

Hik-Connect Android Mobile Client

User Manual

Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website

(https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 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 INSPECTION, 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 MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description					
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.					
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.					
iNote	Provides additional information to emphasize or supplement important points of the main text.					

Contents

Chapter 1 Legal Informationi Chapter 1 Symbol Conventionsiii Chapter 1 Overview1 1.1 System Requirements and Conventions1 1.2 Summary of Changes1 Chapter 2 Select Region at First Time Running2 Chapter 3 Visitor Mode3 3.1 Functions in Visitor Mode3 3.2 Register an Account in Visitor Mode4 Chapter 4 Registration5 4.1 Register by Mobile Phone Number5 4.2 Register by Email Address5 Chapter 5 Device Management7 5.1 Activate an Inactive Device7 5.2 Add Device for Management8 5.2.1 Add an Online Device9 5.2.2 Add a Device by Scanning Device QR Code10 5.2.3 Add a Device by IP/Domain11 5.2.4 Add a Device by Hik-Connect Domain12 5.3 Connect Offline Device to Network13 5.4 Enable Hik-Connect Service for Device14 5.4.1 Enable Hik-Connect Service When Adding Device on Mobile Client15 5.4.2 Enable Hik-Connect Service on Device Web Page15 5.5 Enable DHCP Function on Device Web Page16 5.6 Unbind Device from Its Original Account17 5.7 Device Settings17 5.7.1 Edit Information of Cameras Linked to Added Device17 5.7.2 Set Video and Image Encryption18 5.7.3 Set DDNS19 5.7.4 Change Device's Verification Code20 5.7.5 Set Motion Detection Alarm for Network Camera20 5.7.6 Set Volume for Video Intercom22 5.7.7 Set Light for Floodlight Camera22 5.7.8 Use Mobile Client as Device's Remote Controller23 5.7.9 Remotely Configure Device24 5.7.9.1 View and Edit Basic Information25 5.7.9.2 Set Recording Schedule25 5.7.9.3 Configure Time Settings28

5.7.9.4 Change Device Password29 5.7.9.5 Configure Normal Event29 5.7.9.6 Configure Smart Event30 5.7.9.7 Enable Temperature Measurement31 5.8 Upgrade Device Firmware32 Chapter 6 Favorites Management33 6.1 Add Cameras to Favorites on Device List Page33 6.2 Add Cameras to Favorites During Live View33 6.3 Remove Cameras from Favorites34 Chapter 7 Share Device35 7.1 Share a Specific Device via Its QR Code35 7.2 Share Multiple Devices in a Batch36 7.3 Silenced Mode for Devices Shared by Others37 Chapter 8 Live View39 8.1 Start and Stop Live View39 8.2 Set Window Division40 8.3 Digital Zoom40 8.4 PTZ Control41 8.4.1 Pan and Tilt a Camera41 8.4.2 Set a Preset42 8.4.3 Adjust PTZ Speed42 8.4.4 Other Functions43 8.5 Start Two-Way Audio43 8.6 Capturing and Recording44 8.7 Set Image Quality for Device Added by IP/Domain45 8.8 Set Image Quality for Hik-Connect Device47 8.9 Live View for Fisheye Camera48 8.10 Open Door During Live View49 Chapter 9 Playback51 9.1 Normal Playback51 9.2 Event Playback52 9.3 Capturing and Recording54 9.4 Set Playback Quality for Device Added by IP/Domain54 9.5 Download Video Segment56 9.6 Adjust Playback Speed57 Chapter 10 Access Control58 10.1 Control Door Status58 10.2 Set Door Open Duration59 10.3 Change Super Password60 10.4 View Access Control Logs61 10.5 Enable Opening Door via Fingerprint (Face) Authentication61 Chapter 11 Security Control63 11.1 Video Security Control Panel63 11.1.1 Partition and Zone Control63 11.1.1.1 Control A Zone63 11.1.1.2 Control All Zones in One Partition64 11.1.2 Add a Zone67 11.1.3 Set Zone Parameters67 11.1.4 Bypass a Zone69 11.1.5 Link Camera to Zone69 11.1.6 Enable Voice Prompt70 11.1.7 Delete Zone70 11.2 Axiom Security Control Panel70 11.2.1 Log in to the Security Control Panel71 11.2.2 Configure Axiom Security Control Panel71 11.2.2.1 System Options71 11.2.2.2 Area Management72 11.2.2.3 User Management73 11.2.2.4 Keyfob Management75 11.2.2.5 Card/Tag Management76 11.2.2.6 Set Event Video Parameters77 11.2.2.7 Configure Push Notification Settings for Axiom Security Control Panel78 11.2.2.8 EN50131 Compliant Mode79 11.2.2.9 Other Settings80 11.2.3 Add Device to the Security Control Panel81 11.2.3.1 Add Peripheral Device by Scanning QR Code81 11.2.3.2 Add Peripheral Device in Enrollment Mode82 11.2.3.3 Add Network Camera Channel to Security Control Panel83 11.2.4 Set Area Parameters83 11.2.5 Control Areas84 11.2.6 Set Zone Parameters85 11.2.7 Bypass a Zone87 11.2.8 Link Camera to Zone87 11.2.9 Set Parameters of Wireless Outputs Expander88 11.2.10 Set Siren Parameters90 11.2.11 Set Wireless Keypad Parameters90 11.2.12 Set Wireless Card/Tag Reader Parameters91 11.3 Pyronix Control Panel93 11.3.1 Add Pyronix Control Panel to Mobile Client93 11.3.2 Authorize Mobile Client Account via PyronixCloud94 11.3.2.1 Create a PyronixCloud Account94 11.3.2.2 Connect Device to PyronixCloud95

11.3.2.3 Authorize Mobile Client Account96 11.3.3 Verify Pyronix Control Panel97 11.3.4 Control Areas (Partitions)97 11.3.5 Control Alarm Output Remotely99 11.3.6 Bypass a Zone99 Chapter 12 Facial Data Management100 Chapter 13 Video Intercom101 13.1 Answer Call from Indoor Station101 13.2 Operations on Device Details Page103 13.3 Set Motion Detection Alarm for Wi-Fi Doorbell104 Chapter 14 Notification107 14.1 Enable Alarm Notification107 14.2 Check Event Information or Call Logs110 14.3 Service Notification112 Chapter 15 Other Functions113 15.1 Pictures and Videos113 15.2 Fingerprint Authentication113 15.3 Hik-ProConnect114 Chapter 16 System Settings117 16.1 Enable Push Notification117 16.2 Save Device Parameters117 16.3 Auto-receive Alarm after Power-on117 16.4 Generate a QR Code with Device Information117 16.5 Hardware Decoding118 16.6 View Traffic Statistics118 16.7 Generate a QR Code with Wi-Fi Information118 16.8 Floating Live View119 16.9 Resume Latest Live View119 16.10 Tablet Mode120 16.11 Display/Hide Channel-Zero120 16.12 Auto-Download Upgrade File120 Chapter 17 Reset Password of DVR or NVR via the Mobile Client121 17.1 Reset Password by Hik-Connect121 17.2 Reserve Email Address for Resetting Password122 17.3 Generate QR Code by Reserved Email122 17.4 Reset Password by Reserved Email123

Chapter 1 Overview

The Hik-Connect mobile client (Android), which can generally manage Hikvision products, is designed for the phone or tablet based on Android 4.1 or later. With the Mobile Client, you can remotely control devices (NVRs, DVRs, network cameras, indoor stations, doorbells, security control panels, the Pyronix devices, the access control devices, etc) via Wi-Fi, 3G, or 4G networks. You can also share your devices to other accounts and use devices shared from other users. The Mobile Client provides access to the Hik-Connect service, which is a cloud service developed by Hikvision, to manage your devices.

iNote

Network traffic charges may be produced during the use of the Mobile Client. For details, refer to the local ISP.

1.1 System Requirements and Conventions

System Requirement

Android 4.1 or later versions.

Conventions

In the following chapters, we simplify Hik-Connect mobile client (Android) as "Mobile Client", devices such as DVR, NVR, encoder, and network camera as "device", and devices which support being added to Hik-Connect service as "Hik-Connect Device".

1.2 Summary of Changes

The followings are the key changes of this version of Help (V 4.3.0) compared with the previous version (V 4.2.0).

- Updated Upgrade Device Firmware due to UI design optimization.
- Updated *Reset Password by Hik-Connect* due to the optimization of the mechanism of the functionality. Since this version, resetting the password of the NVR/DVR by Hik-Connect will not lead to the resetting of the device.

Chapter 2 Select Region at First Time Running

The first time you run the Mobile Client, you should select the region where your devices are located. Otherwise, the live view, playback and alarm notification of the devices will fail.

iNote

- The region cannot be changed once you have selected.
- You should select the region where your devices are located, or subsequent operations may be affected.

After running the Mobile Client, tap **Select Region** to select a region.

Chapter 3 Visitor Mode

Visitor mode allows you to manage devices on the Mobile Client without registration. When you log in as a visitor, a visitor account will be created for you automatically, and the account will not change on the same phone or tablet.

ACaution

For information security, please use visitor mode cautiously, which is NOT password-protected.

iNote

In visitor mode, you can only manage your devices on a same phone or tablet. To avoid this inconvenience, you can register an account. For details about registering account in visitor mode, see *Register an Account in Visitor Mode*.

3.1 Functions in Visitor Mode

Most of the functions supported in a registered account are supported in visitor mode. Tap **Visitor Mode** on the Home page or the Login page to enter visitor mode. The followings are the functions supported in visitor mode.

Device Management

Add devices to the Mobile Client and configure device settings. See **Add Device for Management** and **Device Settings** for details.

Sharing Device

Tap $\blacksquare \rightarrow$ Scan QR Code to scan the QR code of another visitor account to share device(s) to the account. For details about sharing device, see *Share Device*.

i Note

To get the QR code of a visitor account, go to **More** \rightarrow **Account Management**.

Live View and Playback

View live video of the added devices and play back the videos. See *Live View* and *Playback* for details.

Access Control

Control door status and check access control events. See Access Control for details.

You should have added access control devices to the Mobile Client.

Security Control Panel Management

Manage partitions (areas) and zones for the security control panel. See *Security Control* for details.

Alarm Configuration

Configure the alarm notifications on Alarm Notification page. See *Notification* for details.

3.2 Register an Account in Visitor Mode

Though the visitor mode allows you to manage devices without registration, you can only manage your devices on one phone or tablet. With a registered account, you can manage devices on different phones or tablets.

Steps

- 1. Tap **Visitor Mode** on the Login page or Home page to enter the visitor mode.
- 2. Tap **More** \rightarrow **Register an Account** to open the Join Us window.
- 3. Tap Terms of Service and Privacy Policy to read the relevant information.
- 4. Tap Agree if you accept our terms of service and privacy policy.
- 5. Register an account by mobile phone number or email address.

INote

See Register by Email Address and Register by Mobile Phone Number for details.

Chapter 4 Registration

You can register an account by your mobile phone number or your email address. With a registered account, you can log in to the Mobile Clients running on different mobile phones or tablets, which provides convenience for managing your devices.

iNote

You can use visitor mode to manage your devices without registration. See *Visitor Mode* for details.

4.1 Register by Mobile Phone Number

You can register an account by your mobile phone number.

Steps

- 1. Tap **Login** on the Home page to enter the Login page.
- 2. Tap **Register** to enter the Register page.
- 3. Tap **Terms of Service** and **Privacy Policy** to read the relevant content and then tap **Agree** to continue.
- 4. Enter your mobile phone number and then tap **Get Security Code** to receive the security code for identity verification.
- 5. Enter the security code you received and tap Next to continue.
- 6. Create a password.

iNote

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

7. Tap **Finish**.

4.2 Register by Email Address

You can register an account by your email address.

Steps

- 1. Tap **Login** on the Home page to enter the Login page.
- 2. Tap **Register** to enter the Register page.

- 3. Tap **Terms of Service** and **Privacy Policy** to read the relevant content and then tap **Agree** to continue.
- 4. Enter your email address and then tap **Get Security Code** to get the security code for identity verification.
- 5. Enter the security code you received and then tap **Next** to continue.
- 6. Create a password.

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

7. Tap Finish.

Chapter 5 Device Management

You can add devices to the Mobile Client, and configure device functions such as video and image encryption.

The devices added to the Mobile Client will be displayed in thumbnail mode or list mode.

Thumbnail Mode

You can tap \blacksquare on the upper-left side of the home page to switch the display mode of the device list to thumbnail mode.

In the thumbnail mode, the video resources are displayed as the thumbnails of their video channel images; the security control resources, doorbells, and access control resources are displayed as device pictures.

List Mode

You can tap 📕 on the upper-left side of the home page to switch the display mode of the device list to list mode.

In the list mode, all the resources are displayed as icons with names on the right.

5.1 Activate an Inactive Device

When adding a device, if the device is not activated, a window will pop up to ask you to activate the device.

Before You Start

The device and the phone or tablet running the Mobile Client should be in the same LAN.

Steps

iNote

For the access control device, you should activate it via other clients (e.g., iVMS-4200 client software).

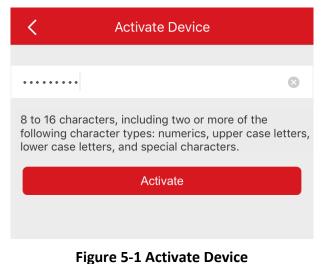
1. Add a device.

iNote

See Add Device for Management for details.

2. On the Activate Device page, tap Set Device Password.

3. Create a password.



Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- 4. Tap **Activate** to activate the device.
- 5. Enable DHCP or manually configure network if you enter the Network Configuration page.

5.2 Add Device for Management

You need to add devices to the Mobile Client first so that subsequent operations such as live view and playback can be available. If you want to receive alarm event information from a device, you should add it by scanning QR code or Hik-Connect domain.

- For details about adding Pyronxi control panel, see Add Pyronix Control Panel to Mobile Client.
- For details about managing alarm event information, see Notification.

5.2.1 Add an Online Device

The Mobile Client can detect the online devices in the same local area network with your phone or tablet, and you can add the detected online devices to the Mobile Client.

Before You Start

Make sure the devices are connected to the same local area network with the phone or tablet.

Steps

- 1. On the device list page, tap $\bigoplus \rightarrow$ **Online Device** to enter the Online Device page. All detected online devices will be in the list.
- 2. Select a device for adding.



Figure 5-2 Online Device

- For network cameras, make sure the device Multicast Discovery function is enabled so that the online network camera can be automatically detected via private multicast protocol in the LAN. For details, see User Manual of the network camera.
- For the inactive device (excluding the access control device), tap **Active** to create a password for it before you can add the device properly. For more information about the device activation, see **Activate an Inactive Device**.
- 3. Optional: Edit the network information.
 - 1) Tap 🧪.
 - 2) Change the device IP address to the same LAN as your phone's by either editing the IP address manually or enabling the device DHCP function.
 - 3) Tap 📄 and input the admin password of the device to save the settings.
- 4. Tap **Add**.
- 5. Enter the required information, including device alias, user name and the password.
- 6. Tap 📘.
- 7. Optional: Delete the device.

 - On the device list, if the list is in thumbnail mode, tap the device name or tap •••, and then tap **Delete Device**.

5.2.2 Add a Device by Scanning Device QR Code

You can add the device by scanning the device's QR code.

Steps

iNote

If adding an access control device, you should activate the device and set the device network information via other clients (e.g., iVMS-4200 client software) before adding it to this client.

- 1. On the device list page, tap $\bigoplus \rightarrow$ Scan QR Code to enter the Scan QR Code page.
- 2. Scan the QR code.
 - Scan the device QR code by aligning the QR Code with the scanning frame.

iNote

- Usually, the QR code is printed on the label, which is on the back cover of the device.
- Tap **f** off to enable the flashlight if the scanning environment is too dark.
- If there are device QR codes in photo album of the phone or tablet, tap in to extract QR code from local album.
- 3. Optional: Perform the following operations if the following situations occur.

 - If the device has been added to another account, you should unbind the device from the account first. See Unbind Device from Its Original Account for details.
 - If the device is offline, you should connect a network for the device. For details, see *Connect Offline Device to Network* for details.
 - If the device is not activated, the Activate Device page will pop up (excluding the access control device). You should activate the device. For details, see *Activate an Inactive Device* for details.
 - If the Hik-Connect service is disabled for the device, you should enable the function (excluding the access control device). For details, see *Enable Hik-Connect Service When Adding Device on Mobile Client* for details.
- 4. Tap Add on the Result page.
- 5. Enter the device verification code.

The device will be added successfully.

- 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.
- For details about enabling Hik-Connect service, see **Enable Hik-Connect Service for Device**.
- 6. Optional: Tap **Configure DDNS** to configure DDNS.

- See *Set DDNS* for details.
- After DDNS being enabled, the device will be accessed via IP address in priority, so that remote configuration of the device will be supported and the streaming speed will be faster than streaming via Hik-Connect service.
- If you skip this step, the device will be accessed via Hik-Connect service.

7. Tap Finish.

- 8. Optional: Delete the device.

 - On the device list, if the list is in thumbnail mode, tap the device name or tap •••, and then tap **Delete Device**.

5.2.3 Add a Device by IP/Domain

You can add the device by fixed IP address or domain name. The streaming speed of devices added by IP/domain is faster than those added by Hik-Connect domain.

Before You Start

- If you want to add the access control device, activate it before adding. See the user manual of the access control device for details.
- You should activate it via other clients such as iVMS-4200 client software. Make sure the device is powered on.

Steps

iNote

The Mobile Client doesn't support receiving alarm event information from devices added by IP/domain. For details about managing event information on the Mobile Client, see **Notification**

- 1. Tap 🕒 and select Manual Adding.
- 2. Select IP/Domain as the adding type.
- 3. Enter the required information, such as alias, address, user name, camera No. and device password.

Address

Device IP address or domain name.

Camera No.

The number of the camera(s) under the device can be obtained after the device is successfully added.

4. Tap 📄 to add the device.

- If the device is offline, you should connect the device to a network. For details, see *Connect Offline Device to Network*.
- If the device is not activated, the Activate Device page will be popped up (exclude the access control device). You should activate the device. For details, see *Activate an Inactive Device*.
- 5. Optional: Perform the following operations after adding the device.

Edit Device Information	On the Device Information page, tap 🧪 to edit the basic information of the device.
Star Live View	Tap Start Live View to view the live view of the device.
Delete a Device	Tap $\ \widehat{\ }$ ond then tap Delete to delete the device.
Configure Device Parameters	Tap \bigcirc and then tap Remote Configuration to remotely configure device parameters such as basic information, time settings, recording schedule, etc. See Remotely Configure Device for details.
Remote Controller	Tap \bigcirc and then tap Remote Controller to remotely control the device. See Use Mobile Client as Device's Remote Controller for details.

5.2.4 Add a Device by Hik-Connect Domain

For devices which support Hik-Connect service (a cloud service provided by Hikvision), you can add them manually by Hik-Connect domain.

Before You Start

- Make sure the device is powered on.
- If adding access control device, you should activate the device and set the device network information via other clients (e.g., iVMS-4200 client software) before adding it to this client.

Steps

- 1. On the device list page, tap $\bigoplus \rightarrow$ Manual Adding to enter the Add Device page.
- 2. Select Hik-Connect Domain as the adding type.
- 3. Enter the device serial No. manually.

- By default, the device serial No. is on the device label.
- For the video intercom devices, when entering the serial No. of the indoor station, the corresponding door station will also be added to the Mobile Client automatically.
- An indoor station can be linked to multiple door stations.

4. Tap 📄 to search the device.

iNote

- If the device has been added to another account, you should unbind the device from the account first. See *Unbind Device from Its Original Account* for details.
- If the device is offline, you should connect a network for the device. For details, see *Connect Offline Device to Network* for details.
- If the device is not activated, the Activate Device page will pop up (excluding the access control device). You should activate the device. For details, see *Activate an Inactive Device* for details.
- If Hik-Connect service is disabled for the device, you should enable the function (excluding the access control device). For details, see *Enable Hik-Connect Service When Adding Device on Mobile Client* for details.

5. Tap Add on the Result page.

6. Enter the device verification code.

The device will be added successfully.

iNote

- 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.
- For details about enabling Hik-Connect service, see *Enable Hik-Connect Service for Device*.
- 7. Optional: Tap **Configure DDNS** to configure DDNS.

INote

- See *Set DDNS* for details.
- After DDNS being enabled, the device will be accessed via IP address in priority, so that remote configuration of the device will be supported, and the streaming speed will be faster than streaming via Hik-Connect service.
- If you skip this step, the device will be accessed via Hik-Connect service.
- 8. Tap Finish.
- 9. Optional: Delete the device.
 - On the device list, if the list is in list mode, swipe the device name to the left and tap
 Delete Device.
 - On the device list, if the list is in thumbnail mode, tap the device name or tap •••, and then tap **Delete Device**.

5.3 Connect Offline Device to Network

When adding a device to the Mobile Client, if the device is offline, you should connect the device to a network first. The Mobile Client provides the following four methods for connecting offline

devices to networks.

iNote

For access control device, you should connect it to a network via other Clients (e.g., iVMS-4200 client software).

Connect to Wired Network

Use this method if a router is available for the device to connect to.

iNote

Make sure the device is powered on.

Connect to Wireless Network

Use this method if a wireless network is available for the device to connect to. "Device" here excludes wireless doorbell, wireless security control panel, and Mini Trooper (a kind of battery camera).

iNote

- Make sure your phone has connected to a Wi-Fi network before using the method.
- The device should support connecting to wireless network.

Connect to Network by Wi-Fi Configuration

You can use this method to connect wireless doorbell to the network by using the doorbell to scan the QR code generated by the Mobile Client.

Tap **Connect to a Network** on the Result page and then follow the instructions on the subsequent pages to connect the device to the network.

Connect to Network by Access Point

In the Mobile Client, Access Point (AP) refers to a networking hardware device (e.g., wireless doorbell or wireless security control panel), which can provide a Wi-Fi network for the phone to connect to.

iNote

You should have turned on WLAN in the phone's operation system.

Tap **Connect to a Network** on the Result page, select **Wireless Connection** as the connection type, and then follow the instructions on the subsequent pages to complete the connection process.

5.4 Enable Hik-Connect Service for Device

Hik-Connect is a cloud service provided by Hikvision. When adding a device via Hik-Connect Domain or scanning QR code, the service should be enabled. You can enable the service via the

Mobile Client, the device web page, or iVMS-4200 client software. This section introduces how to enable the service via the former two methods.

5.4.1 Enable Hik-Connect Service When Adding Device on Mobile Client

When adding a device via Hik-Connect domain or scanning QR code, if the Hik-Connect service is not enabled for the device, the Enable Hik-Connect Service window will pop up to remind you to enable the service first.

Perform the following task to enable the Hik-Connect service in this case.

Steps

1. Add a device via Hik-Connect domain or scanning QR code.

iNote

See *Add a Device by Hik-Connect Domain* or *Add a Device by Scanning Device QR Code* for details.

If the device's Hik-Connect service is not enabled, the following window pops up.

- 2. On the Enable Hik-Connect Service window, tap **Hik-Connect Terms of Service** to read the terms of service.
- 3. Check Read and Agree Hik-Connect Terms of Service.
- 4. Tap Next.
- 5. Create a device verification code.

∎Note

You can change the device verification code. See *Change Device's Verification Code* for details.

6. Tap Enable Hik-Connect Service.

What to do next

Continue the process for adding the device. See *Add a Device by Hik-Connect Domain* or *Add a Device by Scanning Device QR Code* for details.

5.4.2 Enable Hik-Connect Service on Device Web Page

You can enable Hik-Connect service for a device on the device web page.

Steps

- 1. Visit the device IP address on the web browser.
- 2. Enter the device user name and device password to log in to the device web page.
- 3. Tap **Configuration** → **Network** → **Advanced Settings** → **Platform Access** to enter the Platform Access page.

HI	KVISION	Live View	Playback	Pictur	e	Configu	ration
Ţ	Local	SNMP FTP	Email Plat	form Access	HTTPS	QoS	802.1x
	System	Enable					
Ð	Network	Platform Access	Mode Hik-	Connect		•	
	Basic Settings	Server IP	dev.	nik-connect.com	n		Custom 🥑
	Advanced Settings	Register Status	Offli			Ŧ	
Q.	Video/Audio	Verification Code	SVG	IFZ			
1	Image						
Ë	Event	🗎 Sa	ve				
8	Storage						

Figure 5-3 The Platform Access Page

- 4. Check Enable.
- The system will set Hik-Connect as the platform access mode by default.
- 5. Optional: If it is the first time to enable the Hik-Connect service, create a device verification code.
- 6. Tap **Save**.

5.5 Enable DHCP Function on Device Web Page

You can enable DHCP by following the steps below to allow allocating DNS address automatically.

Steps

iNote

If you want to enable the access control device's DHCP function, you should enable it via other systems (e.g. iVMS-4200 client software).

- 1. Visit the IP address of the device.
- 2. Enter the device user name and device password and log in to the device's web page.
- 3. Click **Configuration** \rightarrow **Network** \rightarrow **Basic Settings** to enter the Basic Settings page.
- 4. Enable **DHCP**.
 - DNS address will be allocated automatically.
- 5. Click Save.

5.6 Unbind Device from Its Original Account

When adding a device by scanning QR code or Hik-Connect domain, if the result shows that the device has been added to another account, you should unbind it from the account before you can add it to your account.

Before You Start

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

Steps

1. Add the device by scanning QR code or Hik-Connect domain.

See **Add a Device by Scanning Device QR Code** or **Add a Device by Hik-Connect Domain** for details.

2. On the Result page, tap **Unbind Device** to start unbind the device from its account.

3. Optional: 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.

iNote

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.

5.7 Device Settings

On Settings page, you can view and edit a device's basic information, delete the device, and configure other functions such as video and image encryption, changing device verification code, transferring the device to another user, etc.

5.7.1 Edit Information of Cameras Linked to Added Device

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

Steps

1. Enter the Settings page of a NVR or DVR.

- On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On
- On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
- On the Live View page. Tap •••• and then tap **Settings**.

For details about how to enter the Live View page, see Start and Stop Live View.

2. Tap Linked Camera to enter the Linked Camera page.

Edit Camera Name	Tap 🖍 to edit the camera name, and then tap 📄 to save the settings.
Hide/Show Camera	Tap \odot or $\overbrace{\hspace{5em}\hspace{5em}\hspace{5em}\hspace{5em}}}$ to hide or show the camera on the device list respectively.

5.7.2 Set Video and Image Encryption

For security reasons, you can set the video and image encryption function to encrypt the videos or the pictures.

Steps

iNote

- If you set the video and image encryption function, the device's live video, recorded video, and pictures in event information will be encrypted. You should enter the device verification code the first time you entering these pages.
- If you log in to the Mobile Client with the same account on another phone, you should enter the device verification code again to view the live video, the recorded video, and pictures in event information.

1. Enter the Settings page.

On the device list page, if the page is in the list mode, swipe the device name to left and tap ⁽²⁾.On the device list page, if the page is in the thumbnail mode, tap the device name or tap *******.Enter the Live View page, tap ******* and tap **Settings**.

- 2. Set the Video and Image Encryption switch to ON to enable the function.
- 3. Optional: Change the encryption password (device verification code).
 - 1) Tap Change Password.
 - 2) Tap **Edit** in the pop-up window to enter the Change Password page.
 - 3) Follow the instructions on the page to change the device verification code.

iNote

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. For details about enabling Hik-Connect service, see *Enable Hik-Connect Service for Device*.

5.7.3 Set DDNS

For a device added via Hik-Connect Domain or Scaning QR code, if DDNS is enabled, the device's streams will be accessed via IP address in priority. In this case, you can remotely configure device and the speed of streaming will be faster than that of streaming via Hik-Connect service.

Steps

- 1. Enter the Settings page of the device.
 - On the device list page, if the page is in list mode, swipe the device's name to the left and tap
 On
 - On the device list page, if the page is in thumbnail mode, tap the device's name or tap ••••.
 - On the Live View page. Tap •••• and then tap Settings.

iNote

For details about how to enter the Live View page, see Start and Stop Live View

- 2. On the Settings page, tap **Configure DDNS** to enter the Configure DDNS page.
- 3. Set the required information.

Device Domain Name

The default device domain name is the serial number of the device. If you want to edit it, the edited domain name should contain 1 to 64 characters, including numbers, lowercase letters, and dashes. And it should start with a lowercase letter and cannot end with a dash.

Port Mapping Mode

For details about setting port mapping, tap How to Set Port Mapping.

iNote

The entered port number should be from 1 to 65535.

User Name

Enter the device user name.

Password

Enter the device password.

4. Tap 🗎.

5.7.4 Change Device's Verification Code

The device verification code is used for verifying user identity, as well as encrypting a device's videos (including live videos and recorded video files) and captured pictures. You can change the device verification code for the network camera and Mini Trooper (a kind of camera powered by battery).

Steps

iNote

For details about how to encrypt a device's videos and captured pictures, see *Set Video and Image Encryption*.

- 1. Enter the Settings page of the device.
 - On the device list page, if the page is in the list mode, swipe the device name to the left and tap ⁽²⁾.
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
 - On the Live View page, tap •••• and then tap **Settings**.

⊡Note

For details about how to enter the Live View page, see *Start and Stop Live View*.

- 2. Tap **Change Verification Code**, and then tap **Edit** on the pop-up Window to enter the Change Verification Code page.
- 3. Enter the old verification code, and then tap Next.
- 4. Create a new verification code, and then confirm it.

iNote

If you have enabled the Video and Image Encryption function, new pictures and videos will be encrypted by the new verification code. However, the earlier encrypted pictures and videos still use the old verification code.

5.7.5 Set Motion Detection Alarm for Network Camera

Motion detection is a way of detecting motion in a surveillance 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 alarm notification about the motion detection event.

Steps

- 1. Enter the Settings page of the network camera.
 - On the device list page, if the page is in list mode, swipe the device name to the left and tap

ଡ଼ି.

- On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
- On the Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see Start and Stop Live View.

- 2. Tap Notification to enter the Notification page.
- 3. Draw motion detection area.
 - 1) Tap Draw Motion Detection Area to enter the motion detection area settings page.
 - 2) Swipe on the screen to draw the motion detection area.

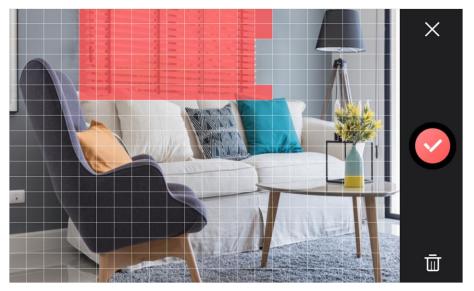


Figure 5-4 Draw Motion Detection Area

- 3) Optional: Tap 🛅 to undo the drawing.
- 4) Tap 👩 to save the motion detection area settings.
- 4. Tap X 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.

What to do next

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

For details about how to enabling notification, see *Enable Alarm Notification*

5.7.6 Set Volume for Video Intercom

You can set video intercom volume as required.

Steps

iNote

Only video intercom devices support this function.

- 1. Enter the Settings page of a video intercom device.
 - On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
 - On the Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see Start and Stop Live View.

2. Tap **Loudspeaker Volume** or **Microphone Volume** to adjust the loudspeaker and the microphone volume respectively.

5.7.7 Set Light for Floodlight Camera

You can set light for the Floodlight camera.

Before You Start

You should have added a Floodlight camera to the Mobile Client.

Steps

1. Enter the Settings page of a Floodlight camera.

- On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On
- On the device list page, if the page is in thumbnail mode, tap the device name or tap
- On the Live View page. Tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see Start and Stop Live View.

- 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.

5.7.8 Use Mobile Client as Device's Remote Controller

For a device added via IP/Domain, you can use the Mobile Client as the device's remote controller.

Steps

iNote

- The function should be supported by the device.
- The remote controller function is supported when your phone or tablet is connected to a Wi-Fi network, and the network latency should be less than 200ms.
- 1. Enter the Settings page.
 - On the device list page, if the page is in the list mode, swipe the device name to the left and tap S^o.
 - On the device list page, if the page is in thumbnail mode, tap the device's name or tap ••••.
 - On the Live View page. Tap *••••* and then tap Settings.

iNote

For details about how to enter the Live View page, see Start and Stop Live View.

2. Tap $\overline{\odot}$ and tap **Remote Controller** to enter the following page.



Figure 5-5 Remote Controller Page

- 3. Swipe the screen to perform remote-control operations such as moving up, down, left, and right.
- 4. Tap the screen to confirm.
- 5. Optional: Tap 🔄 to cancel and return to the previous menu of the device.
- 6. Optional: Tap 📃 to open the main menu of the device.

5.7.9 Remotely Configure Device

After adding a device, you can set the parameters of the device, including basic information, time settings, recording schedule, etc.

iNote

Remote configuration is only available for Android V4.2 or later versions.

View and Edit Basic Information

You can view and edit the basic information of a device.

Before You Start

Add a device to the Mobile Client. See Add Device for Management for details.

Steps

- 1. Enter the Settings page.
 - On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
 - On the Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see *Start and Stop Live View*.

- 2. Enter the Remote Configuration page.
 - − For a device added via IP/Domain, tap \bigcirc → Remote Configuration.

iNote

For details about adding device via IP/Domain, see Add a Device by IP/Domain.

- For a device added via other methods, tap **Remote Configuration** on the Settings page.

iNote

You should have configured DDNS for the device first. See *Set DDNS*.

- 3. Tap **Basic Information** to enter the Basic Information page.
- 4. Tap 💉 to enter the Edit Device page.
- 5. Edit the basic information of the device.
- 6. Tap 📄 to save the settings.

Set Recording Schedule

You can set a recording schedule for a channel of a specific device.

Steps

- 1. Enter the Settings page.
 - On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
 - On the Live View page, tap •••• and then tap Settings.

iNote

For details about how to enter the Live View page, see Start and Stop Live View.

- 2. Enter the Remote Configuration page.
 - − For a device added via IP/Domain, tap \bigcirc → Remote Configuration.

For details about adding device via IP/Domain, see Add a Device by IP/Domain.

- For a device added via other methods, tap **Remote Configuration** on the Settings page.

iNote

You should have configured DDNS for the device first. See Set DDNS.

- 3. Tap **Recording Schedule** to enter the Recording Schedule page.
- 4. Select a channel if the device has multiple channels.
- 5. Set the switch to ON to enable recording schedule.
- 6. Set a recording schedule for a day in the week.
 - 1) Tap a day in the week to enter the schedule settings page.
 - 2) Tap a time period to set the recording type, start time, and end time.

Continuous

The video will be recorded automatically according to the time of the schedule.

Motion Detection

The video will be recorded when the motion is detected.

Alarm

The video will be recorded when the alarm is triggered via the external alarm input channels.

Motion Detection or Alarm

The video will be recorded when the external alarm is triggered or the motion is detected.

Motion Detection and Alarm

The video will be recorded when the motion and alarm are triggered at the same time.

Event

The video will be recorded when any event is detected.

iNote

You can also set the recording type to detailed event type, which should be supported by the device. For details, refer to the user manual of the device.

3) Tap **OK** to save the settings of the time period.

4) Set other time periods in the day.

Up to 8 time periods can be configured for each day. And the time periods cannot be overlapped with each other.

Continuous	00:00 - 04:00	>			
Alarm	04:00 - 08:00	>			
Motion Detection	08:00 - 10:00	>			
Event 10:00 - 12:00					
Motion Detection or Alarm 12:00 - 14:00					
Motion Detection and Alarm 14:00 - 18:00					
Region Entrance Detection 18:00 - 20:00					
Continuous	20:00 - 24:00	>			
Delete All	Copy to				

Figure 5-6 Setting Multiple Time Periods in a Day

7. Optional: Perform the following operations after saving the time periods in one day.

Copy to Other Days Tap **Copy to** to copy all the time periods settings to the other days in the week.

- **Delete All** Tap **Delete All** to clear all the configured time periods.
- 8. Tap 📄 to save the settings.

Configure Time Settings

You can select the time zone and set the time synchronization mode to Manual or NTP mode for the added device.

Steps

1. Enter the Settings page of the device.

- On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On the device name to the left and tap
- On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
- On the Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see *Start and Stop Live View*.

- 2. Enter the Remote Configuration page.
 - − For a device added via IP/Domain, tap \bigcirc → Remote Configuration.

iNote

For details about adding devices via IP/Domain, see Add a Device by IP/Domain.

- For a device added via other methods, tap **Remote Configuration** on the Settings page.

iNote

You should have configured DDNS for the device first. See *Set DDNS*.

- 3. Tap **Time Configuration** to enter the Time Configuration page.
- 4. Select the time zone in which the device locates.
- The device time will be adjusted automatically.
- 5. Select the time synchronization mode.
 - Select NTP Synchronization. And then set the interval for synchronizing the device time with the NTP server.

NTP Synchronization

Synchronize time at a specific interval with the NTP server.

iNote

For details about setting the NTP server details, refer to the user manual of the device.

_

- Select Manual Synchronization. And then tap Synchronize with Phone to synchronize the device time with the OS (Operation System) time of your phone or tablet.
- 6. Tap 📄 to save the settings.

Change Device Password

You can change the password of a device via the Mobile Client.

Steps

1. Enter the Settings page of the device.

- On the device list page, if the page is in list mode, swipe the device's name to the left and tap
 On the device list page, if the page is in list mode, swipe the device's name to the left and tap
- On the device list page, if the page is in thumbnail mode, tap the device's name or tap ••••.
- On the Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see *Start and Stop Live View*.

- 2. Enter the Remote Configuration page.
 - For a device added via IP/Domain, tap \bigcirc \rightarrow Remote Configuration.

iNote

For details about adding device via IP/Domain, see Add a Device by IP/Domain.

- For a device added via other methods, tap **Remote Configuration** on the Settings page.

iNote

You should have configured DDNS for the device first. See *Set DDNS*.

- 3. Tap **Change Password** to enter the Change Password page.
- 4. Enter the old password of the device
- 5. Create a new password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. Confirm the password.

7. Tap 📄 to save the changes.

Configure Normal Event

You can enable a device's normal event such as motion detection, video tampering alarm, video

loss alarm, for the channels of the device.

Steps

- 1. Enter the Settings page.
 - On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
 - On the Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see Start and Stop Live View.

- 2. Enter the Remote Configuration page.
 - − For a device added via IP/Domain, tap \bigcirc → Remote Configuration.

iNote

For details about adding device via IP/Domain, see Add a Device by IP/Domain

- For a device added via other methods, tap **Remote Configuration** on the Settings page.

iNote

You should have configured DDNS for the device first. See *Set DDNS*.

- 3. Tap Normal Event to enter the Normal Event page.
- 4. Optional: Select a channel if the device has multiple channels.
- 5. Set the switch(es) to ON to enable the event(s).

Configure Smart Event

You can enable the smart event for the channels of a device, including audio exception detection, face detection, and intrusion detection, etc.

Steps

Note

The supported event types of smart event vary according to different devices.

- 1. Enter the Settings page.
 - On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
 - On the Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see *Start and Stop Live View*.

- 2. Enter the Remote Configuration page.
 - − For a device added via IP/Domain, tap \bigcirc → Remote Configuration.

iNote

For details about adding device via IP/Domain, see Add a Device by IP/Domain.

- For a device added via other methods, tap **Remote Configuration** on the Settings page.

iNote

You should have configured DDNS for the device first. See *Set DDNS* for details.

- 3. Tap **Smart Event** to enter the Smart Event page.
- 4. Optional: Select a channel if the device has multiple channels.
- 5. Set the switch(es) to ON to enable event(s).

Enable Temperature Measurement

You can enable the temperature measurement function for the thermal camera on the Mobile Client.

Steps

iNote

This function is only available to the thermal camera.

- 1. Enter the Settings page.
 - On the device list page, if the page is in list mode, slide the device name to the left and tap

 On
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap
 - On the Live View page, tap •••• and then tap Settings.

iNote

For details about how to enter the Live View page, see *Start and Stop Live View*.

- 2. Enter the Remote Configuration page.
 - − For a device added via IP/Domain, tap \bigcirc → Remote Configuration.

iNote

For details about adding device via IP/Domain, see Add a Device by IP/Domain.

- For a device added via other methods, tap **Remote Configuration** on the Settings page.

iNote

You should have configured DDNS for the device first. See Set DDNS.

3. Tap **Temperature Measurement** to enter the Temperature Measurement page.

- 4. Optional: Select a camera if camera(s) are linked to the device.
- 5. Set the switch to ON to enable temperature measurement.

5.8 Upgrade Device Firmware

You can upgrade the firmware of a device to its latest version. If the latest version is detected, a red dot will appear on the Device Version field of the Settings page of the device.

Steps

- 1. Enter the Settings page.
 - On the device list page, if the page is in the list mode, swipe the device name to the left and tap ⁽²⁾.
 - On the device list page, If the page is in thumbnail mode, tap the device name or tap ••••.
 - On the Live View page. Tap •••• and then tap Settings.

iNote

For details about how to enter the Live View page, see Start and Stop Live View.

2. Tap **Device Version** to enter the Device Version page.

3. Tap Upgrade.

The Mobile Client will download the upgrade file first and then start upgrading the device.

iNote

You can also enable the Mobile Client to automatically download the upgrade file in Wi-Fi networks once a new device version is detected. For details, see *Auto-Download Upgrade File*.

Chapter 6 Favorites Management

You can add the frequently-used camera(s) to the favorites so that you can access them conveniently.

6.1 Add Cameras to Favorites on Device List Page

On the device list page, you can add the frequently-used camera(s) to the favorites so that you can access them conveniently.

Steps

- 1. On the device list page, tap 🕒.
- 2. Tap Add to Favorites.
- 3. Select devices and cameras on the Select Camera page.
- 4. Тар **ОК**.
- 5. Create a name for the Favorites and then tap **OK**.

iNote

- Up to 32 favorites can be added.
- The favorites name should be no more than 32 characters.

The added Favorites will be displayed on the device list page.

6. Optional: Tap the Favorites name on the device list page to view the cameras' live videos.

6.2 Add Cameras to Favorites During Live View

On the live view page, you can add frequently-used cameras to Favorites so that you can access them conveniently

Steps

1. Enter the Live View page.

iNote

For details about how to enter the Live View page, see Start and Stop Live View

2. Tap •••• and tap Add to Favorites.

- 3. Add cameras to favorites.
 - Create a new favorites in the pop-up window and tap **OK**.
 - 1. Add to existing favorites. Tap **Add to Existing Favorites** in the pop-up window.
 - 2. Select a Favorites folder in the list.
 - -

iNote

```
• Up to 32 Favorites can be added.
```

The favorites name should be no more than 32 characters.

4. Optional: Tap the Favorites on the device list page to view the cameras' live videos.

6.3 Remove Cameras from Favorites

You can delete cameras in the favorites.

Steps

1. Enter the Edit Favorites page.

On the device list page, if the page is in list mode, swipe the Favorites name to the left and tap On the device list page, if the page is in thumbnail mode, tap of the Favorites.

2. Tap a camera that need to be deleted.

3. Tap **Confirm** in the pop-up window to delete the camera.

Chapter 7 Share Device

You can share devices to other users. After that, they can access the devices according to the permissions you configured for them. You can also receive devices shared by other users.

7.1 Share a Specific Device via Its QR Code

You can share a specific device to another Hik-Connect user via the device's QR code. You can also set the device permissions granted to the recipient to determine which operations he/she can do on the device.

Steps

1. Enter the Recipient page.

Option 1	Tap \bigoplus \rightarrow Share Device \rightarrow Share Device.
Option 2	 Tap To display the device list page in list mode. Swipe the target device's name to the left, and then tap S^o.
Option 3	 Tap = to set the display the device list page in thumbnail mode. Tap <.
Option 3	1. Enter the Live View page.
	I Note For details about how to enter the Live View page, see Start and Stop Live View .
	 Select a live view window and than tap . Tap Share.
Option 4	For security control panel, tap the device on device list page to enter the device details page and then tap <.
You will enter the Rec	ipient page.

- 2. Tap **Share via QR Code** and then select a device (if required) to enter the Share via QR Code page.
- 3. Swipe up to show the complete QR code.
- 4. Let the recipient use the Hik-Connect Mobile Client to scan the QR code. The recipient needs to send a device sharing application to you. After that, you'll receive a

notification about the application on your Mobile Client.

- 5. Tap **View** on the notification to view the details of the application.
- 6. Set device permissions for the recipient.
 - Check All Permissions to grant all available permissions to the recipient, including the permissions for live view, remote playback, receiving and viewing alarm information, two-way audio, and PTZ control.
 - − Tap >, and then select permission(s) to grant the selected one(s) to the recipient, and finally tap ■.
- 7. Tap Agree.

The device will be shared to the recipient. And he/she will be able to view the device on the device list of his/her Hik-Connect account.

- 8. Optional: Edit the device permissions.
 - 1) Go to More \rightarrow Manage Sharing Settings.
- 2) Tap the device and then edit the device permissions granted to the recipient.
- 9. Optional: Delete the recipient account and all the sharing information.
 - 1) Go to More \rightarrow Manage Sharing Settings.
 - 2) Tap the device to enter the Sharing Details page and then tap **Delete**.

7.2 Share Multiple Devices in a Batch

If another user of the Mobile Client needs to use multiple devices of yours, you can share them in a batch to him or her with the least operation effort, and at the same time determine the permission(s) that the recipient has to access each device. For example, if you do not grant the two-way audio permission of a device to the recipient, the recipient will have no access to the two-way audio functionality of the device.

Steps

- 1. Enter the Manage Sharing page.
 - Tap $\bigoplus \rightarrow$ Share Device.
 - − Tap More → Manage Sharing Settings.
- 2. Enter the Recipient page.
 - For the first time sharing, tap 🕛
 - For other occasions, tap Share Device.
- 3. Set the account that you want to share device(s) with.

Manually Add a Recipient	1.	Enter the email address or the mobile phone number bound with the recipient's account in the Search box.
	2.	If matched history account(s) exists, select a history account.
		If no matched history account(s) found, tap Add Recipient to enter the Add Recipient page.
	3.	(Optional) Enter a remark for the recipient, such as his or her
		name.
	[iNote

Only you can view the remark content while the user you shared with can not.

- Tap ✓ to select the recipient's account and add it to the history account list.
- 5. Tap Next.
- Add Recipient by1. Tap $\begin{bmatrix} \neg \\ \neg \end{bmatrix}$ on the Recipient page to scan the QR code of the targetScanning QR Codeaccount.

The account will be listed on the account list.

iNote

Go to More \rightarrow Account Management \rightarrow My QR Code to get the QR code of your account.

2. Select the account from the history account list and than tap **Next**.

4. Select device(s).

Note

For devices linked with multiple cameras, you can select camera(s) for sharing.

- 5. Configure permissions for the to-be-shared device(s).
 - Check All Permissions on the Sharing Details page to select all the permissions.
 - Tap the device displayed on the Sharing Details page, and then select permission(s) and tap
 .

Example

For example, if you select Live View and Remote Playback, the recipient will have the permissions to view live video and play back the video footage of the device.

6. Tap Finish to finish sharing.

A message about the sharing will appear on the recipient's Mobile Client. He or she can tap the message, and then accept or reject the shared device.

7. Optional: Tap the account on the history account list and then tap **Delete** to delete the recipient's account and all the sharing information.

7.3 Silenced Mode for Devices Shared by Others

You can enable Silenced mode for the devices shared by others if you don't want to be disturbed by the devices' alarm notifications. When enabled, all the alarm notifications triggered by the device(s) will be silenced. And you can still check the information of all the silenced alarm notifications from the devices on the notification list.

Enter the Settings page of the device in one of the following ways, and then enable the Silenced mode.

- On the device list page, if the page is in the list mode, swipe the device name to the left and tap <a>[6].
- On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
- On the device's Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see *Start and Stop Live View*.

Chapter 8 Live View

You can view live video of the devices' connected cameras. And some basic operations are supported during live view, including picture capturing, manual recording, PTZ control, etc.

8.1 Start and Stop Live View

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

Steps

1. Enter the Live View page to start live view.

 On the device list page, if the device list is displayed in thumbnail mode, tap the device thumbnail to enter the Live View page.

iNote

You can tap **T** or **T** on the device list page to switch between the list mode and the thumbnail mode.

 On the device list page, if the device list is displayed in list mode, and the Floating Live View function is enabled, tap one or more devices to open the floating windows. And then tap the floating window to enter the Live View page.

iNote

- For details about enabling or disabling the Floating Live View function, see *Floating Live View*.
- Up to 256 cameras can be selected.
- On the device list page, if the device list is displayed in list mode, and the Floating Live View function is disabled, tap the device 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 device verification code before the live video starting playing.

iNote

- For details about Video and Image Encryption function, see *Set Video and Image Encryption*.
- 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.
- $\circ\,$ 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. Optional: 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	 Tap 2 to go back to the device list. Reselect cameras and then tap OK.
	INote You can select up to 256 cameras.
Switch to Playback	Tap \cdots \rightarrow Playback to switch to playback.
	☐ i Note For details about playback, see Playback .

- 3. Stop live view of a camera.
 - 1) Press and hold a window under live view.
 - 2) Drag the window upwards to the appearing $\overline{\mathbf{m}}$ at the top of the page.

8.2 Set Window Division

You can adjust window division in different scenarios.

Tap 1, 4, 9, 12 or 16 to set the window division mode to 1-window, 4-window, 9-window, 12-window, or 16-window respectively.

If the added camera number is more than the window division number, you can swipe to the left or right to change the window division group on the current page.

8.3 Digital Zoom

Digital zoom adopts encoding technology to enlarge the image which will result in image quality damage. You can zoom in or zoom out the live video image as desired.

Tap 🔘 to zoom in or zoom out the image.

Or spread two fingers apart to zoom in, and pinch them together to zoom out.

8.4 PTZ Control

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. For some network cameras, you can also enable auto-tracking to make the camera pan, tilt, and zoom to track the detected moving objects.

iNote

PTZ control should be supported by the camera.

8.4.1 Pan and Tilt a Camera

The Mobile Client allows you to pan and tilt a camera's view.

Steps

1. Start live view of a camera supports PTZ control.

iNote

For details about how to start live view, see *Start and Stop Live View*.

- 2. Select a live view window on the Live View page.
- 3. Tap 💿 to open the PTZ Control panel.

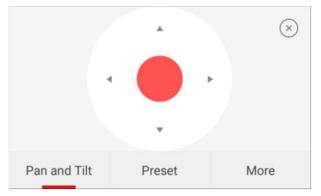


Figure 8-1 PTZ Control Panel

4. Tap Pan and Tilt.

5. Drag the circle button at the center of the PTZ Control panel to pan and tilt the camera.

8.4.2 Set a Preset

A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. You can also set a virtual preset after enabling digital zoom. After you set a preset, you can call the preset and then the camera will move to the programmed position.

Steps

1. Pan and tilt a camera to move the camera direction to a desired position.

See **Pan and Tilt a Camera** for details.

2. In the PTZ Control panel, tap **Add Preset** to open the following window.



Figure 8-2 Set a Preset

3. Swipe the number up or down to set the preset No.

iNote

The preset No. should be between 1 and 256.

- 4. Tap **Set** to complete setting the preset.
- 5. Tap **Call** to call the preset.
- 6. Optional: Tap **Delete** to delete the preset.

8.4.3 Adjust PTZ Speed

You can adjust the PTZ speed.

Steps

- 1. Start live view of a camera which supports PTZ control.
- 2. Tap to open the PTZ control panel.
- 3. Tap **More** \rightarrow to open the PTZ speed panel.
- 4. Drag the slider to adjust the PTZ speed.

8.4.4 Other Functions

The PTZ Control panels provide other functions such as PTZ speed adjustment, auto-scan, focus control, iris control, and auto-tracking.

Tap **More** on the PTZ Control panel to view the functions.

lcon	Description
	Start/stop the auto-scan, which means to make the speed dome pan, tilt, and (or) zoom by a predefined route.
(¢)	 Note You can define the route on the device. For details, see the user manual of the device. The function should be supported by the device.
	Zoom control: 🕵 Zoom+/ 🌇 Zoom-
\oplus	Focus control: 🞯Focus +/🕙 Focus -
	Iris control: 🔞Iris +/ 🐼 Iris -
	Adjust PTZ speed.
	Enable/Disable auto-tracking. After enabled, when the camera detects a moving object, the camera will pan, tilt, and zoom to track the object until the object moves out of the field of view of the camera.
*	IiNote The function should be supported by the device.

8.5 Start Two-Way Audio

Two-way audio function enables the voice talk between the Mobile Client and devices. You can get and play not only the live video but also the real-time audio from the devices, and the devices can

also get and play the real-time audio from the Mobile Client.

Steps

iNote

- The function should be supported by the device.
- The devices added by Hik-Connect domain or by scanning QR code do not support this function.

1. Start live view of the device.

iNote

See Start and Stop Live View for details.

- 2. Tap 📱 in the toolbar to turn on the two-way audio.
- 3. If the device is a NVR, select the device or its linked network camera as the two-way audio channel.

iNote

If not, skip this step.

- If the device is full duplex, two-way audio will be started automatically.
- If the device is half-duplex, you have to tap and hold 🧕 to talk, and release to listen.

4. Tap 🛞 to turn off two-way audio.

8.6 Capturing and Recording

During live view, you can capture pictures of the live video and record video footage.

Steps

1. Start live view of a camera.

INote See *Start and Stop Live View* for details.

2. Capture a picture or record video footage.

Capture Picture Tap **o** to capture a picture.

Record Video Tap **I** to start recording video footage, tap again to stop.

Footage

The captured pictures and recorded videos will be saved in **More** \rightarrow **Pictures and Videos**. For details about managing pictures and videos, see **Pictures and Videos**.

8.7 Set Image Quality for Device Added by IP/Domain

For devices added via IP/Domain, you can set its image quality to Fluent or Clear. You can also customize image quality for the devices.

Steps

iNote

- 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.

iNote

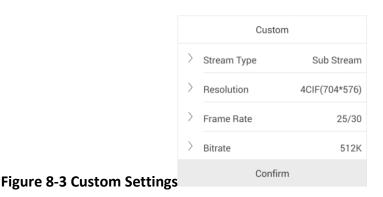
See Start and Stop Live View for details.

2. Tap **BASIC** on the live view page to enter the quality switching panel.

iNote

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.



iNote

• 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 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).

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
H.264 (Software	-	2 0.11		
•				
1080P	V	V		Frame rate: 25fps; Bit rate: 4Mbps
720P	V	٧	٧	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	v	V	v	Frame rate: 25fps; Bit rate: 512Kbps
H.264 (Hardwar	e Decoding)			
1080P	V	V	V	Frame rate: 25fps; Bit rate: 4Mbps
720P	V	V	V	Frame rate: 25fps; Bit rate: 2Mbps
4CIF	v	v	v	Frame rate: 25fps; Bit rate: 512Kbps
H.264+ (Softwar	re Decoding)			
1080P	V	V		Frame rate: 25fps; Bit rate: 4Mbps
720P	V	v	V	Frame rate: 25fps; Bit rate: 2Mbps
H.264+ (Hardware Decoding)				
1080P	V	V	V	Frame rate: 25fps; Bit rate: 4Mbps
720P	V	V	V	Frame rate: 25fps; Bit rate: 4Mbps
H.265 (Software Decoding. Hardware decoding is not supported.)				
1080P	V	V		Frame rate: 25fps; Bit rate: 2Mbps
720P	٧	V	V	Frame rate: 25fps; Bit rate: 4Mbps
4CIF	V	V	V	Frame rate: 25fps; Bit rate: 256Mbps

Table 8-2 Recommended Configuration

8.8 Set Image Quality for Hik-Connect Device

Usually three pre-defined image qualities are provided in the Mobile Client for Hik-Connect device: Basic, Standard, and High Definition.

Steps

iNote

The provided image quality types may vary with different devices.

1. Start live view of a Hik-Connect device.

iNote

See Start and Stop Live View for details.

2. Tap BAS

BASIC to enter the quality switching panel.

iNote

The icon may vary with the actual image quality.

3. Set image quality.

Basic

Basic image quality.

iNote

Basic is the default image quality.

Standard

Standard image quality (the image quality is higher than that of Basic and lower than that of HD).

HD

High definition image quality (the image quality is the highest of the three).

8.9 Live View for 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.

Steps

iNote

The function is only supported by fisheye camera.

1. Start live view of a fisheye camera.



See Start and Stop Live View for details.

- 2. Tap 🔘 to show the fisheye expansion panel.
- 3. Select mounting type.

Table 8-3 Mounting Type

lcon	Description
D	Wall Mounting
\Box	Ceiling Mounting

4. Select fisheye expansion mode.

Table 8-4 Fisheye Expansion Mode

lcon	Description
0	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

Hik-Connect Android Mobile Client User Manual

lcon	Description
	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.
88	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.
0	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.
	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.

8.10 Open Door 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.

iNote

- The device should support this function.
- For face recognition terminals, you can enabling opening door by fingerprint authentication or facial authentication. For details, see *Enable Opening Door via Fingerprint (Face) Authentication*.

For the access control device's related cameras, select a live view window and tap (1), and then enter the device verification code to open the door.

For the video intercom device, select a live view window and tap 6, and then enter the device verification code to open the door.

iNote

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.

Chapter 9 Playback

You can search the recorded video files stored in the added device for remote playback.

9.1 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.

Steps

- 1. On the device list page, tap 💿 at the upper-left corner to enter the Select Item(s) page.
- 2. Set the date and time for playback.

Playback Date

Select a date.

iNote

The date during which video files were recorded is marked with a yellow dot.

Playback Time

Set the start time point for the playback in the selected date.

3. Select camera(s).

iNote

You can select up to 4 cameras.

- 4. Tap **Start Playback** to enter the Playback page.
- 5. Optional: Perform the following operations.

Adjust Playback Time Slide the timeline to adjust the playback time.

INote

represents continuous recording and

represents

event-triggered recording. You can determine the recording type (continuous or event-triggered) when setting recording schedule. For details, see *Set Recording Schedule*.

Scale up and down	Spread two fingers apart to scale up the timeline or pinch them
Timeline	together to scale down.

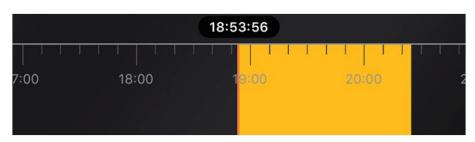


Figure 9-1 Timeline

9.2 Event Playback

Event playback refers to the playback based on the detected events, such as motion detection. You can select an event and then play back the event-related video footage. Duration playback, you can also save the event-related picture if it has been captured by the camera.

Before You Start

You should have configured events for the selected camera. For details, see **Configure Normal Event** and **Configure Smart Event**.

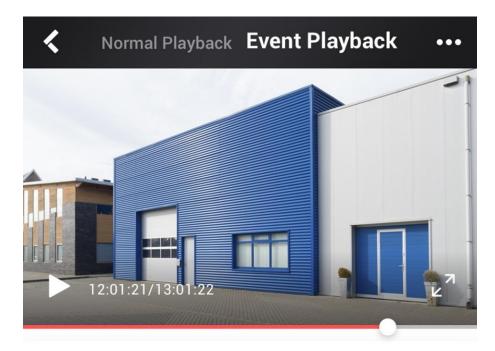
Steps

1. Start normal playback.

iNote

For details, see *Normal Playback*.

2. Tap **Event Playback** to enter the Event Playback page. The event-related video footage within the latest 7 days will be displayed.



12/7 12/6 12/5 12/4 12/3 12/2 12/1



Motion Detection Alarm 11:05:56



Motion Detection Alarm

11:04:23



Motion Detection Alarm

Motion Detection Alarm

Figure 9-2 Event Playback Page

- 3. Select a date and then tap an event to start playback.
- 4. Optional: Tap ••• and then tap **Save Image** to save the event-related picture.

iNote

You should have configured the required event linkage action (capturing event-related picture) for the device. For details, see the user manual of the device.

9.3 Capturing and Recording

During playback, you can capture pictures and record video footage.

Steps

1. Start playback.

i Note	
See Normal Playback for details.	
2. Capture a picture or record video footage.	

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

The captured pictures and recorded videos will be saved in **More** \rightarrow **Pictures and Videos**. For details about managing pictures and videos, see **Pictures and Videos**.

9.4 Set Playback Quality for Device Added by IP/Domain

For devices added by IP/Domain, you can set the image quality of playback for them.

Steps

Note

For details about adding device by IP/Domain, see Add a Device by IP/Domain.

1. Select a device added by IP/Domain on the device list and then start playback.

iNote

For details about starting playback, see Normal Playback.

2. Tap **BASIC** on the playback page to enter the quality switching panel.

iNote

The icon may vary with the actual video quality.

- 3. Set the image quality as desired.
 - Tap **Clear** to tap the image quality to Clear.
 - Tap Custom to open the Custom Settings window, and then configure the parameters (Resolution, Frame Rate, and Bitrate) and tap Confirm to confirm the custom settings.

iNote

- The image effect is related to the performance of your network and phone or tablet. If the image is not fluent or the screen appears blurred, reduce the resolution, frame rate and bitrate of the camera in custom mode.
- The following table shows the recommended 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).

Resolution	1-ch	2-ch	4-ch	Recommended Configuration		
H.264 (Software Decoding)						
1080P	V	V		Frame rate: 25fps; Bit rate: 4Mbps		
720P	٧	V	V	Frame rate: 25fps; Bit rate: 2Mbps		
4CIF	v	v	v	Frame rate: 25fps; Bit rate: 512Kbps		
H.264 (Hardware Decoding)						
1080P	٧	V	V	Frame rate: 25fps; Bit rate: 4Mbps		
720P	٧	V	V	Frame rate: 25fps; Bit rate: 2Mbps		
4CIF	v	V	V	Frame rate: 25fps; Bit rate: 512Kbps		
H.264+ (Software Decoding)						
1080P	٧	V		Frame rate: 25fps; Bit rate: 4Mbps		
720P	٧	V	V	Frame rate: 25fps; Bit rate: 2Mbps		
H.264+ (Hardware Decoding)						
1080P	٧	V	V	Frame rate: 25fps; Bit rate: 4Mbps		
720P	V	V	V	Frame rate: 25fps; Bit rate: 4Mbps		
H.265 (Software Decoding. Hardware decoding is not supported.)						
1080P	٧	٧		Frame rate: 25fps; Bit rate: 2Mbps		

Table 9-1 Recommended Configuration

Resolution	1-ch	2-ch	4-ch	Recommended Configuration
720P	٧	٧	v	Frame rate: 25fps; Bit rate: 4Mbps
4CIF	V	V	V	Frame rate: 25fps; Bit rate: 256Mbps

9.5 Download Video Segment

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

Steps

iNote

The function should be supported by the device.

1. Start playback.

2. Tap M 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.

iNote

In special occasions when 130-seconds duration is not available to be selected following the above-mentioned rule, the segment will extend afterwords 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. Optional: Drag the slider(s) to lessen the duration of the segment for download.

iNote

The duration should not be shorter than 10 seconds.

4. Optional: Tap the Play icon to preview the selected segment.

iNote

If the segment is encrypted, you should enter the device verification code before you can preview it. For details about video encryption, see *Set Video and Image Encryption*.

5. Tap **Download** to start downloading.

iNote

Download at the background is supported. The download continues if you exit the Download page or the Mobile Client.

6. Optional: Go to More \rightarrow Pictures and Videos to view the downloaded video segment.

9.6 Adjust Playback Speed

For the cameras linked to a DVR or NVR, you can adjust the playback speed for them as required.

⊡Note

The function should be supported by the device.

During playaback, you can swipe the toolbar at the bottom to view the hidden icons, and then tap to set the playback speed to 1/8X, 1/4 X, 1/2 X, 1X, 2X, 4X, and 8X. X here refers to the original playback speed.

Chapter 10 Access Control

Access control is the selective restriction of access to a place or other resources. After adding access control devices to the Mobile Client, you can remotely control the doors, and configure duration in which the doors remain open. You can also filter and view access control device's logs, which provide the information of access events and related alarms, such as access controller tampering alarm.

Besides the above-mentioned functionality, you can change supper password of the access control device. And for face recognition terminals, you can enable fingerprint authentication or facial authentication to open doors.

10.1 Control Door Status

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

Before You Start

Add an access control device to the Mobile Client. See Add Device for Management for details.

Steps

iNote

You can change the super password. See *Change Super Password* for details.

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

control page.

INote

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.

iNote

For details about configuring the time period, see *Set Door Open Duration*.

Remain Closed

Keep the door closed. In this status, the door can only be opened by super card or super password.

iNote

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

3. Enter the super password.

iNote

- 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. See *Change Super Password* for details.

The door status will change.

10.2 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.

Before You Start

You should have added an access control device to the Mobile Client. See *Add Device for Management* for details.

Steps

- 1. Enter the Settings page of the access control device.
 - On the device list page, if the page is in the list mode, swipe the device name to the left and tap ⁽²⁾.
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap ••••.
 - On the Live View page, tap •••• and then tap **Settings**.

iNote

For details about how to enter the Live View page, see *Start and Stop Live View*.

- 2. Tap Door Open Duration to open the Door Open Duration list.
- 3. Select a duration from the list.
- 4. Tap \odot to confirm the selection.

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

iNote

For details about controlling door status, see *Control Door Status*.

10.3 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.

Before You Start

Add an access control device to the Mobile Client. See Add Device for Management for details.

Steps

iNote

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

- 1. Enter the Settings page of the access control device.
 - On the device list page, if the device list is in list mode, swipe the name of the access control device to the left and tap
 - On the device list page, if the device list is in thumbnail mode, tap the name of the access control device or tap ***.
 - On the Live View page. tap •••• and then tap Settings.

iNote

For details about how to enter the Live View page, see Start and Stop Live View

- 2. Tap **Change Password** to enter the Change Password page.
- 3. Enter the old password and tap Next.

iNote

If it is the first time to set the super password, skip this step.

4. Create a new password and then tap Finish.

iNote

The password should contain 6 numbers.

10.4 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.

Steps

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 10-1 The Icon Representing Door

The log list will be displayed on the Log section of the page.

2. Perform the following operations.

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.		

10.5 Enable Opening Door via Fingerprint (Face) Authentication

After adding face recognition terminals to the Mobile Client, you can enable opening door via fingerprint authentication or face recognition.

iNote

Your phone or tablet should support fingerprint authentication or face authentication.

After adding a face recognition terminal, when you open the device's related door for the first time, a prompt will pop up asking you whether to enable opening door via fingerprint authentication or face recognition or not. You can follow the prompt to enable this functionality. If you have ignored the above-mentioned prompt, you can go to the Settings page of the device to enable this functionality in one of the following ways:

- On the device list page, if the page is in list mode, you can swipe the name of the device to the left, and tap the appearing 💿 to enter the Settings page, and then set the switch of the functionality to on.
- On the device list page, if the page is in thumbnail mode, you can tap ••• to enter the Settings page, and then set the switch of the functionality to on.
- On the details page of the device, you can tap 🔯 to enter the Settings page, and then set the

switch of functionality to on.

Chapter 11 Security Control

The Mobile Client supports video security control panel, Axiom security control panel (including Axiom Hub and Axiom Hybrid), and Pyronix security control panel.

A security control panel can be used to manage the devices needed in a security system, which can be used for detecting events (e.g., intrusion, smoke, water leakage, etc.,) within predefined regions (zones), triggering event signals and alarm signals, and uploading event information and alarms to the surveillance center.

11.1 Video Security Control Panel

You can add video security control panel to the Mobile Client. Video security control panel supports analog or digital HD video input and can be used cooperatively with the video surveillance and access control system over client software. It supports uploading reports to the alarm receiving centers with various transmission modes such as PSTN, network and GPRS. On the Mobile Client, you can set partition status, manage zones, and set voice prompt for the security control panel.

11.1.1 Partition and Zone Control

The Mobile Client allows you to set arming mode of a partition, and control the zones. You can set arming mode for a specific zone, set zone parameters, link a camera to a zone, etc. Partition, which is an independent control system of a security control panel, allows you to batch arm/disarm all zones in it. If the security control panel has two partitions, you have two independent systems for arming or disarming.

Zone is a basic concept in the security control panel system. It refers to a protection area in the system, and is regarded as the maximum recognizable unit to distinguish the alarm event.

iNote

For more information about partition and zone, see the user manual of the security control panel.

Control A Zone

You can set the arming mode of a single zone to arm or disarm.

Before You Start

Enable single zone arming or disarming via iVMS-4200 client software. For details, see the user manual of the security control panel.

Steps

1. On the device list, tap the arming status icon on the right of the security control to enter the Partition page.

- 2. Optional: If the device contains more than one partition, tap the partition name at the top of the page to switch partitions.
- 3. Select a zone in the partition and tap the switch icon to arm or disarm it.

Control All Zones in One Partition

You can control the arming status of all zones in a partition.

Steps

iNote

- The function should be supported by the device.
- The security control panel's Single Zone Arming or Disarming function should be disabled. For details, see the user manual of the security control panel.
- 1. On the device list, tap the arming status icon on the right of the security control to enter the Partition page.

\leftarrow	Partition1 ~	¢
		Clear Alarm
Away	Stay	Disarm
Zone		+
Zone1		(১) ব্রিট
Zone 2		ţŷţ
Zone 3		ţĊŗ
Zone © Normal		ţĊŗ

Figure 11-1 Partition Page

- 2. Optional: If the device contains more than one partition, tap the partition name at the top of the page to switch partitions.
- 3. Optional: View zone status.

Bypass

The zone is bypassed. For details about bypassing a zone, see **Bypass a Zone**.

Fault

The detector is faulty.

iNote

When a zone is faulty, bypass the zone to ensure the partition which the zone belongs to can be armed.

4. Control all zones in the partition.

Away

When all the people in the detection area leave, turn on the away arming mode to turn on all zones in the partition after the defined dwell time.

Stay

When the people stays inside the detection area, turn on the stay arming mode to turn on all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony). At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarm will not be triggered.

Disarm

In disarming mode, all the zones in the partition will not trigger alarm, no matter alarm events happen or not.

Clear Alarm

When zones in the partition trigger alarms, tap **Clear Alarm** to clear the sound and light alarming prompt.

Delay

Set the enter delay time and the exit delay time for the delayed zone.

Enter Delay Time

The waiting period between the indoor station triggering alarms and sending alarm information to the alarm center. Therefore, during entering delay time, you can disarm the zone without triggering alarms.

Exit Delay Time

The time period between the time when you arm the indoor station and the time when the arming take effect. Exit delay allows you to exit the zone without triggering alarms after arming the zone.

11.1.2 Add a Zone

The Mobile Client allows you to add zones (detectors) to the security control panel.

Before You Start

Add a video security control panel to the Mobile Client. See *Add Device for Management* for details.

Steps

- 1. On the device list page, tap the arming status icon on the right of the video security control panel to enter the Partition page.
- 2. Tap $\,+\,$ to scan the detector's QR code.

iNote

The QR code is usually on the back cover of the detector.

- 3. Optional: Manually add the detector if the QR code is not recognized.
 - 1) Tap 🗾, and then enter the detector's serial number.
 - 2) Tap \subseteq to search for the detector.
- 4. Tap Add on the Result page.
- 5. Tap Finish.

11.1.3 Set Zone Parameters

You can set zone parameters such as zone name, zone type, and detector type. Select a zone on the Partition page and tap 🔯 to enter the Settings page of the zone.

Edit Zone Name

Tap the zone name to edit it.

Note

The zone name should contain 1 to 50 characters.

Set Zone Type

Tap the zone type to select a type from the Zone Type page.

Instant Zone

The zone will be immediately triggered when it detects alarm event without entering and exiting delay. The detectors of this zone are in alert condition for 24 hours every day. The detectors can be affected by arming and disarming operation, and can be bypassed. When the zone detects alarm events, the sound and light alarming prompt will be triggered on the keyboard. The siren output will be triggered when the siren is linked, meanwhile the generated event report will be uploaded to the center receiver (reporting code is different from 24-hour audible alarm zone), and the zone alarm status can be checked on the Mobile Client. It is

generally applied to smoke detector.

iNote

Detectors in instant zone can be affected by arming or disarming operation, and can be bypassed.

24H Silent Alarm Zone

The detectors of this zone are in alert condition for 24 hours every day. The detectors will not be affected by arming and disarming operation or be bypassed. When the zone detects alarm events, the sound and light alarming prompt will be triggered on the keyboard. The siren output will be triggered when the siren is linked, meanwhile the generated event report will be uploaded to the center receiver, and the zone alarm status can be checked on the Mobile Client. This zone type is generally applied to the sites equipped with emergency button (e.g. bank and jewelry counter).

Delayed Zone

The zone will not be in alert condition during exit delay and enter delay. Exit Delay provides you time to leave through the defense area without alarm. Entry Delay provides you time to enter the defense area to disarm the system without alarm. This zone type is mainly used in entrance/exit route (e.g. front door/main entrance), which is a key route to operate keyboard for users.

Internal Zone

The internal zone is usually set within a delayed zone. After arming the partition, if the delayed zone is triggered first, the system will provide entry delay for both the delayed zone and the internal zone. If not, the internal zone will trigger alarm instantly. The delay parameters of internal zone are the same with that of the delayed zone. It is usually set in the rest room or hall (e.g. motion detector), which is a key place to operate keyboard for users.

iNote

For the introduction of other zone types, see the user manual of the security control panel.

Set Detector Type

Tap **Detector Type** to select a detector type.

Active Infrared Detector

The detector consists of infrared emission device and infrared receiving device. If the infrared ray sent from the emission device is blocked, and the receiver cannot receive the infrared ray, the device will send an alarm.

Passive Infrared Detector

The detector doesn't emit any energy itself. It only receives emissions from environments. When the infrared rays from living things are detected, the detector will send an alarm.

Dual Technology Motion Detector

The detector consists of a Passive Infrared Receiver (PIR) and microwave sensor, the two need to be activated simultaneously to trigger an alarm.

iNote

For the introduction of other detector types, see the user manual of the security control panel.

11.1.4 Bypass a Zone

If you bypass a zone, the zone will NOT be in alert condition (related alarms will not be triggered and related faults will not be detected) even when the system (or partition) which it belongs to is armed. Bypassing a zone is usually used in the following two scenarios. The first is that if a zone is faulty, other zones of the same system (or partition) can be armed only when the faulty zone is bypassed. The second is that you simply want a specific zone NOT to trigger alarms in special occasions.

Select a zone on the Partition page and tap 🔯 to enter the Settings page of the zone, and then enable zone bypass.

iNote

For details about how to enter the Partition page, see Partition and Zone Control.

11.1.5 Link Camera to Zone

After linking a camera to a zone, you can view the live video of the zone on the Mobile Client.

Steps

- 1. On the device list, tap the arming status icon on the right of the security control to enter the Partition page.
- 2. Optional: If the device contains more than one partition, tap the partition name at the top of the page to switch partitions.
- 3. Tap 🔯 to enter the Setting page of the zone.
- 4. Select a camera in Available Camera section.

iNote

You can swipe the camera group to the left or right to view all the available cameras.

- 5. Tap **Link** to link the selected camera to the zone.
- 6. Tap **Finish**

ive will be displayed on the right side of the zone in the zone list. You can tap it to view the zone's live video.

11.1.6 Enable Voice Prompt

For a security control panel, the voice prompt offers you information about system operations or the triggered alarms.

iNote

The function should be supported by the device.

On the device list page, slide the device to the left and tap 🙆 or … to enter the Settings page. Tap the switch icon of Device Voice Prompt to enable or disable the function.

11.1.7 Delete Zone

You can delete a specific zone from a security control panel.

Steps

- 1. On the device list, tap the arming status icon on the right of the security control to enter the Partition page.
- 2. Optional: If the device contains more than one partition, tap the partition name at the top of the page to switch partitions.
- 3. Select zone and tap 🔯 to enter the Settings page.
- 4. Tap **More** \rightarrow **Delete** to delete the zone.

11.2 Axiom Security Control Panel

After adding the Axiom security control panel to the Mobile Client, you can add peripheral devices (including detectors, keyfobs, wireless outputs expander, and siren) and cards/tags to the control panel. After that, you can control the alarm system by remotely arming or disarming areas via the Mobile Client, remotely pressing keys on keyfob, or swiping card.

Currently the supported Axiom security control panel includes Axiom Hub and Axiom Hybrid. The former only supports wireless peripheral devices, the latter supports both wired and wireless peripheral devices.

iNote

For details about how to add an Axiom security control panel to the Mobile Client, see Add a Device by Scanning Device QR Code or Add a Device by Hik-Connect Domain.

11.2.1 Log in to the Security Control Panel

If the installer (or setter), which is a type of user of the security control panel, has enabled EN50131 Compliant mode, you should log in to the device before you can access the device.

Note

For details about EN50131 Compliant mode, see EN50131 Compliant Mode.

On the device list page, tap the security control panel to enter the Verify Device page and then log in to the device.

11.2.2 Configure Axiom Security Control Panel

On the Settings page of the security control panel, you can view and edit the basic information such as device name. You can also do configurations such as device time settings, area management, use management, etc.

iNote

There are four types of users, including administrator (or owner), operator, installer (or setter), and manufacturer. Different types of users have different permissions for the configuration of the security control panel. For details about the four types of users, see the user manual of the security control panel.

System Options

You can set system options such as system fault report, siren delay time, alarm duration, etc. On the device list page, tap the security control panel and log in to the device (if required) to enter the Area page, and then tap $\bigcirc \rightarrow$ **System Options** to enter the System Options page.

Option Management

On the Option Management tab, you can do the following configurations.

Wireless Device Supervision

If enabled, the system will detect the status of all wireless devices.

System Fault Report

If enabled, the system will upload a report automatically when there is a system fault.

Disable Function Key

If enabled, all function keys will be disabled.

Siren Delay Time (Perimeter Alarm)

The delay time to trigger the linked siren when a perimeter zone is triggered.

iNote

- For details about perimeter zone, see the user manual of the security control panel.
- The valid duration is from 0 s to 600 s.

Alarm Duration

If you have set the perimeter zone, you can set the time duration of the alarm.

iNote

The valid duration is from 1 s to 900 s.

Fault Check

On the Fault Check tab, you can do the following configurations.

Detect Network Camera Disconnection

If enabled, when the linked network camera is disconnected, alarm will be triggered.

Panel Battery Fault Check

If enabled, when battery is disconnected or out of charge, the device will upload an event.

Wired Network Fault Check

If enabled, when the wired network is disconnected or has other faults, alarm will be triggered.

Wi-Fi Fault Check

If enabled, when the Wi-Fi is disconnected or has other faults, alarm will be triggered.

Cellular Network Fault Check

If enabled, when the cellular data network is disconnected or has other faults, alarm will be triggered.

SIM Card Fault Check

If enabled, the alarm will be triggered when the SIM card has faults.

AC Power Down Check Time

An alarm will be triggered if the AC power-down duration exceeds the configured time. To comply with the EN 50131-3 standards, set the value to 10 s.

Area Management

You can enable specific area(s), and configure the public area.

On the device list page, tap the security control panel and log in to the device (if required) to enter the Area page, and then tap $\bigcirc \rightarrow$ Area Management to enter the Area Management page.

Enable Area

On the Enable Area tab, you can select area(s) to enable them. After the selected area(s) being enabled, you can do configurations such as linking zones to the area, delay time configuration, and

weekend exception. For details, see Set Area Parameters.

Public Area Configuration

On the Public Area Configuration tab, you can set the switch to on to set area 1 as the public area, and then set other areas (e.g., area 2 and area 3) as the areas linked to the public area.

- Logic: Public area is a special area which can be shared with other areas. The public area is armed automatically when all areas linked with the public area are armed; And the public area is disarmed automatically when any one of areas linked with the public area is disarmed. The user can also arm or disarm the public area independently.
- Usage Scenario: Public area is usually applied to manage or control a public area which is related with other areas controlled by other areas in one building.

User Management

The administrator and the installers can manage users. If you are the administrator, you can add, edit, and delete users, and assign different permissions to the newly-added users. If you are a installer, you can only add and delete users.

Steps

iNote

There are four types of users for the security control panel, including administrator (or owner), operator, installer (or setter), and manufacturer. Different types of users have different permissions for accessing the functionality of the security control panel. For details, see the user manual of the security control panel.

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
- 2. Tap $\bigcirc \rightarrow$ User Management \rightarrow User.
- 3. Tap Add User.
- 4. Configure the required information.

User Type

Different user types have different permissions to access the functionality of the security control panel.

iNote

For details, see the user manual of the security control panel.

User Name

Enter the user name.

Password

Create a password for the user.

iNote

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Keypad Password

Create a password (4 to 6 characters) for the keypad.

iNote

The keypad password +1 or -1 is the duress code. If under duress, you can enter the duress code on the keyboard to arm and disarm area(s) and upload a duress alarm. For example, if the keypad password is 123456, the duress code is 123455 or 123457.

- 5. Tap **Add** to add the user.
- 6. Optional: Perform the following operations if required.

Enable/Disable User	If you log in as an administrator, you can tap an installer, an operator, or a manufacturer on the user list, and then enable/disable the user on the user details page. If you log in as an installer, you can tap an operator or a manufacturer on the user list, and then enable/disable the user on the user details page.	
	i Note	
	Only the administrator and installer can enable/disable users.	
Set Linked Area	If the target user is a an operator, tap the target user on the user list and then tap Area Linkage to set the area linked to the target user.	
	i Note	
	Only the administrator can do such an operation.	
Set Permissions for the User	If the target user is a manufacturer, an installer, or an operator, you can tap the target user on the user list and then tap Permission to set the permissions authorized to the target user.	
	I INote	
	Only the administrator can do such an operation.	

Delete User If the target user is an operator, tap the target user on the user list

and then tap **delete** to delete the target user.

iNote

Only the administrator and installer can do such an operation.

Keyfob Management

You can add keyfobs to the Axiom security control panel to remotely control the area of the panel.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the area page.
- 2. Tap **◎** → User Management → Keyfob Management → Add New Keyfob to enter the Card/Tag Management page.
- 3. For Axiom Hybrid, select a wireless receiver or keypad.

iNote

For Axiom Hub, skip this step.

- 4. Perform one of the followings according to the type of the security control panel.
 - For Axiom Hybrid, bring the keyfob close to the wireless receiver or keypad.
 - For Axiom Hub, bring the keyfob close to the security control panel.
- 5. Press any button on the keyfob to learn.
- 6. Create a keyfob name.

iNote

- If you log in as an installer, skip this step.
- The keyfob name should contain 1 to 32 characters.
- 7. Select area(s) to be linked to the keyfob.

iNote

If you log in as an installer, skip this step. Selecting area is only available for administrator.

You can remotely control the selected area(s) by the keyfob based on the permission(s) configured in step 9.

8. Set the Enable Keyfob switch to on to enable the keyfob.

iNote

If you log in as an installer, skip this step. Enabling keyfob is only available for administrator.

9. Select permissions (such as the permission to disarm and clear alarm) for the keyfob to define what operations can be done via keyfob.

iNote

If you log in as an installer, skip this step. Setting permissions for keyfob is only available for administrator.

10. Tap **Add**.

Card/Tag Management

After adding cards/tags to the wireless security control panel, you can swipe the card/tag to arm or disarm all the detectors added to specific area(s) of the security control panel, and clear alarms.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the area page.
- 2. Tap **○** → User Management → Card/Tag Management → Add New Card/Tag to enter the Card/Tag Management page.
- 3. For Axiom Hybrid, select a keypad.

iNote

For Axiom Hub, skip this step.

4. When hearing the voice prompt "Swipe Card", you should present the card/tag on the control panel card presenting area.

When hearing a beep sound, the card/tag is recognized.

5. Create a card/tag name.

iNote

- If you log in as an installer, skip this step. Editing card/tag name is only available to administrator.
- The name should contain 1 to 32 characters.

The card/tag will be displayed on the Card/Tag Management page. 6. Select area(s) to be linked to the card/tag.

iNote

If you log in as an installer, skip this step. Selecting area is only available for administrator.

You can remotely control the selected area(s) by the card/tag based on the permission(s) configured in step 9.

7. Set the Enable Card/Tag switch to on to enable the card/tag.

iNote

If you log in as an installer, skip this step. Enabling card/tag is only available for administrator.

8. Select permissions (such as the permission to disarm and clear alarm) for the card/tag to define what operations can be done via card/tag.

iNote

If you log in as an installer, skip this step. Setting permissions for card/tag is only available for administrator.

9. Tap **Add**.

Set Event Video Parameters

Event video refers to the video cached when specific events occur. You can configure parameters (video channel, stream type, resolution, etc.) for the event video of the security control panel. On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.

Tap $\bigcirc \rightarrow$ Event Video Settings to enter the page, and then configure the following parameters.

Video Channel

Set the channel for caching video.

iNote

You should have added network cameras to the security control panel. For details about adding network camera, see *Add Network Camera Channel to Security Control Panel*.

Stream Type

Main Stream

Used in recording and HD preview, it provides higher resolution, code rate and image quality.

Sub-Stream

Used to transmit network and preview pictures as a video streaming with features of lower resolution, bit rate and image quality.

Bitrate Type

Constant

A constant bitrate (hence the bandwidth) is used for the video regardless of the complexity of the video scenes. Increased activities in the video scenes will result in a poorer image quality

because the restricted constant bitrate doesn't reach the level to maintain sound image quality.

You can use constant bitrate when only limited network bandwidth is available.

Variable

A changeable bitrate (hence the bandwidth) is used for the video. The variability of bitrates allows videos to be recorded at a lower bitrate when there's no motion in the video scene, and at a higher bitrate when there are a lot of activities.

It is recommended that you use variable bitrates when the network bandwidth is not limited and there is a need for high quality videos. Variable bitrates provide better image quality at the expense of a higher video storage requirements as the bitrate changes with the complexity of the video scenes.

Resolution

Set the resolution for the video.

Bitrate

The higher the value is, the higher the video quality at the expense of higher bandwidth requirements.

Before Alarm

Set the time point before the alarm to start caching video.

After Alarm

Set the time point after the alarm to stop caching video.

Configure Push Notification Settings for Axiom Security Control Panel

You can set a phone number to allow the security control panel to call the phone number or send SMS messages to the phone number when specific alarms (events) are triggered.

Steps

- 1. On the device list page, tap the security control panel and log in to the device (if required) to enter the Area page.
- 2. Tap $\bigcirc \rightarrow$ Communication Parameters \rightarrow Push Notification(s).
- 3. Tap Add Phone Number to enter a phone number.
- 4. Allow the security control panel to call the phone number or send SMS messages to the phone number when specific alarms (events) are triggered.

Phone Call

1. Tap Phone Call.

- 2. Set the Phone Call switch to on.
- 3. Tap **Numbers of Calling** to set the maximum calling times if the call is not accepted.
- 4. Select the event(s) for triggering the phone call.

Event Filtering Interval

Set a time interval for avoid receiving excessive notifications about

the same event (alarm) type within a short period of time. If the alarm is triggered for more than one time within the configured time interval, the alarm is considered as only being triggered for one time.

SMS

- 1. Tap **SMS**.
- 2. Set **SMS** switch to on.
- 3. Select the event(s) for triggering the SMS notification.
- 4. In the Permission Settings section, select the area(s) that you (installer) have permissions to arm, disarm, and clear alarm via sending control messages to the number of the SIM card installed in the security control panel.

iNote

For details about control messages, see *Table 1* below.

After receiving the phone calls or SMS messages about the alarms (events), you can use your phone to send a control messages to arm/disarm the selected area(s) or clear alarm for the area(s) you selected on the Permission Settings page of the SMS tab.

The control message is **Command + Operation + Target**, and the details are shown below.**Table 11-1 Control Message Description**

Command	Operation Type	Target
The number representing the command should be 2 digits. 00: Disarm 01: Away 02: Stay	The number representing the operation type should be 1 digit. 1: Area Operation	The number representing the target area should be no more than 3 digits. 0: All Areas 1: Area 1
03: Clear Alarm		4: Area 4

For example, the control message which reads **00+1+1** means to disarm area 1; And **01+1+1** means to set the status of area 1 to Away.

EN50131 Compliant Mode

You can enable EN50131 Compliant mode to make the security control panel be compliant with the EN50131 standards.

On the device list page, tap the security control panel and log in to the device (if required) to enter

the Area page, and then tap **(**) to enter the Settings page to set the **EN 50131 Compliant** switch to on.

After enabling the mode, the adding user functionality will be available, and all users of the security control panel should log in to the device by user name and device password before they can access the device.

Caution

If the mode is disabled, the security control panel will NOT be compliant with EN 50131 standard. Please contact the after sales or our technical support for information about the risks that may be incurred in your country if you disable the mode.

iNote

- Only the installer (or setter) has the permission to enable/disable EN50131 Compliant mode.
- Enabling/Disabling EN50131 Compliant mode is not available for Axiom Hybrid, which only has the version compliant with the EN50131 standards.

Other Settings

You can do other settings including setting time zone for the security control panel (hereafter simplified as device), configuring device network, enabling Arming Process to auto detect the device faults during arming process, etc.

On the device list page, tap the security control panel and log in to the device (if required) to enter the Area page, and then tap **o** to enter the Settings page.

Device Information

View device information such as device model, battery level, and Wi-Fi status; And set time zone and enable Daylight Saving Time (DST) for the device.

System Maintenance

Reboot the device or partly restore the device.

iNote

If the device is partly restored, the device will restore to its default settings except for admin parameters, wired network parameters, Wi-Fi parameters, detector parameters, and wireless device parameters.

Configure Network

Follow the instructions to configure network for the device.

Cellular Data Network Settings

Tap Communication Parameters \rightarrow Cellular Data Network Settings to configure the related

parameters.

Mobile Network

If disabled, the device will not be available to use in mobile network.

Parameter Configuration

You can set the phone number, user name, access password, MTU, etc.

Access Password

Ask the network carrier the access password and then enter it.

APN

Ask the network carrier to get the APN information and then enter the APN information.

Data Usage Limit

If enabled, the cellular data usage of the security control panel per month will be limited. You can view the data used in the current month, and set the limit per month.

Arming Process

Set the Enable Arming Process switch to on to enable the mode.

After enabled, the device will automatically detect its fault(s) during the arming process. You can determine whether to continue arming or not if fault(s) are detected.

11.2.3 Add Device to the Security Control Panel

You should add detectors (zones), peripheral devices, keyfobs, cards/tags to the panel before you can perform further operations such as arming and disarming. The peripheral devices include wireless outputs expanders, and sirens, etc.

Add Peripheral Device by Scanning QR Code

You can add peripheral devices to the panel by scanning the device QR code.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the Area page.
- 2. Add a peripheral device.
 - Tap **Zone** \rightarrow **H** to enter the Scan QR Code page to add a detector.
- 3. Scan the QR code of the device.

iNote

The QR code is usually on the back cover of the device.

4. Optional: If the QR code fails to be recognized, tap 💋 and enter the serial number of the device, and then select the device type.

iNote

The serial number is usually on the back cover of the device.

5. For Axiom Hybrid, tap **Select Wireless Receiver** to select a wireless receiver.

iNote

For Axiom Hub, skip this step.

6. Tap **Add**.

7. Optional: Tap the device on the zone list or the peripheral device list to enter the Settings page and then tap **Delete** to delete the device.

Add Peripheral Device in Enrollment Mode

In Enrollment mode, when you bring the peripheral device (or detector) close to a wireless receiver, wireless communication between them will be established after you confirm such an establishment. And at the same time through the wired connection between the security control panel and the wireless receiver, which plays the role of intermediary, the connection between the peripheral device (or detector) and the security control panel will be established.

Before You Start

Make sure you have added wireless receiver(s) or keypad to the Axiom Hybrid security control panel. For details, see the user manual of the device.

Steps

iNote

Enrollment mode is only supported by the Axiom Hybrid security control panel.

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the Area page.
- 2. Tap 💿 to enter the Settings page.
- 3. Tap **Enrollment Mode** to enter the Device Type page.

The Device Type page displays four device types, including detector, wireless output expander, and wireless siren.

- 4. Select a device type.
- 5. Select a wireless receiver or a keypad which has a built-in wireless receiver.

iNote

Select the wireless receiver or keypad which is the nearest to the security control panel to ensure the device works after enrolling (adding) the device to the security control panel.

6. Present the peripheral device to the wireless receiver or keypad, and then press the Learn button on the peripheral device.

The peripheral device will be enrolled (added) to the security control panel.

Add Network Camera Channel to Security Control Panel

You can add network cameras to the security control panel as the video channel for the security control panel.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
- 2. Tap $\bigcirc \rightarrow$ Network Camera Channel to enter the Network Camera Channel page.
- 3. Tap the+ icon or **Add Channel** to enter the Add Channel page.
- 4. Set the required information, including IP address, protocol type, port, user name, and password.
- 5. Tap 📄 to add the channel.
- 6. Optional: Perform the following operations if required.

Edit a Channel	Select a channel from the channel list, and then tap 🧪 to edit it, such as IP address and user name.
Delete a Channel	Select a channel from the channel list, and then tap Delete to delete it.

11.2.4 Set Area Parameters

The Mobile Client allows you to set area parameters such as alarm duration, auto arm, and auto disarm. A area is an independent control system of a security control panel. It allows you to batch arm/disarm all zones in it. If the security control panel has two areas, you have two independent systems for arming or disarming.

Steps

- 1. On the device list, tap the security control panel and then log in to the device (if required) to enter the Area page.
- 2. Tap More to enter the Settings page.
- 3. Configure parameters for the area.

Auto Arm

Enable the area to automatically arm itself in a specific time point.

Auto Arm Time

Set the time point for the area to automatically arm itself.

Late to Disarm

Enable the device to push a notification to the phone or tablet to remind the user to disarm the area when the area is still armed after a specific time point.

iNote

You should have enabled Operation Event Notification on the Web Client of the security control panel, or the notification will not be pushed to the phone or tablet. For details about the Web Client, see the user manual of the security control panel.

Late to Disarm Time

Set the time point mentioned in Late to Disarm.

Weekend Exception

If enabled, Auto Arm, Auto Disarm, and Late to Disarm are disabled on the weekend.

Entry Delay 1

Entry Delay 2

Set a value for **Entry Delay 1** and **Entry Delay2**. Entry delay is a time concept. If entry delay is configured for the delayed zone, when you enter an armed delayed zone, the zone alarm will not be triggered until the end of entry delay.

iNote

After set value for **Entry Delay 1** and **Entry Delay 2**, you should set the entry delay of a specific zone to the value of **Entry Delay 1** or **Entry Delay 2**. see *Set Zone Parameters* for details.

Exit Delay

Set exit delay for the delayed zone. If exit delay is configured for the delayed zone, after you arm the zone on the indoor unit, you can exit the zone without triggering alarm until the end of exit delay.

11.2.5 Control Areas

You can set arming mode and clear alarms for areas of the security control panel via the Mobile Client. Area, which is an independent control system of a security control panel, allows you to batch arm/disarm all zones in it. If the security control panel has multiple areas, you have multiple independent systems for arming or disarming.

On the device list page, tap the security control panel and then log in to the device (if required) to enter the Area page and then control the area. You can swipe to the left or right to switch areas.

iNote

- You can also tap the arming status icon on the device list to arm or disarm the area(s).
- If EN 50131 Compliant mode is turned on for the device, controlling area(s) is not available by tapping the arming status icons.

Operations for a Single Area

- Away: When all the people in the detection area leave, turn on the Away mode to arm all zones in the area after the defined dwell time. For example, assume that you have set your apartment as a zone, you can set the zone status to Away when you go to work.
- Stay: When the people stays inside the detection area, turn on the Stay mode to turn on all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony). At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarm will not be triggered. **Disarm**: In Disarm mode, all the zones in the area will not trigger alarm, no matter the selected events are detected or not.
- Clear Alarm: Clear all the alarms triggered by the zones of the area.

Operations for All Areas

- Away: When all the people in the detection area leave, turn on the Away mode to arm all zones in all areas after the defined dwell time.
- Stay: When the people stays inside the detection area, turn on the Stay mode to turn on all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony) set in all the zones of all areas. At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarm will not be triggered. **Disarm**: In Disarm mode, all the zones of all areas will not trigger alarm, no matter the selected events are detected or not.
- **Clear Alarm**: Clear all the alarms triggered by the all the zones of all the areas.

11.2.6 Set Zone Parameters

You can set zone parameters, such as zone type, linked camera, and Stay/Away settings. Zone is a basic concept in the security control panel system. It refers to a protection area in the system, and is regarded as the maximum recognizable unit to distinguish the alarm event.

Before You Start

You should have linked detector(s) to the wireless security control panel. For details, see the user manual of the security control panel.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the control panel page.
- 2. Tap **Zone** and then tap a detector (zone) on the zone list to enter the Settings page.

< Settings	
001	>
Serial No.	Q00186581
Detector Type	Other Detector
Zone Type	Instant Zone 💙
Zone Bypass	OFF
Link Camera	>
Stay/Away	OFF
The zone will be auto-bypassed when enabled.	during stay-arming
Chime	OFF

Figure 11-2 Zone Settings Page

3. Set parameters for the zone (or detector).

Zone Type

See the descriptions of each zone type on the Zone Type page. If you select **Delayed Zone**, you should select an entry delay (Entry Delay 1 or Entry Delay 2) on the pop-up page.

iNote

You can set Entry Delay 1 and Entry Delay 2. See *Set Area Parameters* for details.

If you select Timeout Zone, you should select a timeout value or tap Custom to set a custom

value.

Linked Camera

Link a camera to the zone. See *Link Camera to Zone* for details.

Stay/Away

If enabled, the zone will be auto-bypassed during stay arming.

iNote

For details about bypassing a zone, see Bypass a Zone.

Chime

Enable the security control panel to chime when the zone is triggered.

Enable Silent Zone

If enabled, no siren will be triggered if alarm occurs.

11.2.7 Bypass a Zone

If you bypass a zone, the zone will NOT be in alert condition (related alarms will not be triggered and related faults will not be detected) even when the system (or area) which it belongs to is armed. Bypassing a zone is usually used in the following two scenarios. The first is that if a zone is faulty, other zones of the same system (or area) can be armed only when the faulty zone is bypassed. The second is that you simply want a specific zone NOT to trigger alarms in special occasions.

On the Settings page of a detector (or zone), turn on Zone Bypass to bypass the detector (or zone).

iNote

For details about how to enter the Settings page of a detector (or zone), see Set Zone Parameters.

11.2.8 Link Camera to Zone

If a network camera has already been linked to the wireless security control panel, you can link the camera to a zone managed by the control panel via the Mobile Client. After that, you can view the zone's alarm-related video when receiving the zone's alarm notification. You can also link a network camera added to the Mobile Client to a zone managed by the control panel, so as to view the zone's live video and play back the zone's videos.

Before You Start

- You should have mounted the network camera in the zone. See the user manual of the network camera for details.
- To view the alarm-related video when receiving zone's alarm notification, you should have linked the network camera to the wireless security control panel via the panel's Web Client. For details, see the user manual of the Axiom wireless security control panel.

Steps

iNote

The zone's alarm-related video lasts 7 seconds (from 5 seconds before the alarm to 2 seconds after the alarm).

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the Area page.
- 2. Tap **Zone** and then select a detector from the zone list.
- 3. Tap Link Camera to enter the Link Camera page.

K Lir	nked Camera	
wirelessZone3	G	\bigcirc
Available Cameras	DS-2CDVT-CMPT	HIKVISION
	Link	

Figure 11-3 Link Camera Page

- 4. Drag a camera from the Available Cameras section to 💽
- 5. Tap **Link** .

11.2.9 Set Parameters of Wireless Outputs Expander

You can set the alarm output type and the output delay for the relays of a wireless outputs expander. Alarm output is the node signal or other signal sent from the alarm controller to the peripheral devices when the alarm is triggered.

Before You Start

You should have added wireless outputs expander(s) to the wireless security control panel.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the Area page.
- 2. Tap **Peripheral Device** and then tap a wireless outputs expander on the device list. The relays of the expander will be displayed.
- 3. Optional: Set the disconnection duration.

Offline Duration

If the time during which the wireless outputs expander loses communication with the security control panel exceeds the configured offline duration, the wireless outputs expander will be regarded as offline.

iNote

The default offline duration is 1 hour.

4. Configure the relay.

Edit Relay Name	Tap a relay and then tap the relay name to edit its name. And then tap 📄 to save the changes.
Select Alarm Output Type	Tap a relay and then select an alarm output type. Jarm Alarm outputs will be activated when the zone alarms. rming Alarm outputs will be activated when the area (system) is armed. Jisarming Alarm outputs will be activated when the area is disarmed.
	fanual Set the switch icon to ON on the relay list to manually activate alarm outputs of the relay. one
Set Delay Time for the Relay to Close	Alarm outputs will be activated when the selected zone is triggered or tampered. Tap a relay and then tap Output Delay to set the delay time for the relay to close. In other words, output delay refers to the duration of the alarm output.

11.2.10 Set Siren Parameters

You can edit the siren name and set the siren's volume.

Before You Start

You should have added siren(s) to the security control panel.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the Area page.
- 2. Tap **Peripheral Device** and then tap a siren on the device list to enter the siren settings page.
- 3. Perform the following operations.

Edit Siren Name	Tap the siren name to edit it, and then tap 📄.
Set Siren Volume	Drag the slider to set the volume.
	iNote
	The function should be supported by the siren.

Set Siren Type for Wired Siren	 Alarm: The siren will be activated when the zone alarms. Arming: The siren will be activated when the area (system) is armed. Disarming: The siren will be activated when the area is disarmed. Manual: Set the switch icon to ON on the relay list to manually activate the siren. Zone: The siren will be activated when the selected zone is triggered or tampered.
Set Offline Duration	If the time during which the siren loses communication with the security control panel exceeds the configured offline duration, the siren will be regarded as offline.

11.2.11 Set Wireless Keypad Parameters

You can set the wireless keypad parameters, including device name, buzzer, card/tag swiping, backlight, and security settings, etc.

Before You Start

You should have added wireless keypad to the security control panel.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the Area page.
- 2. Tap Peripheral Device and then tap a wireless keypad on the device list.
- 3. Set the parameters.

Linked Area

Set the area linked to the keypad. The linked area can be arm/disarm or clear alarm by the keypad.

Buzzer

Enable the buzzer.

Card/Tag Swiping

Enable swiping card/tag on the keypad to arm/disarm the linked area or clear alarms.

Keypad

Enable using keypad to arm/disarm the linked area or clear alarms.

Backlight

Enable the backlight of the keypad.

Offline Duration

If the time during which the keypad loses communication with the security control panel exceeds the configured offline duration, the keypad will be regarded as offline.

Security Settings

Locked Duration

Specify the duration that the keypad remains locked if the failed keypad password attempts reach the specified maximum times.

Maximum Failed Attempts

Specify the maximum failed attempts for entering the incorrect keypad password consecutively. If the failure times reaches the specified value, the keypad will remain locked for a specified duration.

11.2.12 Set Wireless Card/Tag Reader Parameters

You can set the wireless card/tag reader parameters, including device name, linked area, buzzer, offline duration, and security settings.

Before You Start

You should have added wireless card/tag readers to the security control panel.

Steps

- 1. On the device list page, tap the security control panel and then log in to the device (if required) to enter the Area page.
- 2. Tap **Peripheral Device** and then tap a wireless keypad on the device list.
- 3. Set the parameters.

Linked Area

Set the area linked to the wireless card/tag reader. The linked area can be arm/disarm or clear alarm by swiping card/tag on the card/tag reader.

Buzzer

Enable the buzzer of the card/tag reader.

Offline Duration

If the time during which the siren loses communication with the security control panel exceeds the configured offline duration, the siren will be regarded as offline.

Security Settings

Locked Duration

Specify the duration that the card/tag reader remains locked if the failed card/tag swiping attempts reach the specified maximum times.

Maximum Failed Attempts

Specify the maximum failed attempts for swiping card/tag. If the failure times reaches the specified value, the card/tag reader will remain locked for a specified duration.

11.3 Pyronix Control Panel

On the Mobile Client, Pyronix control panel refers to the security contorl panel (or alarm panel) designed and manufactured by Pyronix. You can add the Pyronix control panels to the Mobile Client for management, such as arming and disarming areas (or partitions), viewing zone history event, and bypassing zone.

iNote

After adding the device to the Mobile Client, you should authorize the account of the Mobile Client to access the device, and verify the device before you can manage it. The flow chart of the overall process is shown below.



Figure 11-4 Flow Chart

11.3.1 Add Pyronix Control Panel to Mobile Client

You can add Pyronix control panels to the Mobile Client for management of the devices.

Steps

- 1. Tap 🕒 on the device list page and then select Manual Adding.
- 2. Select **Pyronix** as the adding type.
- 3. Enter the device alias and serial number.
- 4. Tap 📄 to save the settings.

The device will be displayed on the device list.

What to do next

Authorize your account of the Mobile Client via PyronixCloud, otherwise you won't have the permission to access the device via the Mobile Client. See *Authorize Mobile Client Account via PyronixCloud* for details.

And then verify the device on the Mobile Client. See *Verify Pyronix Control Panel* for details.

11.3.2 Authorize Mobile Client Account via PyronixCloud

Before you can manage a Pyronix control panel on the Mobile Client, you should authorize your account of the Mobile Client via PyronixCloud first, which operates as a gateway between the device and the Mobile Client.

The flow chart is shown below:

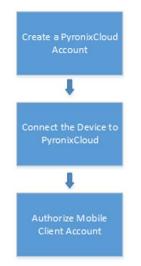


Figure 11-5 Flow Chart of the Authorization

Create a PyronixCloud Account

You should create a PyronixCloud account before you can connect a Pyronix control panel to PyronixCloud.

Steps

1. Visit *http://www.pyronixcloud.com*.

Pyronix Cloud
Email Address
Create an account Reset Password
Language:
English (UK)

Figure 11-6 The Web Page of PyronixCloud

2. Click **Create an account** and complete the form.

You will receive an email with a confirmation link from admin@pyronixcloud.com.

3. Click the link to complete confirmation.

What to do next

Connect the Pyronix control panel to PyronixCloud. See *Connect Device to PyronixCloud* for details.

Connect Device to PyronixCloud

After creating a Pyronix account, you should connect a Pyronix control panel to the PyronixCloud before you can authorize your account of the Mobile Client.

Before You Start

Create a Pyronix account. See *Create a PyronixCloud Account* for details.

Steps

- 1. Visit *http://www.pyronixcloud.com* and log in to your account.
- 2. Register a new system.
 - 1) Enter the required information.

System ID

The system ID is an unique ID for a Pyronix control panel. You can get the system ID via the device. For details, see the user manual of the device.

Cloud Password

Enter the cloud password that you have entered in the Pyronix control panel (or alarm

panel). The cloud password is set via the device. For details, see the user manual of the device.

2) Click Submit.

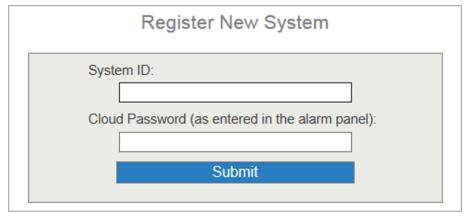


Figure 11-7 Register a New System

- 3. Enter a system reference to create an alias for the device.
- 4. Click Submit.
- You will receive an email with a confirmation link.
- 5. Click the confirmation link to continue.
 - The device will be displayed on View Systems page.
- 6. Click the tick at the upper-right corner of the page to make sure the device is connected.

What to do next

Authorize your account of the Mobile Client. See *Authorize Mobile Client Account* for details.

Authorize Mobile Client Account

Perform the following task to authorize your account of the Mobile Client.

Before You Start

Create a PyronixCloud account and connect the Pyronxix control panel to PyronixCloud. See *Create a PyronixCloud Account* and *Connect Device to PyronixCloud* for details.

Steps

- 1. Connect the Pyronix control panel to PyronixCloud to enter the View Systems page.
- 2. On the View Systems page, click a system ID to enter the device user list page.
- 3. Select your account of the Mobile Client from the User column.
- 4. Switch the permission to ON.

User	Last Connected	Permission	Notifications
1111	28/03/2017 13:49:58	On Off	Senabled

Figure 11-8 Device User List Page

5. Click Save Now.

You can access the Pyronix control panel via the Mobile Client.

11.3.3 Verify Pyronix Control Panel

If a Pyronix control panel is not verified, you should verify it before you can manage it on the Mobile Client.

Before You Start

- Add a Pyronix control panel to the Mobile Client. See *Add Pyronix Control Panel to Mobile Client* for details.
- Set the user code and APP password via the Pyronix control panel. For details, see the user manual of the device.

Steps

- 1. On the device list page, tap a Pyronix control panel to enter the Verify Device page.
- 2. Enter the user code and the APP password.
- 3. Tap **Finish**.

11.3.4 Control Areas (Partitions)

For a Pyronix control panel, an area (partition) is an independent control system of a security control panel. It allows you to batch arm/disarm all zones in it. If the security control panel has two partitions, you have two independent systems for arming or disarming.

Before You Start

- Add the Pyronix control panel to the Mobile Client. See *Add Pyronix Control Panel to Mobile Client* for details.
- Authorize your account of the Mobile Client to access the device. See *Authorize Mobile Client Account via PyronixCloud* for details.

Steps

iNote

For more information about partition, see the user manual of the security control panel.

1. Tap the Pyronix control panel on the device list page and verify the device to enter the Area (Partition) page.

iNote

For details about verifying device and authorize the phone, see *Verify Pyronix Control Panel*.

The alarm outputs and areas (partitions) will be displayed on the page.

\leftarrow	Device 01	¢
Cellar	Gate Key	(o o o More
Area A Arming		
Input 01test ⊗Offline	t	
Input 02 ⊗Offline		Ś
♥ Input 03 ⊗Offline		ţŷ}
	View All Zones	
Area B Disarmed		\bigcirc
Input 01test ⊗Offline	t	503
♥ Input 02 ⊗Offline		Ś
Area C Disarmed		\bigcirc
Input 01test ⊗Offline	t	ij

Figure 11-9 Area (Partition) Page

2. Set the switch to ON to arm the area (partition).

11.3.5 Control Alarm Output Remotely

When the Pyronix control panel is connected with alarm outputs, such as siren and alarm lamp, you can control the alarm output status.

Before You Start

Connect an alarm output to the Pyronix control panel. For details, see the user manual of the device.

Steps

1. Tap a Pyronix control panel on the device list page and verify the device to enter the Area (Partition) page.

iNote

For details about verifying device and authorizing the phone, see Verify Pyronix Control Panel.

The alarm output(s) and all areas (partitions) will be listed on the page.

- 2. Tap 💮 to enter the Alarm Output page.
- 3. Tap the alarm output icon to trigger an alarm.

The time for outputting the alarm starts count down.

iNote

The time for outputting the alarm varies with different types of alarm outputs.

11.3.6 Bypass a Zone

If you bypass a zone, the zone will NOT be in alert condition (related alarm will not be triggered and related faults will not be detected) even when the area (or partition) is armed. Bypassing a zone is usually used in the following two scenarios. The first is that if a zone is faulty, other zones of the same area (or partition) can be armed only when the faulty zone is bypassed. The second is that you simply want a specific zone NOT to trigger alarms in special occasions. Select a zone on the Area page and tap is to enter the Settings page of the zone, and then enable zone bypass.

iNote

For details about how to enter the Area page, see Control Areas (Partitions).

Chapter 12 Facial Data Management

For the DeepinMind server on the same LAN with the Mobile Client, you manage the facial data stored in it via the Mobile Client. The facial data can be used for facial comparison in related applications.

Before You Start

- You should have added DeepinMind server to the Mobile Client.
- You should have added face libraries to the server. For details, see the user manual of the device.

Perform the following task to upload facial data to the DeepinMind server.

Steps

- 1. Enter the Settings page of the server.
 - On the device list page, if the page is in list mode, swipe the device name to the left and tap
 On
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap •••.
- 2. Tap Facial Data Management to enter the Facial Data Management page.

iNote

For the first time usage, you should enter the user name and password of the device to verify you identity first. Once verified, the verification is not required afterwords.

- 3. Select a face library to enter the face library page.
- 4. Tap 😑 (if there's no facial data) or 🖶 and then tap **Capture Picture** or **Select from Photo Album** to use your phone or tablet to capture a face picture or select a face picture from the photo album respectively.

The face picture will be uploaded to the server and the server will start recognizing the facial data. Once recognized, the face picture will be displayed in the face library.

- 5. Optional: Delete face picture(s).
 - 1) Tap 💉 on the face library page and then select face picture(s) .
 - 2) Tap $\overline{\square}$ to delete the selected one(s).

Chapter 13 Video Intercom

The Mobile Client supports video intercom functions. Video intercom is an audiovisual communication and security technique used in a building or a small collection of buildings. With microphones and video cameras at both sides, it enables the intercommunication via video and audio signals.

13.1 Answer Call from Indoor Station

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.

Before You Start

You should have added an video intercom device to the Mobile Client. See *Add Device for Management* for details.

Steps

iNote

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.

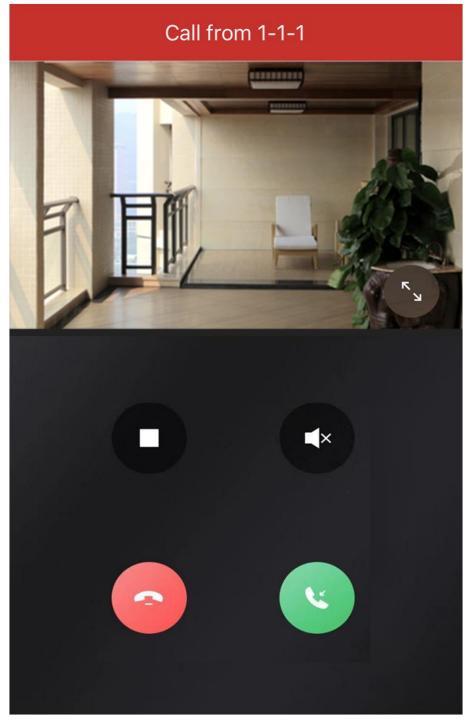


Figure 13-1 Call Page

2. Perform the following operations.

Answer the Call Tap Sto answer the call.

Stop/Restart Live View Tap \square to stop the live view. And tap \triangleright 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.

13.2 Operations on Device Details Page

On the device details page of the video intercom devices, you can perform the operations including viewing the live videos streamed from the cameras linked to the door stations or doorbells, starting two-way audio, playing back video footage, viewing call logs and history events, controlling doors linked to door stations, etc.

Tap the video intercom device on the device list to enter the device details page.

Live View

The live video will start playing when you enter the device details page. You switch live videos if multiple door stations are linked to the video intercom device.

During live view, you can tap the image to show the hidden icons, and then perform operations such as starting two-way audio, capturing picture, recording, full-screen live view, and setting image quality.

iNote

For details about the above-mentioned operations during live view, see **Start Two-Way Audio**, **Capturing and Recording**, **Set Image Quality for Device Added by IP/Domain**, and **Set Image Quality for Hik-Connect Device**.

Playback

Tap $\blacksquare \rightarrow$ **Playback** to start playing back video footage.

View Call Logs and Events

You can view the call logs and device-related events in the latest 7 days (the events or call logs of the current day will be displayed by default).

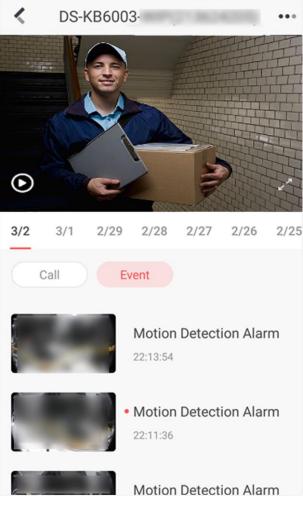


Figure 13-2 Calls and Events

Control Door

You can tap 💽 to control the door linked to the video intercom device.

13.3 Set Motion Detection Alarm for Wi-Fi Doorbell

Motion detection is a way of detecting motion in a surveillance 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 alarm notification about the motion detection event.

Before You Start

You should have added a Wi-Fi doorbell to the Mobile Client. See *Add Device for Management* for details.

Steps

1. Enter the Settings page of the Wi-Fi doorbell.

- On the device list page, if the list is displayed in list mode, swipe the name of a Wi-Fi doorbell to the left and then tap
- On the device list page, if the list is displayed in thumbnail mode, swipe the name of Wi-Fi doorbell to the left and then tap
- On the Live View page of the device, tap **…** and then tap **Settings**.
- 2. Tap Notification to enter the Notification page.
- 3. Draw motion detection area.
 - 1) Tap Draw Motion Detection Area to enter the Motion Detection Area page.



In the selected area, alarm and video recording will occur when the object is detected to move. in the horizontal screen mode, the area selection is more convenient

Figure 13-3 Draw Motion Detection Area

- 2) Tap the grid(s) on the live video image to select the motion detection area.
- 3) 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.

What to do next

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

iNote

For details about how to enabling notification, see Enable Alarm Notification

Chapter 14 Notification

In the Notification module, you can view the notifications about the events (alarms) triggered by the devices, the call logs of the video intercom devices, and the notifications related to Hik-ProConnect.

14.1 Enable Alarm Notification

You can allow the Mobile Client to receive and push notifications of the events detected by a device. 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, if required, to avoid the disturbance of push notifications (and the audio and strobe light alarm) while still being able to receive event information on the Notification page.

Before You Start

You should have configured event settings on device (except for the video intercom device). See the user manual of the device for details.

Steps

iNote

- 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. Enter the Settings page of the device.
 - On the device list page, if the list is displayed in list mode, swipe the device to the left and then tap
 - On the device list page, if the list is displayed in thumbnail mode, swipe the device to the left and then tap ***.
 - On the Live View page of the device, tap
 and then tap Settings.
- 2. Tap **Notification** to enter the Notification page.
- 3. Turn on **Notification** 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. Optional: 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).

1) Tap Notification Schedule.

2) Tap Set a Time Scheduletoenter the Schedule Settings page.

 Schedule Settings 			
Start Time	00:00 >		
End Time	23:59 >		
Apply to			
Mon. Tue. Wed. Thu. Fri.	Sat. Sun.		

Figure 14-1 Schedule Settings Page

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

iNote

The date(s) marked in blue is selected.

- 5) Tap 📄.
- 6) Optional: 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.
- 7) Go back to the Notification page.
- 6. Optional: 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.

iNote

The function should be supported by the device.

Intensive

Intense warning for the intrusion.

Soft

Soft warning for the intrusion.

Mute

No audible warning.

14.2 Check Event Information or Call Logs

You can check the alarm or event information on the Notification page when alarms are triggered on the devices. You can also check the call log generated from the video intercom devices.

Before You Start

- Configure alarm or event 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.

Steps

iNote

Since the operations for checking event information and call log are similar, here we only introduce how to check event information.

- 1. Tap **Notification** \rightarrow **Alarm Event** to enter the Alarm Event page.
- 2. Optional: Tap Filter and then select a date and (or) select a device to filter the events.
- 3. Tap an event to enter the details page and check the details of the alarm event.

Zoom in/out Event-related Picture	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.
	i Note
	If you have enabled Video and Image Encryption for the device, you should enter the device verification code before you can view the picture. For details about Video and Image Encryption, see Set Video and Image Encryption for details.
Save Event-related Picture	Tap \blacksquare \rightarrow Save Picture to save the picture to the Photo Album of the phone or tablet.
	i Note
	You should have configured the event linkage action for capturing event-related picture for the device. See the user manual of the

device for details.

View Event-related	Tap Playback to view the video footage.
Video Footage	I Note
	You should 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 \blacksquare \rightarrow Live View to view the live video of the device.
	~
	iNote
	The function should be supported by the device.
View External Linked Video	Tap External Linked Video to view the video footage recoded by the device's externally linked device.
	i Note
	 You can configure such a linkage (the configuration is called as "Configuring External Linkage Rule) on Hik-ProConnect. For details, see the user manual of the Hik-ProConnect Portal. Only the Installer on Hik-ProConnect can configure such a linkage.

4. Optional: Go back to the Notification page and then edit the event information.

Mark All Events as Read	Tap Edit on the Notification page and then tap Mark as All Read to mark all event information as "already read".
Mark a Specific Event as Read	Tap Edit on the Notification page and select an event, ans then tap Mark as Read to mark the selected event information as "already read".
Clear All Events	Tap Edit on the Notification page and then tap Clear All.
Delete a Specific Event	Tap Edit on the Notification page and select an event, ans then tap Delete to delete it.

14.3 Service Notification

On the Service tab, you can view the notifications from Hik-ProConnect, such as the to-be-site-owner invitations from the Installer or other users.

iNote

For details about Hik-ProConnect, see *Hik-ProConnect*.

There are two types of notifications on the Service tab, the to-be-site-owner invitations and the site permission applications.

Accept Invitation

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

Approve Site Permission Application

You can tap **View Details** on a site permission application to view the details, including the Installer name, site, and the authorized device, and so forth, and then check the checkbox(es) to authorize device permissions to the Installer, and finally tap **Agree**

After you approve the application, the Installer will be able to provide device management and maintenance services based on the permissions you authorized to him/her.

Chapter 15 Other Functions

The Mobile Client provides other functions, including fingerprint authentication, management of the recorded (or clipped) video and captured pictures, and Hik-ProConnect related functions, such as handing over your sites (created on Hik-ProConnect) to others and viewing details of the sites owned by you.

15.1 Pictures and Videos

In Picture and Video Management module, you can view and mange the recorded (or clipped) video footage and the captured pictures.

Tap More \rightarrow Pictures and Videos to enter the Pictures and Videos page and then you can perform the following operations.

- Play Video File
- Tap a video file and then tap **D** to play it.

You can rotate the phone to view the video in landscape mode.

- Delete a Video File or Picture
- : Tap a video file or a picture, and then tap 🔟 to delete it.
- Share a Picture or Video File to Another Application
- : Tap a video file or a picture, and then tap 😵 to share it to another application.
- Batch Delete Video Files and (or) Pictures
- : Tap Edit and select video files and (or) pictures, and then tap 🛅 to delete them.
- Batch Share Pictures and (or) Video Files to Another Application
- : Tap Edit and select pictures and (or) video files, and then tap 😵 to share it to another application.

15.2 Fingerprint Authentication

For information security, the Mobile Client provides the function of fingerprint authentication, which requires you to verify your identity before you can access it.

iNote

- The phone operation system should support fingerprint authentication.
- You should have enabled fingerprint authentication on the phone operation system, or you will fail to enable the function on the client software.

Tap **More** \rightarrow **Account Management** to enter the Account Management page and then enable the function.

15.3 Hik-ProConnect

Hik-ProConnect is a cloud service platform for the Installers (installation companies) in the security industry. On the platform, the Installers can provide services such as site (website for managing devices) management, device management and configuration, device health monitoring, etc., for you after you authorize devices and permissions to him/her. The Mobile Client provides Hik-ProConnect related functions including viewing site details, editing the permissions authorized to the Installer, handing over sites to others, and canceling all authorizations to the Installer, etc. Tap **More** \rightarrow **Hik-ProConnect** to enter the Hik-ProConnect page.

iNote

You should have been the owner of at least one site, and have authorized device(s) on the site to the Installer. Or the menu cascade above will be unavailable.

On the Hik-ProConnect page, you can do the following operations.

View Site Details

On the Hik-ProConnect page, you can view the site owned by you. You can tap a site to enter the Site Details page to view the details of the site, including details of the Installer who is managing the devices of the site, site name, and the devices of the site.

Edit or Copy Site Information

- Edit Site Name: Tap a site to enter the Site Details page, and then tap a site name to edit it.
- Copy Information: Tap a site to enter the Site Details page, and then tap \Box to copy the site ID. You can also tap **View Details** on the Site Details page and then tap \Box to copy the site ID, website, or address of the Installer.

View History External Linkage

Tap is to view the history external linkages and the linkage results (succeeded or failed). The external linkage refers to the process in which an event detected by device A triggers actions of device B, device C, device D, and so forth. You can configure such a linkage (the configuration is called as "Configuring External Linkage Rule) on Hik-ProConnect. For details, see the user manual of the Hik-ProConnect Portal.

iNote

- The retention period of the history external linkage is 30 days.
- The information of the external linkages will not be pushed to you as notifications.

<	History Linkage			
2019-12-12 (Thursday)				
Line Crossing Dete	W(D72821507) trigger	15:07:13		
	W(D72821507) detected ade DS-2CV2026G0- trigger Capture.	15:06:44		
	W(D72821463) detected ade DS-2CV2026G0- trigger Capture.	15:06:13		
	W(D72821463) detectec ade DS-2CV2G46G0- trigger Capture.	15:06:13		
	W(D72821463) detectec ade D60999959 + 1 trigg			
Line Crossing Dete	W(D72821507) trigger	15:03:26		
	W(D72821507) detected ade DS-2CV2026G0- trigger Capture.	15:02:57		
Line Crossing Dete	W(D72821507) trigger	15:02:52		

Figure 15-1 History Linkage

Edit Permission

Tap a site to enter the Site Details page, and then tap $\cdots \rightarrow$ Edit Permission to edit the permissions authorized to the Installer.

Hand Over Site

Tap a site to enter the Site Details page and tap $\cdots \rightarrow$ Site Handover, and then enter the registered mobile phone number or email address of the user or Installer to finish handover.

Cancel Authorization

Tap a site to enter the Site Details page and tap $\dots \rightarrow$ **Cancel Authorization** to cancel all authorizations (related to site and the devices on the site) to the Installer.

Chapter 16 System Settings

This section introduces system settings of the Mobile Client, including hardware decoding, floating live view, resuming latest live view, etc.

16.1 Enable Push Notification

If push notification is enabled, the Mobile Client will push alarm notifications related to the added devices to you.

iNote

For details about alarm notifications, see *Notification* for details.

Tap **More** \rightarrow **Settings** to enter the Settings page, and then enable the function.

16.2 Save Device Parameters

If the function is enabled, the Mobile Client will remember the device parameters you set. Take video and image encryption for an example, you only need to enter the device verification code for once to view the encrypted live view, playback, or picture.

iNote

- For details about video and image encryption, see Set Video and Image Encryption.
- For details about setting device parameters via the Mobile Client, see Device Settings.

Tap **More** \rightarrow **Settings** to enter the Settings page, and then enable the function.

16.3 Auto-receive Alarm after Power-on

If you enable this function, the Mobile Client will run automatically and receive alarm event information when the phone or tablet is powered on.

Tap $More \rightarrow Settings$ to enter the Settings page and then enable the function.

iNote

The power consumption of the phone or tablet may increase.

16.4 Generate a QR Code with Device Information

For devices added via IP/domain, the Mobile Client allows you to generate a QR code containing

the information of up to 32 devices. The QR code can be used to quickly add multiple devices. For example, if user A has generated a QR code containing the information of 10 devices, user B can scan the QR code to batch add the 10 devices to his or her account.

Steps

iNote

Only devices added by IP/domain support this function.

- 1. Tap **More** \rightarrow **Settings** to enter the Settings page.
- 2. Tap Generate QR Code.
- 3. Tap Generate QR Code in the IP/Domain field to enter the Select Device page.
- 4. Select device(s).
- 5. Tap Generate QR Code.

The QR code picture will be generated.

6. Tap **Save** to save the picture to the photo album of your phone or tablet.

16.5 Hardware Decoding

Hardware decoding provides better decoding performance and lower CPU usage when you play high definition videos during live view or playback.

Tap **More** \rightarrow **Settings** to enter the Settings page, and then enable the function.

iNote

- The function is available only when the phone OS is Android 4.1 or later version.
- Hardware decoding is only supported when the resolution is 704*576, 704*480, 640*480, 1024*768, 1280*720, 1280*960, 1920*1080, 2048*1536, or 2560*1920. For other resolutions, only software decoding is supported.
- For H.265 video compression, hardware decoding is not supported.
- Hardware decoding should be supported by the device. If not, the device will adopt software decoding by default.

16.6 View Traffic Statistics

The Mobile Client automatically calculates the network traffic consumed during live view and playback. You can check the mobile network traffic and Wi-Fi network traffic separately. Tap **More** \rightarrow **Settings** to enter the Settings page, and then tap **Traffic Statistics**.

16.7 Generate a QR Code with Wi-Fi Information

You can generate a QR code with Wi-Fi information, and then use a network camera or wireless

doorbell to scan the QR code to connect the device to the Wi-Fi network.

Steps

iNote

Connecting device to a Wi-Fi network by scanning QR code should be supported by the device.

1. Tap **More** \rightarrow **Settings** to enter the Settings page.

- 2. Tap **Wi-Fi Settings** to enter the Wi-Fi Settings page.
- 3. Set the required information.

Wi-Fi Name

Enter the SSID of the Wi-Fi network.

Password

Enter the password of the Wi-Fi network.

Encryption

Select the encryption type as the one you set for the router.

iNote

If you select NONE as the encryption type, the password of the Wi-Fi network is not required.

4. Tap **Generate** to generate a QR code for the Wi-Fi network.

What to do next

Use a network camera or wireless doorbell to scan the QR code to connect the device to the Wi-Fi network.

16.8 Floating Live View

If you enable this function, floating live view window(s) will be displayed on the device list page when you select one or more device(s). You can preview the live video(s) in the floating window(s).

iNote

• If you select more than 16 cameras, the number of the selected cameras will be displayed.

• Up to 256 cameras can be displayed as floating windows.

Tap **More** \rightarrow **Settings** to enter the Settings page and then enable the function.

16.9 Resume Latest Live View

If you enable the function, the latest live view will be resumed each time you enter the Mobile Client. The window division mode, and the live view windows' sequence (if in multiple-window mode) will also be restored.

Tap More \rightarrow Settings to enter the Settings page, and then enable the function.

16.10 Tablet Mode

If the Mobile Client is installed on a tablet, you can enable tablet mode so that the interfaces will be displayed in landscape mode by default.

Tap **More** \rightarrow **Settings** to enter the Settings page and then enable the function.

16.11 Display/Hide Channel-Zero

Channel-zero, known as virtual channel, can show the videos from all channels of the device, reducing the bandwidth while simultaneously previewing from multi-channel. It can acquire image information and save bandwidth for transmission through encoding and configuring output images.

Tap More \rightarrow Settings and then enable the Mobile Client to display channel-zero.

16.12 Auto-Download Upgrade File

If you enable Auto-Donwload Upgrade File, the Mobile Client will automatically download the upgrade file in Wi-Fi networks, which helps speed up the device upgrade process.

iNote

For details about upgrading device, see **Upgrade Device Firmware**. Tap **More** \rightarrow **Settings** to enter the Settings page and then enable the function.

Chapter 17 Reset Password of DVR or NVR via the Mobile Client

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. Two verification methods are provided for resetting the password of DVR or NVR: verifying by reserved email or verifying by Hik-Connect.

Procedures of Resetting Password via Hik-Connect Verification

It is recommended that you use this way to reset the password of DVR or NVR, which is comparatively simpler and more convenient. For details, see *Reset Password by Hik-Connect*.

Procedures of Resetting Password via Email Verification

The flow chart below shows the procedures of resetting password by email verification.

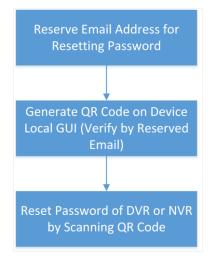


Figure 17-1 Flow Chart

- Reserve Email Address for Resetting Password: See *Reserve Email Address for Resetting Password* for details.
- Generate QR Code on Device Local GUI (Verify by Reserved Email): See *Generate QR Code by Reserved Email* for details.
- Reset Password of DVR or NVR by Scanning QR Code: See *Reset Password by Reserved Email* for details.

17.1 Reset Password by Hik-Connect

You can reset the password of DVR or NVR via 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, and then tap **More** → **Reset Device Password** to enter the Reset Device Password page.
- 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.

17.2 Reserve Email Address for Resetting Password

You should 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

iNote

The DVR or NVR should support the function.

- 1. Go to **Configuration** \rightarrow **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**.

17.3 Generate QR Code by Reserved Email

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

You should have reserved an email address for resetting password.

Steps

iNote

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.

17.4 Reset Password by Reserved Email

If you forgot the admin password of DVR or NVR, you can reset the password by scanning the QR code generated on the local GUI of the device.

Before You Start

- You should have allowed the Mobile Client to access your phone's camera.
- You should have reserved email address for resetting device password and generated QR code on the device's local GUI. For details, see *Reserve Email Address for Resetting Password* and *Generate QR Code by Reserved Email* for details.

Steps

- 1. Tap More \rightarrow Reset Device Password to enter the Reset Device Password page.
- Scan the QR code on the local GUI of the DVR or NVR.
 A verification code will be sent to the reserved email address.

iNote

- 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.
- 3. Go to the device's local GUI.
- 4. Enter the received verification code on the Verify by Reserved Email window and then click **OK** to reset the password.

