them as the light linkage areas.

5.9 How to set motion detection for cameras?

Motion detection is a way of detecting motion in a security scene by analyzing image data and differences in a series of images. After setting motion detection area within the field of view of the network camera, the network camera will be able to detect the objects in motion within the area you set and at the same the Mobile Client will receive an event notification about the motion detection alarm.

Make sure the network camera is properly configured and connected to the Mobile Client.

1. On the device list page, tap ··· → **Settings** on a device card to enter the Settings page of the network camera.
2. Tap **Notification** to enter the Notification page.
3. Draw motion detection area.
   - Tap **Draw Motion Detection Area** to enter the motion detection area settings page.
   - Swipe on the screen to draw the motion detection area.



Figure 5-12 Draw Motion Detection Area

- Tap to undo the drawing.
- Tap to save the motion detection area settings.

4. Tap to go back to the Notification page and tap **Motion Detection Sensitivity**, and then adjust the slider to adjust the motion detection sensitivity.
   - **Low**: Moving persons, large moving pets, and any other large moving objects in the motion detection area will trigger the alarm, while smaller objects will not.
   - **Medium**: Moving small pets and any other medium-sized moving objects in the motion detection area will trigger the alarm, while smaller objects will not.
   - **High**: Moving insects, moving leaves, and any other larger objects will trigger the alarm.

Go back to the Notification page and make sure **Notification** is enabled.

5.10 How to manage cameras linked to NVRs/DVRs?

5.10.1 How to batch arm/disarm cameras linked to NVRs?

For cameras linked to NVRs and areas of NVRs, you can batch arm/disarm them, and silence alarms.

Steps

Note

Only NVRs with the firmware version 4.63.000 and newer support these updates.

1. On the device list page, find the device card of an NVR.

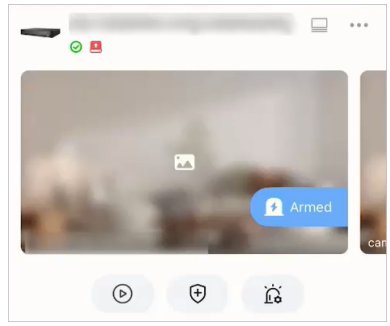


Figure 5-13 NVR

2. **Optional:** You can perform the following operations.

Batch Arm/Disarm Cameras and Areas or Arm Them Silently	Tap , and tap **Arm** / **Arm Silently** / **Disarm** at the bottom of the page, and all cameras linked with the NVR will be armed / armed silently / disarmed.
Arm/Disarm a Single Camera or Area or Arm One Silently	Tap to go to the area and camera details page.

	Tap a camera or area, and tap **Arm** / **Arm Silently** / **Disarm** at the bottom of the page, and the selected camera or area will be armed / armed silently / disarmed.
Edit Area/Camera Details	Tap to go to the area and camera details page. Tap ••• in the lower-right corner of an area or camera to edit its information.

5.10.2 How to edit the settings of cameras linked to NVRs/DVRs?

For cameras linked to NVR/DVR, you can edit their names, hide or show them in the device list, and enable camera cascading.

Steps

1. On the device list page, tap ••• → **Settings** on a device card to enter the Settings page of an NVR or DVR.
2. Tap **Linked Camera** to enter the Linked Camera page, and then edit camera settings.

Edit Camera Name	Tap › to enter the camera details page, and then tap **Channel Name** to edit the camera name, and finally tap ✓ to save the settings.
Hide/Show Camera	Tap or to hide or show the camera on the device list respectively.

5.11 How to reset passwords of NVRs/DVRs?

If you forgot the admin password of a DVR or NVR, you can reset the password by using the Mobile Client to scan the QR code generated on the local GUI of the device.

5.11.1 How to reset passwords by Hik-Connect?

Steps

1. On the user login interface of the device, click **Forgot Password**.
2. On the password reset type interface, select **Verify by Hik-Connect**.

   The QR code will be generated on the local GUI of the device.
3. Go to the Hik-Connect Mobile Client, enter the Reset Device Password page.
   - Tap **Applications → Basic Tool → Reset Device Password** .
   - Tap **Me → Reset Device Password** .
4. Scan the QR code.

   A verification code will be displayed on the Mobile Client.
5. Go to the local GUI of the device and enter the received verification code, and then click **OK** to continue.
6. Create a new password and then confirm the password on the local GUI of the device.

5.11.2 How to reset passwords by reserved Email address?

Make sure you have reserved email address for resetting the admin password of NVR or DVR if you want to change the password by scanning QR code.

Before You Start

- Upgrade the firmware of the NVR or DVR to make the device support self-service password reset.
- If the device is inactivated, check **Reserved Email Settings** when activate it. For details about activating NVR or DVR, see the user manual of the device.

Steps

Note

The DVR or NVR should support the function.

1. Go to **Configuration → User** on the local GUI of the device.
2. Select admin user and then click **Edit**.
3. Enter the password of the device in the Old Password field.
4. Click the Settings icon in Reserved E-mail Settings field.
5. Enter an email address for receiving verification code, and then click **OK**.
6. Enter the Reset Device Password page.
   - Tap **Applications → Basic Tool → Reset Device Password** .
   - Tap **Me → Reset Device Password** .
7. Scan the QR code on the local GUI of the DVR or NVR.

   A verification code will be sent to the reserved email address.

   Note

   - The verification code will be valid for 48 hours.
   - If you reboot the device or change the reserved email address, the verification code would be invalid.
8. Go to the device's local GUI.
9. Enter the received verification code on the Verify by Reserved Email window and then click **OK** to reset the password.

5.11.3 How to reset passwords by generated QR codes?

If you forgot the admin password of the DVR or NVR, you can generate a QR code on the device's local GUI and then scan the QR code via the Mobile Client to reset the admin password.

Before You Start

Make sure you have reserved an email address for resetting password.

Steps

Note

The DVR or NVR should support this function.

1. On the login page of the device's local GUI, click **Forgot Password**.
2. Select **Verify by Reserved Email** and then click **OK**.
3. Read and agree the Legal Disclaimer, and click **OK** to continue.

   The QR code for resetting password pops up.

Chapter 6 Alarm Devices

Refer to our ***release notes*** for more alarm device updates.



External Power Supply Disconnected / Connected with External Power Supply



Device Online / Devcie Offline



Tamper Alarm



Door/Window Opening Detected



Poor Contact of Network Cable and Panel Disconnected with Hik-Connect Service
Network Cable Connected and Panel Connected with Hik-Connect Service



24-Hour Zone



Ignore Tamper Alarms



Alarm Triggered



Alarm Trigger Delay When Entering Protected Area



Alarm Trigger Delay When Leaving Protected Area



RF Signal Exception / RF Singal Normal



Data Used / Data Limit Reached



WiFi Signal Excellent



WiFi Singal Good

WiFi Signal Fair

WiFi Singal Weak



WiFi Disconnected / No WiFi Signal



Mobile Signal Excellent

Mobile Signal Good

Mobile Signal Fair

Mobile Signal Poor

Mobile Signal Very Poor



Mobile Network Abnormal / No Signal



Battery 100% (Normal)



Battery 80% (Normal)



Battery 60% (Normal)



Battery 40% (Normal)



Battery 20% (Low Battery / Abnormal)



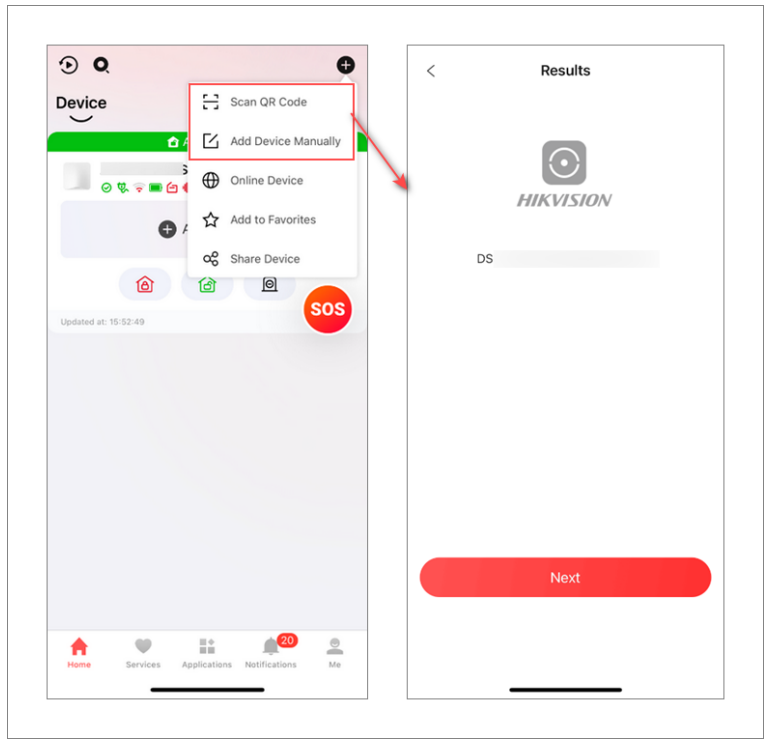
Battery Missing / Battery 0%

Device Authorized to Service Provider

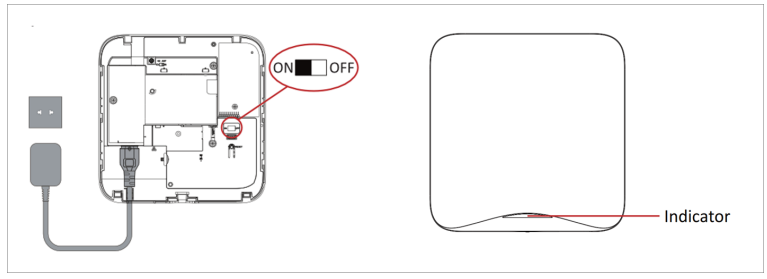
6.1 How to Add Security Control Panels

You can add a panel in one of the following ways:

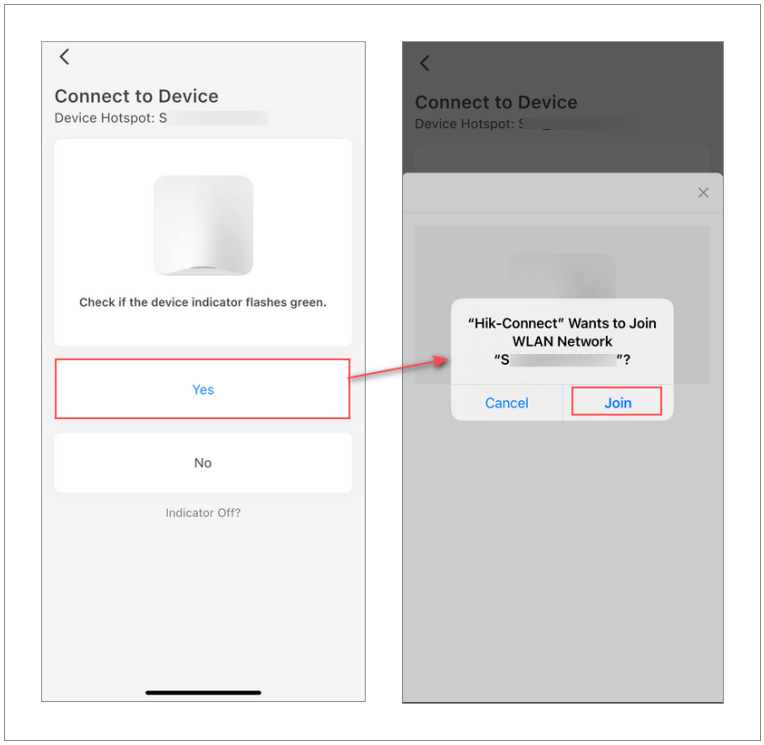
6.1.1 By Wi-Fi



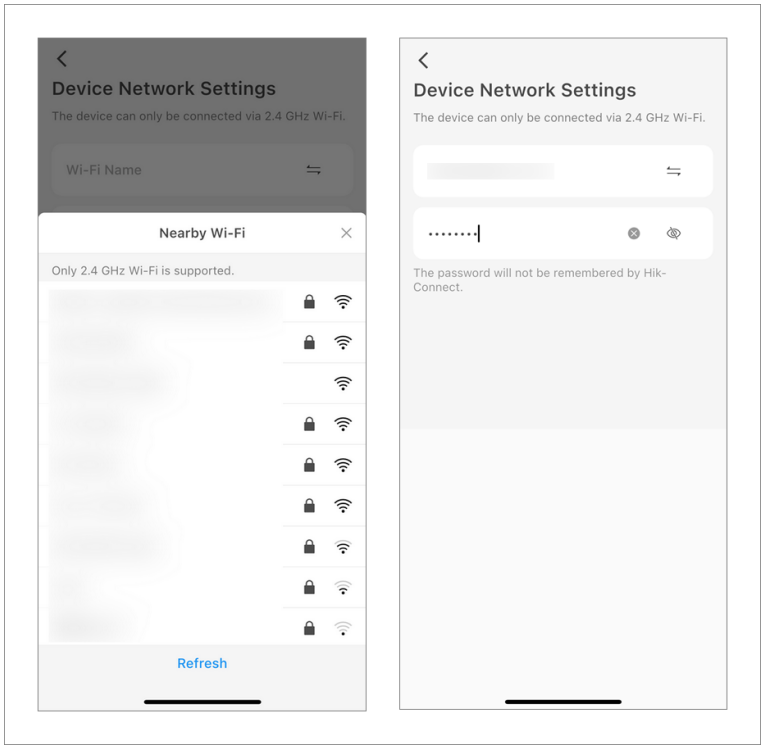
Add a security control panel.



Power on the device. After the device is powered on, the indicator light flashes green.



Join the device's hotspot.



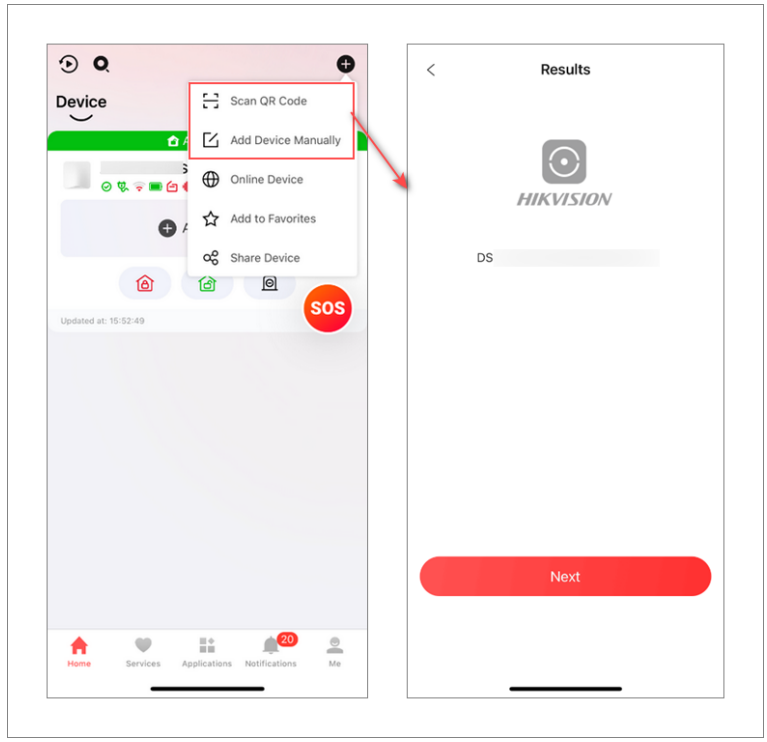
Connect the device to your Wi-Fi.

6.1.2 By SIM Card

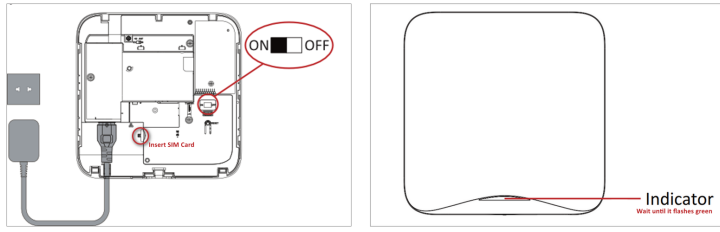
Prerequisite

SIM card can only be used in a security control panel supporting cellular communication.

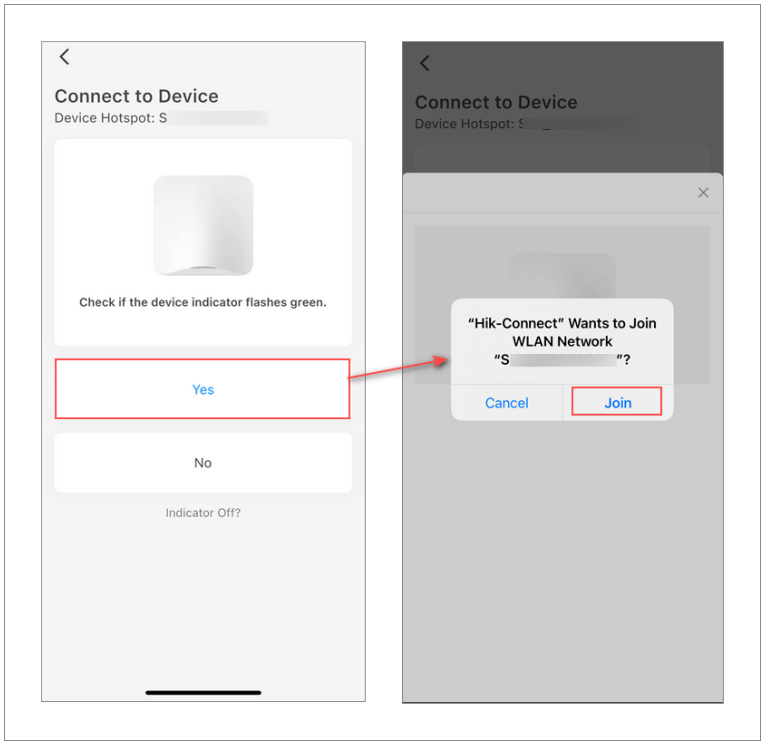
Steps



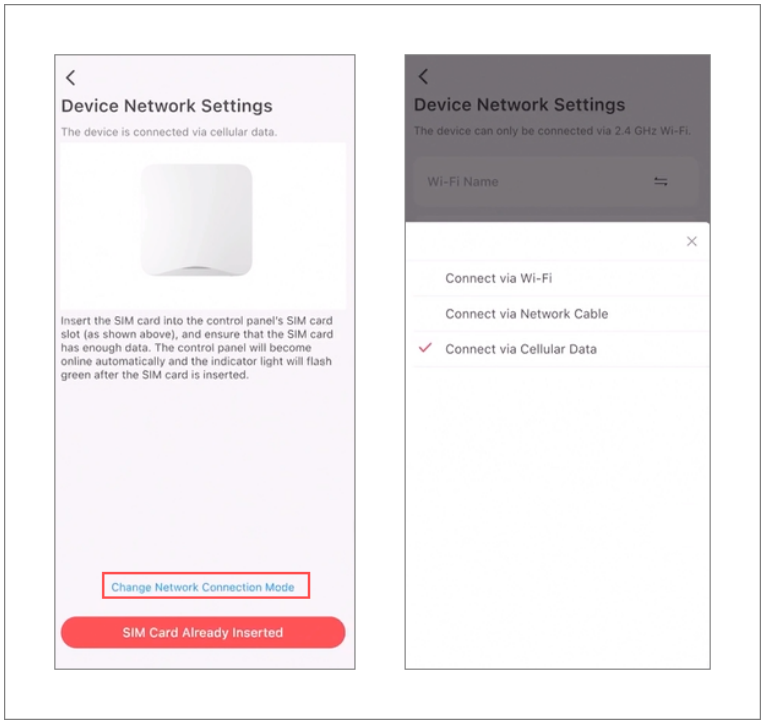
Add a security control panel.



Insert the SIM card, power on the device, and wait until the indicator light flashes green.

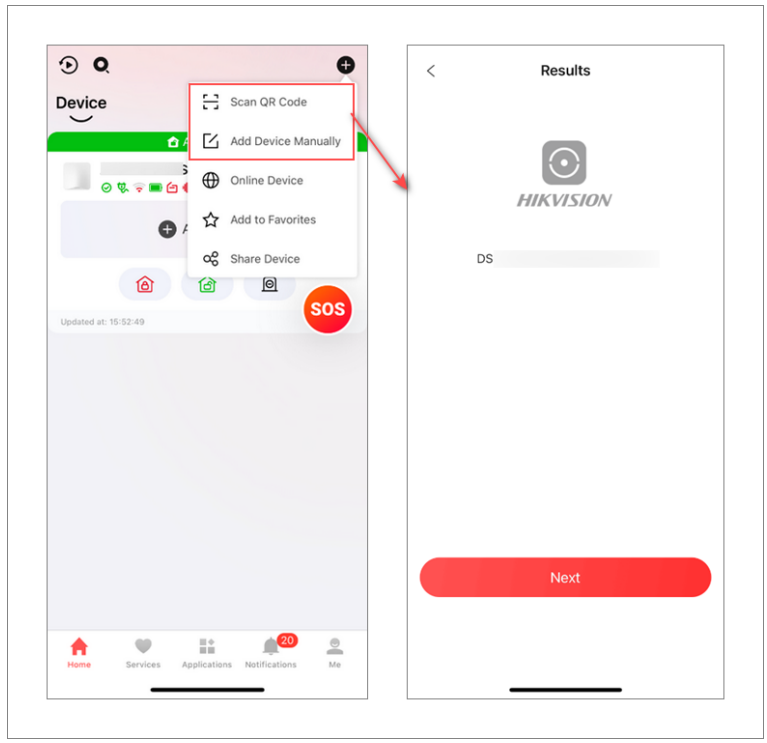


Join the device's hotspot.

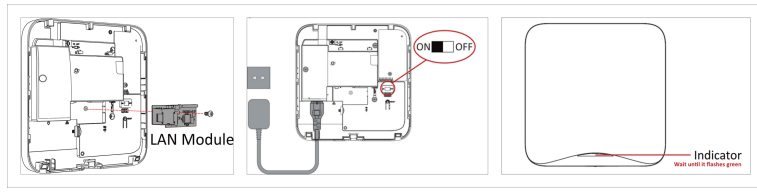


Change the network connection mode to Cellular Data and wait until the indicator turns solid white.

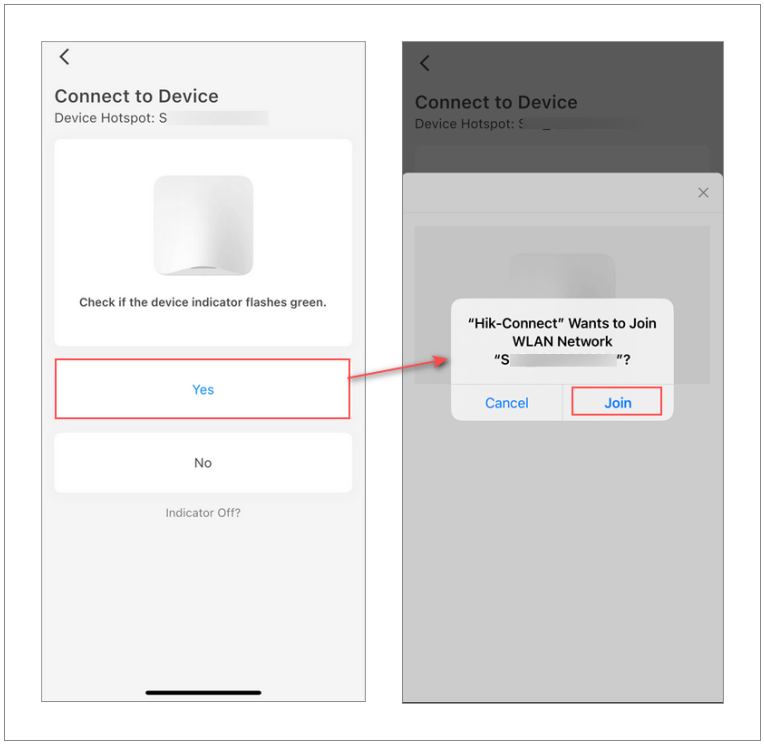
6.1.3 By Ethernet



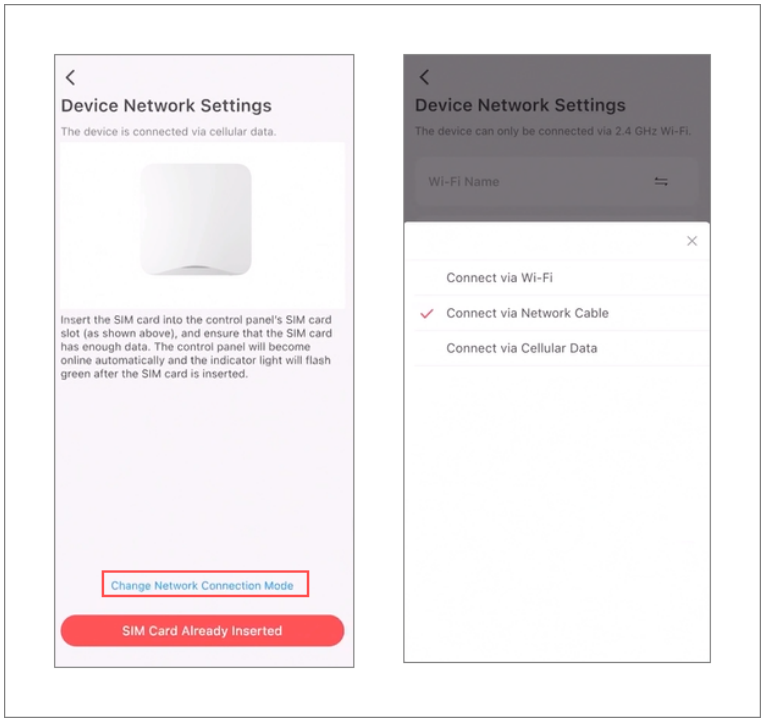
Add a security control panel.



Install the LAN module (sold separately), connect the device to the network, and wait until the indicator light flashes green.



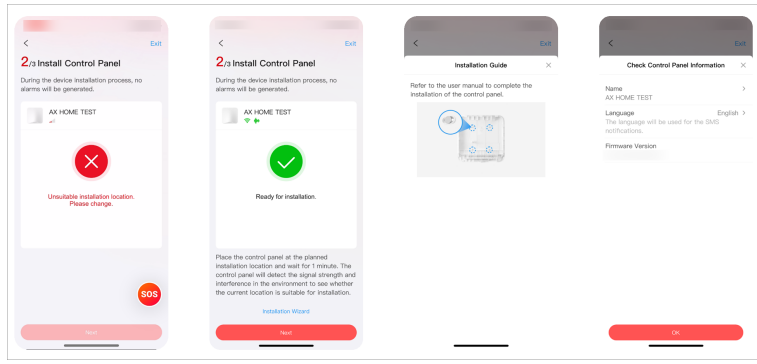
Join the device's hotspot.

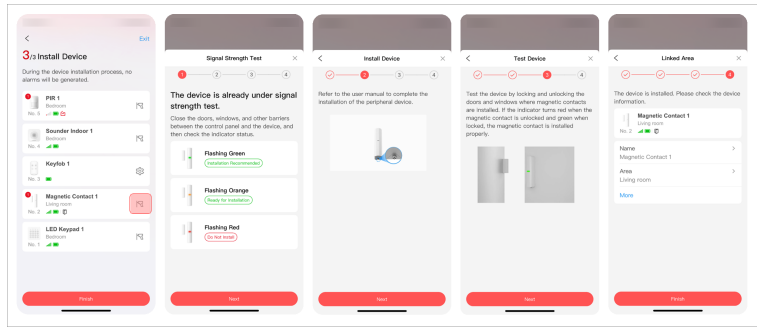


Change the network connection mode to Network Cable and wait until the indicator turns solid white.

6.1.4 Install Devices

After the panel is added, you can launch the installation wizard to install the panel, detectors, or peripherals.





6.2 How to Unbind Devices

Unbind Devices on Your Own Account

On the **Device** tab, tap a security control panel to enter this details page, tap ⚙ to enter the settings page, and then tap **Delete Device**.

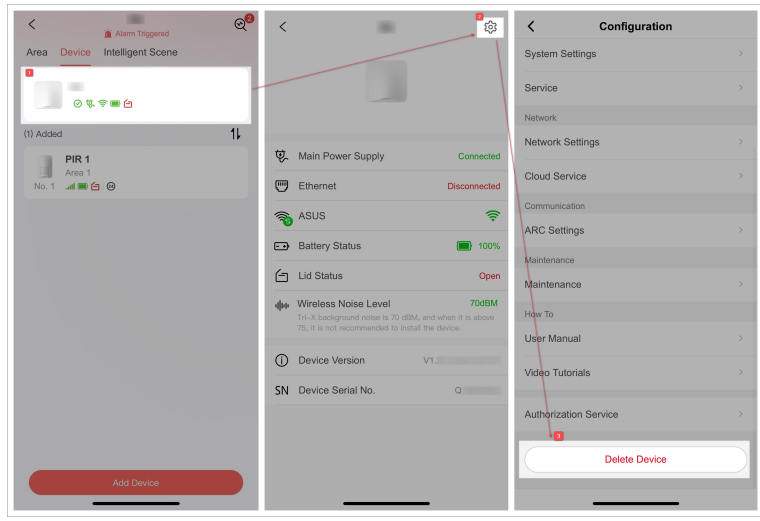


Figure 6-2 Unbind Devices on Your Own Account

Unbind Devices Added on Another Account

1. On the homepage, tap ⊕ to add a device.
2. For the device added by another account, tap **Unbind Device**.
3. Press the rest button for more than 10 seconds.

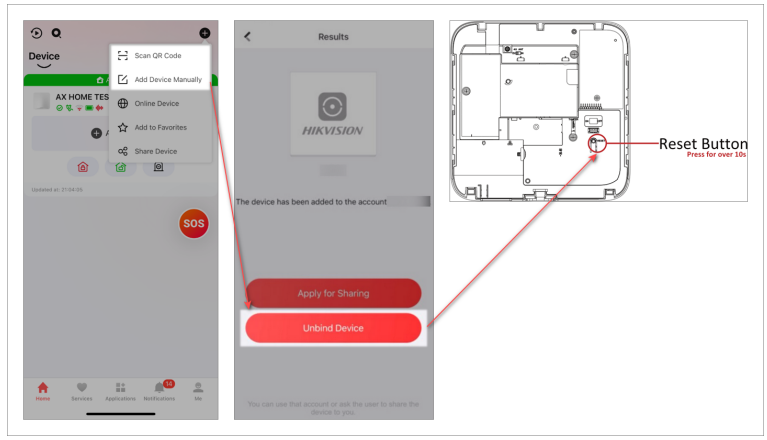


Figure 6-3 Unbind Devices added on Another Account

6.3 How to Configure Security Control Panels

The user interface for OTAP-enabled security control panels differs from that of ISAPI-enabled panels. This document primarily covers operations for OTAP-enabled control panels.

6.3.1 How to Add an Area and Link Devices to it?

1. Tap the Area tab, select + and enter the area name.

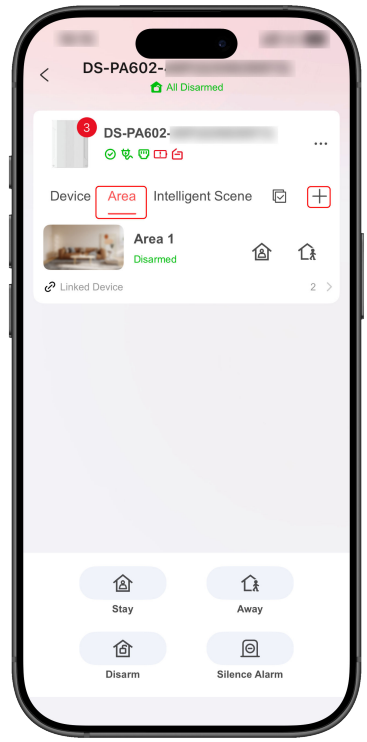


Figure 6-4 Add Area

2. Tap an area to enter the area settings page, tap **Link to More Devices**, select devices, and tap **OK**.

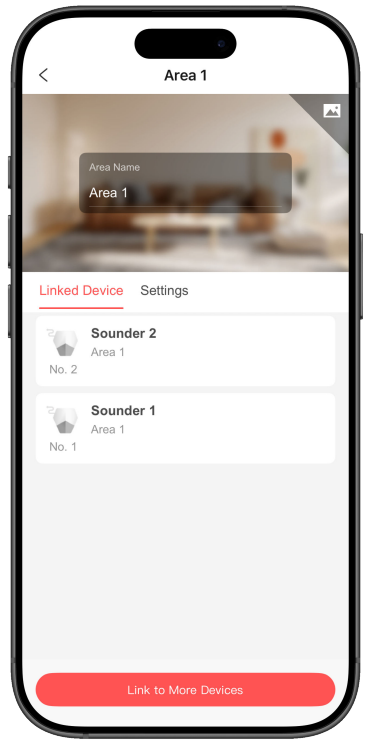


Figure 6-5 Link Devices to Area

Caution

You can link only one detector to an area. If you select a detector that is linked to another area, it will be unlinked with the area. A peripheral can be linked to multiple areas.

6.3.2 How to Batch Control Areas?

For AX PRO (V1.2.9 or V1.3.1 or later), AX HYBRID PRO, and AX HOME, tap under the **Area** tab and select multiple areas to arm/disarm areas.

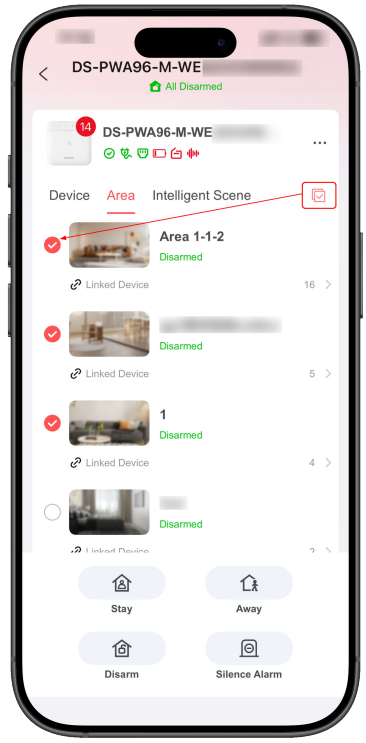


Figure 6-6 Batch Arm/Disarm Areas

6.3.3 How to Configure Delayed Disarm Alerts?

Tap an area to enter the area settings page, tap **Settings**, enable **Late to Disarm** and set the late time, the control panel will report an alarm if the area is not disarmed at the specified late time.

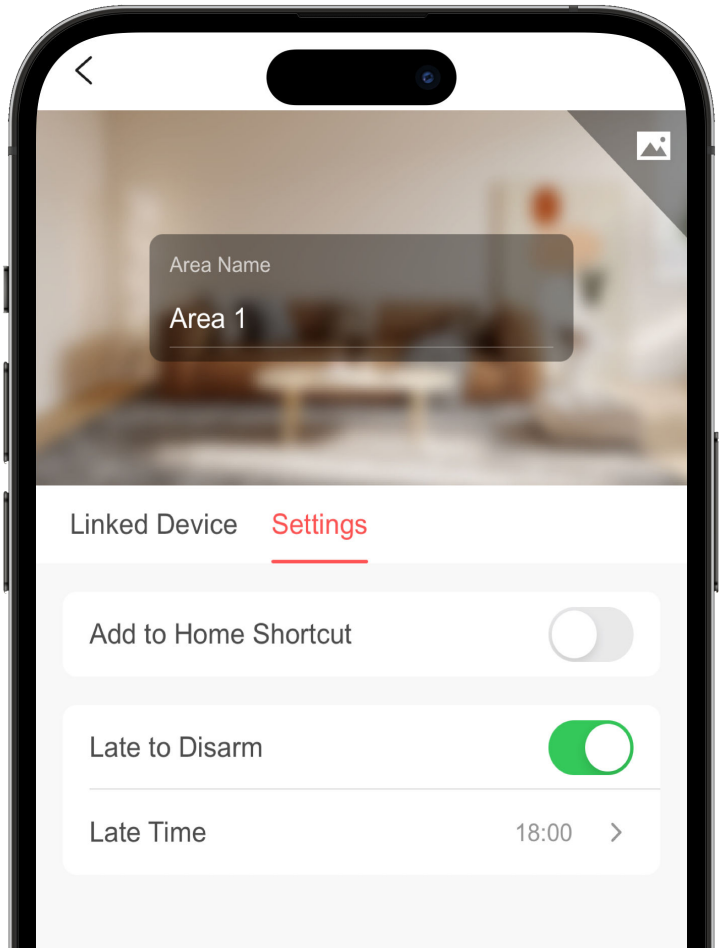


Figure 6-7 Late to Disarm Areas

6.3.4 How to Add Areas to Shortcuts on Homepage?

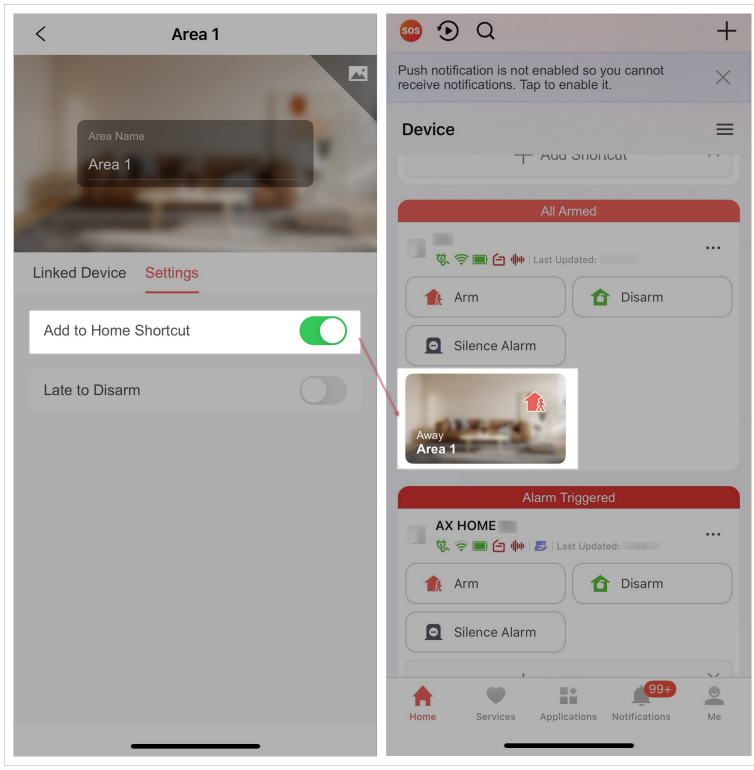


Figure 6-8 Add Area to Shortcut

6.3.5 How to Quickly Control Automation Devices?

For AX PRO (V1.3.0 or later) and AX HYBRID PRO (V2.0 or later), you can control automation devices under the **Control** module.

Note

The supported device models are as follows:

- DS-PM1-O1L-WE
- DS-PM1-O1L-WB
- DS-PM1-O1H-WE
- DS-PM1-O1H-WB
- DS-PSP1-WE
- DS-PSP1-WB
- DS-PM401R2H-WE
- DS-PM401R2H-WB
- DS-PM401R2H-WA

1. Go to the Controls tab, tap **Control** → ＋ **Add Manual Controls**.
2. Tap **Scene** → **Tap to Run** , and set the scene name.
3. Add an action.
   a. Tap **Add Action**.
   b. Select control devices as needed.
   c. Set the action and click **OK**.
4. Go back to the **Control** tab; tap the **power icon** on the device card to switch it on or off.

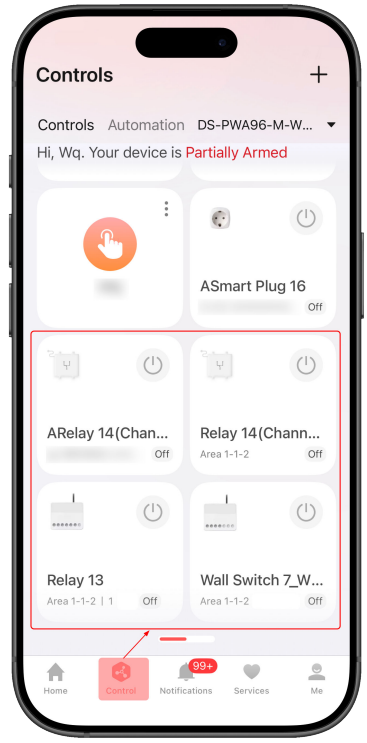
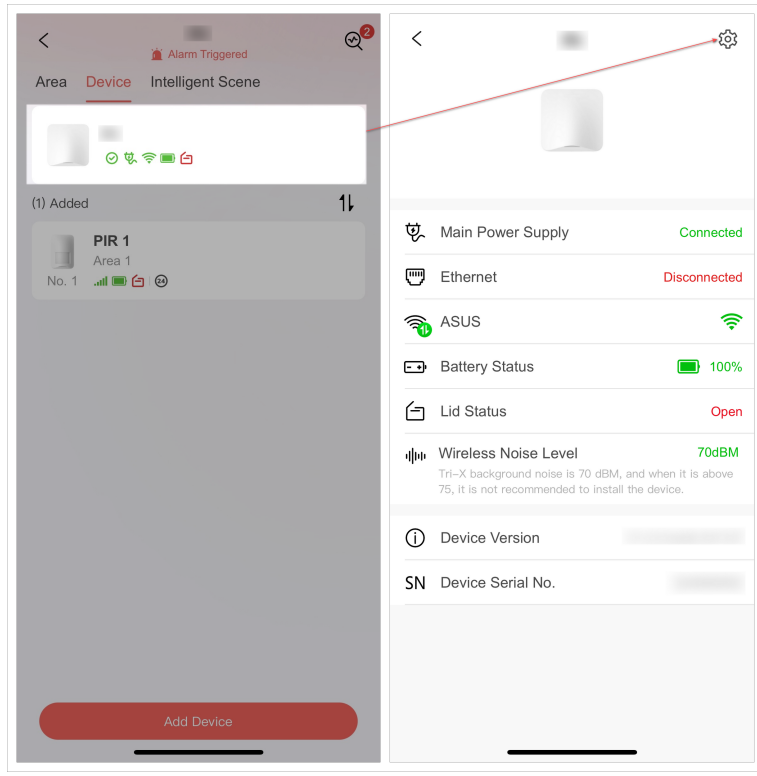


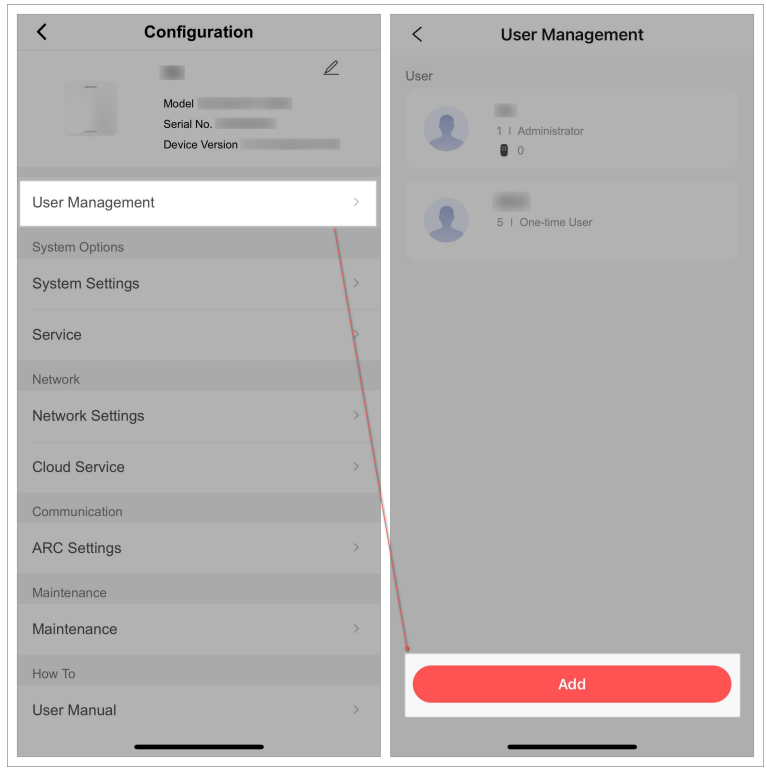
Figure 6-9 Relay Control

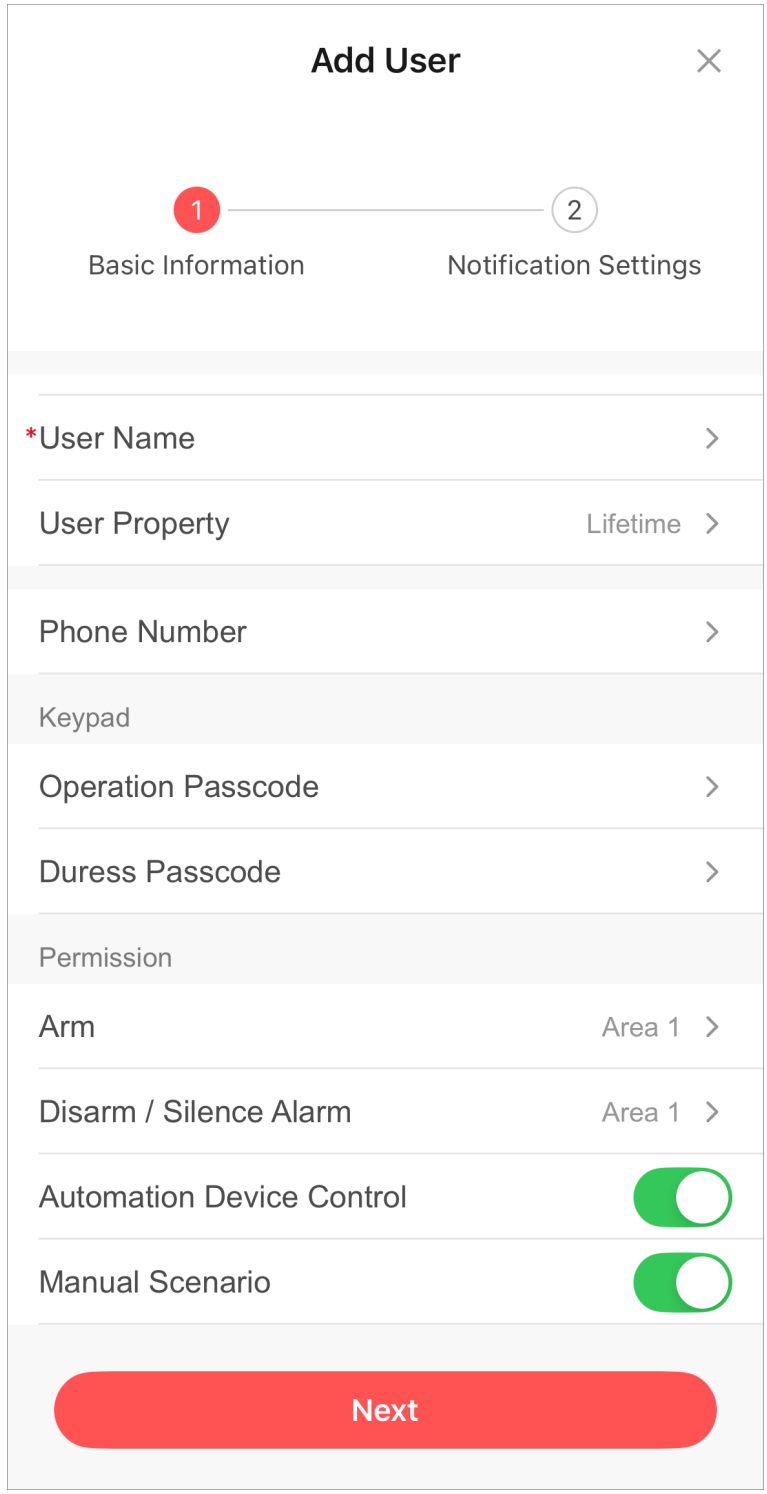
6.3.6 How to Add Users?

Add Local Users

The admin can share the devices to local users who can use a keypad to arm/disarm the selected areas and receive the selected notifications.

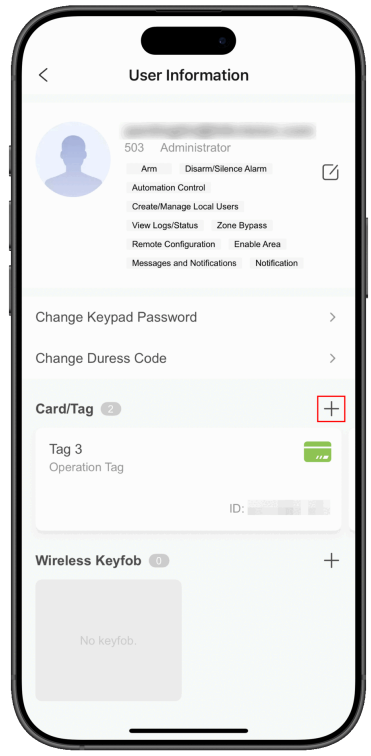

Alarm Triggered
Area
Device
Intelligent Scene
(1) Added
PIR 1
Area 1
No. 1
Add Device
Main Power Supply
Connected
Ethernet
Disconnected
ASUS
Battery Status
100%
Lid Status
Open
Wireless Noise Level
70dBM
Tri-X background noise is 70 dBM, and when it is above 75, it is not recommended to install the device.
Device Version
SN
Device Serial No.


Configuration
Model
Serial No.
Device Version
User Management
System Options
System Settings
Service
Network
Network Settings
Cloud Service
Communication
ARC Settings
Maintenance
Maintenance
How To
User Manual
User Management
User
1 I Administrator
0
5 I One-time User
Add



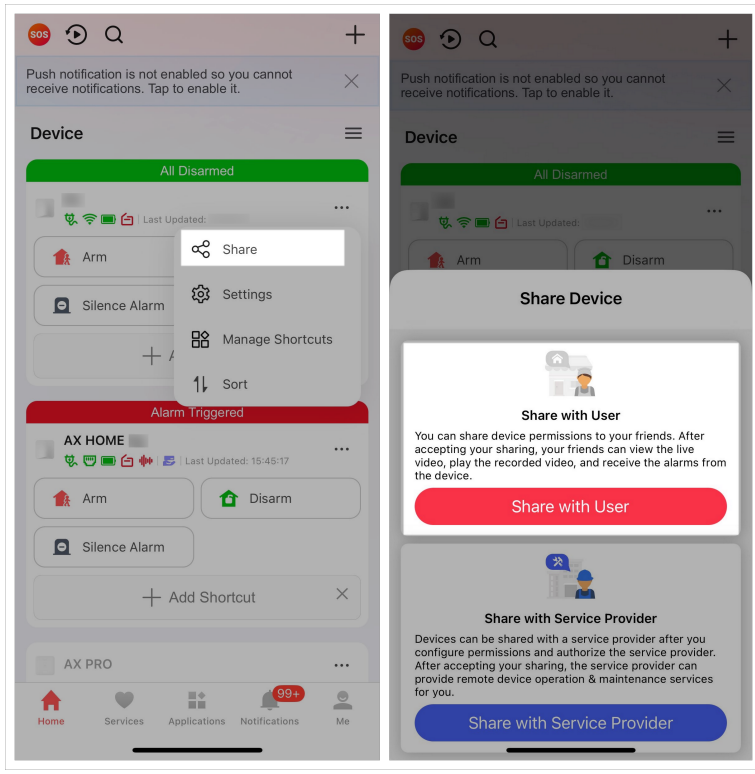
After adding a local user, you can add a tag for the user.

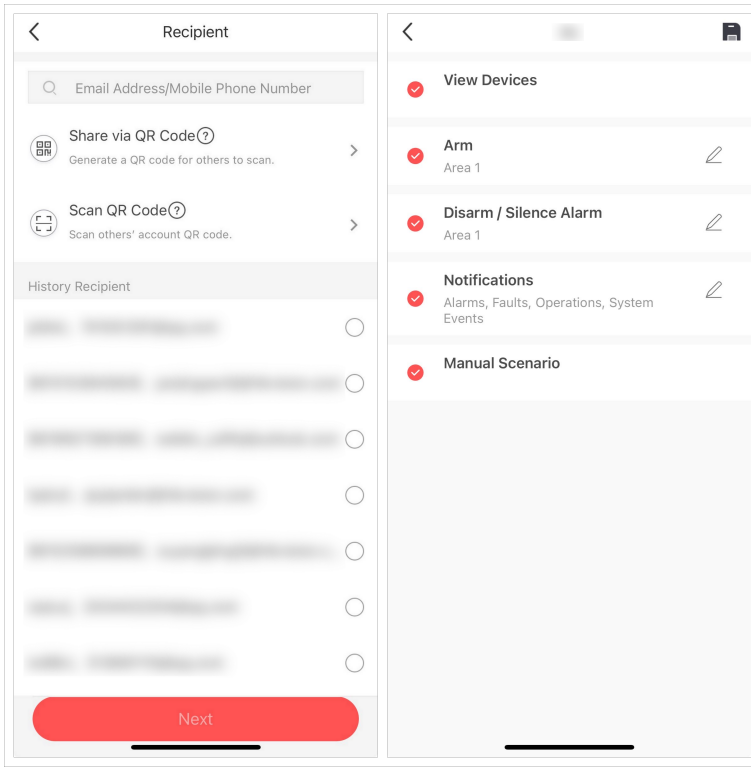
Note

Panel Version	Adding Methods
AX HYBRID PRO (V1.1.2)	Select a wireless tag reader or keypad to add tags.  **Figure 6-10 Add Tag via Tag Reading Device** **Note** The supported tag readers are as follows: DS-PT1-WE(O-STD), DS-PT1-WB(O-STD), DS-PT1-WE(B)(O-STD), and DS-PT1-WB(B)(O-STD).
AX HYBRID PRO (V2.0 or later)	Select a keypad to add tags.
AX PRO	Put a tag on a tag reading device such as a tag reader or keypad within 30 seconds to add the tag. **Note** For the following models, you can put a tag on the control panel within 30 seconds to add the tag: DS-PWA96-M-WB and DS-PWA96-M-WE.

Add Cloud Users

- The admin can share the devices to cloud users who can use this App to view the devices, arm/ disarm the selected areas and receive the selected notifications.



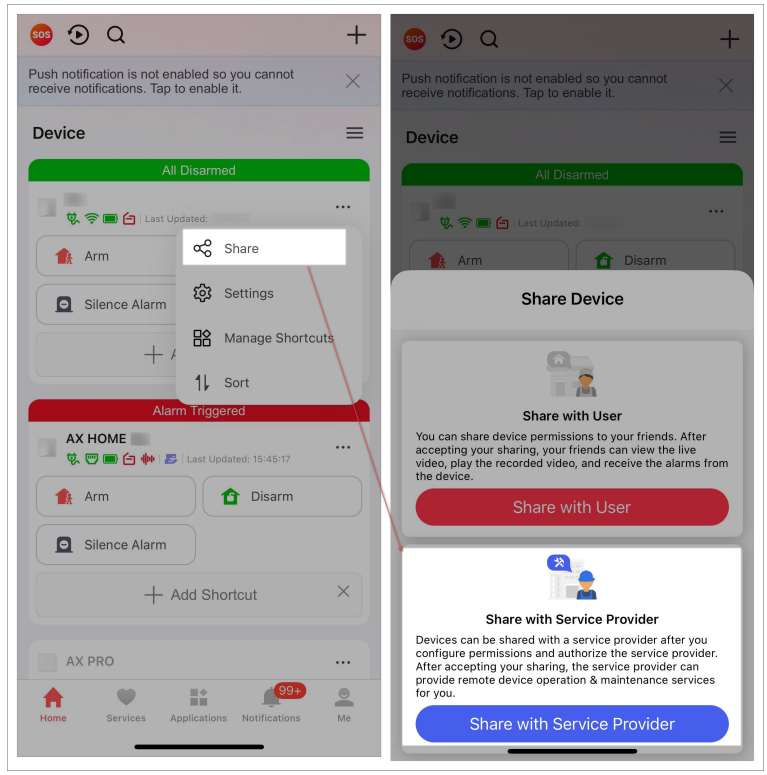


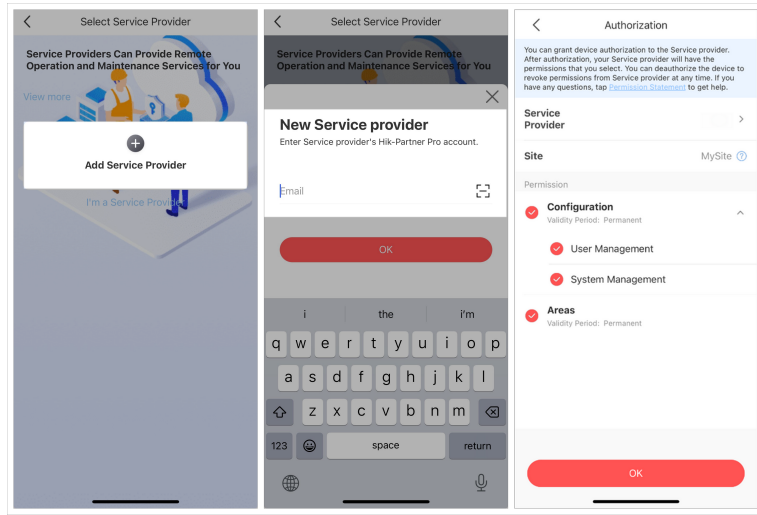
Note

For AX PRO (V1.3.0 or later), AX HYBRID PRO (V2.0 or later), and AX HOME, admin or users can control the Capture Pictures by PIRCAM permission. See the following table for details.

User Type	Permission
Cloud admin	Can control the Capture Pictures by PIRCAM permission.
Cloud user who has authorized the installer's request for picture capture.	Can control the Capture Pictures by PIRCAM permission after devices are transferred by sharing.

- The admin can share/authorize the devices to a service provider who can use the Hik-Partner Pro App to view the devices, arm/disarm the selected areas and receive the selected notification.





After a service provider is authorized, an installer account will be created and displayed in the User Management page.

6.3.7 How to Cancel Authorization of Service Provider?

To cancel authorization, enter the Services page and then tap a service provider, and select **Cancel Authorization**.

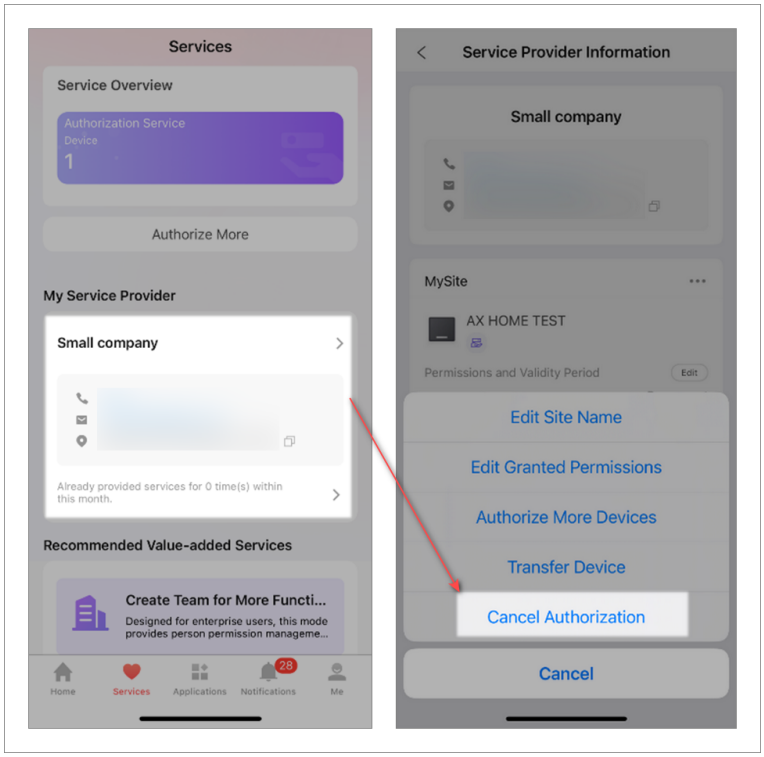
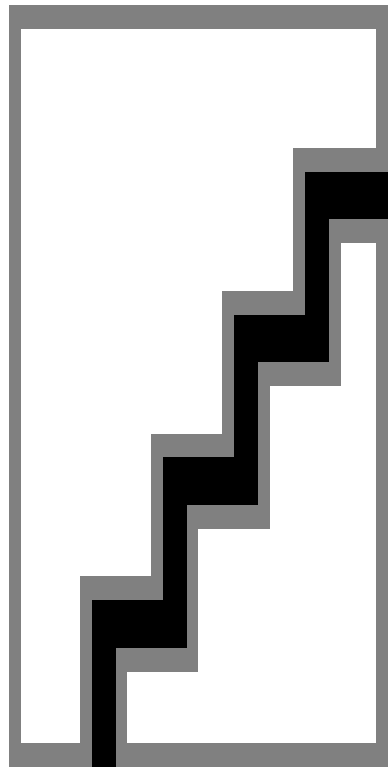


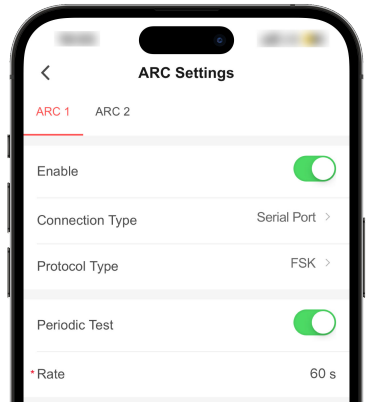
Figure 6-11 Cancel Authorization

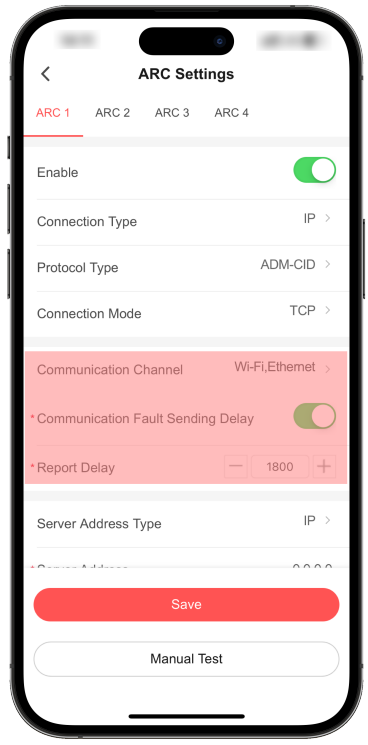
6.3.8 How to Configure an ARC?

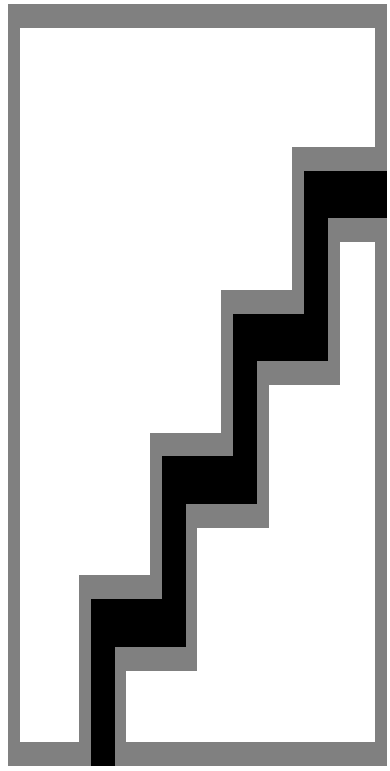
1. Select the **Device** tab, tap a panel, and tap ⚙ to enter the settings page.
2. Select **ARC Settings** and enable an ARC.
3. Set the parameters. The following table will introduce major parameters.

Parameter	Description	Note
Protocol Type	- If you set the type to **OTAP or ISUP**, IP Receiver Pro will convert events triggered by devices into supported protocols and transmits events to an ARC. - If you set the type to **SIA-DCS, *SIA-DCS, ADM-CID, or *ADM-CID**, devices will directly transmit alarms to an ARC. **Note** For AX HYBRID PRO V1.1.2 or later, support selecting a device identity type when reporting alarms via	/

Parameter	Description	Note
	protocols like ADM-CID/SIA-DCS/*ADM-CID/*SIA-DCS to an ARC.  **Figure 6-12 Select Device Identity When Reporting Alarms to ARC**	
Server Address	- If you set the type to **OTAP or ISUP**, the server address is the IP address of IP Receiver Pro. - If you set the type to **SIA-DCS, *SIA-DCS, ADM-CID, or *ADM-CID**, the server address is the ARC IP address.	/
Port	- If you set the type to **OTAP or ISUP**, set the port to the ISUP/OTAP port for registering devices on IP Receiver Pro. - If you set the type to **SIA-DCS, *SIA-DCS, ADM-CID, or *ADM-CID**, enter the ARC communication port.	/
Account Code	Account ID for identifying a device when alarms are transmitted to an ARC.	/
Connection Type & Periodic Test	A module such as an FSK module can receive alarms from a control panel on its serial port. If you connect a	Periodic test is only for AX

Parameter	Description	Note
	module with a control panel with a serial cable and set the connection type to **Serial Port**, you can the periodic test of the connection between the FSK, RDC, or IDS module and the control panel to ensure that the control panel and these modules are communicating normally and to identify any abnormalities immediately.  **Figure 6-13 Periodic Test**	HYBRID PRO V2.1.0 or later and AX PRO V1.3.1 or later
Communication Fault Sending Delay	After you set the connection mode to **TCP** and enable communication channels, you can set the delay time for reporting Wi-Fi/Ethernet/Cellular communication failures to the ARC. If the failure is recovered before the delay ends, no alarm will be reported. If the failure persists after the delay, the control panel will report a Communication Fault alarm to the ARC.	Only for AX HYBRID PRO V2.1.0 or later and AX PRO V1.3.1 or later

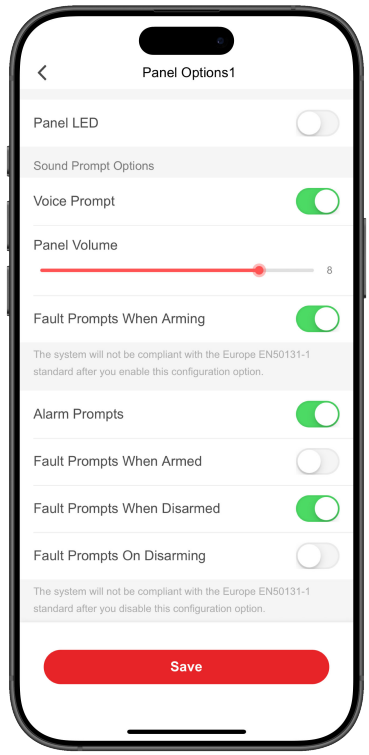
Parameter	Description	Note
	 **Figure 6-14 Communication Fault Sending Delay**	
Device Identity	Select a device identity type when reporting alarms via protocols like ADM-CID/SIA-DCS/*ADM-CID/*SIA-DCS to an ARC.	Only for AX HYBRID PRO V1.1.2 or later

Parameter	Description	Note
	 **Figure 6-15 Select Device Identity When Reporting Alarms to ARC**	

6.3.9 How to Configure Control Panel Services?

1. Select the **Device** tab, tap a panel, and tap ⚙ to enter the settings page.
2. Select **System → Control Panel Options** .
3. Set the parameters. The following table will introduce major parameters.

Parameter	Description
Re-Arm on Restore	Before enabling Arm LED, Fault LED, and Cloud LED, you should enable Panel LED.
Motion Detector Restore Report	When the control panel is connected to the Hik-Connect service, the LED indicator will flash.
Fault Checklist When Arming	You will be notified of detected faults when you arm an area. You can go to **System Settings → Control Panel Option** to enable **Fault Prompts When Arming**.

Parameter	Description
	 **Figure 6-16 Control Panel Options**
Panel Fault Check	You will be notified of detected faults when an area is armed.
Panel Lockup Button	All operations will be unavailable if the control panel is locked.

6.4 How to Add Controls & Automations

Manual controls and automations allow you to control multiple devices with a single command or through automation. You should have related permissions before adding controls and automations.

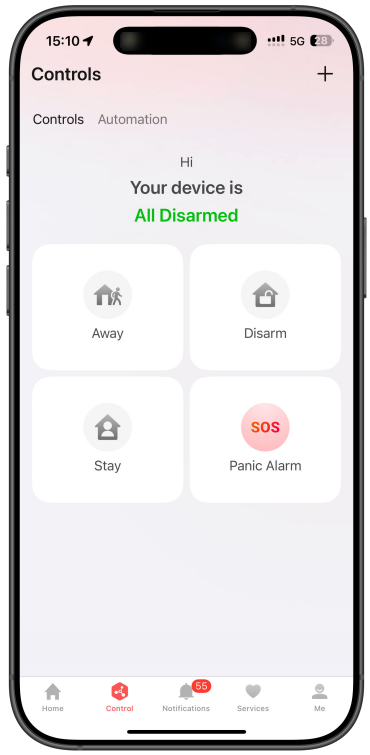
Table 6-1 Intelligent Scene Overview

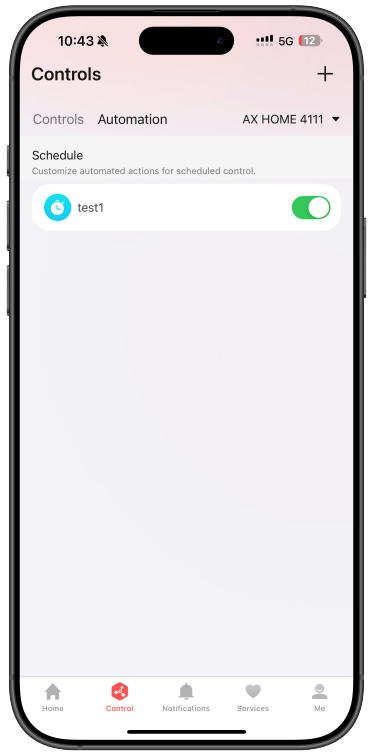
Scene Type	Supported Device	Supported Zone	Typical Scenario	Trigger Source	Action
Group	AX HYBRID PRO V2.0 or later	All	Batch arm/disarm areas.	NA	NA
Tap to Run	AX PRO V1.3.1 or later, AX HYBRID PRO V2.0 or later, and AX HOME V1.2.0 or later	NA	Control multiple automation devices like smart plugs and relays at once, such as turning on the AC and lights in the living room with one tap when you get home.	Manually trigger	Control automation devices
Automation	AX HYBRID PRO V2.0 or later	Depends	Trigger automation devices or sounders when control panel/ detector exception occurred like tampering, overheat, or heartbeat timeout.	• Device alarm triggered • Areas armed/ disarmed	Control automation devices or link sounders
Schedule	AX HYBRID PRO V2.0 or later	All	Arm/disarm areas or control lights/AC via automation devices like relays at scheduled times.	Set trigger time and holiday exception	• Control automation devices • Arm/disarm areas
Arm/Disarm with One Button	AX HYBRID PRO V2.0 or later	Keyswitch Zone	Arm area by emergency button when intrusion is detected.	Zone triggered	Arm/Disarm area
Alarm Video Verification	AX HYBRID PRO V2.0 or later	Non-Keyswitch Zones / Network Cameras / PIR-	On intrusion detection, network cameras or PIR-Camera detectors will capture a photo / video for alarm verification.	Alarm triggered	

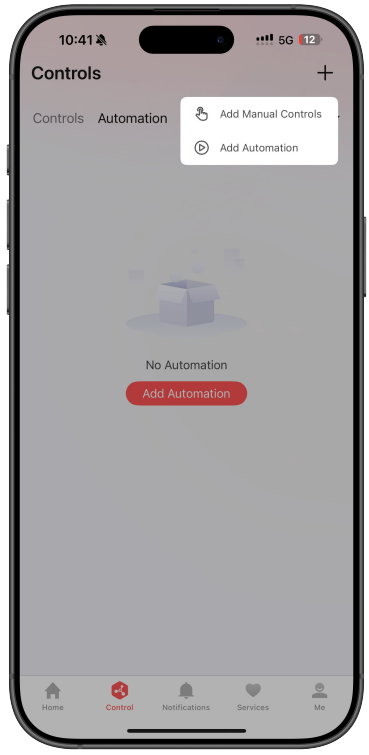
Scene Type	Supported Device	Supported Zone	Typical Scenario	Trigger Source	Action
		Camera Detector			
Chime	AX HYBRID PRO V2.0 or later	Instant Zone / Delay Zone	When a customer enters the store, the detector at the entrance detects movement. Instantly, the keypad emits a doorbell chime. Staff members hear the alert and can promptly greet guests.	Zone triggered	Device like keypad or sounder emits a doorbell
Alarm Cross Confirm	AX HYBRID PRO V2.0 or later	Non-Keyswitch Zones	When smoke detectors in both your dining room and living room trigger alarms within a specified period, the alarm will be confirmed.	Alarms triggered by multiple zones	Confirm alarm
Timeout Alert	AX HYBRID PRO V2.0 or later	Instant Zone / 24-h Zone	Nighttime flying animal impact detected: Treat as false alarm if isolated. Trigger alert if impacts persist within a specified period.	Constant alarm	Confirm alarm

6.4.1 Entry

Tab	Feature	Supported Devices
Control	• Arm/Disarm/Silence Alarm • Group: Batch arm/disarm areas. • Tap to Run: Control multiple automation devices like smart plugs and relays at once, such as turning on the AC and lights in the living room with one tap when you get home.	Group and Tap to Run are available only for AX PRO V1.3.0 or later & AX HYBRID PRO V2.0 or later.
Automation	• Automation: Trigger outputs or sounders when control panel/detector exception occurred like tampering, overheat, or heartbeat timeout. • Schedule: Arm/disarm areas or control lights/AC via outputs at scheduled times.	AX HOME & AX HYBRID PRO V2.0 or later **Note** Energy-efficient panels only support Schedule.




10:43
5G
Controls
Controls
Automation
AX HOME 4111
Schedule
Customize automated actions for scheduled control.
test1
Home
Control
Notifications
Services
Me


10:41
5G
Controls
Controls
Automation
Add Manual Controls
Add Automation
No Automation
Add Automation
Home
Control
Notifications
Services
Me

6.4.2 Group

After adding multiple areas, you can add a Group scene to the homepage for batch arming/disarming areas.

1. Add a group.

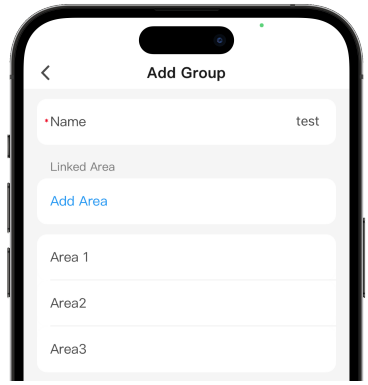


Figure 6-17 Add Group Scene

- Control Tab
  Tap **Control** → ＋ → **Add Manual Controls** → **Group** .
- Intelligent Scene Tab
  Tab a device card, and tap **Intelligent Scene** → **Add Scene** → **Group** .

2. Set the group name and add areas.
3. Control the group.
   - Control Tab
     Tab the group card and select the action to perform.

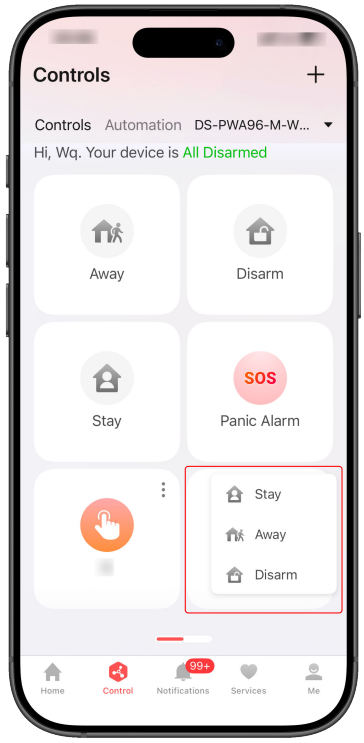


Figure 6-18 Group Control

- Intelligent Scene Tab
  a. On the **Intelligent Scene** page, select a Group scene and swipe it left, and then tap .

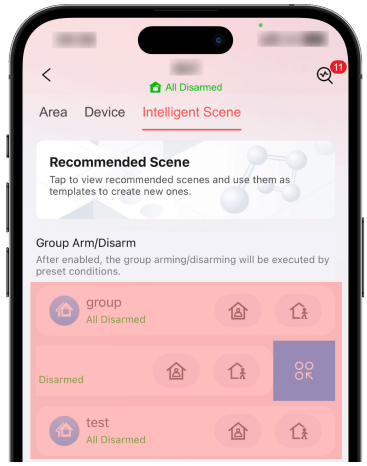


Figure 6-19 Add Group Scene to Homepage

  b. Tap the shortcut to batch arm/disarm areas on the homepage.

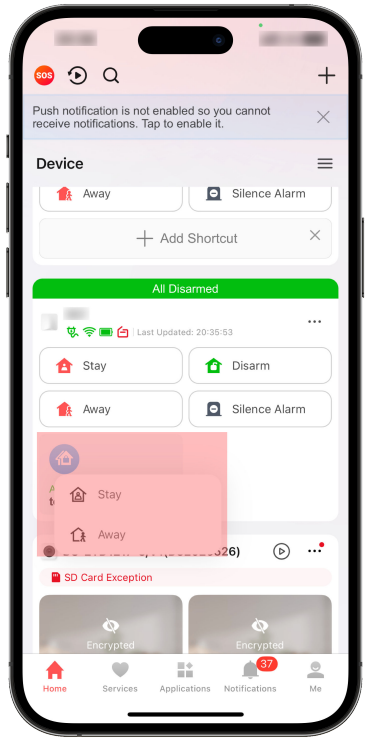


Figure 6-20 Batch Control Area Group

6.4.3 Tap to Run

Tap to Run lets you trigger a custom sequence of actions with a single tap. Ideal for quick control, emergency alerts, or arming your system on the go.

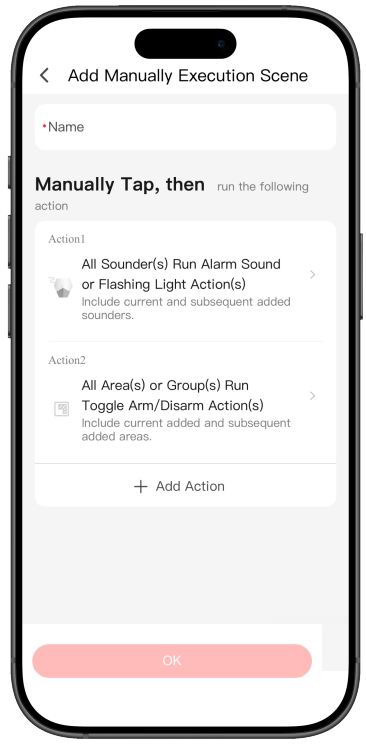


Figure 6-21 Tap to Run

1. Go to the Controls tab, tap **Control** → ＋ **Add Manual Controls**.
2. Tap **Scene** → **Tap to Run** , and set the scene name.
3. Add actions as needed.

Note

Add up to 8 actions.

a. Tap **Add Action**.
b. Select devices/areas/groups and set actions as needed.

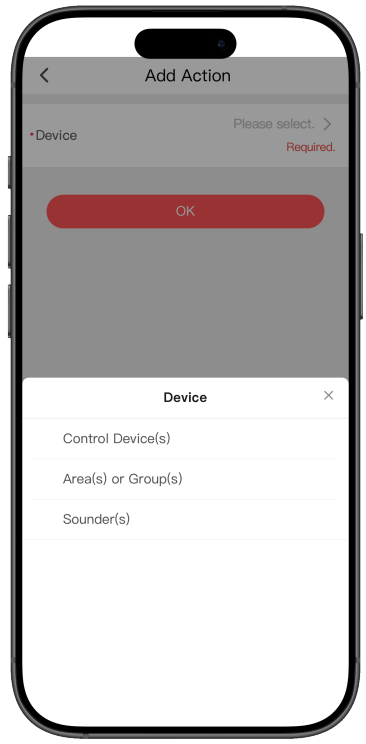


Figure 6-22 Select Objects

- Control Devices (Outputs)
  Actions:
  - Switch On/Off
  - Reverse Switch
  - Pulse (1-600s)
- Sounders
  Action: Trigger sound (low/medium/loud) and/or strobe for 10 seconds to 15 minutes.

  Note

  Setting the sound levels requires compatible bus or wireless sounders.
- Areas/Groups
  Actions:
  - Stay/Away Arm
  - Disarm
  - Toggle Arm/Disarm

4. Click **OK**. Go back to the **Control** tab and run the action.

6.4.4 Automation

You can create a device linkage scene where your device automatically performs an action when a condition (trigger) is satisfied.

1. Add automations as needed.
   - Control Tab
     Tap **Control** → ＋ → **Add Automation** → **Automation** .
   - Intelligent Scene Tab
     Tab a device card, and tap **Intelligent Scene** → **Add Scene** → **Automation** .
2. Set the scene name.
3. Select a condition and configure its parameters.

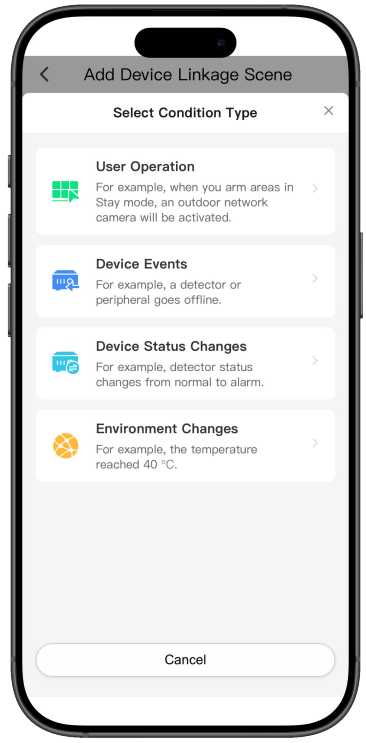


Figure 6-23 Four Conditions Types on App

- User Operations

Table 6-2 User Operations

Object	Description
Any Area/Group	Operations: - Away Arm - Stay Arm

Object	Description
	- Disarm - Arming Failed

- Device Events

Table 6-3 Device Events

Object	Events
Any Devices	- Detector Alarm / Lid Opened - Peripheral Lid Opened - Panic Alarm / Medical Alarm / Fire Alarm - Mains Power Lost - Battery Disconnected / Battery Low - Communication Faults - Detector/Peripheral Heartbeat Timeout / Offline - Network Camera Offline - Enter Walk Test - Exit Walk Test

- Device Status Changes

Table 6-4 Device Status Changes

Object	Switched Status
- Area/Group - Detector	- Area/Group - Away Arm - Stay Arm - Disarm - Ready to Arm - Alarm - Detector - Alarm - Trigger/Trigger Restored - Open/Close - Panic Alarm / 24H Alarm / Masking Alarm / Follow Alarm / Gas Alarm

Note

You can set the delay before action. If all Device Status Changes conditions restore during the delay, the pending action will be canceled.

- Environment Changes

Table 6-5 Device Status Changes

Object	Environmental Conditions
- Area/Group - Detector	- Temperature - Humidity

Note

You can set the delay before action. If all Environment Changes conditions restore during the delay, the pending action will be canceled.

4. Set the action.
   - Control Devices (Outputs)
     - Switch on/off
     - Switch on if condition/off after restored
     - Switch off if condition/on after restored
     - Reverse Switch
     - Pulse

     Note

     The switching action supports only the following conditions: Device Status Changes and Environment Changes.
   - Sounder
     Sound/Strobe

     Note

     The action supports only the following conditions: Device Status Changes (Ready To Arm, Arm, Disarm) and Environment Changes.
   - Area/Group
     - Away Arm/Stay Arm
     - Disarm
     - Toggle Arm/Disarm

     Note

     The action supports only the following conditions: Device Status Changes (Ready To Arm, Open, Close) and Environment Changes.
5. Tap **OK**.

6.4.5 Schedule

You can arm/disarm areas or control lights/AC via automation devices like relays at scheduled times.

You can set the timer, and an automation device will automatically perform actions at the scheduled time, such as power off, turn on, pulse activation, or toggle the switch status. For example, configure the smart plug with an automation:

- Power off at 9:00 (work departure)
- Power on at 19:00 (return home)

1. Add schedule scenes as needed.
   - Control Tab
     Tap **Control** → ＋ → **Add Automation** → **Schedule** .
   - Intelligent Scene Tab
     Tab a device card, and tap **Intelligent Scene** → **Add Scene** .
2. Set the scene name and set scheduled time.
3. Add a device and set the action.
   - Control Devices

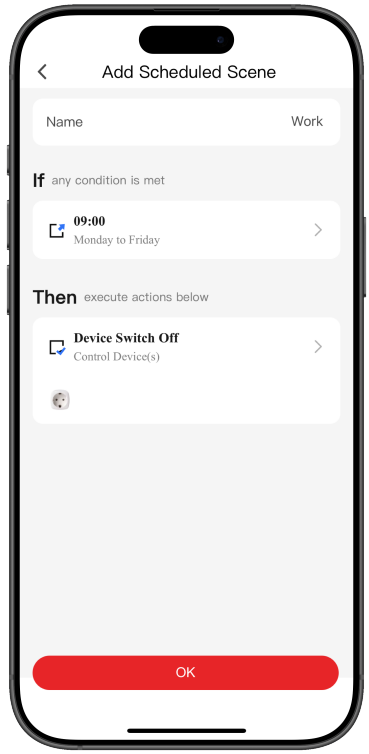


Figure 6-24 Link Automation Devices

   - Areas/Groups
     When the action is set to **Auto Arm**, you can configure the **delay count** and **delay time** before the action triggers.

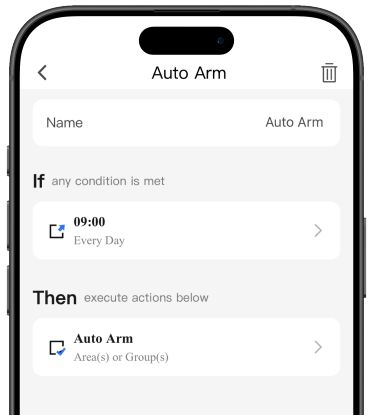


Figure 6-25 Auto Arm/Disarm

4. Enable the scene.

6.4.6 Arm/Disarm with One Button

Arm/disarm area when intrusion is detected in a keyswitch zone.

1. Tap **Control** → + → **Add Automation** → **Recommended Scene** → **Arm/Disarm with One Button** .
2. Add a condition by adding a **keyswitch** zone and setting the Condition to **Switcher**.

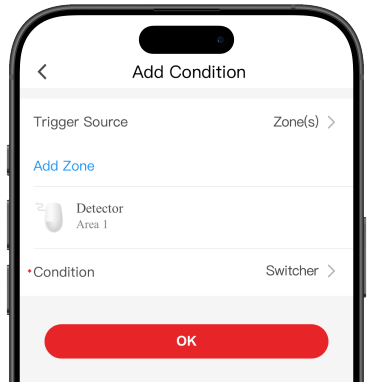


Figure 6-26 Add Condition

3. Select an area or area group to arm or disarm.

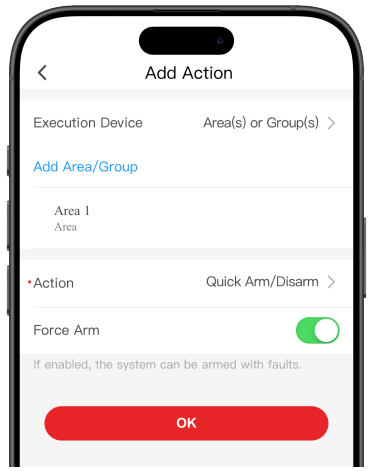


Figure 6-27 Add Action

4. Enable the scene.

6.4.7 Alarm Video Verification

You can create a device linkage scene where you can link an added network camera with a zone for alarm video verification. For example, when someone breaks into your house, the alarm is triggered by a PIR-camera detector, and you can verify the alarm via the captured picture.

Take the following steps to add a device linkage scene:

1. Tap **Control** → + → **Add Automation** → **Alarm Video Verification** .
2. Add a condition by adding a zone and setting the Condition to **Alarm**.

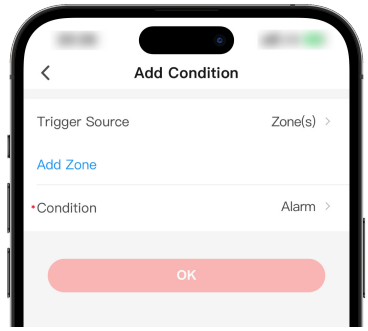


Figure 6-28 Add Condition

3. Set the video/picture verification action by adding a network camera or PIR-Camera detector and setting the Action to **Video Verification**.

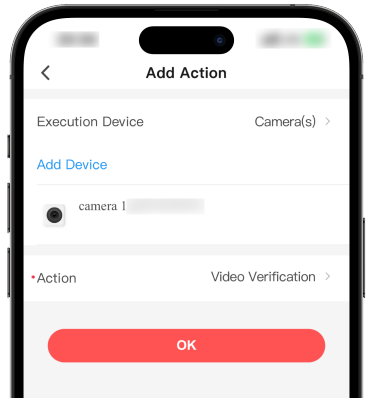


Figure 6-29 Add Action

4. Enable the scene. If the automation runs, you can receive a notification for alarm verification.

6.4.8 Chime

After enabling the Chime function for supported keypads, wireless/bus sounders, tag readers, or detectors, you can create a Chime scene where you can hear doorbell when a zone is triggered. For example, when a customer enters the store, the detector at the entrance detects movement. Instantly, the keypad emits a doorbell chime. Staff members hear the alert and can promptly greet guests.

1. Tap **Control** → + → **Add Automation** → **Recommended Scene** → **Chime** .
2. Set the scene name, select the trigger source, and set the condition to **Triggered**.
3. Add a device and set the action.

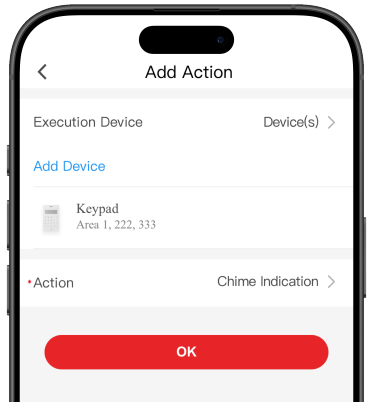


Figure 6-30 Add Chime Device

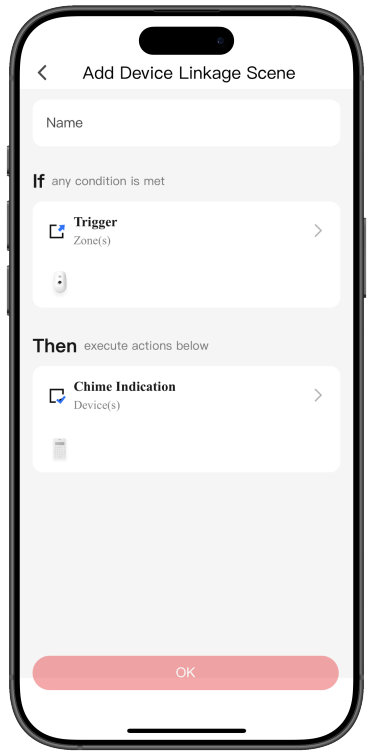


Figure 6-31 Configure Chime Scene

4. Enable the scene.

6.4.9 Alarm Cross Confirm

An alarm event is only triggered if multiple detectors report abnormal conditions within a defined time window. For example, when smoke detectors in both your dining room and living room trigger alarms within a specified period, the alarm will be confirmed.

1. Tap **Control** → ＋ → **Add Automation** → **Recommended Scene** → **Alarm Cross Confirm** .
2. Set the scene name, add two conditions, and set the trigger time window. Confirm alarm if Condition 2 triggers within a specified period of Condition 1.

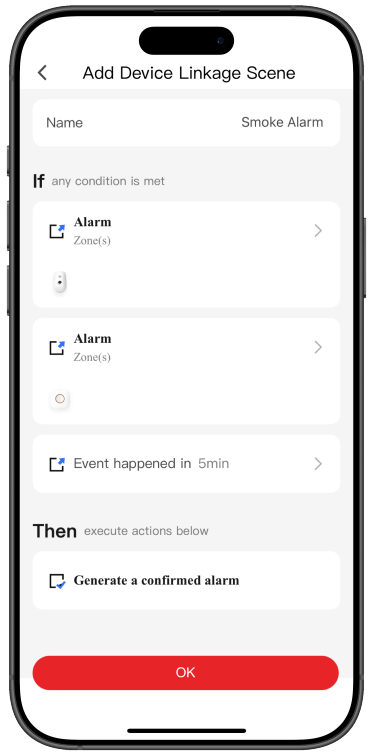


Figure 6-32 Add Condition

3. Enable the scene.

6.4.10 Timeout Alert

Alarms trigger only after multiple verified detections within a set time window. For example, a single nighttime flying animal impact is ignored as a false alarm, but persistent impacts within a defined period activate an alarm.

1. Tap **Control** → + → **Add Automation** → **Recommended Scene** → **Timeout Alert** .
2. Set the scene name, add a condition, and set the trigger time window. Confirm alarm if the condition constantly triggers within a specified period.

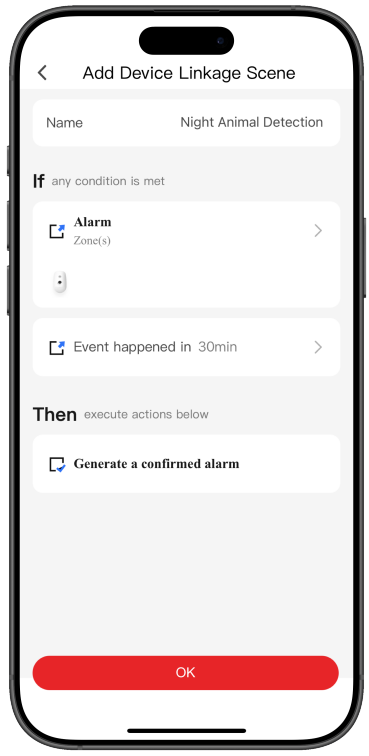


Figure 6-33 Add Condition

3. Enable the scene.

6.5 How to Add Peripherals

This document will introduce how to add the supported peripherals for AX HOME include keyfobs, keypads, indoor sounders, and PIR detectors. For AX PRO (V1.3.0 or later) and AX HYBRID PRO (V2.0 or later), follow the enrollment guidance to add peripherals and detectors.

6.5.1 Add Bus Devices

After connecting bus devices to a security control panel via a shared communication bus, you can tap **Add Device → BUS Device** to scan and add bus devices.

Scanning devices may fail under the following conditions:

- The bus PIR camera is uploading a picture.
- The control panel is detecting the baud rate of PIR cameras.
- The control panel is detecting the bus topology.

Note

For AX HYBRID PRO V2.1.0 or later, you can select which bus to scan and add detectors and peripherals. In loop mode, Bus 1 is automatically selected as the default for adding devices.

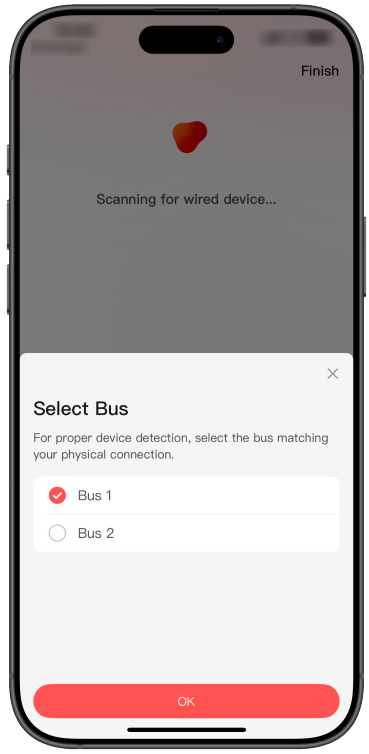
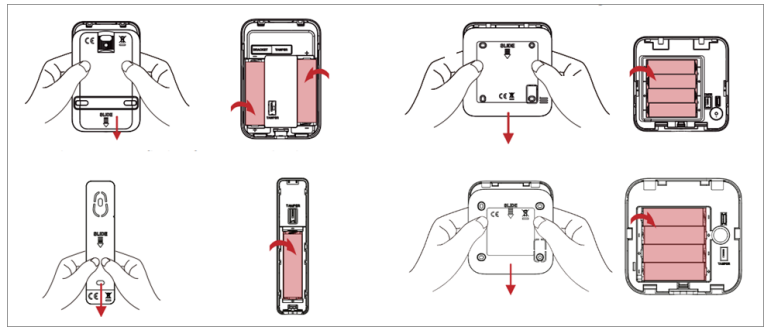


Figure 6-34 Select Bus to Add Devices

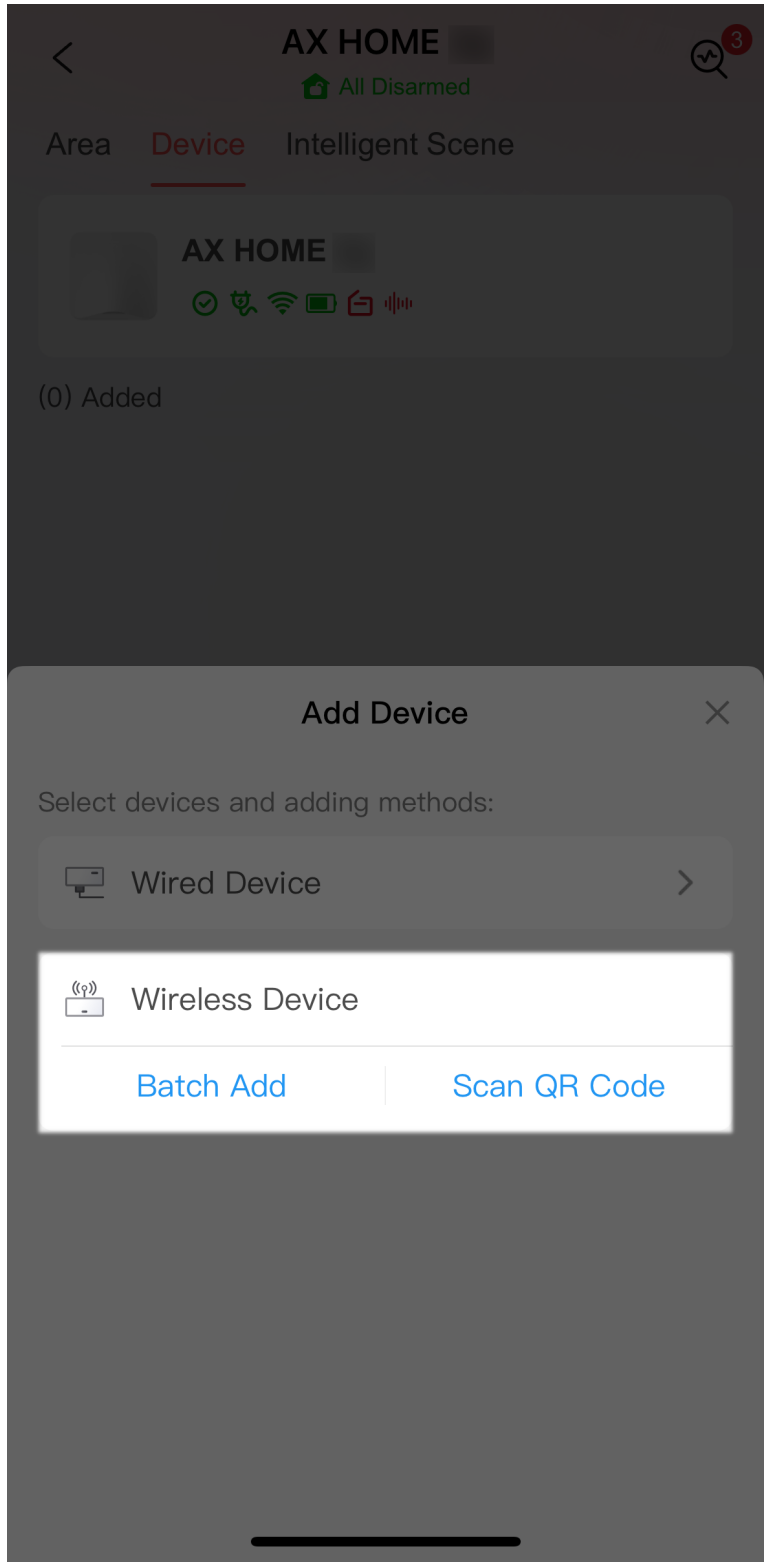
6.5.2 Add Wired Devices

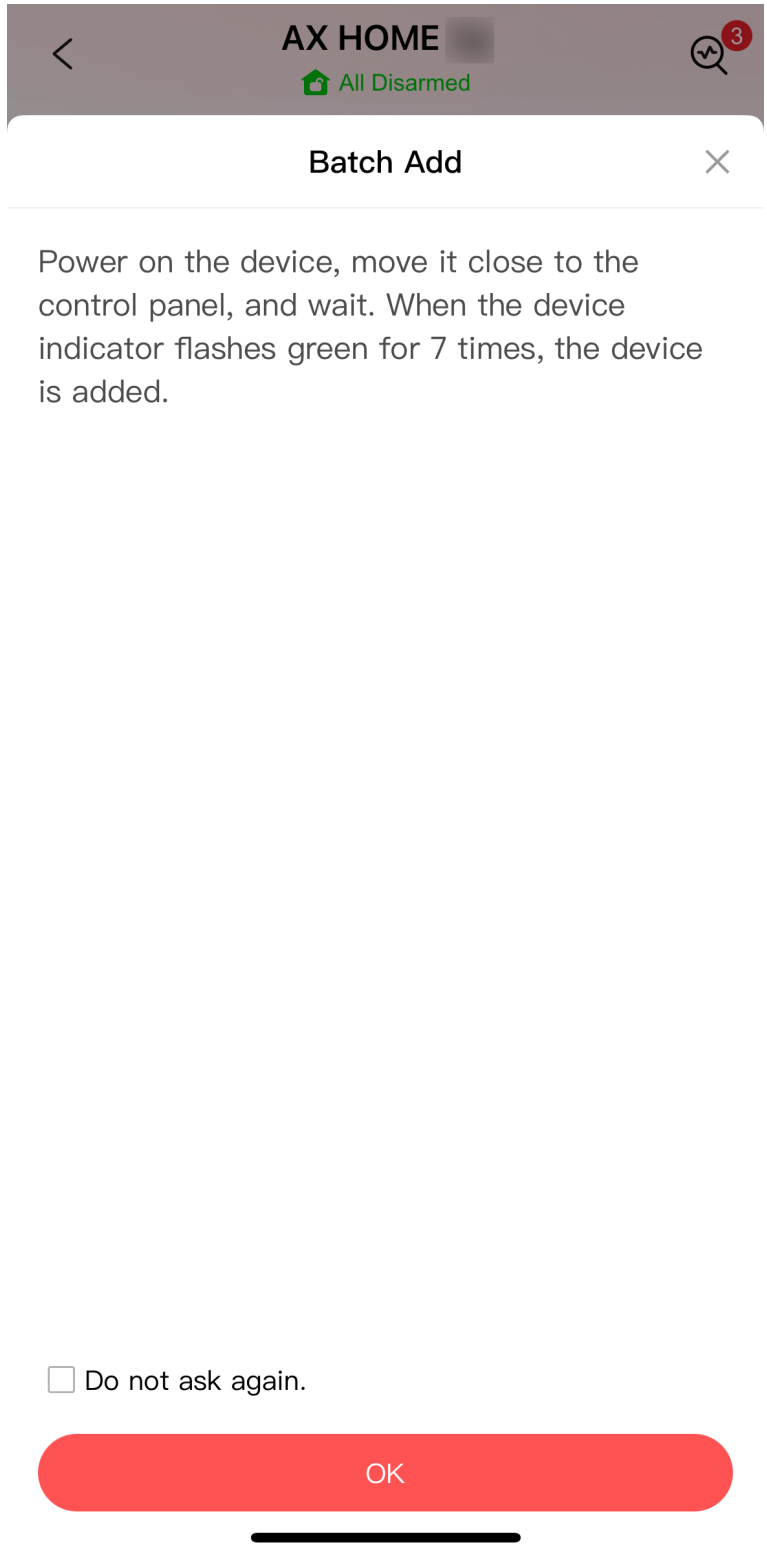
6.5.3 Add Wireless Devices

This section will introduce how to batch add detectors or peripherals. You can also tap **Scan QR Code** to scan the QR code on the security control panel to add peripherals one by one.




AX HOME
All Disarmed
3
Area
Device
Intelligent Scene
AX HOME
(0) Added
Add Device


AX HOME
All Disarmed
Area
Device
Intelligent Scene
AX HOME
(0) Added
Add Device
Select devices and adding methods:
Wired Device
Wireless Device
Batch Add
Scan QR Code


AX HOME
All Disarmed
3
Batch Add
Power on the device, move it close to the control panel, and wait. When the device indicator flashes green for 7 times, the device is added.
Do not ask again.
OK

6.6 How to Add Zones for Network Camera Channel

For AX HYBRID PRO V2.1.0 or later and AX PRO V1.3.1 or later, you can add a single zone or multiple zones for a network camera channel. After specifying events or rules for a zone, an alarm will be reported when the rule or one of the events is detected.

6.6.1 Prerequisite

Add the following supported cameras:

Device Type	Model
Security Thermal Cameras (HeatPro Series)	• DS-2TD1217-2/QA • DS-2TD1217-3/QA • DS-2TD1217-6/QA • DS-2TD1228-2/QA • DS-2TD1228-3/QA • DS-2TD1228-7/QA • DS-2TD1228T-2/QA • DS-2TD1228T-3/QA • DS-2TD1228T-2/QA(B) • DS-2TD1228T-3/QA(B) • DS-2TD2608-1/QA • DS-2TD2608-2/QA • DS-2TD2608-1/QA/FP • DS-2TD2608-2/QA/FP • DS-2TD2617-3/QA • DS-2TD2617-6/QA • DS-2TD2617-10/QA • DS-2TD2628-3/QA • DS-2TD2628-7/QA • DS-2TD2628-10/QA • DS-2TD2628-3/QA/GLT • DS-2TD2628-7/QA/GLT • DS-2TD2628-10/QA/GLT • DS-2TD2628-3/QA/GLT(JP) • DS-2TD2628-10/QA/GLT(LA) • DS-2TD2628T-3/QA • DS-2TD2628T-7/QA
Wi-Fi Camera	• DS-2CV1023G2-LIDWF(B) • DS-2CV1F23G2-LIDWF(B) • DS-2CV1043G2-LIDWF(B)

Device Type	Model
	• DS-2CV1F43G2-LIDWF(B) • DS-2DE2C200MWG/W • DS-2DE2C400MWG/W

6.6.2 Steps

1. On the Device tab, tap **Add Device** to add a network camera.
2. To add a zone, tap + and select a channel.

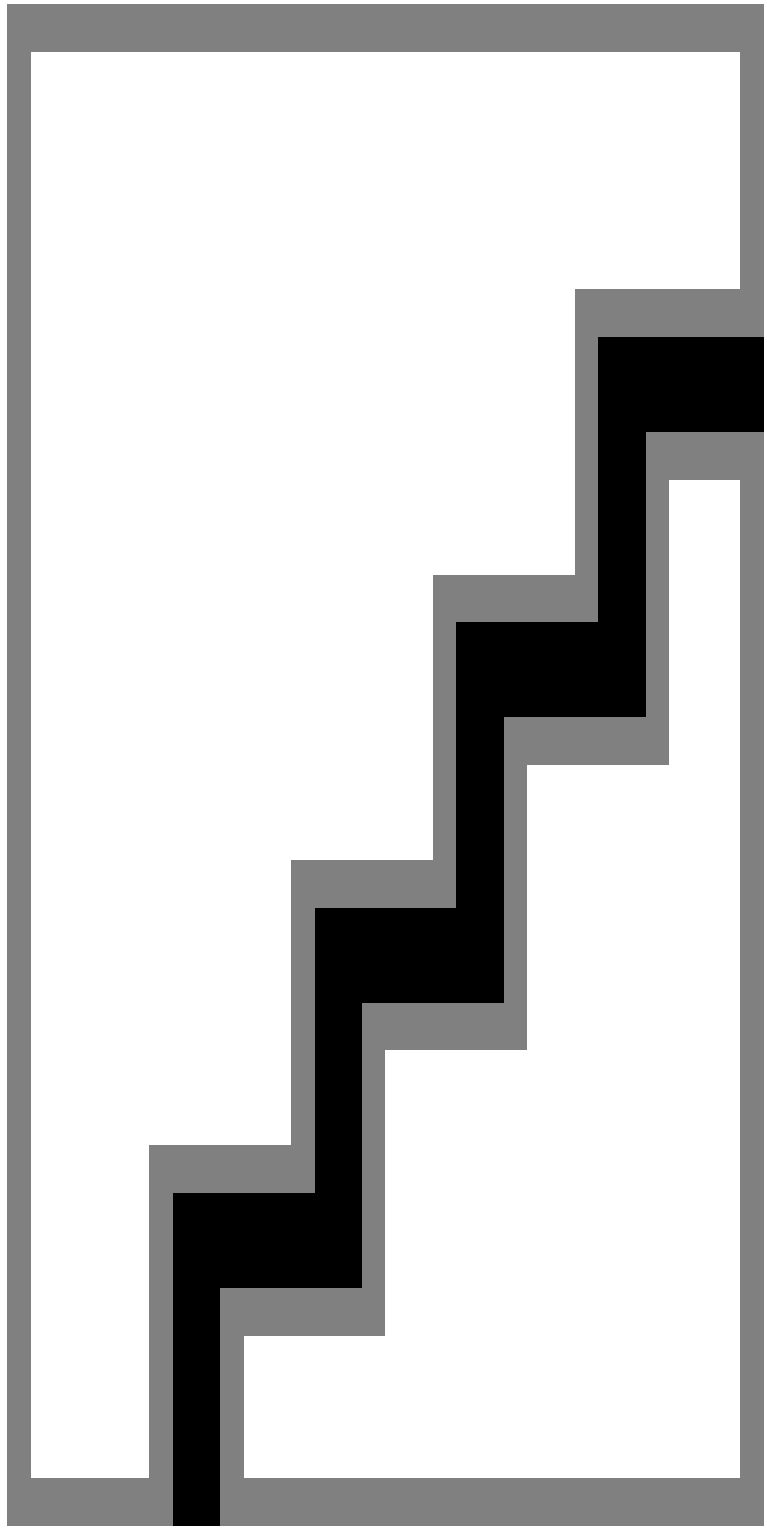


Figure 6-35 Add Zones for Network Cameras

3. Tap the zone card to enter the settings page and select a rule or events.

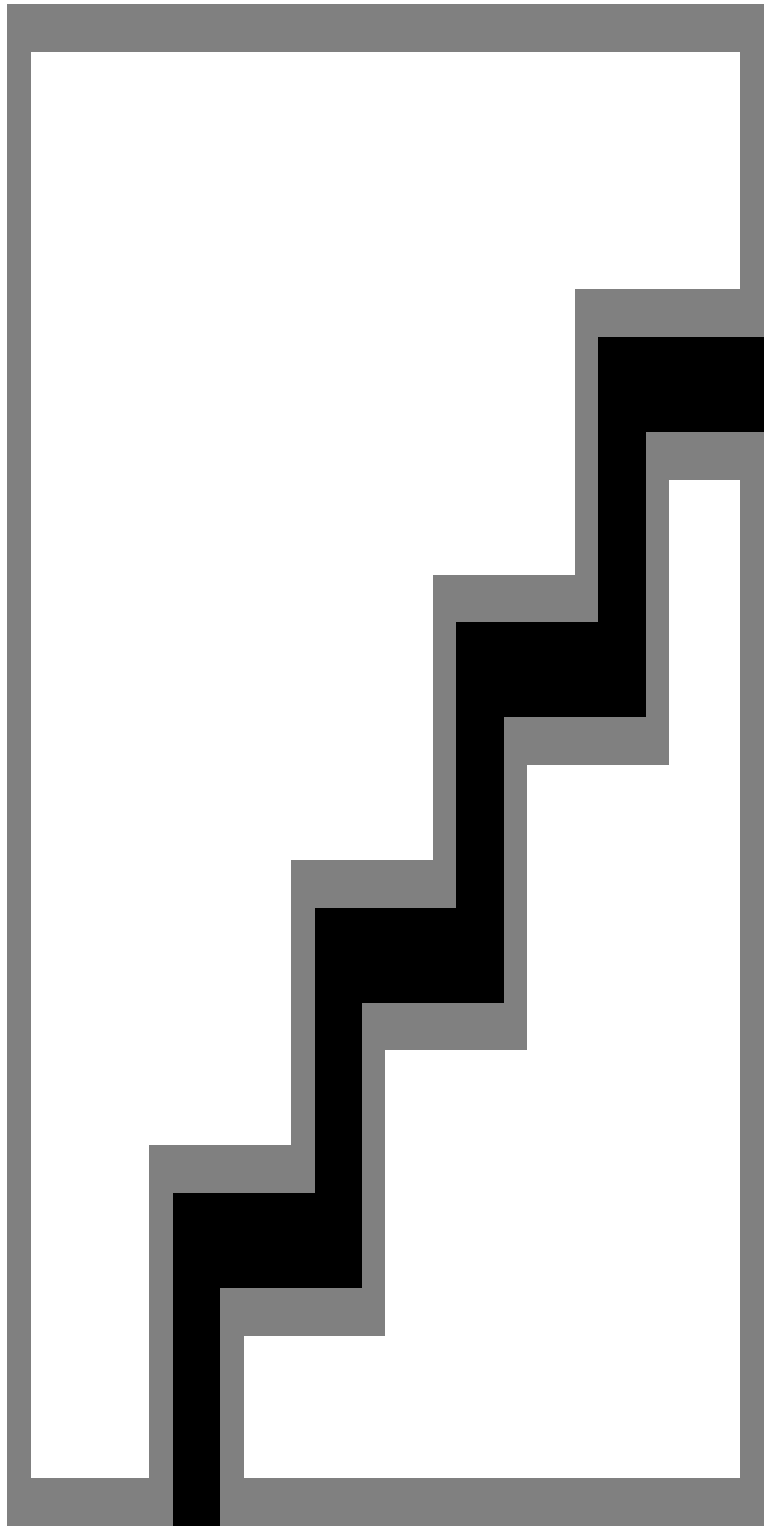


Figure 6-36 Set Event/Rule for Zones

Camera Protocol Type	Description
Added via ISAPI	You can select a detection rule or multiple events for different zones. When the rule or one of the events is detected, an alarm will be reported. **Note** - Selecting a rule is only supported by certain types of cameras. You can go to the camera's web configuration page and select **VCA → Rule** to set the detection rule. Up to 8 rules will be displayed. - You can only set the Event Type to either Event or Rule.
Added via Hikvision SDK or ONVIF	You cannot select events. All supported events will be detected by default. When one of the events is detected, an alarm will be reported.

6.7 How to Configure Detectors & Peripherals

This document mainly introduce how to configure major parameters of detectors and peripherals such as keyfobs, keypads, indoor sounders, PIR detectors, and electric fence energizers. For more peripherals, refer to the device's user manual for details.

6.7.1 Common Parameters

Deactivation

For AX HYBRID PRO V2.1.0 or later and AX PRO V1.3.1 or later, the deactivation status of linked devices is divided into two statuses:

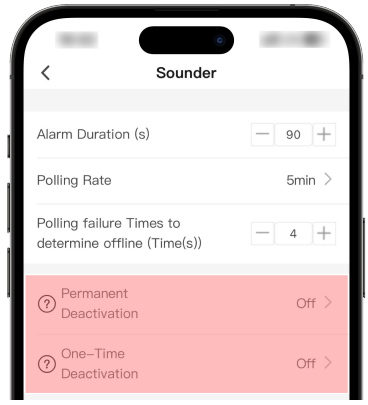


Figure 6-37 Deactivation Status

Status	Description	Options
Permanent Deactivation	Exclude the device from the system or disable its tampering alarms permanently.	• Off: the device operates in normal mode and transmits all events and alarms. • Entirely: The system will ignore all alarms reported by the device. • Lid Only: The system will ignore only tamper alarms.
One-Time Deactivation	Exclude the device from the system or disable its tampering alarms for a time the armed mode is active.	• Off: the device operates in normal mode and transmits all events and alarms. • Entirely: The system will ignore all alarms reported by the device. • Lid Only: The system will ignore only tampering alarms.

Link All Areas

For AX HYBRID PRO V2.1.0 or later and AX PRO V1.3.1 or later, you can tap **Link All Areas**to link bus peripherals to all current areas and subsequently added areas.

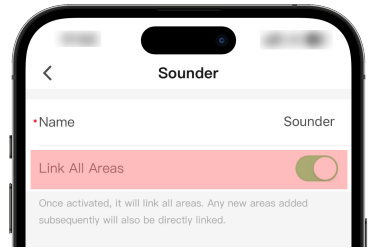


Figure 6-38 Link Bus Peripherals to All Areas

6.7.2 Electric Fence Energizer

An **Electric Fence Energizer** is a device that generates high-voltage pulses to electrify a fence, typically used for security or livestock containment. When connected with a **security control panel**, the energizer can serve as a **detector** to monitor the fence's integrity and detect intrusions or tampering.

How to Add Sub-Devices for Energizer?

1. Select + , and then set the device type to **Detector** and the channel No. The detector details are as follows:

Table 6-6 Detector Parameters

Parameter	DS-PF201-1-WB/DS-PF201-1-WE	DS-PF201-2-WB/DS-PF201-2-WE
Maximum Electric Fence Detectors	1	2
Channel No. of Added Electric Fence	No.1	No.1/No.2
Maximum Detectors	1	2
Channel No. of Added Detector	No.2	No.3/No.4

2. Tap the added device, tap ⚙ to go to the settings page, and set the parameters. The following table will introduce major parameters.

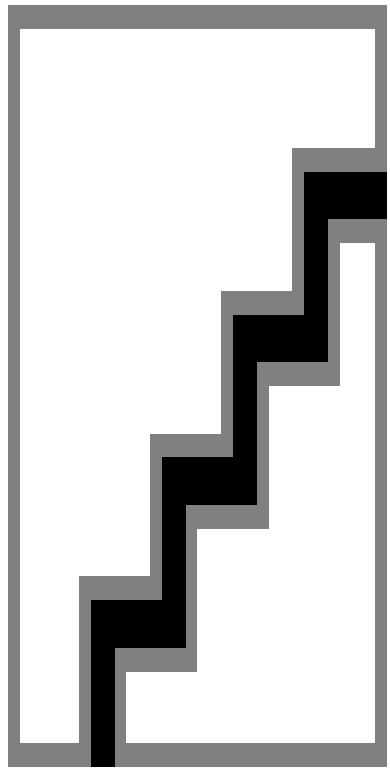


Figure 6-39 Add Detectors

Table 6-7 Zone Configuration Differences

Parameters	Electric Fence	Detector
Zone Type	Instant Zone	Instant Zone \ Delay Zone \ 24-Hour Zone \ Follow Zone \ Timeout Zone
High Voltage	√	×

Parameters	Electric Fence	Detector
	Note You can configure the **start time** and **end time** for when the energizer sends high-voltage pulses to electrify the fence. - High Voltage: 1.1 - 9.0 kV - Low Voltage: 0.5 -1.0 kV	
Sensitivity	√	×

6.7.3 Keyfob

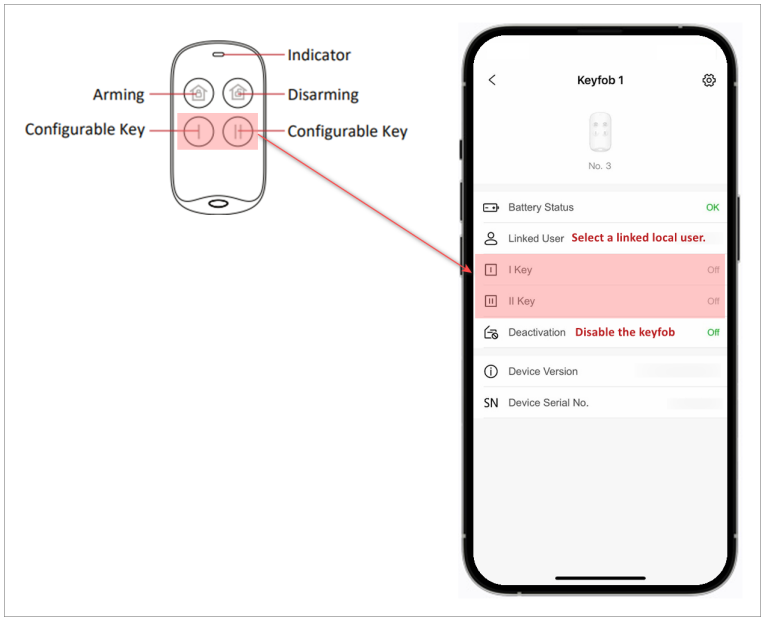


Figure 6-40 Keyfob Configuration

Table 6-8 Key Operations

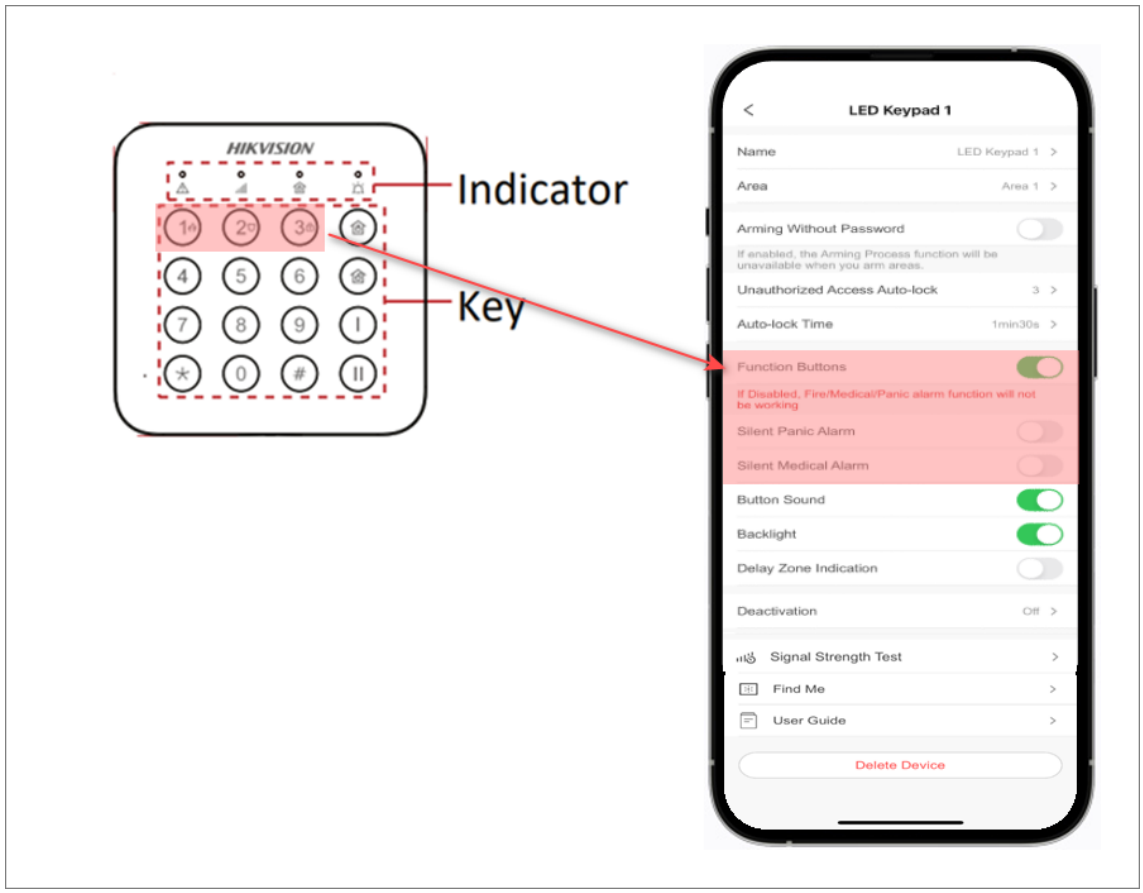
Function	Key	Description
Arming		1. Press to arm the system. 2. Wait for arming: Green LED flashes for 3 s. 3. Check fault: If a fault is detected, orange LED flashes.

Function	Key	Description
		Press arming key to confirm, or press disarming key to cancel. 4. Exit delay: Green Led flashes. Press arming key to skip delay, or press disarming key to cancel. 5. Check result: Blue LED flashes twice for successful arming.
Disarming		Press to disarm the system. Green LED flashes twice for successful disarming.
Silence Alarm	or	Press to mute alarm sound from the control panel, sounder, or keypad when an alarm is triggered in the same area.
Silent Panic Alarm	or	Press to mute panic alarm sound.
Audible Panic Alarm	or	Press to link sound indication for panic alarm.
Lock	+	Press to lock all keys.
Unlock	+	Press to unlock all keys. The data transmission between a keyfob and a control panel recovered.

6.7.4 Keypad

Settings

Tap the flashing hotspot for operation details, including indicator status, triggering alarms, backlight, and signal strength test.



1.

2.

3.

4.

5.

6.

7.

8.

9.

10
.

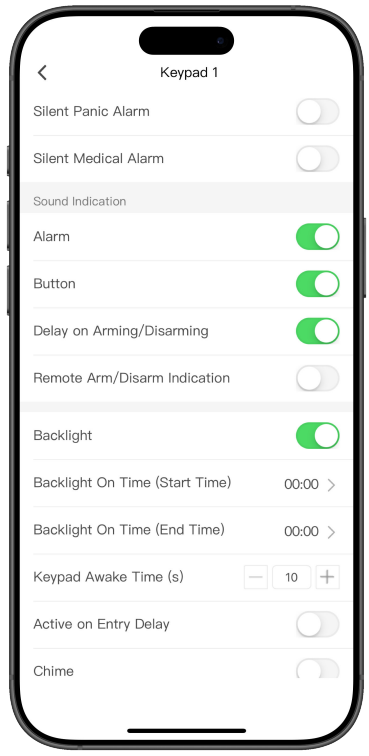
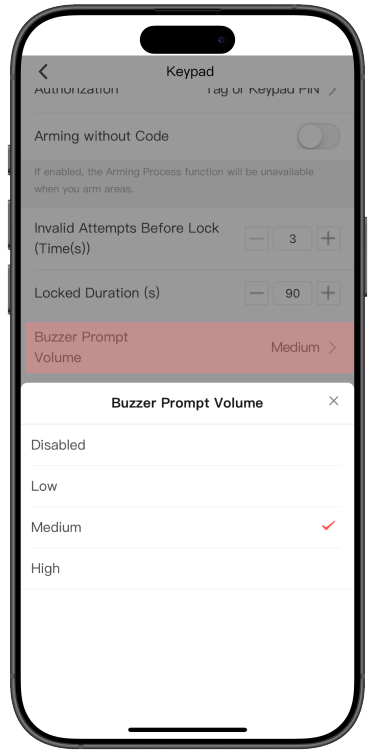


Figure 6-41 More Settings for Keypads

Table 6-9 More Settings Description

Parameter	Description
Operation Mode	• Simple Mode: You can directly arm an area. • Standard Mode: You can arm an area after the fault check.
Arming Without Code	You can arm/disarm an area in both simple mode and standard mode.
Remote Arm/Disarm Indication	Arming/disarming via non-keypad devices triggers audible alerts.
Chime	After enabling this function for supported keypads, wireless/bus sounders, tag readers, and detectors, you can create a Chime scene where you can hear a doorbell when a zone is triggered.
Buzzer Prompt Volume	For AX HYBRID PRO V2.1.1 or later, support adjusting the buzzer prompt volume of the following models of keypads: DS-PK501LTM-HWB and DS-PK501LTM-HWE.

Parameter	Description
	 **Figure 6-42 Adjust Buzzer Prompt Volume**

For AX HYBRID PRO V2.1.1 or later, you will receive a notification when someone uses a keypad to arm or disarm the system.

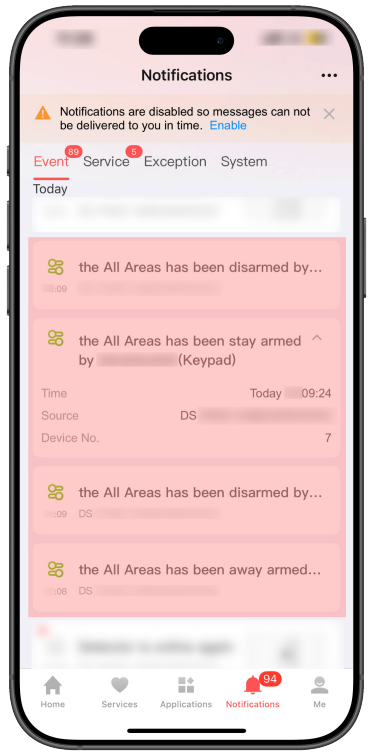


Figure 6-43 Notification of Keypad User Information

Create Intelligent Scene

After enabling the Chime function for supported keypads, you can create a Chime scene where you can hear doorbell when a zone is triggered. For example, when a customer enters the store, the detector at the entrance detects movement.Instantly, the keypad emits a doorbell chime. Staff members hear the alert and can promptly greet guests.

1. Tap **Intelligent Scene → Recommended Scene → Chime** .
2. Set the scene name, select the trigger source, and set the condition to **Triggered**.
3. Add a device and set the action.

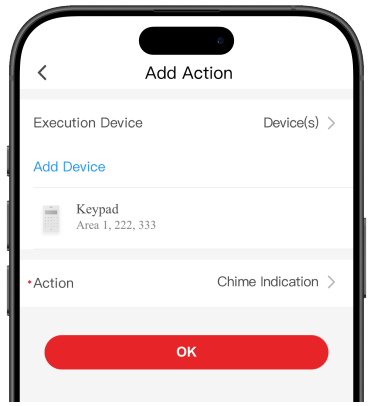


Figure 6-44 Add Chime Device

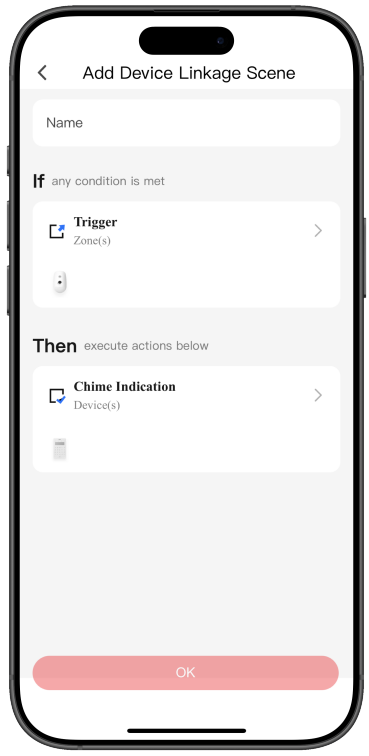


Figure 6-45 Configure Chime Scene

4. Enable the scene.

6.7.5 Tag Reader

Caution

Ensure tags are added.

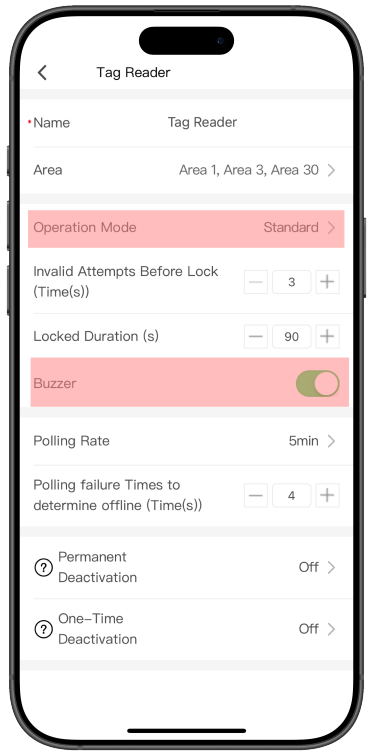


Figure 6-46 Tag Reader Major Settings

Table 6-10 More Settings

Parameter	Description
Operation Mode	Standard: • Select an area for arming/disarming • Quick tap: Arm in Away mode • Double tap: Disarm • Long press: Arm in Stay mode Simple: • When armed: Tap to disarm • When disarmed: ◦ Quick tap: Arm in Away mode ◦ Long press: Arm in Stay mode **Note** Only operation tags can be used to arm/disarm.
Buzzer	You will hear a buzz for a successful tag tap on the reader.

For AX HYBRID PRO (V1.1.2), you can add tags via both wireless tag readers and keypads. The supported tag readers are as follows: DS-PT1-WE(O-STD), DS-PT1-WB(O-STD), DS-PT1-WE(B)(O-STD), and DS-PT1-WB(B)(O-STD).

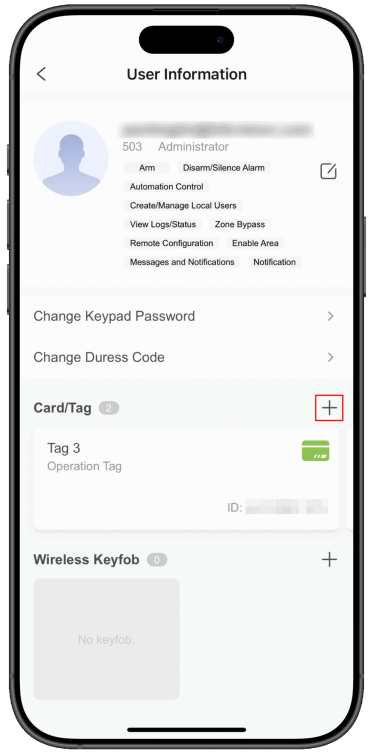


Figure 6-47 Add Tag via Tag Reading Device

6.7.6 Sounder

Intercom Sounder

For AX PRO V1.3.1 or later, you can add full-duplex sounders for two-way audio. You can start two-way audio in one of the two ways:

- On the Device tab, tap to start two-way audio.

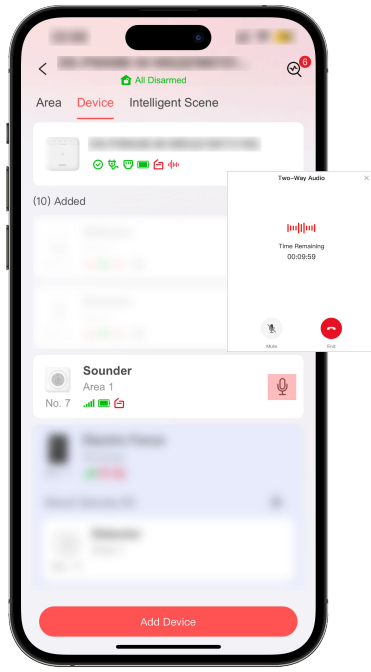


Figure 6-48 Start Two-Way Audio on Device Tab

- You can start two-way audio in the **Notifications** module. Take the following steps: After adding a full-duplex sounder, go to the control panel's settings page, enable **Intercom Service**, and select the added sounder as the intercom sounder.
  1. After adding a full-duplex sounder, go to the control panel's settings page, enable **Intercom Service**, and select the added sounder as the intercom sounder.
  2. Go to the sounder's settings page, enable **Intercom Service**, and set the intercom duration.
  3. When an alarm is triggered, you can go to the Notifications module to start two-way audio within the intercom duration. Otherwise, the notification will expire and you cannot start two-way audio.

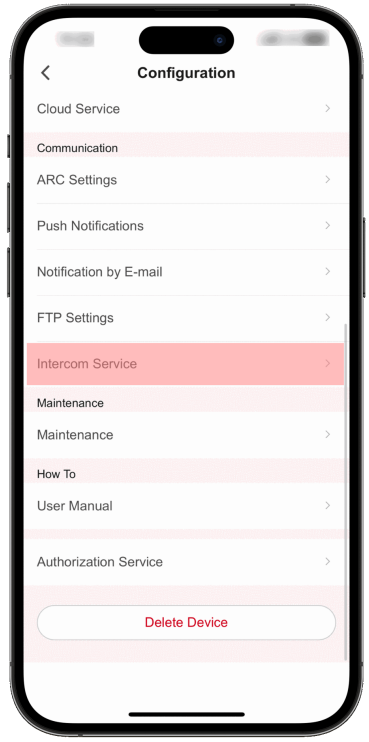
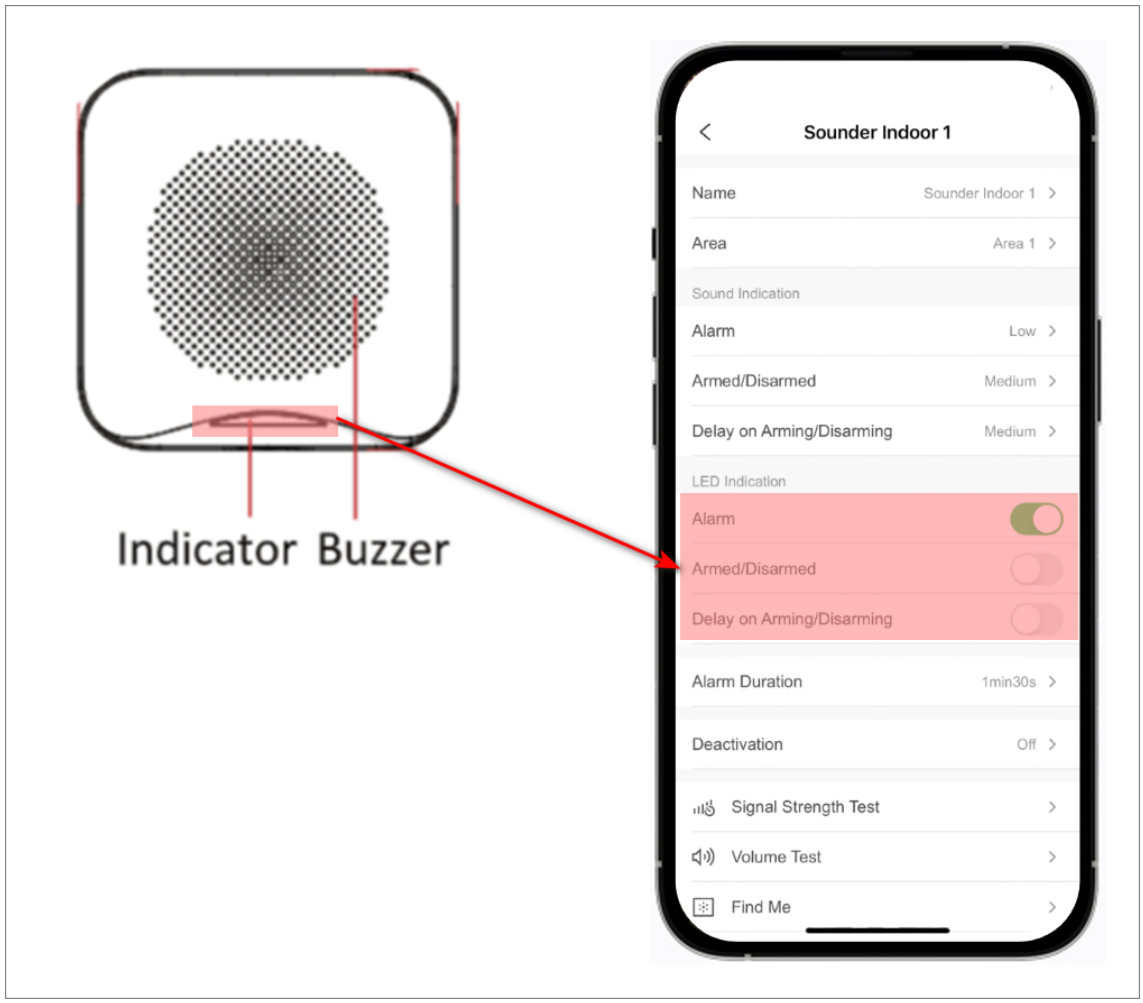


Figure 6-49 Start Two-Way Audio in Notifications Module

Internal/External Sounder

Tap the flashing hotspot for internal sounder details, including the volume setting, indicator status, and alarm duration.



1.

2.

3.

For external sounders, if you enable **Confirm LED**, the LED indicator will flash every 15 seconds to indicate the control panel is in operating mode.

For AX HYBRID PRO V2.1.0 or later and AX PRO V1.3.1 or later, you can **Silent During Arming** to silence sounders when the linked area is armed in Stay mode.

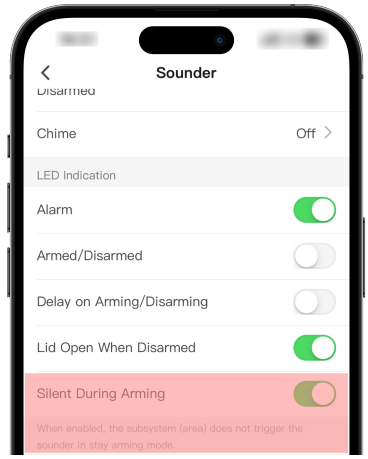


Figure 6-50 Silence Sounder in Stay Arm Mode

6.7.7 Automation (Relay / Smart Plug / Wall Switch)

Directly Switch on/off Automation Devices

For AX HOME, AX PRO V1.3.0 or later, and AX HYBRID PRO V2.0.0 or later, support directly switching on/off automation devices on the device list. To switch on/off automation devices with pulse, you need to create a Tap to Run scene or Schedule scene.

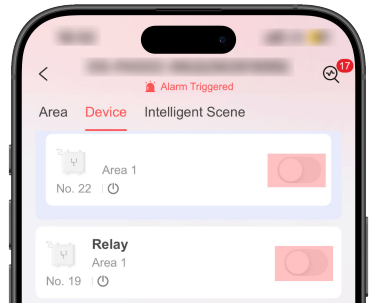


Figure 6-51 Switch on/off Relay

Create Intelligent Scenes

For AX HYBRID PRO V2.0 or later, you can create various intelligent scenes (Only Tap to Run scene for AX PRO V1.3.1 or later) for automation devices. To

Schedule Scene

You can set the timer, and an automation device will automatically perform actions at the scheduled time, such as power off, turn on, pulse activation, or toggle the switch status. For example, configure the smart plug with an automation:

- Power off at 9:00 (work departure)
- Power on at 19:00 (return home)

1. Tap **Intelligent Scene → Create Scene → Schedule** .
2. Set the scene name and set scheduled time.
3. Add a device and set the action.

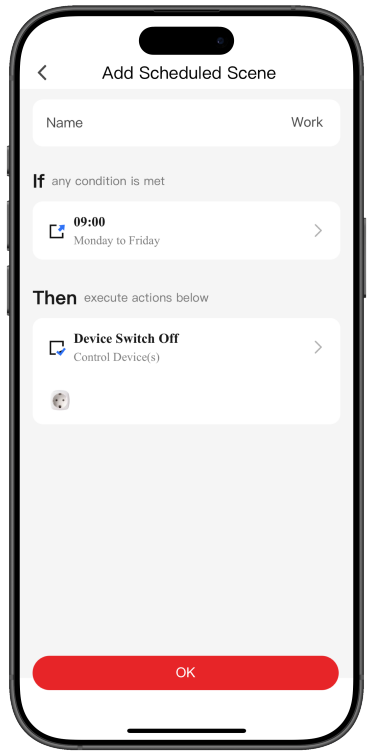


Figure 6-52 Set Scheduled Scene

4. Enable the scene.

Tap to Run Scene

You can run an action pre-defined in a Tap to Run scene with just a tap. For example, when you hear suspicious sounds at night, tap to activate the connected strobe light/flashing lamp without shouting or physical confrontation.

1. Tap **Intelligent Scene → Create Scene → Tap to Run** .
2. Set the scene name.
3. Add a device and set the action.

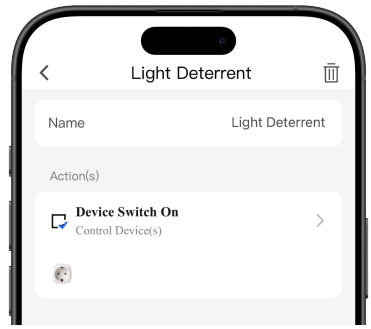


Figure 6-53 Create Tap to Run Scene

4. Tap  to run the action.

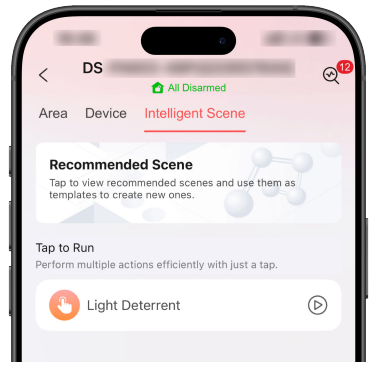


Figure 6-54 Run Pre-Defined Action

5. Swipe the scene left, and then tap to add it to the homepage.

Automation Scene

You can create a device linkage scene where your device automatically performs an action when a condition (trigger) is satisfied. For example:
Trigger: A PIR-Camera detector detects unauthorized movement at night. The detector triggers an alarm and captures photos/video.
Actions: The smart plug activates connected strobe light (flashing brightly).

1. Tap **Intelligent Scene → Create Scene → Automation** .
2. Set the scene name.
3. Set the condition by specifying the trigger source and condition.
4. Set the action.

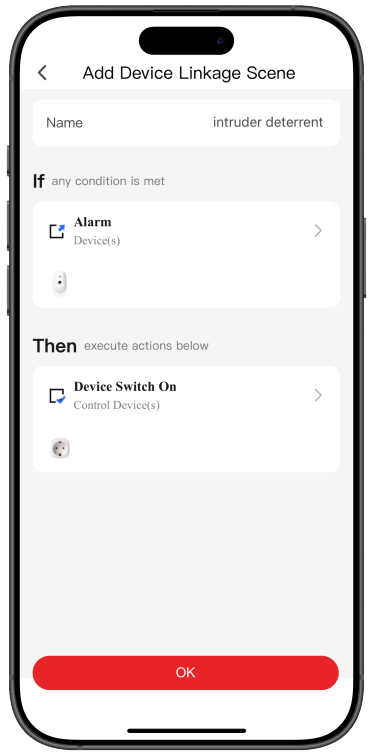


Figure 6-55 Configure Automation Scene

5. Enable the scene.

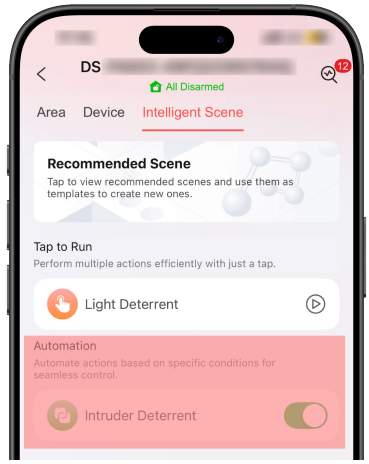


Figure 6-56 Enable Automation Scene

Set Original Status

For AX PRO V1.3.0 or later and AX HYBRID PRO V2.0.0 or later, you can set the original device status.

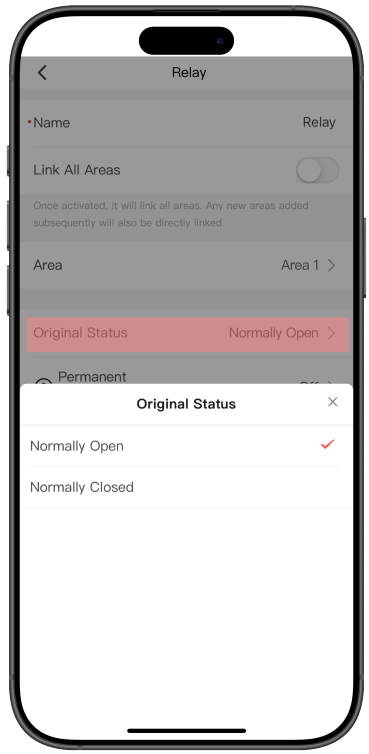
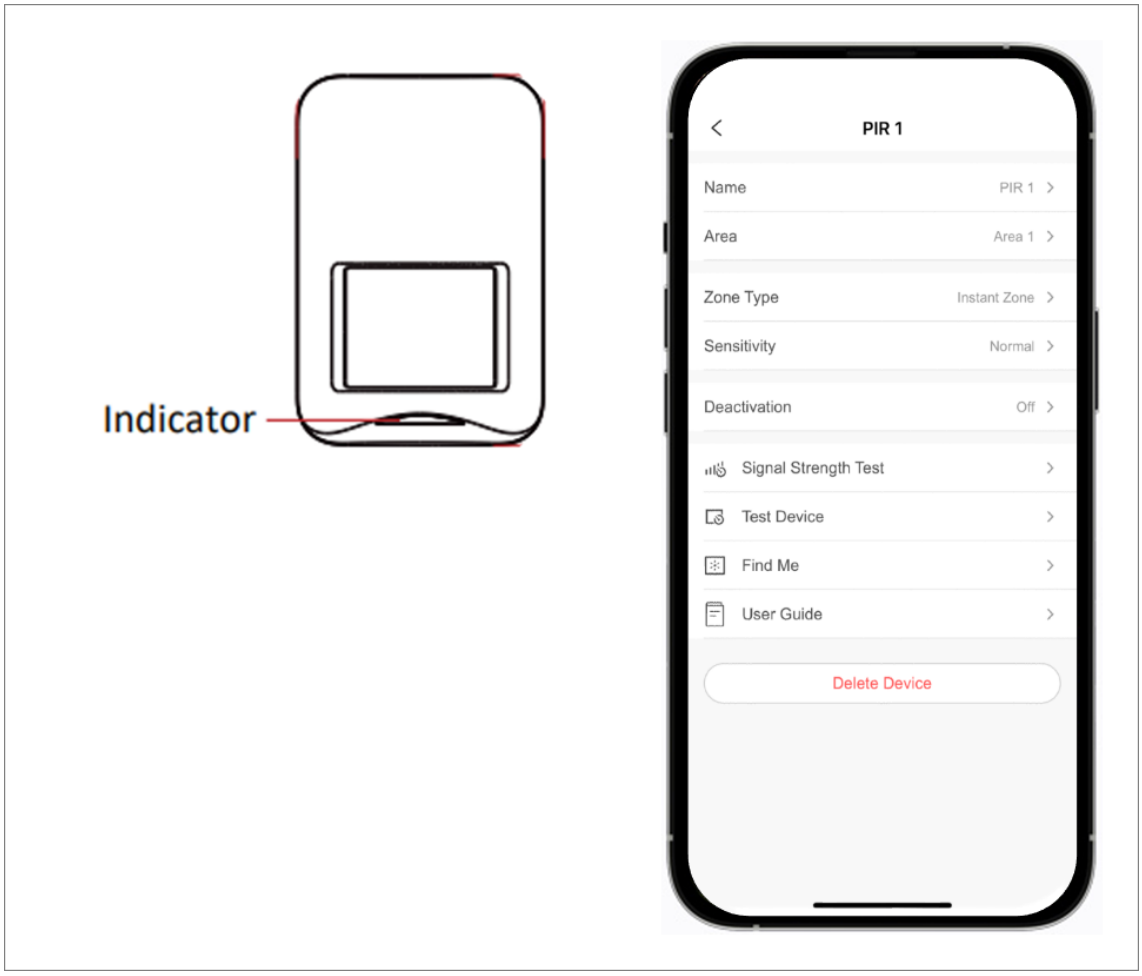


Figure 6-57 Set Original Status

Status	Description
Normally Open	• Open circuit (no connection) when the relay coil is **not energized**. Used to **start a process** or enable a circuit only when actively triggered. • Example: ◦ **Scenario**: A smart home uses an NO relay to control a lamp. › **Default**: Lamp is off (NO contact is open). › **When Activated**: Relay coil powers on, **closing** the NO contact to turn the lamp on.
Normally Closed	• Closed circuit (connected) when the relay coil is **not energized**. Used to **stop a process** or maintain safety during failures. • Example: ◦ **Scenario**: A factory machine uses an NC relay in its emergency stop circuit. › **Normal Operation**: NC contact keeps the circuit closed, allowing the machine to run. › **Emergency Pressed**: Relay coil energizes, **opening** the NC contact to **cut power** and stop the machine immediately.

6.7.8 PIR Detector

Tap the flashing hotspot for details, including the zone type and detector sensitivity level.



1.

2.

3.

6.8 How to Add an Alarm Widget for Quick Control

For both Android and iOS(17.0 or later), you can add widgets for AX HYBRID PRO V1.0.3 or later and AX PRO V1.2.6 or later, and AX HOME to quickly arm/disarm areas or trigger an alert for emergencies.

Take the following steps to add a widget for iOS:

1. Log in your Hik-Connect account.
2. Go to the Home Screen page, then touch and hold an empty area until the apps jiggle.

3. - For iOS 18.0 or later, tap **Edit → Add Widget** in the upper-left corner, and search ***Hik-Connect***.
   - For iOS 17, tap + in the upper-left corner and search ***Hik-Connect***.
4. Find the widget you want, and tap **Add Widget**.

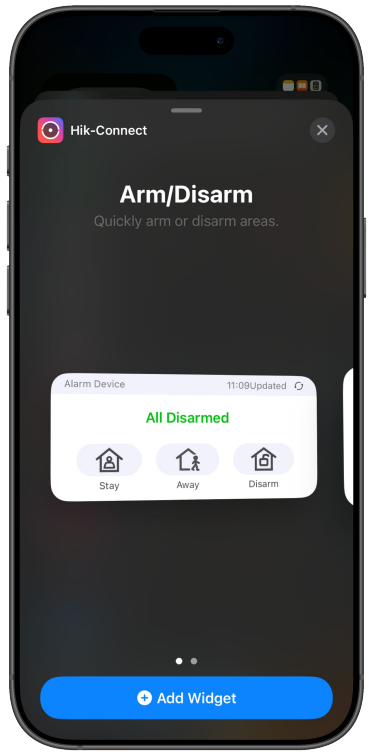


Figure 6-58 Add Widget

5. Configure the widget.
   - Arm/Disarm
     a. Link a control panel.

     Note

     Ensure you have operation permissions and the control panel is online.

     b. Select all areas or specify an area.
     c. Use the widget. You can arm areas in Stay/Away mode, disarm areas, and update the arming status.



Figure 6-59 Use Widget

Note

If you enable **Fault Checklist when Arming** or set a delayed zone, go to the Hik-Connect App for further operations.

- Peripheral Control

a. Link a control panel.

Note

Ensure you have operation permissions and the control panel is online.

b. Select an automation device.

Note

The supported models are as follows:

- DS-PM1-O1L-WE
- DS-PM1-O1L-WB
- DS-PM1-O1H-WE
- DS-PM1-O1H-WB
- DS-PSP1-WE
- DS-PSP1-WB
- DS-PM401R2H-WE

- DS-PM401R2H-WB
- DS-PM401R2H-WA

Relays in the Roller Shutter mode are not supported.

c. Use the widget. You can switch on/off the device directly from the widget.

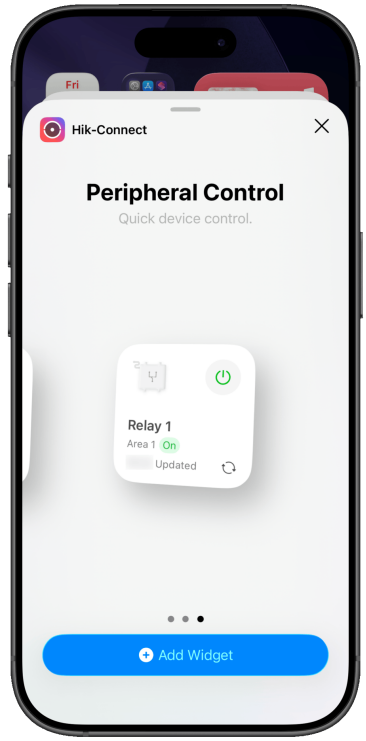


Figure 6-60 Relay Control Widget

Chapter 7 Access Control Devices

7.1 How to control door status?

The Mobile Client supports controlling the status of the access control devices' related doors by the super password of the device.

1. On the device list page, tap  on the right of the access control device to enter the door control page.

   Note

   The door icon varies with different door status.
2. Control the door status.
   - **Remain Open**: Keep the door open.
   - **Open Door**: Open the door for a configurable time period. When the time period expires, the door will close.
   - **Remain Closed**: Keep the door closed. In this status, the door can only be opened by super card or super password.

     Note

     For details about super card, see the user manual of the access control device.
3. Enter the super password.

   Note

   - For face recognition terminal, this step is not required. You can control door status directly in step 2.
   - By default, the super password is the device verification code. You can change the super password.

   The door status will change.

7.2 How to set door open duration?

You can set the door open duration for the access control device. When the duration expires, the door will close automatically.

1. On the device list page, tap to enter the Settings page of the access control device.
2. Tap **Door Open Duration** to open the Door Open Duration list.
3. Select a duration from the list.
4. Tap to confirm the selection.

If you tap **Open Door** in the door control page, the door will open for the configured time duration.

7.3 How to change super password?

The Mobile Client allows you to change the super password of the access control device, which can be used to open all the access control points (e.g., doors), even when the access control point is in remaining closed status.

Note

For details about super password of the access control device, see the user manual of the device.

1. On the device list page, tap ⚙ to enter the Settings page of the device.
2. Tap **Change Password** to enter the Change Password page.
3. Enter the old password and tap **Next**.

   Note

   If it is the first time to set the super password, skip this step.
4. Create a new password and then tap **Finish**.

   Note

   The password should contain 6 numbers.

7.4 How to view access control logs?

You can view the access control device's logs including the access control events and alarm information. You can also filter the logs.

1. On the device list page, tap the door icon on the right of the access control device to enter the door control page.



Figure 7-1 The Icon Representing Door

   The log list will be displayed on the Log section of the page.
2. Perform the following operations.

Table 7-1 Operations

Operations	Descriptions
Refresh Log List	Swipe the log list downward to refresh it.
View All Logs	Tap **View All Logs** to enter the Log page and view all access control device logs.
Filter Logs	On the Log page, tap **Filter** and then set the filtering condition (time and event type) to filter.

7.5 How to manage sliding gate openers?

Supported Model: Devices: DS-K3GL606WX-WB and DS-K3GL606WX-WE (Scheduled Release in September, 2025)

7.5.1 Wired Connection Setup

You can connect your sliding gate opener via wired network, scan the QR code on HC to activate the device, enable the Hik-Connect service, and bind it to your account.

7.5.2 Quick Door Controls

You can trigger instant door actions with one tap.

- Trigger: Open/pause the door
- Pedestrian: Keep the door half open as configured
- Locked Open: Keep the door open
- Lock: Disable the door (highest priority)

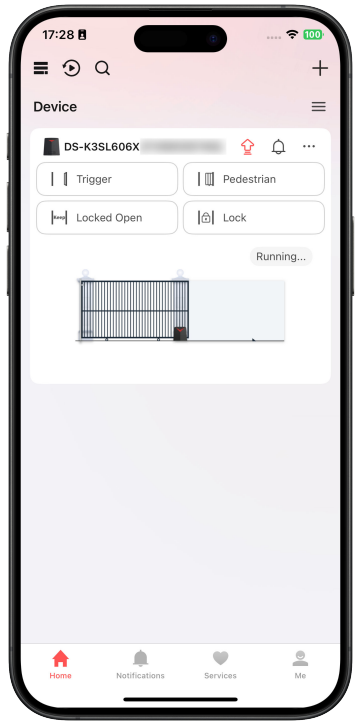


Figure 7-2 Control Doors

7.5.3 Real-Time Event Monitoring

On the app, you can view real-time and history logs.

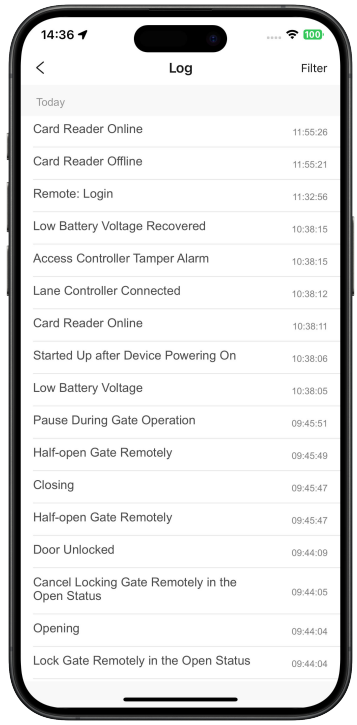


Figure 7-3 Log

7.5.4 Real-time Exception Notifications

You can receive instant push notifications on the app for device issues like low battery or door state changes. Stay informed about system health automatically.

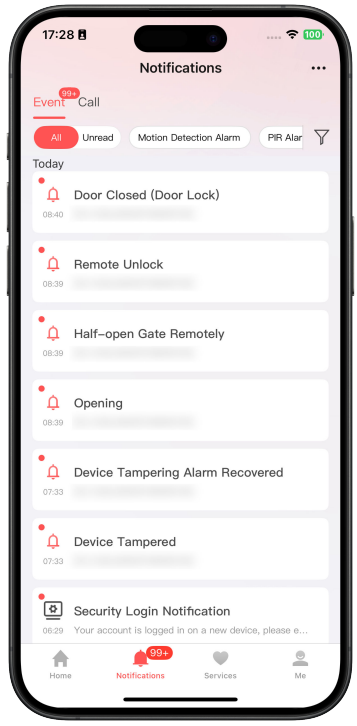
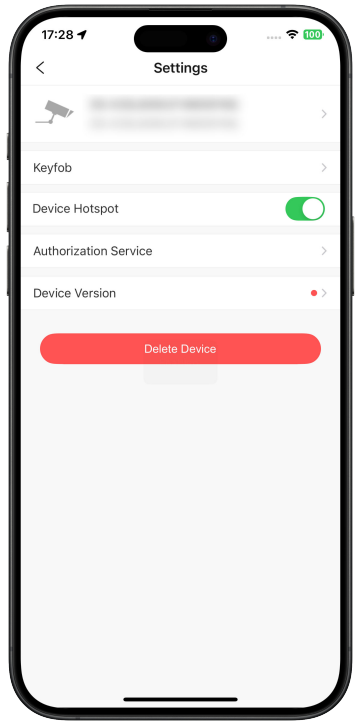
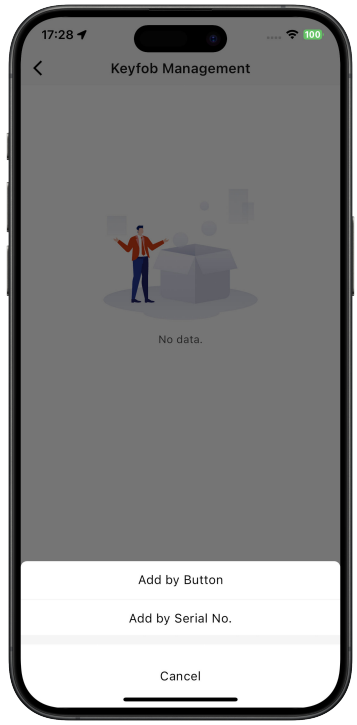


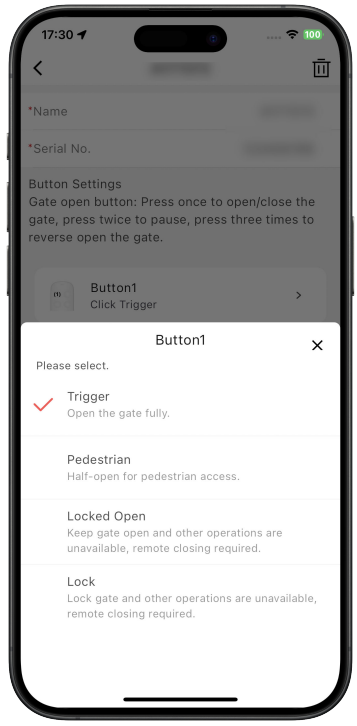
Figure 7-4 Exception Notifications

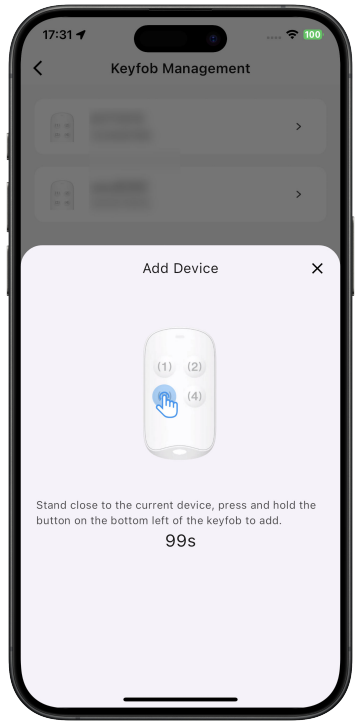
7.5.5 Keyfob Management

On the app, you can link keyfobs to sliding gate openers via serial number or button press. Keyfobs can be used to open doors.


17:28
Settings
Keyfob
Device Hotspot
Authorization Service
Device Version
Delete Device


17:28
Keyfob Management
No data.
Add by Button
Add by Serial No.
Cancel


17:30
*Name
*Serial No.
Button Settings
Gate open button: Press once to open/close the gate, press twice to pause, press three times to reverse open the gate.
Button1
Click Trigger
Button1
Please select.
Trigger
Open the gate fully.
Pedestrian
Half-open for pedestrian access.
Locked Open
Keep gate open and other operations are unavailable, remote closing required.
Lock
Lock gate and other operations are unavailable, remote closing required.


17:31
Keyfob Management
Add Device
Stand close to the current device, press and hold the button on the bottom left of the keyfob to add.
99s

7.5.6 Device Sharing

On the app, you can share the sliding door openers and door control and event viewing permissions to an HPP user or an HC user. The keyfob management permissions cannot be shared.

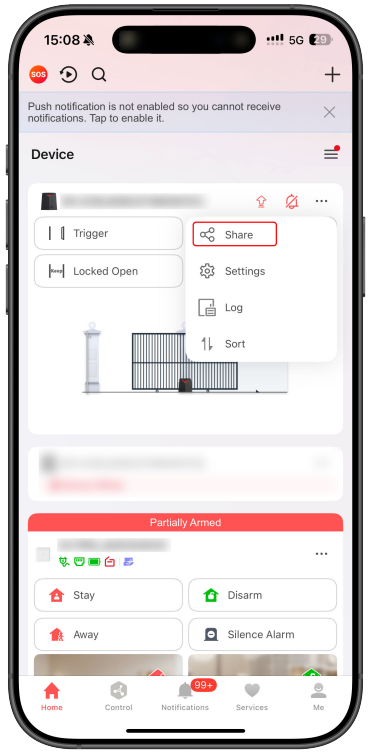


Figure 7-5 Share Device

Chapter 8 Video Intercom Devices

8.1 How to manage indoor stations?

8.1.1 How to set indoor station parameters?

Supports configuring indoor station parameters on the Mobile Client.

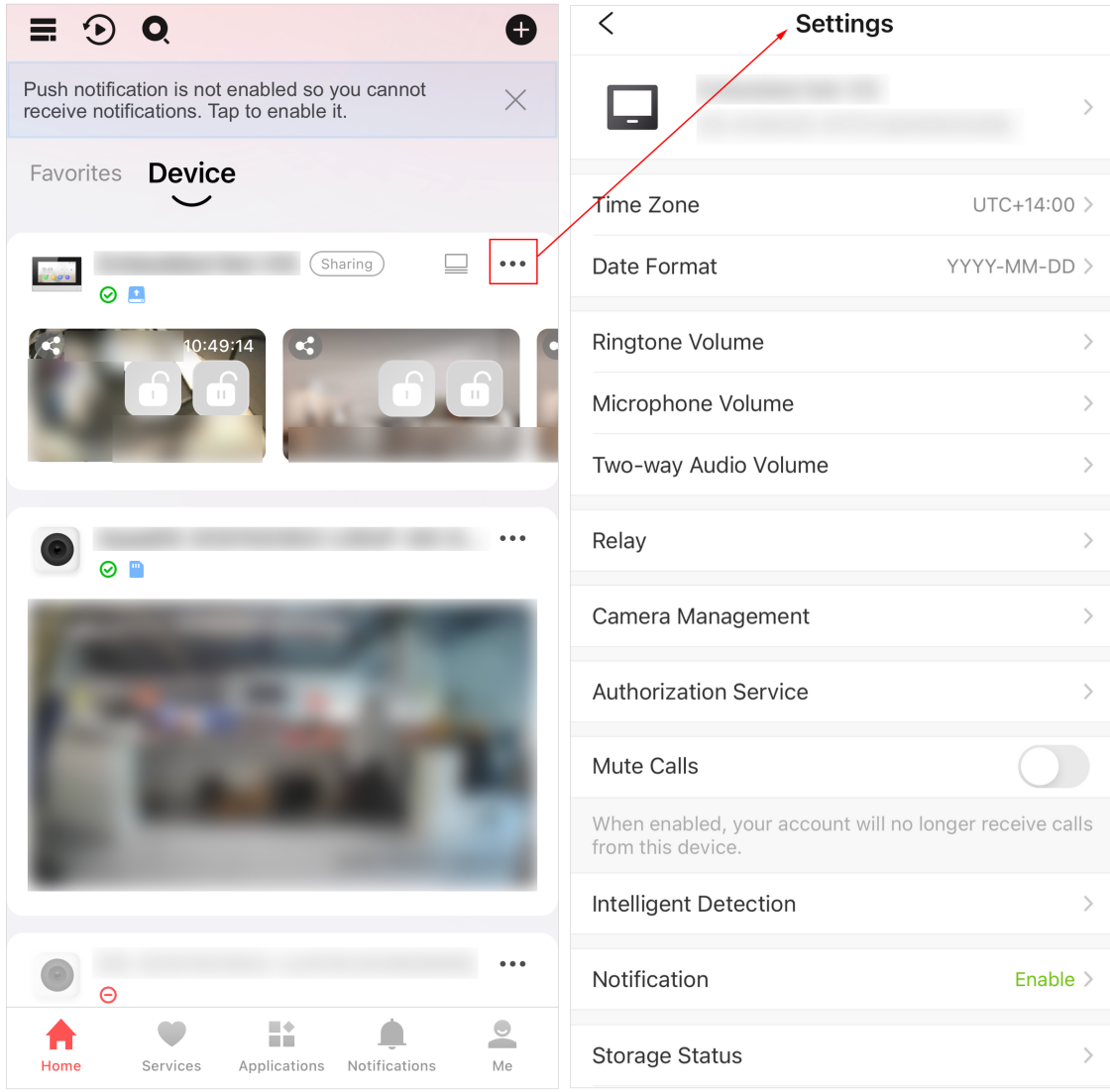


Figure 8-1 Configure Indoor Stations

8.1.2 How to add temporary passes for indoor stations?

Supported device models:

1. DS-KH8350-WTE1, DS-KH8350-TE1, DS-KH8520-WTE1, DS-KH6320-WTE1, DS-KH6320-TE1, and DS-KH6320Y-WTE2 with firmware version V2.2.80build240725 or later.
2. DS-KH6320-WTDE1 and DS-KH6320-TDE1 with firmware version V2.2.80build240725 or later.
3. DS-KH6350-WTE1, DS-KH6350-TE1, DS-KH6351-TE1, and DS-KH6351-WTE1 with firmware version 2.2.82 build240725 or later.
4. DS-KH6110-WE1 with firmware version V2.2.80build240725 or later.

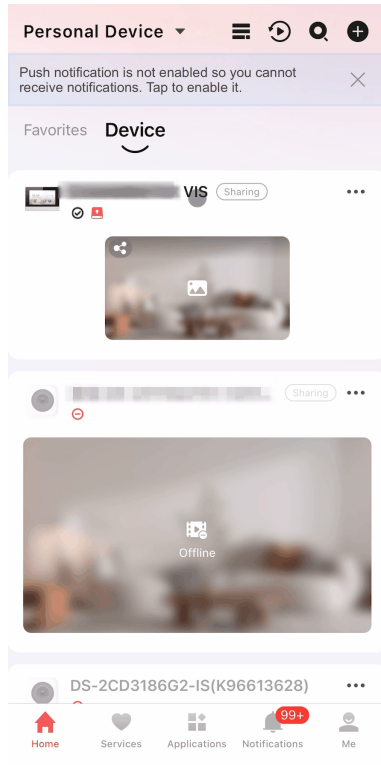


Figure 8-2 Add Temporary Passes

8.1.3 How to view linked devices of indoor stations?

You can view linked door stations, cameras, and station extensions of an indoor station.

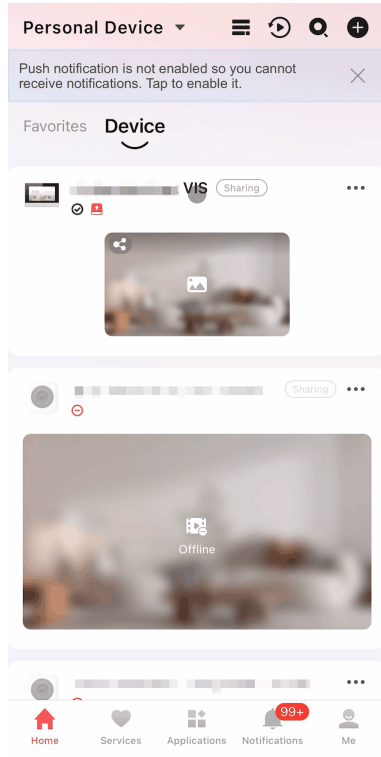


Figure 8-3 View Linked Devices

8.1.4 How to control linked devices of indoor stations?

You can control devices linked with indoor stations.

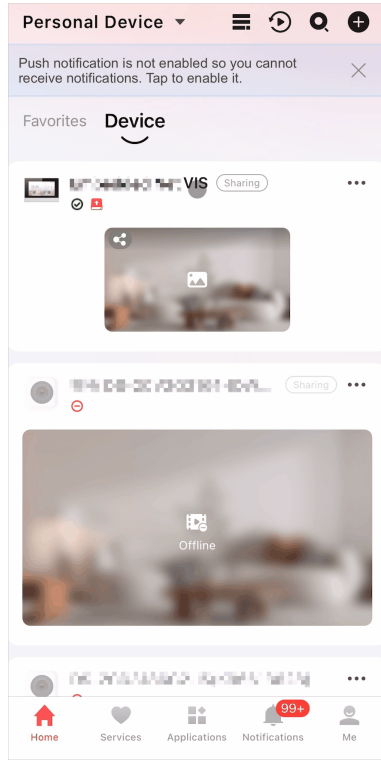


Figure 8-4 Control Linked Devices

8.1.5 How to answer call from indoor stations?

If no one answers the call via the indoor station for a while, the call will be forwarded to the Mobile Client. You can answer the call, view the live video of the door station, as well as open the door.

Note

Up to 6 users can view the live video of the same door station at the same time. If there's already been 6 users viewing the live video, you can only use the audio function of the video intercom device.

1. Tap the call message to enter the following page.

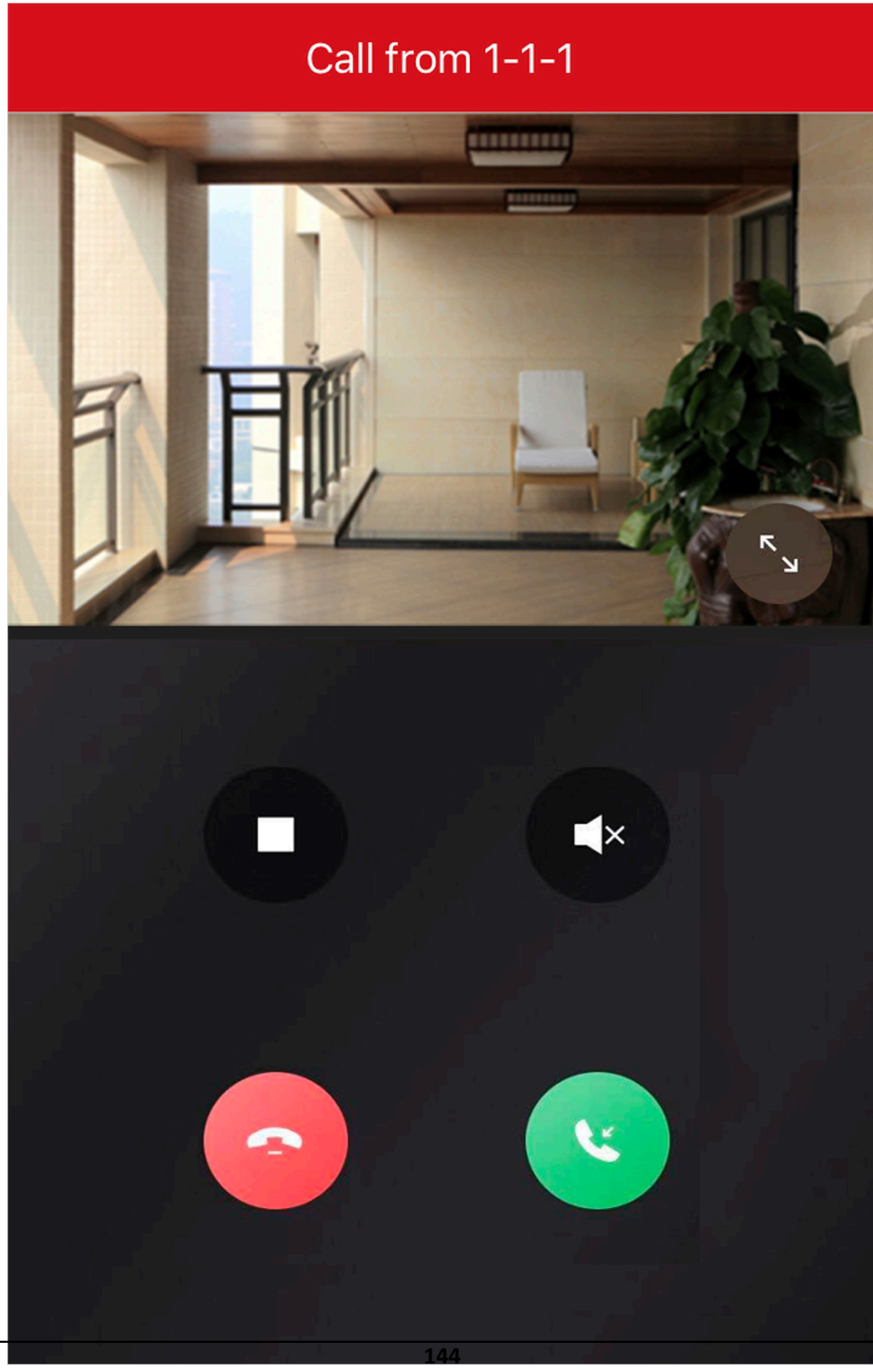


Figure 8-5 Call Page

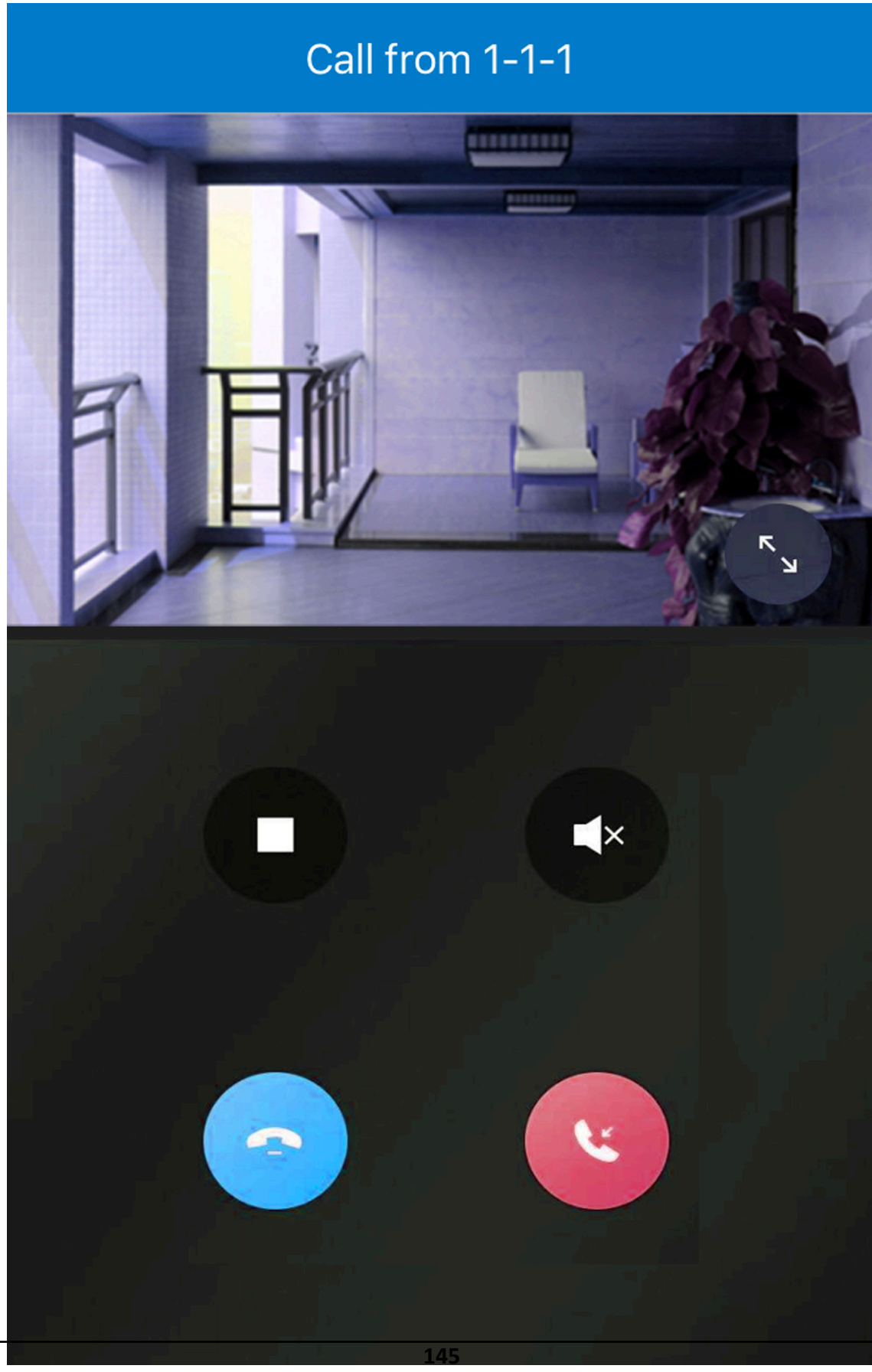


Figure 8-6 Call Page

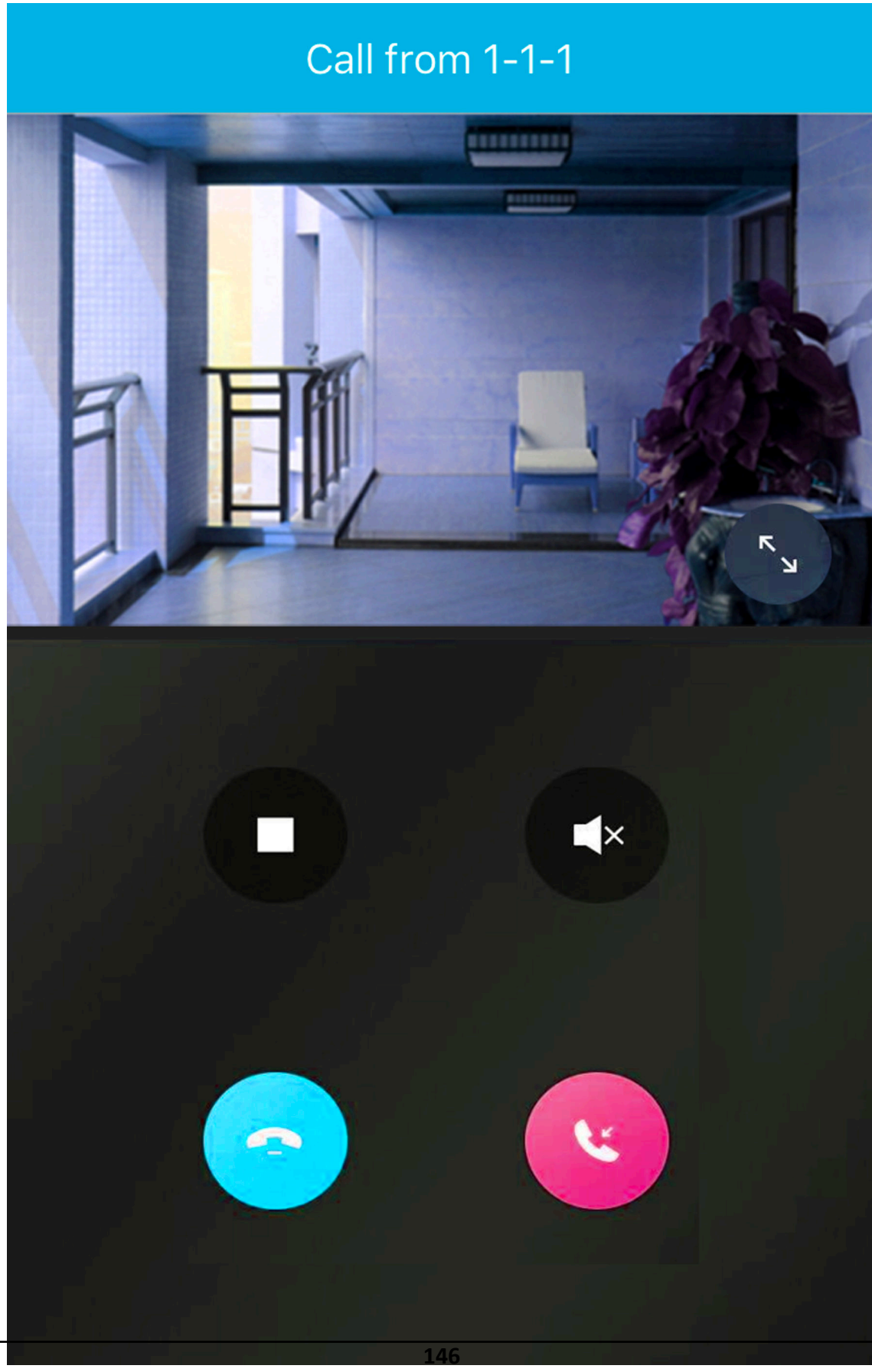


Figure 8-7 Call Page

2. Answer the call.
3. Perform the following operations.

Option	Description
Stop/Restart Live View	Tap to stop the live view. And tap to restart it.
Mute	Tap to mute the live video.
Open Door	Tap to open the door.
Digital Zoom	Pinch two fingers together to zoom in the live video image, and spread them apart to zoom out.

8.2 How to manage door bells?

8.2.1 How to set motion detection alarm for Wi-Fi doorbells?

Motion detection is a way of detecting motion in a security scene by analyzing image data and differences in a series of images. After setting motion detection area for Wi-Fi doorbell, the device will be able to detect the object in motion and at the same time the Mobile Client will receive an event notification about the motion detection alarm.

1. On the device list page, tap to enter the Settings page of the Wi-Fi doorbell.
2. Tap **Notification** to enter the Notification page.
3. Draw motion detection area.
   - Tap **Draw Motion Detection Area** to enter the Motion Detection Area page.

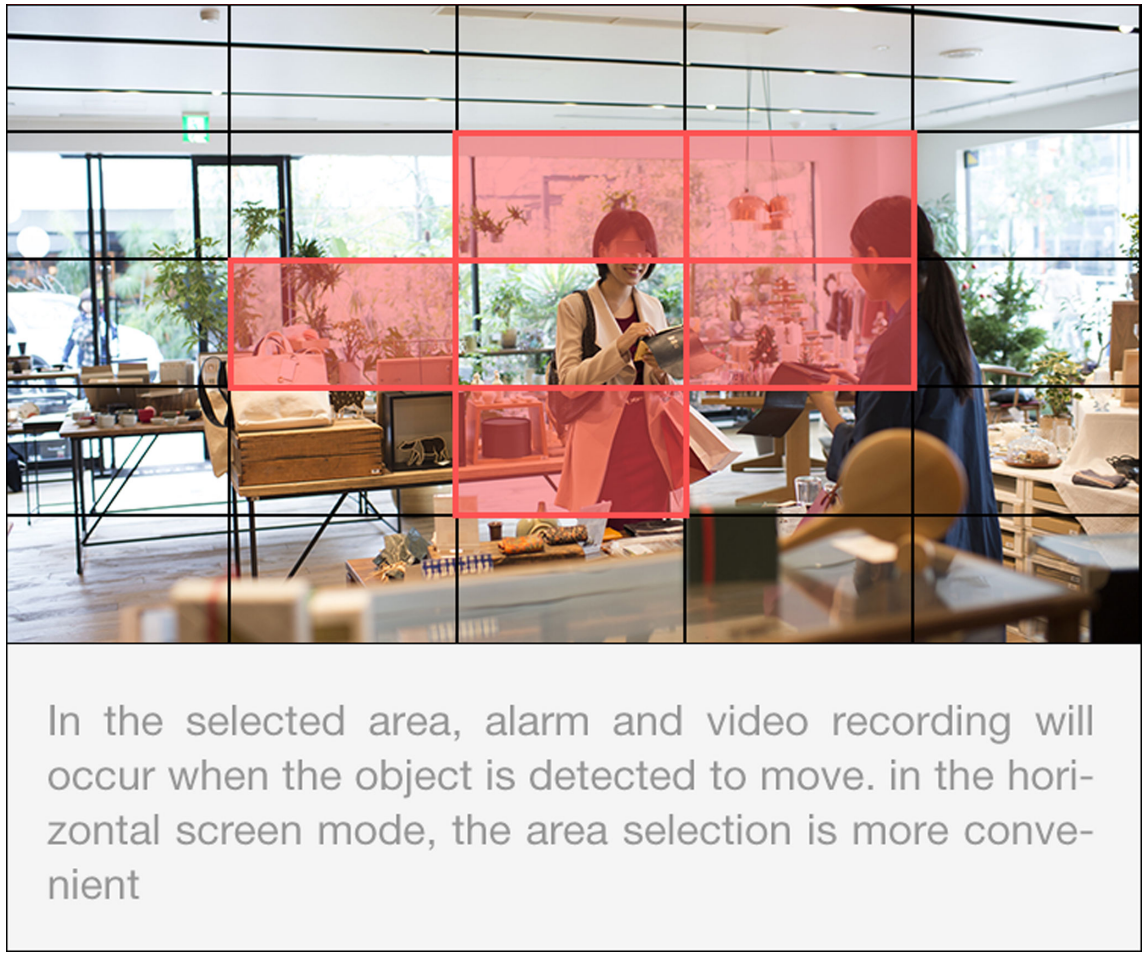


Figure 8-8 Draw Motion Detection Area

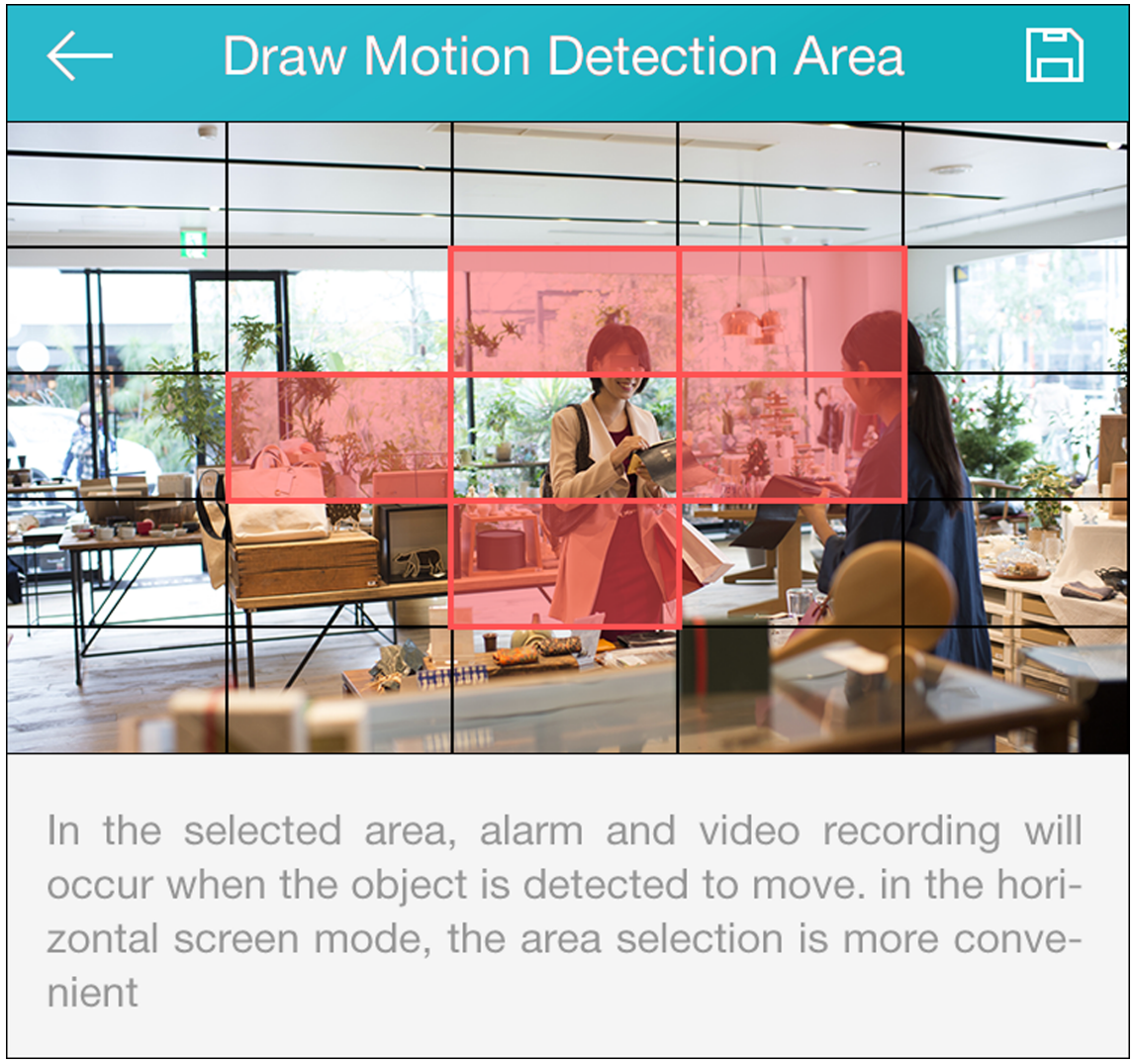


Figure 8-9 Draw Motion Detection Area

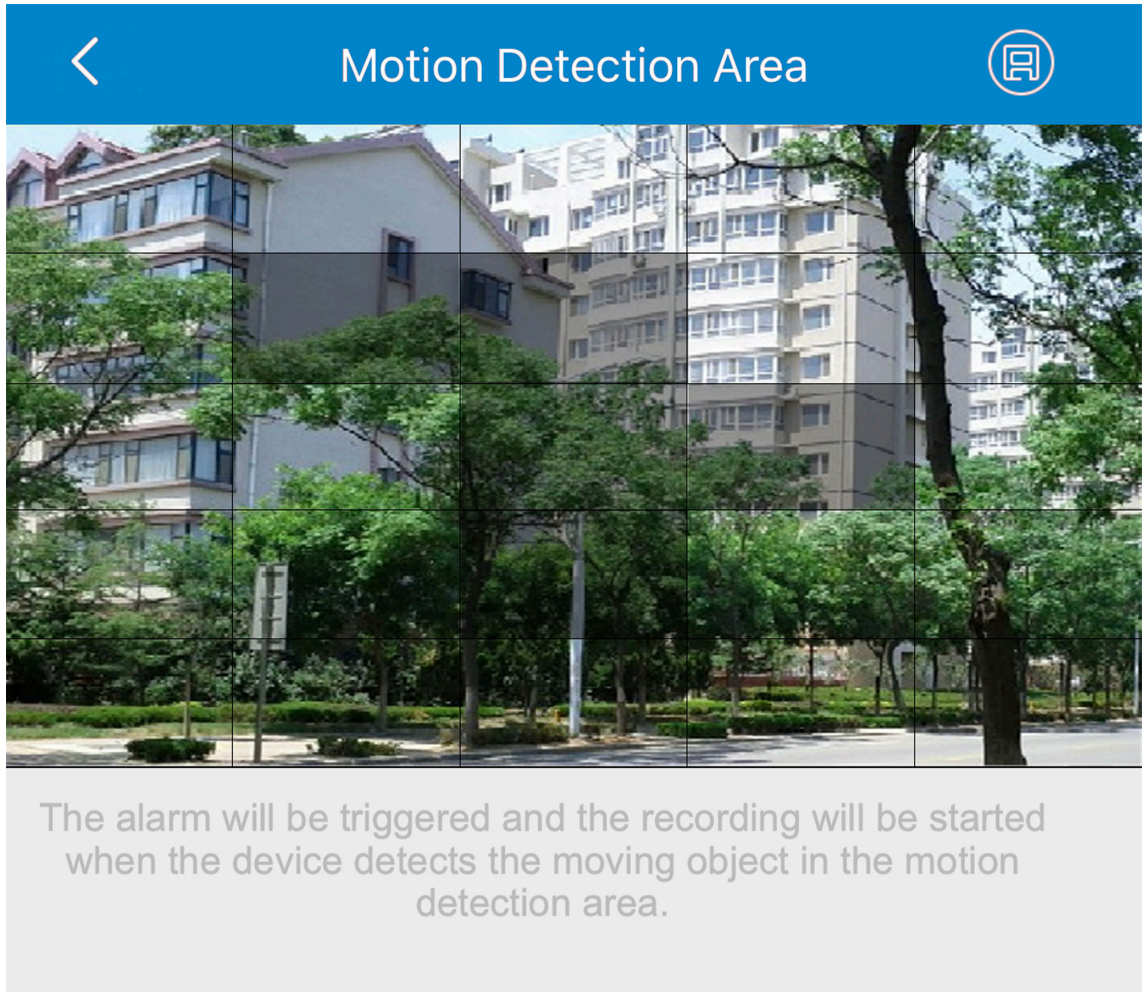


Figure 8-10 Draw Motion Detection Area

- Tap the grid(s) on the live video image to select the motion detection area.
- Tap to save the settings.

4. Tap **Motion Detection Sensitivity** on the Alarm Notification page and then drag the slider to adjust the sensitivity.
   - **Low**: Moving persons, large moving pets, and any other large moving objects in the motion detection area will trigger the alarm, while smaller objects will not.
   - **Medium**: Moving small pets and any other medium-sized moving objects in the motion detection area will trigger the alarm, while smaller objects will not.
   - **High**: Moving insects, moving leaves, and any other larger objects will trigger the alarm.

Go back to the Notification page and make sure **Notification** is enabled.

8.2.2 How to link smart chimes with doorbells?

You can add a smart chime to the Mobile Client and link it with a doorbell so that the doorbell will standby for longer and be more responsive.

Add a Smart Chime

- To add an EZVIZ smart chime, tap + → **Scan QR Code** on Hik-Connect. Select Doorbell as the Device Type, enter the serial number, tap **Add**.
- You can also tap + → **Manual Adding** to add a smart chime.

After adding a smart chime, you can tap the smart chime in the device list to mute all devices with one tap and enable/disable Ring Alert for linked doorbells.

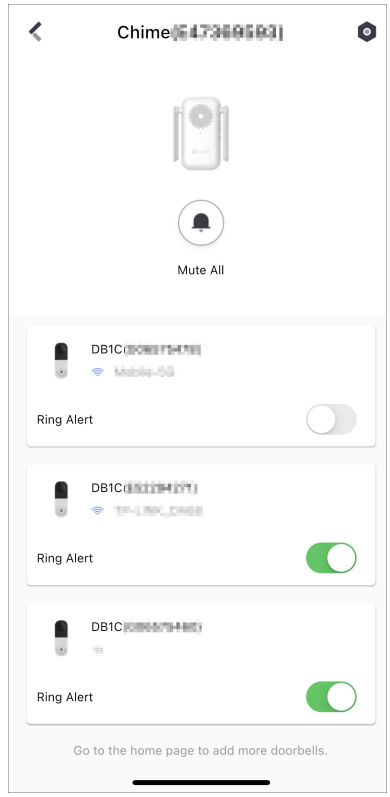


Figure 8-11 View Smart Chime

Link Smart Chime with Doorbell

- After successfully adding a smart chime, tap **Next** and link the smart chime with up to two doorbells.



Figure 8-12 Link Doorbell

- You can also go to the doorbell Settings page and tap **Chime Type → Smart Chime** to link a smart chime with the doorbell.

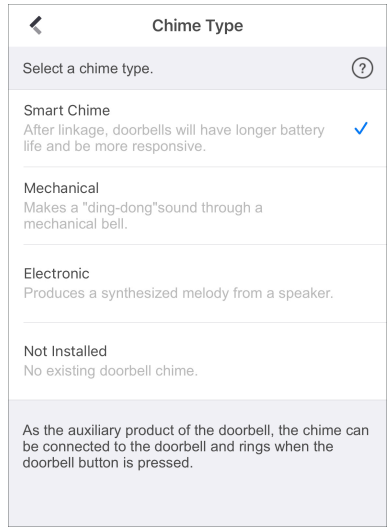


Figure 8-13 Link Smart Chime

Note

When you link a smart chime with a doorbell, make sure they are near to each other and they are both online.

Chapter 9 Network Devices

After your service provider hands over network devices and security devices, you can use the Mobile Client to configure them together.

9.1 What are network devices?

1. Cameras and APs: APs extend the wireless coverage of the network, allowing wireless devices like network cameras to connect to the network. Network cameras and APs are connected to the network infrastructure through PoE switches, ensuring they have both power and network connectivity.
2. PoE Switch: Provides power and data connectivity to APs and cameras. This simplifies the deployment of APs by eliminating the need for separate power supplies.
3. Aggregation Switch: Collects data traffic from multiple sources, including PoE switches (and thus, from APs and cameras connected to those switches) and directs it towards the network's core or NVRs for storage and analysis. The switch manage large volumes of data and may implement quality of service (QoS) policies to prioritize video traffic, ensuring high-quality video recording and playback. It supports VLAN tagging and can enforce VLAN policies, ensuring that data from different VLANs remains separate as it moves through the network.
4. AC Router (combing AC and router): Offers both routing capabilities to connect the local network with the public internet and include AP management. It also supports VLANs, allowing for different routing rules based on VLAN membership, which might include restricting external access to sensitive VLANs or applying different NAT policies.
5. Connectivity to the Public Network: This connectivity is typically provided through the AC router. It enables remote access to the NVRs or network cameras for video monitoring and system management.

9.2 What are AC router operations?

After you add the AC router and initialize the network, you can perform some operations, including rebooting and remotely configuring the device.

On AC Router Device Card

On an AC router device card, you can view the number of APs and clients, uplink & downlink rates, and tap buttons for resetting the password, editing the device name, remotely configuring the device, and setting the Wi-Fi netowrks (host and guest Wi-Fi networks).

On AC Router Device Details Page

You can tap an AC device card to view its details such as the port status, the uplink & downlink bandwidth utilization rate, and the Wi-Fi list. You can perform the following operations.

Operation	Description
One-Tap Network Optimization	Quick optimize the wireless network performance.
Reboot Device	Tap to reboot the AC.
Configure Wi-Fi	Tap a Wi-Fi to set its name, encryption mode, frequency band, and VLAN ID.
Configure AC	Tap to remotely configure the AC, including setting the LAN, Wi-Fi, password, and health status.
View Diagram Explanation	Tap to know what different types of diagrams mean.

Table 9-1 List of Ports, APs, and Clients

Type	Description
Port	• You can view the port type (WAN/LAN), port name, IP address of WAN port, connection status, uplink & downlink rate, negotiation rate, and peer device. • You can tap a WAN port to go to the WAN settings page.
AP	• You can view the AP name, IP address, online/offline status, connected clients, MAC address, and number of Aps. • Tap an AP to go to the AP details page • Tap → **Find Me** to manually make the AP indicator flash to find the AP. • Tap → **Reboot** to reboot the AP. • Tap 0 to view the client list of an AP. • Tap **AP Indicator Switch**to turn on/off the indicators of all APs.
Client	• You can view the client name, connection mode, connected AP, and uplink & downlink rates. • Tap a client device to jump to its details page.

9.3 What are cloud AP operations?

Unified Wi-Fi Settings for Cloud APs on Site

For cloud APs added to the site, you can set one or more Wi-Fi networks (up to 8) for these cloud APs. For each Wi-Fi network, you can select one or more cloud APs to apply the Wi-Fi settings.

One Tap to Adopt New APs on Site

For new APs found on the same LAN as your phone's, you can tap to adopt these new APs, which is to activate the APs, set the APs to cloud mode, and add the APs to the site.

9.4 What are network switch operations?

On the device list, tap the switch card to enter the device details page.

VLAN Management

Virtual Local Area Networks (VLANs) are used to partition a physical network into smaller, isolated subsections. By isolating devices within a VLAN, network administrators can restrict communication between devices in different VLANs to reduce the risk of unauthorized access or data breaches, and easily troubleshoot issues to reduce downtime.
For example, a company has multiple departments, such as Marketing, Finance, IT, and Human Resources, all located on different floors of the same building. The company has a single physical network infrastructure, and all devices are connected to the same network. The company wants to ensure that each department's network traffic is isolated for better performance, security, and manageability. To achieve this, the network administrator decides to implement VLANs.
This section will guide you through configuring VLANs without going to the device's web configuration page.

1. Tap ⚙ in the upper right corner of the switch detail page, and then tap **VLAN**.
2. Create a VLAN on your switch.
   a. Tap **VLAN ID → Add** .
   b. Select an adding mode.
   c. Set the VLAN ID to identify and differentiate VLANs within a Layer 2 network domain, and tap **Save**.

   Note

   - The maximum number of VLANs that can be added in a batch varies with device models.
   - VLAN ID 1 and 4095 are typically reserved for special purposes. VLAN ID 1 is typically used for the default VLAN. Most switches are assigned to the default VLAN by default if no other VLAN is specified. VLAN ID 4095 is reserved for the use of VLAN trunking protocols. It is not used for regular VLAN traffic.
3. Assign ports to the VLAN to enable logical segmentation of the network.
   a. Tap **Configure**, and select the desired ports.

   Note

   The VLAN configuration is not allowed for ports in an aggregation group. Aggregation groups, also known as link aggregation or port trunking, are used to combine multiple physical ports into a single logical port to increase bandwidth and provide redundancy.
   b. Select a port VLAN type.

Note

Port Type	Description	Following Operation
ACCESS	Used to connect devices that need to connect devices that need to communicate within a single VLAN. An access port is like a door that leads directly into a specific room (VLAN). When you enter through that door, you can only communicate with the people inside that room. For example, if you have an access port assigned to VLAN 10, any device connected to that port can only communicate with other devices.	None
TRUNK	Used to connect devices that need to communicate with multiple VLANs. A trunk port is like an elevator in the building. The elevator can carry people (data) to multiple rooms (VLANs) based on the floor (VLAN tag) they want to go to. For example, if you have a server that needs to communicate with devices in VLANs 10, 20, 30, you would connect the server to a trunk port. The trunk port would carry traffic for all the three VLANs, and the VLAN tags in the data packages would help the switch determine which VLAN the traffic belong to.	Set the accessible VLANs. For example, consider a switch with VLANs 10, 20, and 30. If you have a trunk port connecting to a server, you might only want the server to communicate with devices in VLANs 10 and 20, but not VLAN 30. In this case, you would configure the trunk port to have VLANs 10 and 20 as accessible VLANs, while excluding VLAN 30.

c. Set the PVID (Port VLAN ID) to ensure untagged traffic is routed to the correct VLAN, and tap **Save**.

Note

The PVID is used to used to determine which VLAN an incoming packet belongs to when the packet does not carry any VLAN tag. In simpler terms, the PVID is the default VLAN assigned to a switch port. When a device connected to that port sends a packet without a VLAN tag, the switch will associate the packet with the VLAN specified by the PVID. For example, consider a switch with VLANs 10, 20, and 30. If you have a port connected to a device that doesn't support VLAN tagging, you can assign a PVID to that port. If the PVID is set to VLAN 10, any untagged traffic received on that port will be considered part of VLAN 10 and forwarded accordingly.

Available Operations

Perform the following operations according to your requirements.

Operation	Description
Reboot Switch	Tap to reboot the switch.
View Peer Device	Tap **Device** to view the details of the device connected to this port.
Clear Alarm	For port with alarm(s), tap → **Clear Alarm** to clear the alarm(s) of this port.
Restart Port	For the abnormal port, tap → **Restart Port** to restart this port.
Enable/Disable Extend Mode for Port	Tap **Enable Extend Mode/Disable Extend Mode** to extend or not to extend the transmission range of this port. **Note** After enabled, the transmission range of the port will be extended to 200 to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.
Detect Cable Status	Tap → **Cable Detection** , tap a port, and then tap **Detect**. When the detection is finished, you can view the detection result and cable length.

Chapter 10 Notifications

10.1 How to enable notifications?

You can allow the Mobile Client to receive and push notifications of the events detected by a device, services, exceptions, etc. If you want to block notifications during specific time, you can set a notification schedule to define the time period(s) during which the Mobile Client is allowed to receive event information and push them to you. You can also set notification mode to avoid the disturbance of push notifications (and the audio and strobe light alarm) while still being able to receive information on the Notifications page.

Make sure you have configured event settings on device (except for the video intercom device). See the user manual of the device for details.

Note

- For Android, make sure your phone supports Google Play service, or notifications may fail to be pushed to you.
- For iOS, when Critical Alerts is enabled, you will get notifications on critical alerts even if your device is muted or in Do Not Disturb mode. You can enable Critical Alerts for the Mobile Client in **Settings → Notifications** of iOS.

  Note

  Critical Alerts requires iOS 12 or later.
- The Mobile Client will ignore alarm events triggered out of the time period defined by the notification schedule.
- The security control panel does not support setting notification schedule.
- For specific thermal device, you can also set custom voice prompt for the detected events, such as fire detection.

1. On the device list page, tap ••• → **Settings** to enter the Settings page of the device.
2. Tap **Notifications** to enter the Notification page.
3. Turn on **Notifications** to allow the Mobile Client receive and push notifications of events detected by device all the time.
4. Select a notification mode.
   - For normal devices, select one of the following two modes.
     - **Receive Events and Push Notifications**: The Mobile Client will receive event information from the device and push related notifications in real time. In other words, you can not only get notified by the push notifications, but also view all the received event information in Notification page.
     - **Receive Events but NOT Push Notifications**: The Mobile Client will receive event information in real time from the device but NOT push related notifications. In other words,

although you will NOT be disturbed by the event-related push notifications, you can view all the received event information in the Notification page.

- For audible strobe light, select one of the following two modes.
  - **Receive events and push notifications, and allow Audio and Strobe Light alarms on device**: The Mobile Client will receive event information from the device, and push related notifications in real time. And the audio and strobe light alarm is allowed to be triggered on the device once an event is detected. In other words, you can not only get notified by the push notifications and the audio and strobe light alarms, but also view all the received event information in the Notification page.
  - **Receive events but NOT push notifications, and NOT allow Audio and Strobe Light alarms on device**: The Mobile Client will receive event information from the device in real time, but NOT push related notification. And the audio and strobe light alarm is NOT allowed to be triggered on the device once an event is detected. In other words, although you will NOT be disturbed by the event-related push notifications and the audio and strobe light alarms, you can view all the received event information in the Notification page.

5. Enable notification schedule to set a time schedule for receiving event information from the device and push related notifications (if allowed in the previous step).
   - Tap **Notification Schedule**.
   - Tap **Set a Time Schedule** to enter the Schedule Settings page.

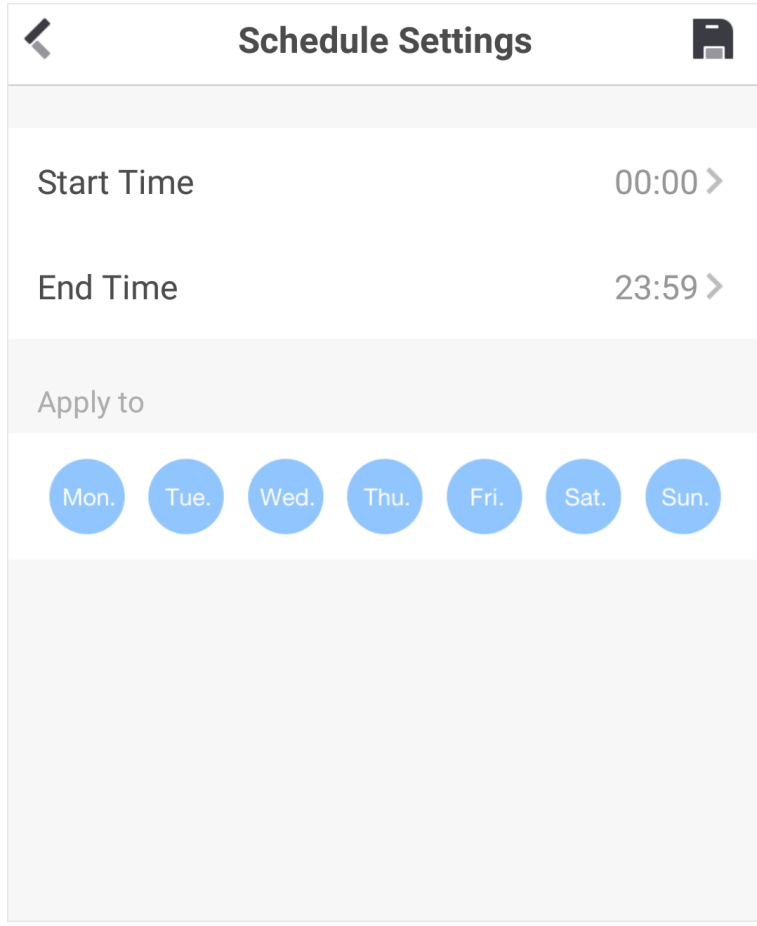


Figure 10-1 Schedule Settings Page

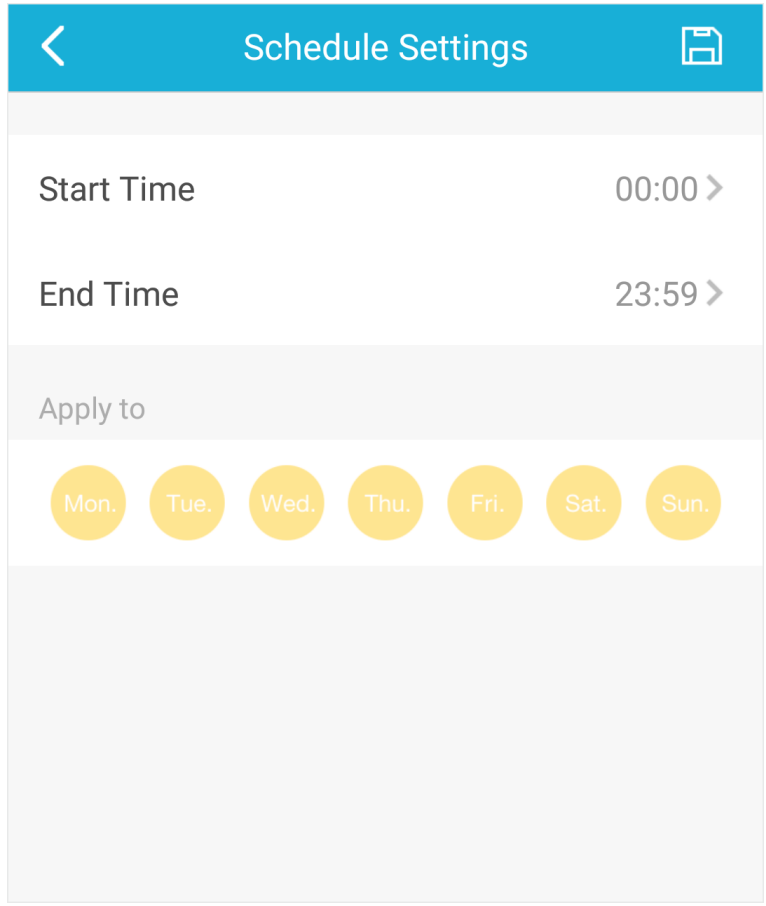


Figure 10-2 Schedule Settings Page

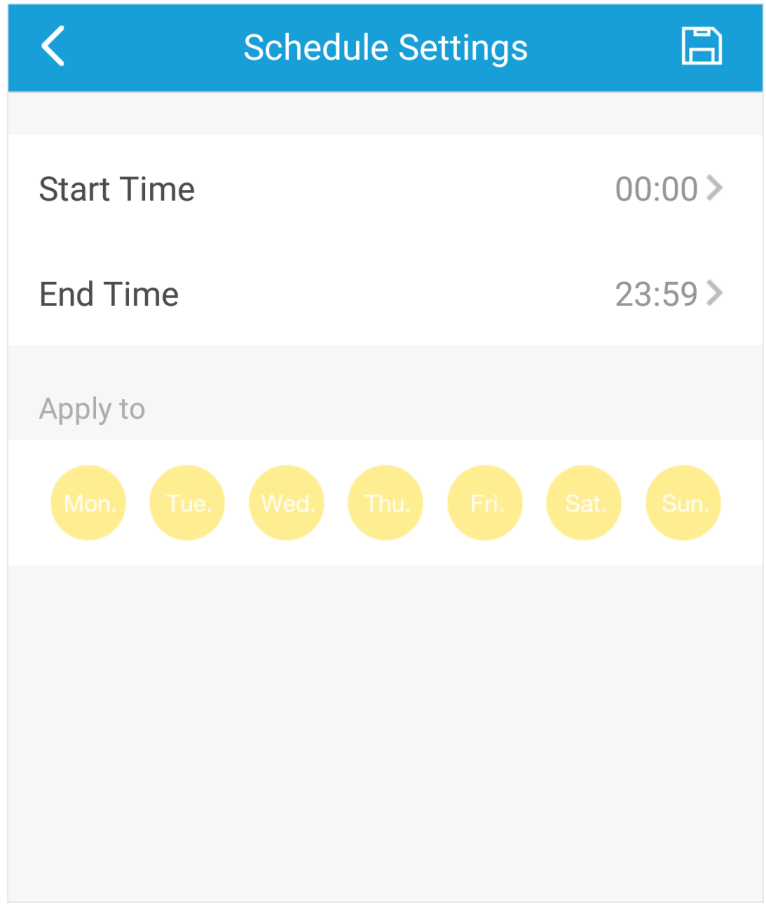


Figure 10-3 Schedule Settings Page

- Set the start time and the end time.
- Select the date(s) to which the configured time period applies to.

Note

The date(s) marked in blue is selected.

- Tap .
- Tap the configured schedule to enter the Schedule Settings page, and then edit the start time, end time, and the date(s) to which the configured time period applies to. Or tap **Delete** to delete the schedule.
- Go back to the Notification page.

6. Tap **Notification Sound Mode** and then select one of the following sound mode and tap to set a notification sound mode for the detected intrusion.

Note

The function should be supported by the device.

- **Intensive**: Intense warning for the intrusion.
- **Soft**: Soft warning for the intrusion.
- **Mute**: No audible warning.

10.2 How to set notifications?

Tap **Notification → Settings** to open the Settings page.

Device Notification

If it is enabled, the Mobile Client will receive and push events notifications detected by devices.

Alarm Audio Notification

If it is enabled, the Mobile Client will receive and push alarm notifications.

For **Alarm Audio Settings**, you can set the alarm audio type for specified alarm devices including voice, ring tone, and customized alarm audio, and you can add an audio file to customize the alarm audio.

Call Notifications

If it is enabled, the Mobile Client will receive and push call notifications when someone calls.

You can also set notification parameters for specified devices on the Call Notification Settings page.

Device Exception Notifications

If it is enabled, the Mobile Client will receive and push the exception notifications of your devices that are managed by the Service Provider.

Service Provider Notifications

If it is enabled, the Mobile Client will receive and push the notifications related to services offered by your Service Provider via the Hik-Partner Pro platform.

10.3 How to set AI notifications?

Leveraging AI's natural language understanding, the system turns your everyday descriptions into custom alert rules—so you'll get timely notifications for the events you care about. For non-customized motion detection events with AI service enabled, notifications now include a description like "A man in black placed a package at the door."

Go to **Notifications**.



Figure 10-4 AI Notification

1. **Natural Language Input:** Describe an alert scenario in plain text, e.g., "Alert me if the passageway at entrance is obstructed by any objects".
2. **Effect Preview:** After configuration, the system instantly check matching results from the past 24 hours to verify accuracy, and then presents a structured rule for your review and fine-tuning.
3. **AI Processing:** The system automatically identifies targets (person/vehicle), behaviors (appear/linger/loiter).
   - Supports a maximum of 16 rules per channel.
   - Only available for channels with the Video AI service enabled.

10.4 How to view and handle notifications?

10.4.1 How to view and handle event notifications?

You can check event notifications on the Notification page when events are detected by the devices. The unread notifications are marked with a red dot.

- Set event parameters for the device and arm the device. For details, see the user manual of the device.
- For indoor station, it should have been linked to the sensor. For details, see the user manual of the video intercom device.

1. Tap **Notifications → Event** to enter the Event Notifications page.
2. Tap and then select a date and (or) select a device to filter the events.
3. Tap an event notification to show the detailed information such as time and source.

Option	Description
View and Download Event-related Picture	If there are multiple event-related pictures, you can swipe left/right to switch pictures. You can also tap a picture and then tap to download the picture.
Zoom In/Out Event-related Picture	Tap the picture, and then spread two fingers apart to zoom in the picture and pinch them together to zoom out, or double-tap the picture to zoom in or zoom out. **Note** - Make sure you have configured the event linkage action for capturing event-related picture for the device. See the user manual of the device for details. - If you have enabled Video and Image Encryption for the device, you need to enter the device verification code before you can view the picture.
View Event-related Video Footage	Tap **Playback** to view the video footage. **Note** Make sure you have configured the event linkage action for recording video for the device. See the user manual of the device for details.
View Live Video	Tap **Live View** to view the live video of the device. **Note** The device should support this function.
View External Linked Video	Tap **External Linked Video** to view the video footage recorded by the device's externally linked device. For example, if a camera is linked to a detector, once the detector detects an event, the camera will record video footage. **Note** - Such a linkage (the configuration is called as "Configuring Linkage Rule) can be set by a Service Provider on Hik-

Option	Description
	Partner Pro. For details, see the *Hik-Partner Pro Portal User Manual*. - Only the Service Provider on Hik-Partner Pro can configure such a linkage.

4. Go back to the Notifications page and then edit the event information.

Option	Description
Mark All Events as Read	Tap ••• → **Mark as All Read** , and then tap to mark all event information as "already read".
Clear All Events	Tap ••• → **Edit** → **Clear All** to clear all event notifications.
Delete a Specific Event	Tap and hold an event notification until a prompt pops up, and then tap **Delete** to the prompt to delete the notification. Or, swipe from the right end of the card that displays the event notification towards the left, and then delete this event notification.

10.4.2 How to view and handle service notifications?

Hik-Partner Pro is a cloud service platform for the Service Providers (installation companies) that configure and maintain your devices and provide value-added services for you. In **Notifications** → **Service** , you can view the notifications related to services offered by your Service Provider via the Hik-Partner Pro platform, including applications for device handover, device authorization and permissions, and device password reset. You can also view notifications about cross-device linkages, device exceptions and corresponding handling results, and logs about Service Provider's operations on your devices.

How to accept invitations to be site owner?

You can tap on an invitation to view the details such as the site and the devices authorized to the Service Provider, and then tap **Agree** to accept the invitation and therefore become the owner of the site.

How to approve device handover and authorization applications?

If a Service Provider hands over devices to you or applies for device permissions on the Hik-Partner Pro platform, you will receive an application notification. After you approve the application, the

Service Provider will be able to provide device configuration and maintenance services based on the permissions you granted.

- If the Service Provider hands over devices to you, you will receive device handover and authorization applications.
- If the Service Provider applies for device permissions, you will receive device authorization applications.

1. Go to **Notifications → Service** .
2. Tap on a Device Handover and Authorization Application notification.
3. Accept device handover.

Note

After handover, your Service Provider does not have any permissions to operate or configure the devices. Service Provider usually applies for device permissions so as to configure and maintain the devices for you. If your Service Provider has applied for the permissions, you need to accept it in device authorization application.

4. Open the Device Authorization Application.
   - If the Service Provider has applied for device permissions when handing over the devices, the device authorization application will show up right after you accept device handover.
   - If the Service Provider has not applied for device permissions, open the application after the Service Provider sends one.

Note

In device authorization application, you can view details such as Service Provider information, permissions that the Service Provider applies for, and the Alarm Receiving Center (ARC) information.

5. Select the permissions you want to grant to the Service Provider.

Note

   - If the Service Provider enabled ARC service for you, you can check **ARC Service** to activate it.
   - If you activate ARC service, the ARC will provide 24/7 alarm responding service for you, including receiving events from devices, responding to events, and sending out emergency dispatches (if needed).

6. Tap **Agree** to approve the application.

10.4.3 How to view and handle other notifications?

Tap **Notifications** to enter the notifications page.

- You can see all exception notifications in **Notifications → Exception** . You can receive and view the exception notifications of your devices that are managed by the Service Provider.
- Go to **Notifications → System** to view linkage notifications. Under system notifications, you can view linkage notifications. Linkage refers to the process in which an event detected by a resource triggers actions in other resources. The linkage can be used for notifying security personnel,

upgrading security level, saving evidence, etc., when specific events happen. You can view notifications about linkages in Service Notifications. You can tap on each notification to view the detected event, event time, devices in the linkage, and triggered actions.

Note

- This feature is not available in all countries or regions.
- The linkage can only be set by the Service Provider via the Hik-Partner Pro platform.

- Tap **Notifications → Pyronix** to view Pyronix notifications.
- Tap **Notifications → Call** to view call notifications.

Chapter 11 Services

You can invite a service provider to link with your account, so that your service provider can provide you with value-added services.

11.1 View My Services

Go to → **Service Market** → **My Services** .

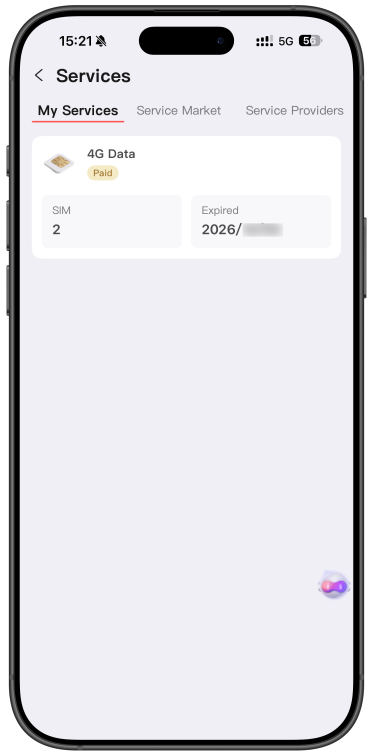


Figure 11-1 My Services

You can view all services active, activated channels for each service, and service expiry date.

Tap a service card to view more details.

11.2 View Service Market

Go to → **Service Market** → **Service Market** .

Tap a service to view details.

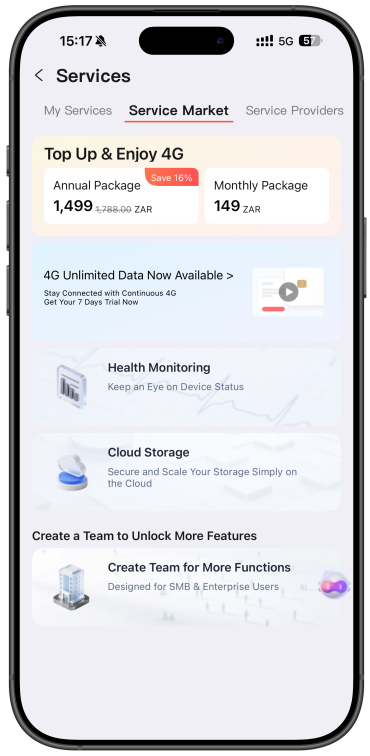


Figure 11-2 Service Market

11.3 Invite a Service Provider to Manage Your Devices

Register an account and invite service providers to link with your account. They can offer value-added services with assigned permissions, which can be revoked whenever needed.

Go to → **Service Market** → **Service Providers** .

Enter the email of a service provider, and tap **Confirm**.

Select permissions for the service provider, and tap **Confirm**.

Service Management Permission

The service management permission is selected and set as **Permanent** by default and can not be changed.

System Access Permission

The system access permission can be set to **1 Hour**, **2 Hours**, **4 Hours**, **8 Hours**, **Permanent**, and **Custom Days**, and the maintenance personnel or service provider can only log in to the platform within the validity period.

An invitation will be sent to the service provider. After the invitation is accepted, you can perform the following operations.

View Service Provider Information	After a service provider accepts the invitation, you can view the service provider's information including the email, phone number, account name, and location by tapping the name of the service provider.
Activate License to Expand Capacity or Renew Services	1. Tap ⋮ → **Activate License** , enter the license code, and tap **Verify**. 2. Select **Expand Capacity** or **Renew**. After a license is activated, tap **Activate License → View License Activation Records** to view the activation details.

11.4 Manage 4G SIM Data Service

Please long press to view the ***video demonstrations of these steps*** .

In this article, you will learn:

- ***How to get started with the 4G SIM data service?***
- ***How to renew the service?***
- ***How to view my order?***
- ***How to subscribe to / unsubscribe from the service?***
- ***How to check 4G data notifications?***
- ***How to use the AI assistant?***
- ***How to contact the customer service via email?***

Note

1. **Unlimited Data Service:** This 4G SIM Data Service plan provides unlimited data usage specifically for the connected Hikvision 4G camera, ensuring stable operation of core functions like live video streaming and playback.
2. **Device-Specific Use:** This SIM card is designed exclusively for Hikvision 4G cameras and must not be inserted into mobile phones, tablets, routers, or any other unauthorized devices.
3. **Violation Consequences:** Any breach of these usage rules will result in the user bearing full responsibility for all resulting consequences and legal liabilities.
4. The specific SIM data services are governed by the applicable local service provider's terms.

11.4.1 How to get started with the 4G SIM data service?

What are the supported device models of the 4G service?

Table 11-1 Supported Device Models

Device Name	Model
4MP 24/7 Solar 4G Camera	DS-2CFS04/4G
4MP 24/7 Solar 4G PT Camera	DS-2CFSP4/4G
8MP 24/7 Solar 4G Dual-lens PT Camera	DS-2CFSP8-D/4G

How to add a 4G AOV camera and get a free trial service?

Before You Begin

Before you begin, please make sure a SIM card is inserted to your camera.

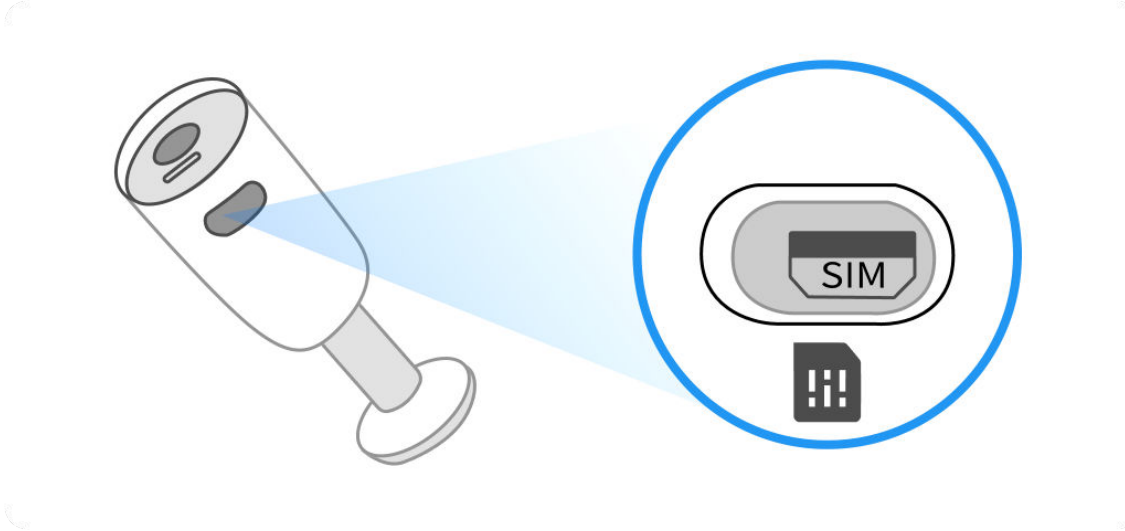


Figure 11-3 Card Location of DS-2CFS04/4G

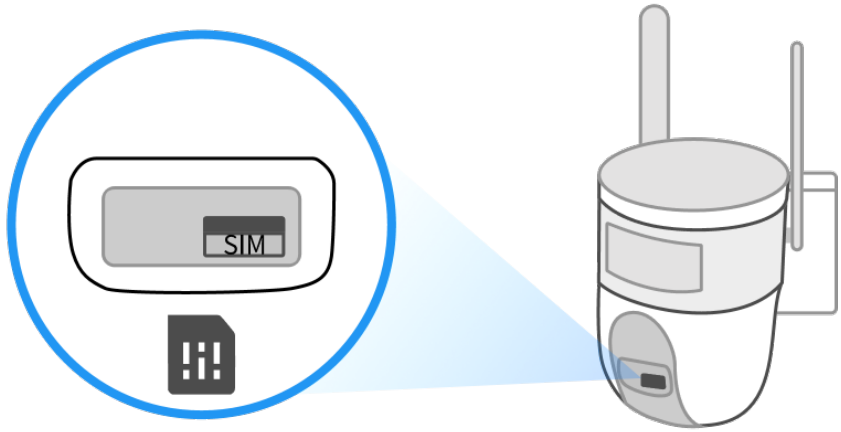


Figure 11-4 Card Location of DS-2CFSP4/4G and DS-2CFSP8-D/4G

Steps

1. On the Home page, tap + .
   - Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
   - Make sure the device has been activated and connected to Hik-Connect service.

Table 11-2 Methods of Adding Devices

Adding Methods	Application Scenario
Add by IP Address or Domain Name	- You can use the method if you know the IP address or domain name of a device. - Only encoding devices mapped in WAN support this function. - When you need to share devices via QR code. Download or update the Hik-Connect Mobile Client (version 4.5 and later), so you can share the device by sending the QR code generated after the device setup.
Add by Scanning QR Code	You can add a device to a site by scanning the QR code on the device.
Add by Entering Serial No.	If a device is connected to Hik-Connect service, you can manually add it to a site by entering the device serial number and device verification code. Enter the device serial number and device verification code.

Adding Methods	Application Scenario
	Note The device serial number and the default device verification code are usually on the device label. If no device verification code found, enter the verification code you created when enabling Hik-Connect service.

2. After the device is successfully added, you will get a 7-day free trial 4G unlimited service, and a window will pop up showing the expiration date of your free trial.

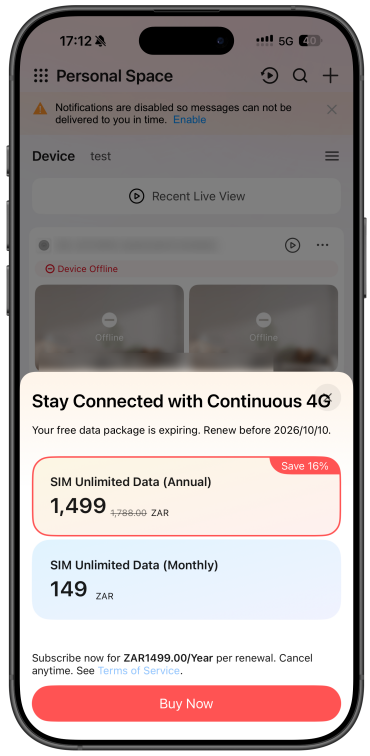


Figure 11-5 Trial Service

How to purchase the service?

- In the pop-up window, tap **Buy Now**.

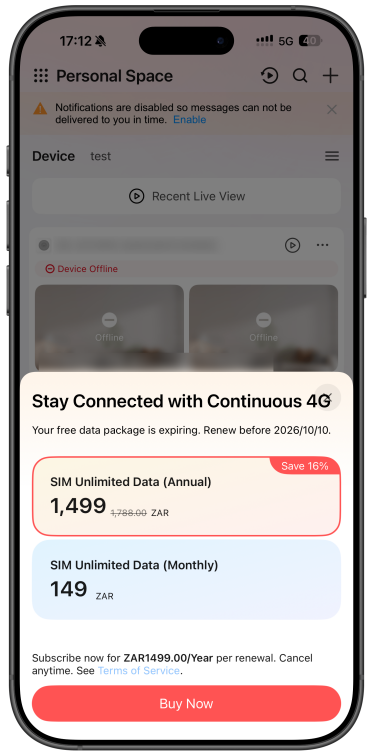
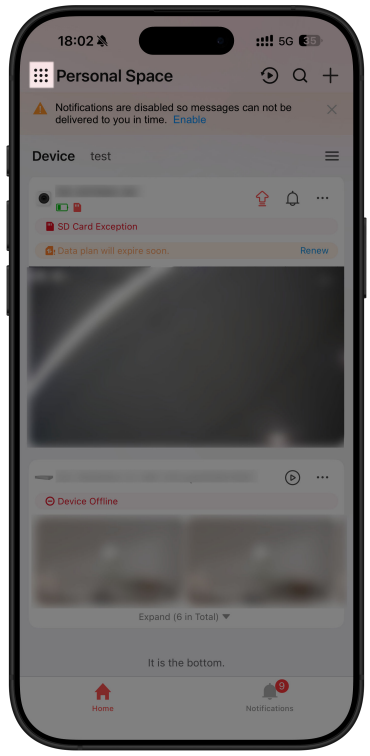
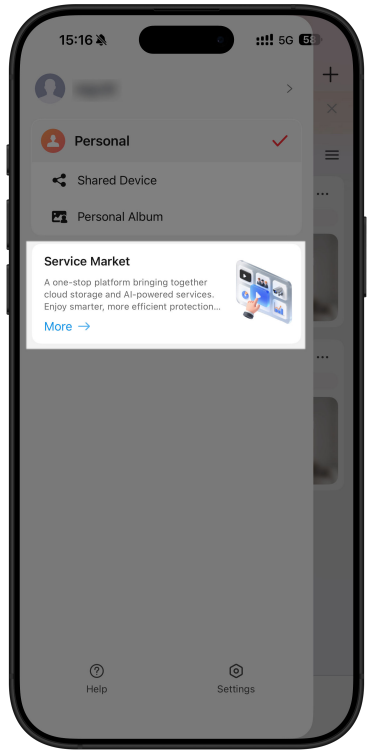
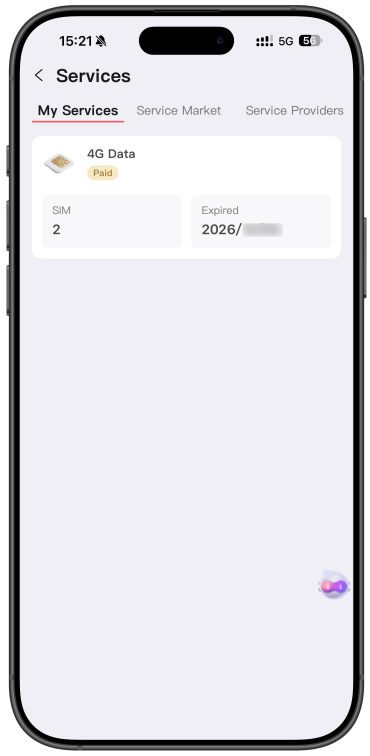


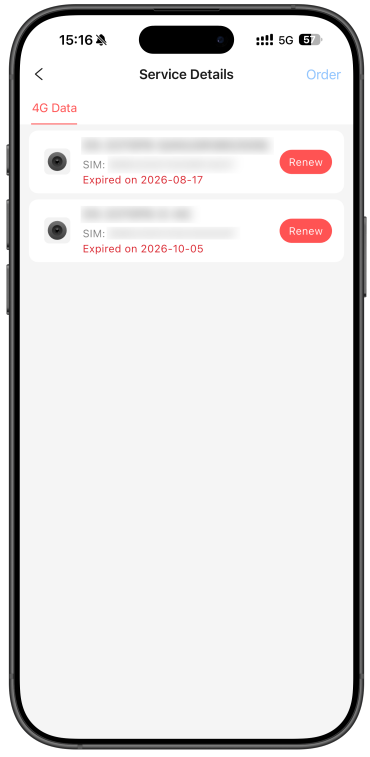
Figure 11-6 Trial Service

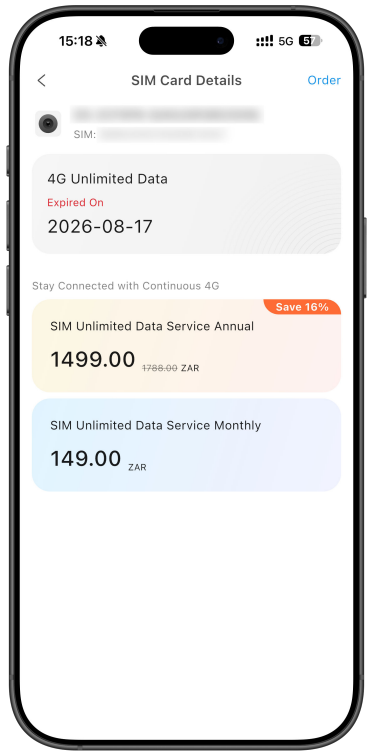
- Go to **Service Market**, select the card of interest, select a plan, and tap **Buy Now** to purchase the service.

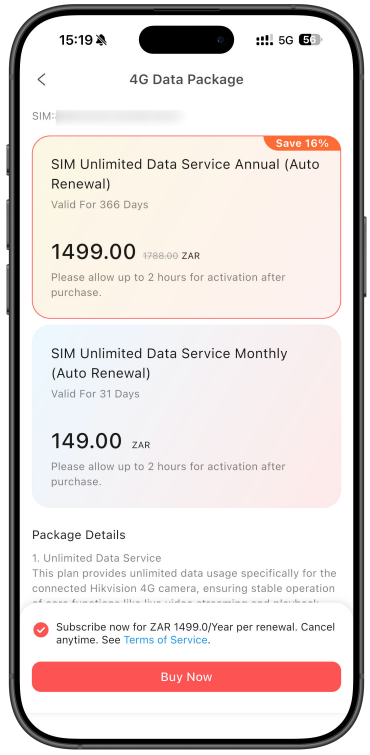

18:02
5G
Personal Space
Notifications are disabled so messages can not be delivered to you in time. Enable
Device test
SD Card Exception
Data plan will expire soon.
Renew
Device Offline
Expand (6 in Total)
It is the bottom.
Home
Notifications

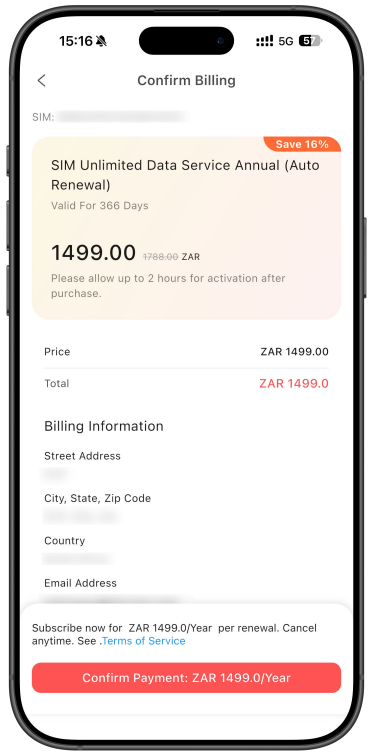

15:16
5G
Personal
Shared Device
Personal Album
Service Market
A one-stop platform bringing together cloud storage and AI-powered services. Enjoy smarter, more efficient protection...
More
Help
Settings

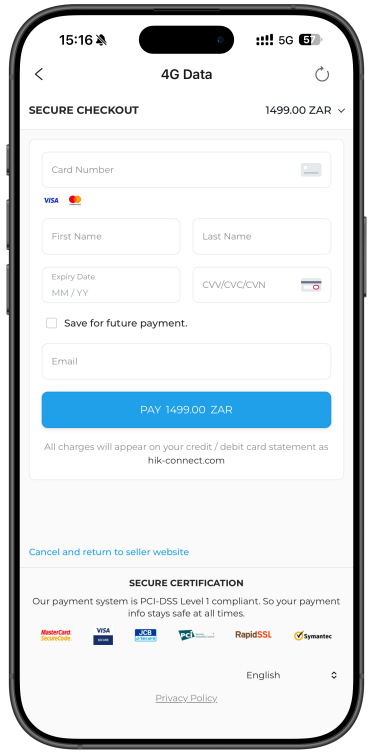

15:21
5G
Services
My Services
Service Market
Service Providers
4G Data
Paid
SIM
2
Expired
2026/


15:16
5G
Service Details
Order
4G Data
SIM:
Expired on 2026-08-17
Renew
SIM:
Expired on 2026-10-05
Renew


15:18
5G
SIM Card Details
Order
SIM:
4G Unlimited Data
Expired On
2026-08-17
Stay Connected with Continuous 4G
Save 16%
SIM Unlimited Data Service Annual
1499.00 1788.00 ZAR
SIM Unlimited Data Service Monthly
149.00 ZAR


15:19
5G
4G Data Package
SIM:
Save 16%
SIM Unlimited Data Service Annual (Auto Renewal)
Valid For 366 Days
1499.00 1788.00 ZAR
Please allow up to 2 hours for activation after purchase.
SIM Unlimited Data Service Monthly (Auto Renewal)
Valid For 31 Days
149.00 ZAR
Please allow up to 2 hours for activation after purchase.
Package Details
1. Unlimited Data Service
This plan provides unlimited data usage specifically for the connected Hikvision 4G camera, ensuring stable operation
Subscribe now for ZAR 1499.0/Year per renewal. Cancel anytime. See Terms of Service.
Buy Now


15:16
5G
Confirm Billing
SIM:
Save 16%
SIM Unlimited Data Service Annual (Auto Renewal)
Valid For 366 Days
1499.00 1788.00 ZAR
Please allow up to 2 hours for activation after purchase.
Price
ZAR 1499.00
Total
ZAR 1499.0
Billing Information
Street Address
City, State, Zip Code
Country
Email Address
Subscribe now for ZAR 1499.0/Year per renewal. Cancel anytime. See .Terms of Service
Confirm Payment: ZAR 1499.0/Year


15:16
5G
4G Data
SECURE CHECKOUT
1499.00 ZAR
Card Number
First Name
Last Name
Expiry Date
MM / YY
CVV/CVC/CVN
Save for future payment.
Email
PAY 1499.00 ZAR
All charges will appear on your credit / debit card statement as hik-connect.com
Cancel and return to seller website
SECURE CERTIFICATION
Our payment system is PCI-DSS Level 1 compliant. So your payment info stays safe at all times.
RapidSSL
Symantec
English
Privacy Policy

11.4.2 How to renew the service?

1. - If your service expires within 7 days or has expired within the past 7 days, a pop-up reminder will appear prompting you to renew the service on the live view / playback page.

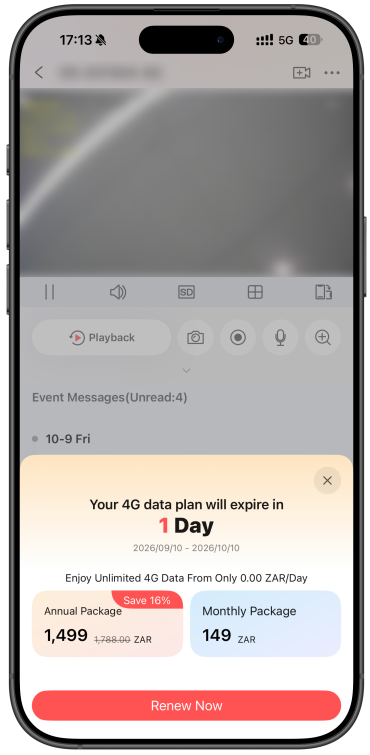


Figure 11-7 Pop-up Window for Service Renewal

- a. Tap ⁝⁝ → **Service Market → My Services → SIM** to enter the Service Details page.

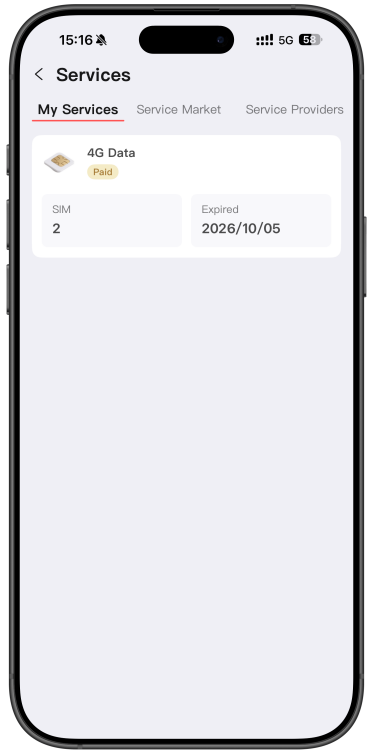


Figure 11-8 Services

b. Tap **Renew**.

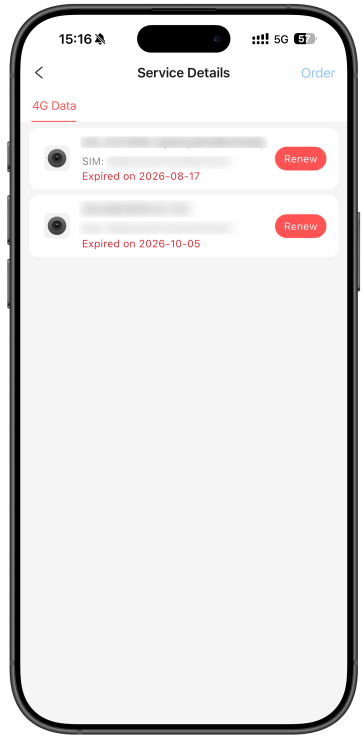


Figure 11-9 Renew

- Tap → **Service Market** → **Service Market** , and tap the banner to quickly renew your 4G SIM data service.

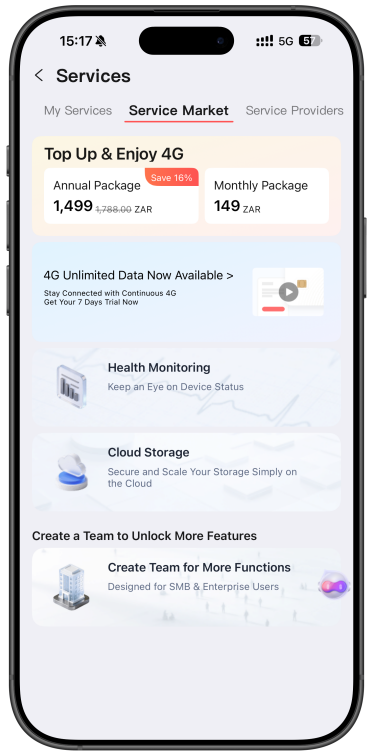


Figure 11-10 Service Banner

- Tap **Notifications → Value-Added Services → Renew** .

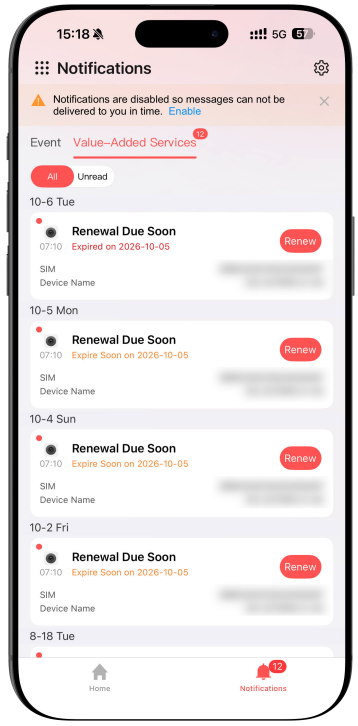


Figure 11-11 Renew Service

- Go to the device Settings page, and tap the 4G banner to enter the service page to renew the service.

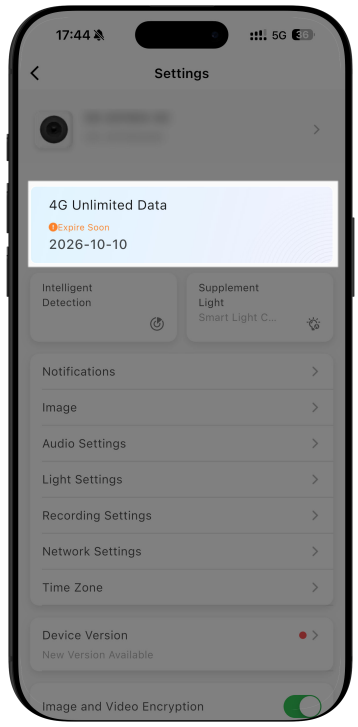


Figure 11-12 Services

2. Select a monthly or annual plan, tap **Buy Now** and confirm the payment.

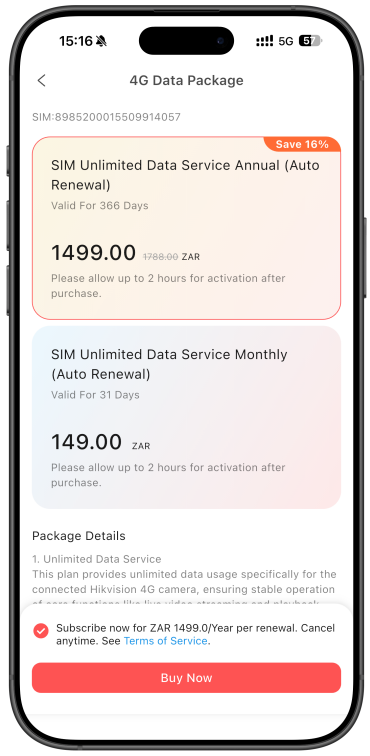


Figure 11-13 Buy Now

3. Enter your payment information to complete the purchase.

11.4.3 How to view my order?

1. Tap **Services**.
2. - Tap → **Service Market → My Services → SIM** to enter the Service Details page.

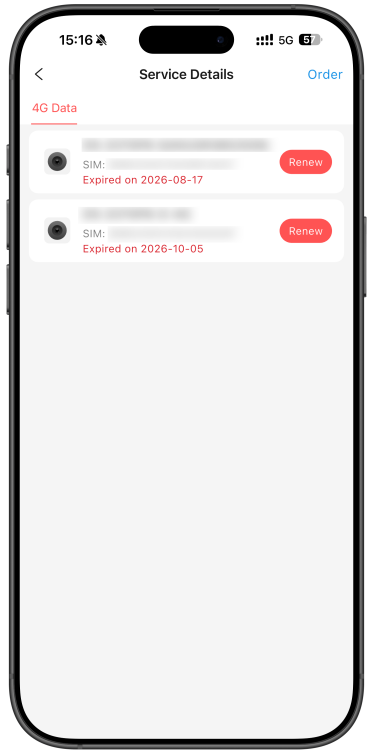


Figure 11-14 Service Details

- Tap a card, and tap **Order** to view all orders.

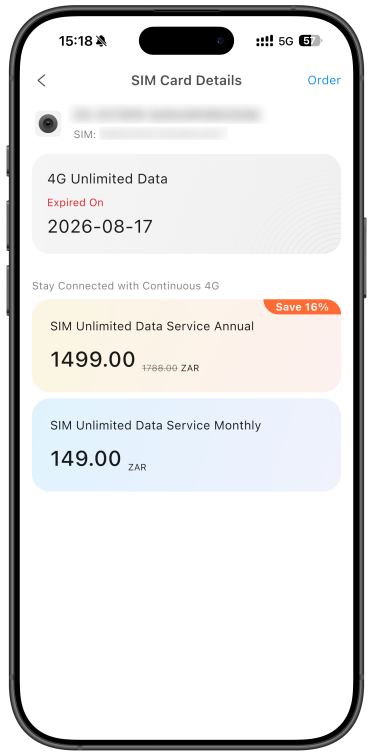


Figure 11-15 Card Details

11.4.4 How to subscribe to / unsubscribe from the service?

How to subscribe to the service?

1. Select a monthly or annual plan, tap **Buy Now** and confirm the payment.

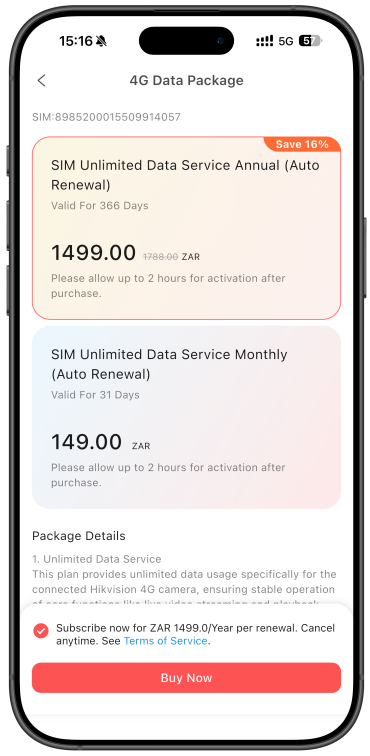


Figure 11-16 Buy Now

2. Check the subscription item to subscribe to the service.

How to unsubscribe from the service?

1. Tap → **Service Market** → **My Services** → **SIM** to enter the Service Details page.

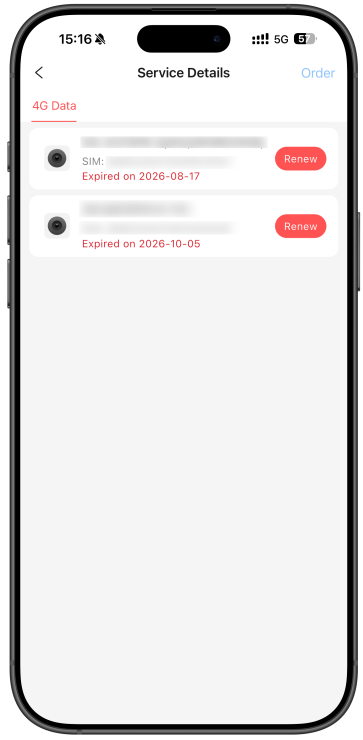


Figure 11-17 Service Details

2. Tap a card of interest.
3. Tap **Cancel Subscription**.

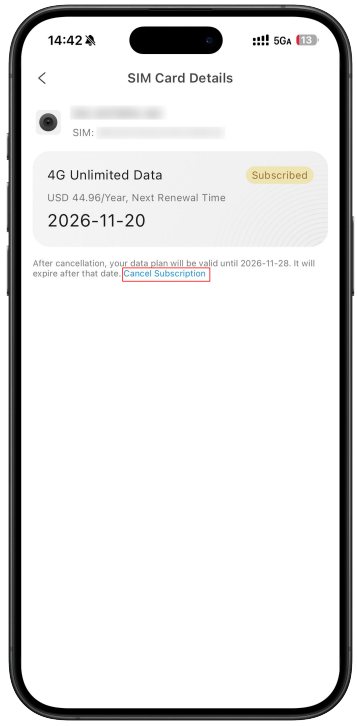


Figure 11-18 Cancel Subscription

4. You will see the exact date your service will expire.

11.4.5 How to check 4G data notifications?

1. Tap **Notifications → Value-Added Services** .

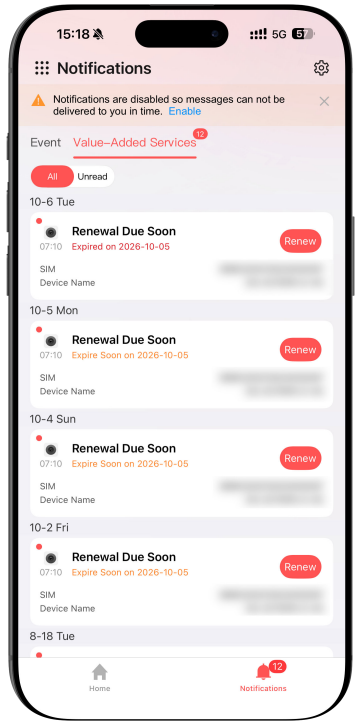
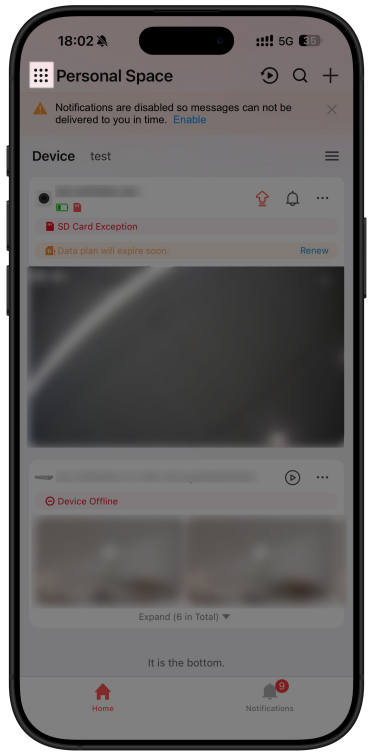


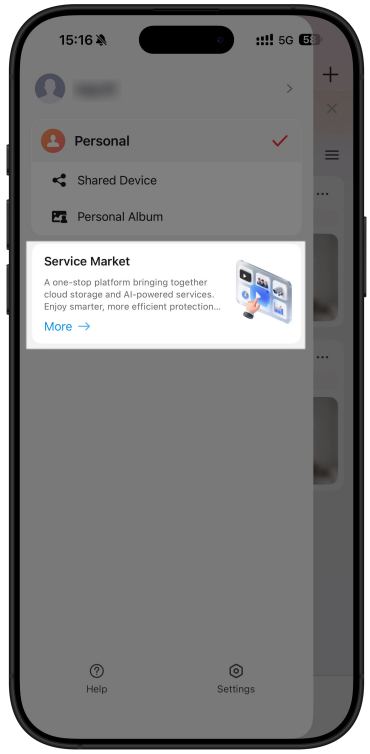
Figure 11-19 Notifications

2. You can view the service-related notifications and renew the service here.

11.4.6 How to use the AI assistant?

1. Open the AI Assistant.
   - Go to **Service Market**.


18:02
5G
Personal Space
Notifications are disabled so messages can not be delivered to you in time. Enable
Device test
SD Card Exception
Data plan will expire soon.
Renew
Device Offline
Expand (6 in Total)
It is the bottom.
Home
Notifications

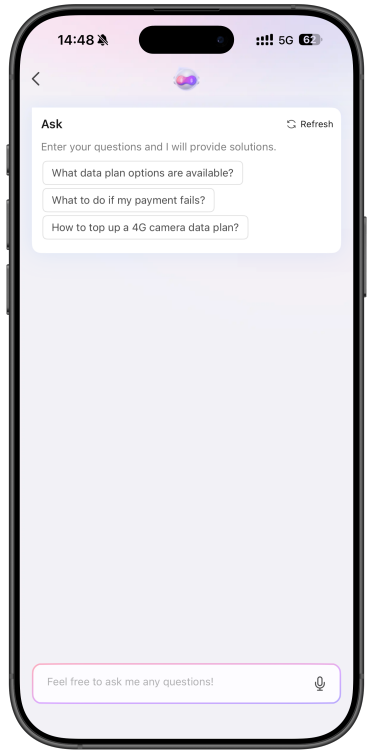

15:16
5G
Personal
Shared Device
Personal Album
Service Market
A one-stop platform bringing together cloud storage and AI-powered services. Enjoy smarter, more efficient protection...
More
Help
Settings

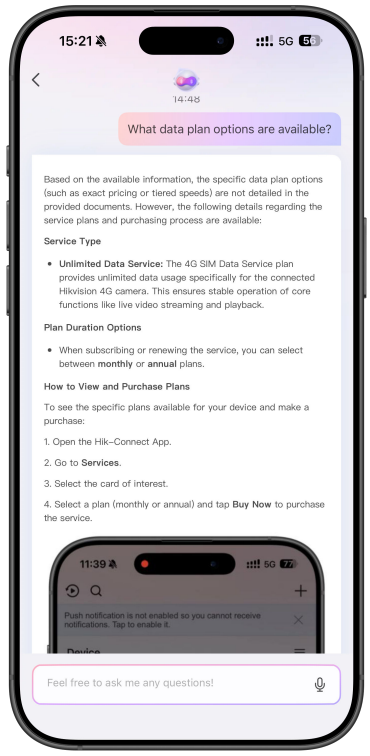


- Scenarios such as 4G AOV live view failure or device offline will also trigger the AI assistant.

2. Open the AI Assistant and describe your question to the assistant and get an answer.

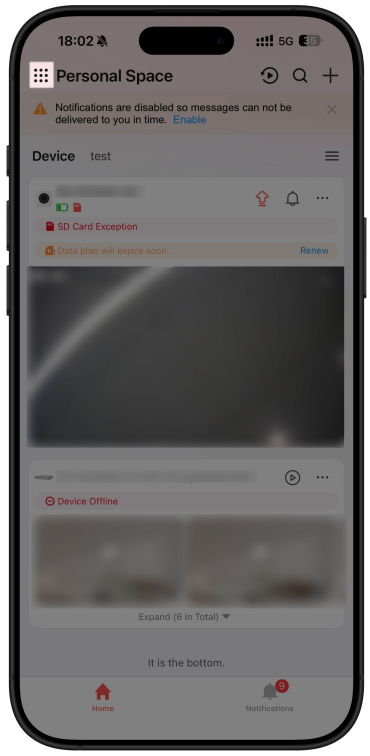

15:16
5G
Services
My Services
Service Market
Service Providers
4G Data
Paid
SIM
2
Expired
2026/10/05

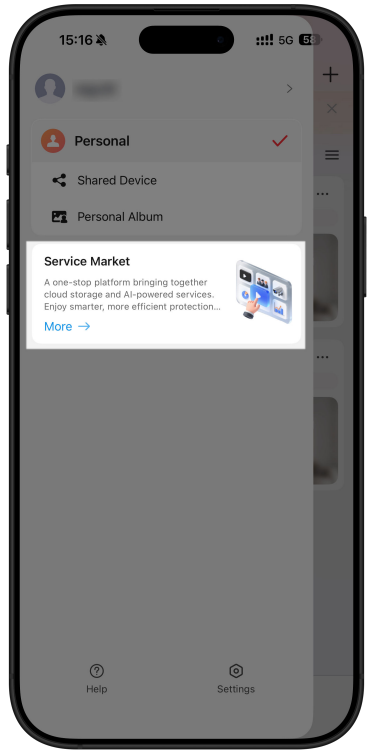

14:48
5G
Ask
Refresh
Enter your questions and I will provide solutions.
What data plan options are available?
What to do if my payment fails?
How to top up a 4G camera data plan?
Feel free to ask me any questions!



11.4.7 How to contact the customer service via email?

1. Open the AI Assistant.
   - Go to **Service Market**.


18:02
5G
Personal Space
Notifications are disabled so messages can not be delivered to you in time. Enable
Device test
SD Card Exception
Data plan will expire soon.
Renew
Device Offline
Expand (6 in Total)
It is the bottom.
Home
Notifications

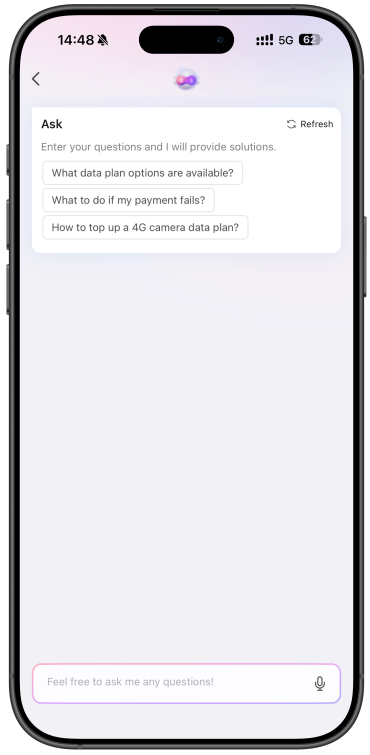

15:16
5G
Personal
Shared Device
Personal Album
Service Market
A one-stop platform bringing together cloud storage and AI-powered services. Enjoy smarter, more efficient protection...
More
Help
Settings

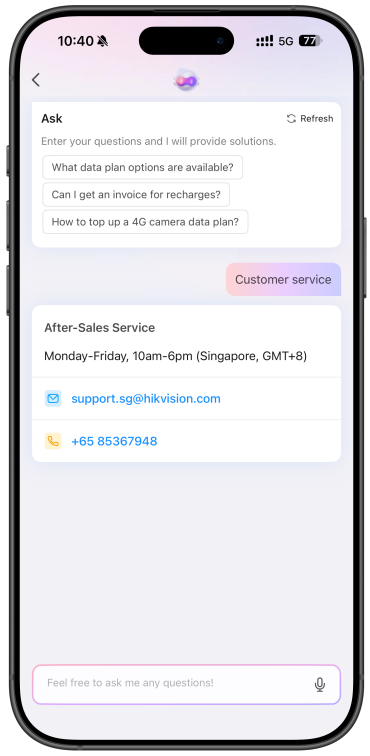


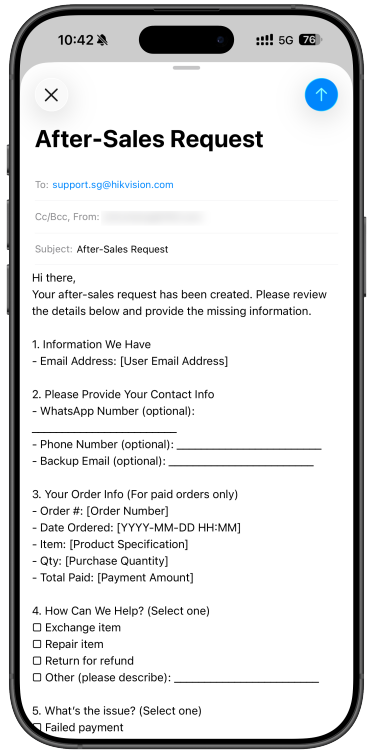
- Scenarios such as 4G AOV live view failure or device offline will also trigger the AI assistant.

2. Open the AI Assistant and send customer service to the AI Assistant. Tap the customer service email and enter your information in the pop-up email.


15:16
5G
Services
My Services
Service Market
Service Providers
4G Data
Paid
SIM
2
Expired
2026/10/05


14:48
5G
Ask
Refresh
Enter your questions and I will provide solutions.
What data plan options are available?
What to do if my payment fails?
How to top up a 4G camera data plan?
Feel free to ask me any questions!


10:40
5G
Ask
Refresh
Enter your questions and I will provide solutions.
What data plan options are available?
Can I get an invoice for recharges?
How to top up a 4G camera data plan?
Customer service
After-Sales Service
Monday-Friday, 10am-6pm (Singapore, GMT+8)
support.sg@hikvision.com
+65 85367948
Feel free to ask me any questions!


10:42
5G
After-Sales Request
To: support.sg@hikvision.com
Cc/Bcc, From:
Subject: After-Sales Request
Hi there,
Your after-sales request has been created. Please review the details below and provide the missing information.
1. Information We Have
- Email Address: [User Email Address]
2. Please Provide Your Contact Info
- WhatsApp Number (optional):
- Phone Number (optional):
- Backup Email (optional):
3. Your Order Info (For paid orders only)
- Order #: [Order Number]
- Date Ordered: [YYYY-MM-DD HH:MM]
- Item: [Product Specification]
- Qty: [Purchase Quantity]
- Total Paid: [Payment Amount]
4. How Can We Help? (Select one)
☐ Exchange item
☐ Repair item
☐ Return for refund
☐ Other (please describe):
5. What's the issue? (Select one)
☐ Failed payment

Chapter 12 Top Questions

12.1 What to do when my camera turns offline?

- Please check the power supply first to confirm that the device is connected with power supply.
- Please check the network connection of the device. Please check whether the network is stable or whether the network settings are changed. If the network settings are changed, please re-configure the device network in → **Account Name → Device Wi-Fi Configuration** .
- Check the device's TCP/IP settings.
  1. Enter the IP address of the device on a web browser and then visit the address.
  2. Go to **Configuration → Network → Basic Settings** .
  3. Perform the following operations.
     - Make sure the device IP address, subnet mask, and gateway address are correctly configured.
     - Set the DNS address to "8.8.8.8".
     - Enable DHCP.
  4. Go to **Configuration → Network → Advanced Settings → Platform Access** and then make sure Hik-Connect is enabled and the Hik-Connect status is online.

Note

Make sure the device is connected to a public network, and if the network is restricted, it may result in device offline.

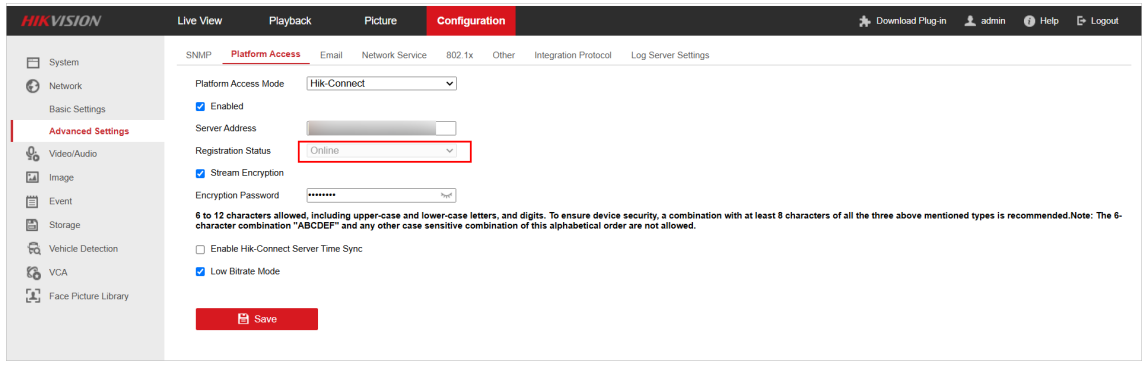


Figure 12-1 Platform Access

12.2 How to unbind devices?

Make sure the device and the phone running the Mobile Client are in the same local area network.

1. Add the device by scanning QR code or Hik-Connect domain.
2. On the Result page, tap **Unbind Device** to start to unbind the device from its account.

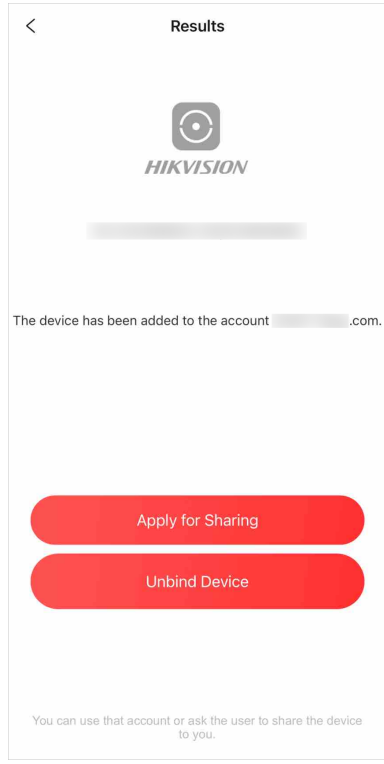


Figure 12-2 Unbind Devices

3. If the network exception occurs, perform the following operations.
   - Tap **Connect to Wi-Fi** to connect the phone to the Wi-Fi network and make sure the device is in the same local area network with the phone.
   - Tap **Or you can unbind the device from its account in local GUI** to unbind the device via local GUI.

   Note

   Unbinding the device via local GUI should be supported by the device.
4. On the Unbind Device page, enter the device password and the verification code displayed on the image.
5. Tap **Finish**.

12.3 My camera time zone, time, or date is incorrect.

For changing device time zones: You can configure **Time Zone** of a device by tapping ••• → **Settings** in the upper-right corner of a device card.

For correcting time and date:

- Go to the device web page.
- Go to **Configuration → System → System Settings → Region & Time** .

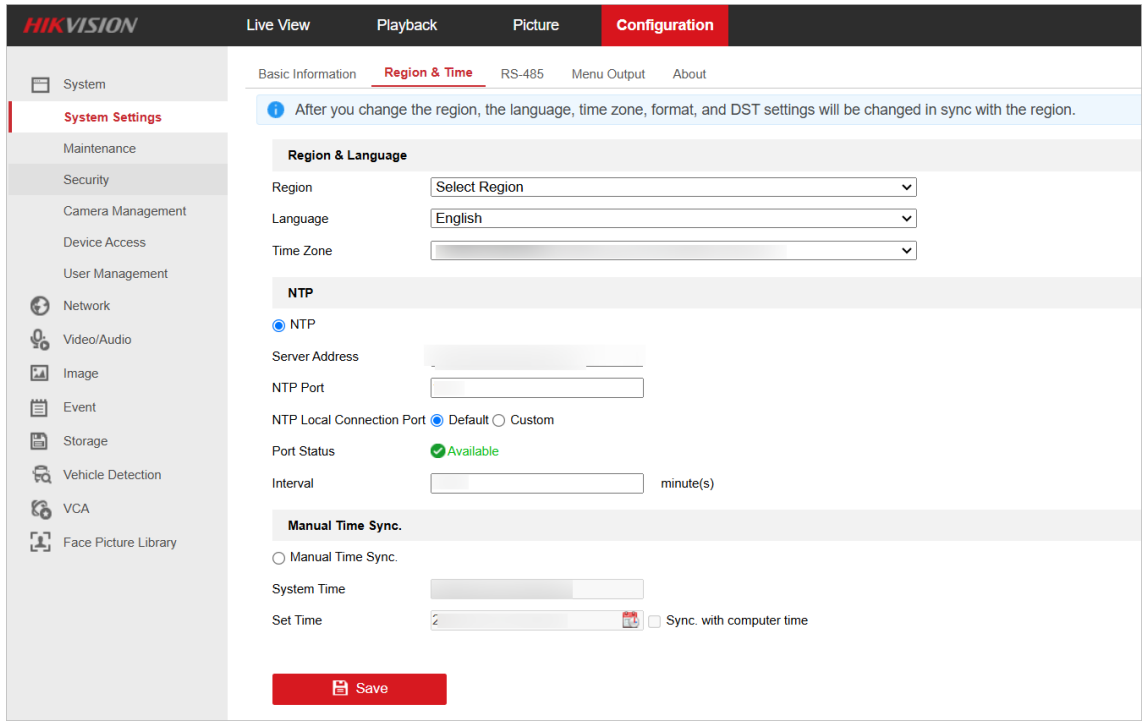


Figure 12-3 Time Settings

- Select region and then select NTP.

Note

NTP (Network Time Protocol) is a tool that keeps your device's clock accurate by syncing it with a reliable time source, like an atomic clock or GPS. It works over the internet to ensure your device always has the correct time, even if the network connection is unstable.

12.4 How do I set or change the device encryption password?

On the top right corner of a device card on the Home page, tap ··· → **Settings** .

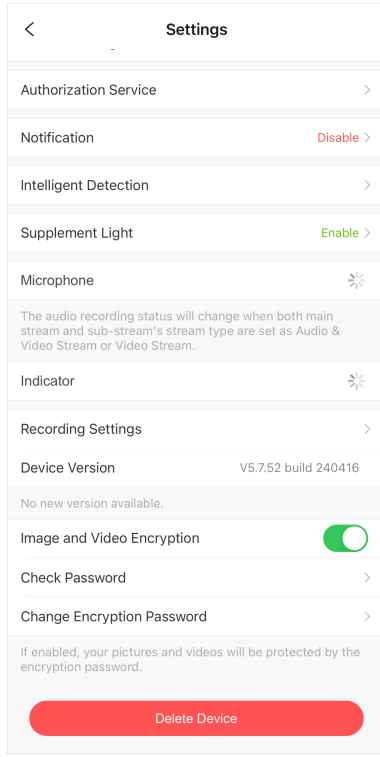


Figure 12-4 Set Encryption Password

Enable or disable **Image and Video Encryption** on the page.

If you forget the encryption password, tap **Check Password**, and a security code will be sent to your account email. Enter this code to check your password.

For changing your encryption password, tap **Change Encryption Password**

12.5 Why can't I receive alarm notifications?

1. Configure alarm and event settings for the device on the device's web page.
   a. Enter the IP address of the device on a web browser and then visit the address.
   b. Go to **Configuration → Event** .

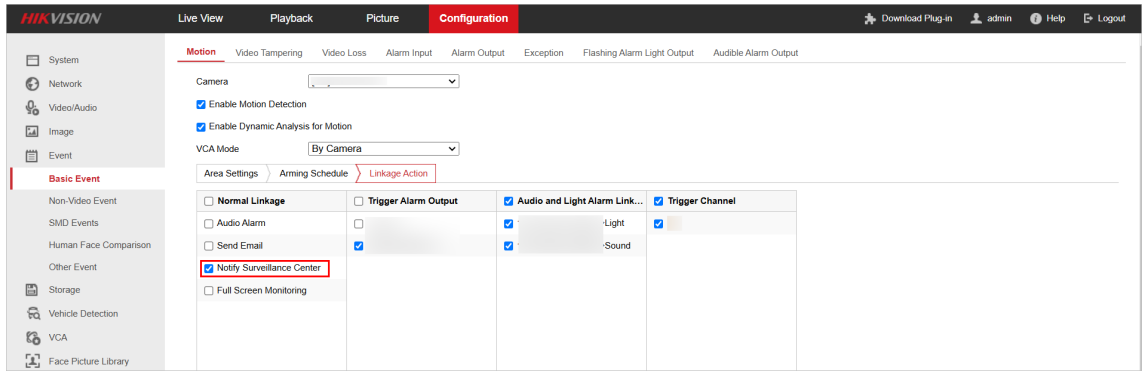


Figure 12-5 Notify Surveillance Center

c. Select an event type.
d. Select the required camera.
e. Check the checkbox to enable the event and then configure the relevant settings such as arming schedule.
f. Click **Linkage Action** and then check **Notify Surveillance Center**.

2. Go to **Settings** in the operation system of your phone or tablet and then turn on Notification for the Mobile Client.
3. Re-enable alarm notification for the cameras of the device and make sure the notification schedule is correctly configured.

Note

See *Enable /Disable Alarm Notification* in Help for details.

4. Enable the Mobile Client to push notifications to your phone or tablet.

Note

See *Message Push Notification* in Help for details.

12.6 How to use another email / phone number to manage the account?

1. Log in to ***https://www.hik-connect.com/*** .
2. Click **My Account**.
3. Click **Modify** to change the email or phone number of the account.

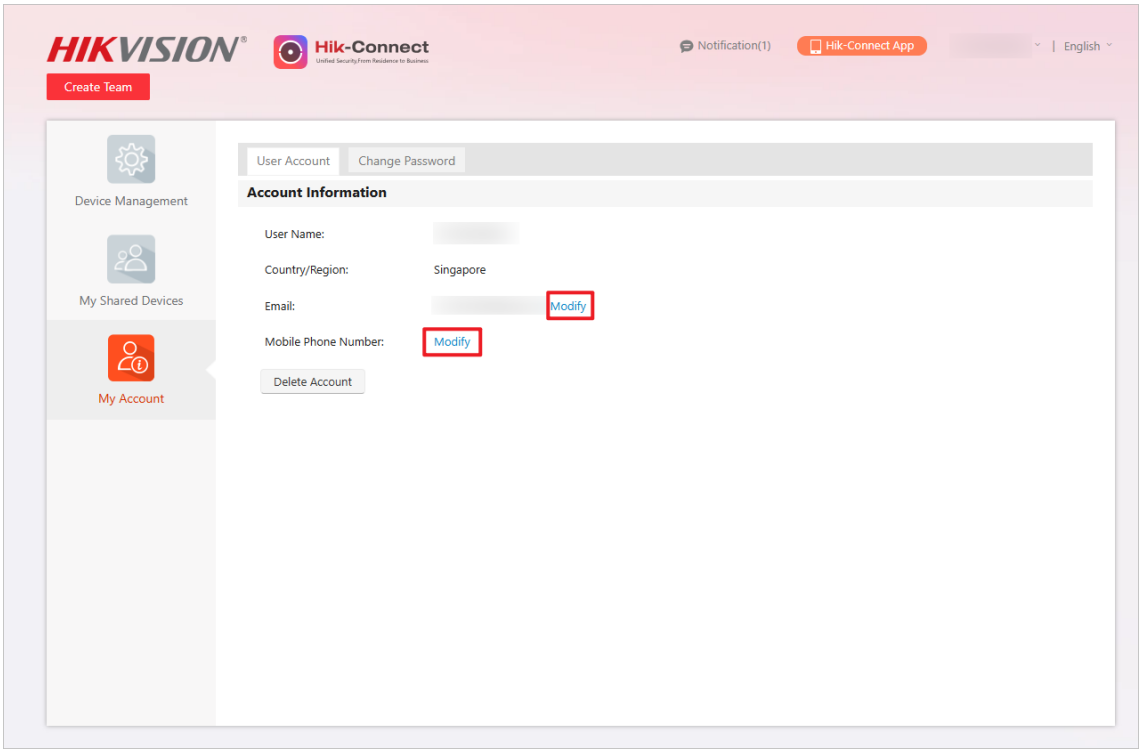


Figure 12-6 Change Email or Phone Number

Chapter 13 More Documents

13.1 Personal Mode

Table 13-1 Documents for Personal Mode

User Intention	Document
To get what's new, fixed, and important for you in a software update.	Long Press to Open ***Release Notes***
To get the key features, system requirements, and technical specifications of the Personal mode.	Long Press to Open ***Datasheet***
To get the frequently asked questions.	Long Press to Open ***FAQ***

13.2 Team Mode

User Intention	Document
To get what's new, fixed, and important for you in a software update.	Long Press to Open ***Release Notes***
To get fast and handy instructions for the most common features of the Team Portal.	Long Press to Open ***Portal User Manual***
To get fast and handy instructions for the most common features of the mobile client.	Long Press to Open ***Mobile Client User Manual***
To get the key features, system requirements, and technical specifications of the Personal mode.	Long Press to Open ***Datasheet***
To get the frequently asked questions.	Long Press to Open ***FAQ***


See Far, Go Further