Hik-Connect Android Mobile Client

User Manual

Contents

Chapter 1 Overview

Hik-Connect Android Mobile Client runs on phones and tablets with Android 4.4 or later. With the Mobile Client, you can remotely control devices (NVRs, DVRs, network cameras, indoor stations, doorbells, security control panels, access control devices, etc) via Wi-Fi or cellular network. 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.

Note

Network traffic charges may be incurred during the use of the Mobile Client. Consult your local carriers for details.

1.1 System Requirements and Conventions

System Requirement

Android 4.4 or later.

Conventions

In the following chapters, this manual simplifies Hik-Connect Mobile Client as "Mobile Client", device such as DVR, NVR, encoder, and network camera as "device", and device which supports being added to Hik-Connect service as "Hik-Connect Device".

1.2 Summary of Changes

See detailed descriptions on feature changes on the Mobile Client in ***Hik-Connect Mobile Client Release Notes*** .

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.

Note

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 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.

Note

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

3.1 Register by Email Address

You can register an account by your email address.

Steps

1. Tap **Login/Register** on the Home page.
2. Tap **Register** to enter the Join Us page.
3. Tap **Terms of Service** and **Privacy Policy** to read the relevant content and then tap **Agree** to continue.
4. Select the region where your devices locate.
5. In the Register page, enter your email address and then create a password.

   Note

   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.
6. Tap **Get Security Code** to get the security code for verification.
7. Enter the security code you received, and then tap **Finish**.

3.2 Register by Mobile Phone Number

You can register an account by your mobile phone number.

Steps

1. Tap **Login/Register** on the Home page.
2. Tap **Register** to enter the Join Us page.
3. Tap **Terms of Service** and **Privacy Policy** to read the relevant content and then tap **Agree** to continue.
4. Select the region where your devices locate.

5. In the Register page, tap **Register by Mobile Phone Number**.
6. Enter your mobile phone number and then create a password.

Note

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 **Get Security Code** to get the security code for verification.
8. Enter the security code you received, and then tap **Finish**.

Chapter 4 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.

Caution

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

Note

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*** .

4.1 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 → **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*** .

Note

To get the QR code of a visitor account, go to **More → 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.

Note

Make sure you 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.

4.2 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 → 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.

Note

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

Chapter 5 Device Management

You need to add devices to the Mobile Client before you can do further remote operations such as live view and playback.

The devices added to the Mobile Client will be displayed in the device list.

In the device list, 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.

If a device is authorized to an Installer for device health monitoring, the device will be marked with . For details about authorizing Installer with device permissions, see ***Device Authorization Management*** .

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 on the same LAN.

Steps

1. Add a device.

Note

See ***Add Device for Management*** for details.

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

3. Create a password.

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.

Note

- For details about adding Pyronix 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 ⊕ → **Online Device** to enter the Online Device page.

   All detected online devices will be in the list.
2. Select a device for adding.

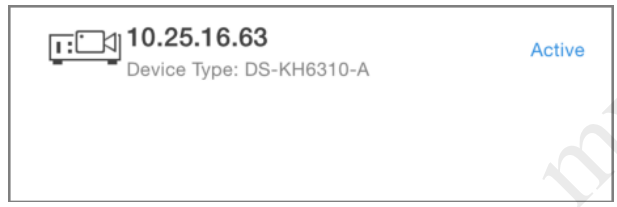

Figure 5-1 Online Device

Note

- 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:** Tap the device name or tap ••• , and then tap **Delete Device**.

5.2.2 Add Device(s) by Scanning Device QR Code

You can add the device by scanning the device's QR code. You can also add device(s) by scanning the QR code obtained via the web page of the device.

Steps

1. On the device list page, tap ⊕ → **Scan QR Code** to enter the Scan QR Code page.

2. Scan the QR code.

- Scan the QR code by aligning the QR Code with the scanning frame.

Note

- Usually, the device QR code is printed on the label, which is on the back cover of the device.
- Tap Off to enable the flashlight if the scanning environment is too dark.

- If there are QR codes in photo album of the phone or tablet, tap to extract QR code from local album.

3. Optional: Perform the following operations if the following situations occur.

- If the system fails to recognize the QR code, tap to add the device manually. See ***Add a Device by Hik-Connect Domain*** or ***Add a Device by IP/Domain*** for details.
- 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.

Note

- The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling Hik-Connect service.
- For details about enabling Hik-Connect service, see ***Enable Hik-Connect Service for Device*** .

6. Optional: Tap **Configure DDNS** to configure DDNS.

Note

- 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: 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.

Steps

Note
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.

Note
- 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 ⋯ and then tap **Delete** to delete the device.
Configure Device Parameters	Tap ⋯ 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 ⋯ 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.

Steps
1. On the device list page, tap ⊕ → **Manual Adding** to enter the Add Device page.
2. Select **Hik-Connect Domain** as the adding type.
3. Enter the device serial No. manually.

Note
- 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.

Note
- 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.

Note
- The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling Hik-Connect service.
- For details about enabling Hik-Connect service, see ***Enable Hik-Connect Service for Device*** .

7. **Optional:** Tap **Configure DDNS** to configure DDNS.

Note

- 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: 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.

Connect to Wired Network

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

Note

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).

Note

- 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.

Note

Make sure you 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 service 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 Hik-ProConnect 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.

   Note

   See ***Add a Device by Hik-Connect Domain*** or ***Add Device(s) 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 Device(s) 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.

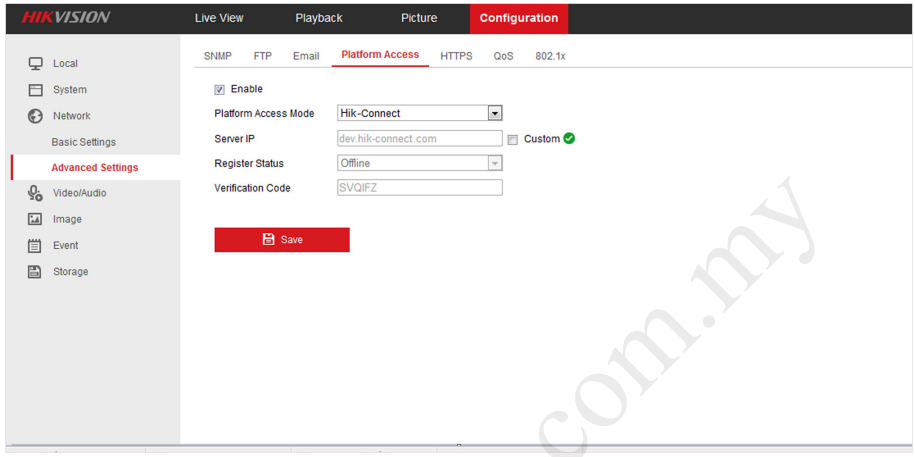

Figure 5-2 The Platform Access Page

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

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 → Network → 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 Device(s) 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.

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

5.7 Manage Solar Camera

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

Wake Up Solar Camera

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

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

View Network Signal Strength

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

Switch Power Consumption Mode

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

Note

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

5.8 Device Settings

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

Note

The available functions on the Settings page vary with different device types and device models.

5.8.1 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

Note

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

1. On the device list page, tap to enter the Settings page of the device.
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.

Note

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.

5.8.2 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

Note

- 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. On the device list page, tap to enter the Settings page of the device.
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.

Note

The default device verification code is usually on the device label. If no verification code found, enter the device verification code you created when enabling Hik-Connect service. For details about enabling Hik-Connect service, see ***Enable Hik-Connect Service for Device*** .

5.8.3 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. On the device list page, tap to enter the Settings page of the device.

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**.

Note

The entered port number should be from 1 to 65535.

User Name

Enter the device user name.

Password

Enter the device password.

4. Tap .

5.8.4 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. On the device list page, tap to enter the Settings page of the device.
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.

Note

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*** .

5.8.5 Set Light for Floodlight Camera

You can set light for the Floodlight camera.

Before You Start

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

Steps

1. On the device list page, tap to enter the Settings page of a Floodlight camera.

2. Tap **Light Settings** to enter the Light Settings page.
3. Set the parameters.

Adjust Brightness

Adjust the brightness of the camera light.

Light Linkage

If enabled, when activities of human beings or animals are detected at night in the areas specified by you (see **Light Linkage Area Settings**, the camera light will be automatically turned on.

Light Linkage Area Settings

Tap the areas to specify them as the light linkage areas.

5.8.6 Edit Settings of Cameras Linked to NVR/DVR

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

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

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

5.8.7 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 event notification about the motion detection alarm.

Steps
1.

On the device list page, tap to enter the Settings page of the network camera.
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 5-3 Draw Motion Detection Area

3) **Optional:** Tap to undo the drawing.

4) Tap to save the motion detection area settings.

4. Tap to go back to the Notification page and tap **Motion Detection Sensitivity**, and then adjust the slider to adjust the motion detection sensitivity.

Low

Moving persons, large moving pets, and any other large moving objects in the motion detection area will trigger the alarm, while smaller objects will not.

Medium

Moving small pets and any other medium-sized moving objects in the motion detection area will trigger the alarm, while smaller objects will not.

High

Moving insects, moving leaves, and any other larger objects will trigger the alarm.

What to do next

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

Note

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

5.8.8 View Network Topology of NVR

You can view network topology of the cameras connected to an NVR.

Note

The NVR should support the network topology functionality.

On the device list page, tap to enter the Settings page of the NVR, and then tap **Network Camera Topology** to enter the topology page. On the page, you can perform the following operations.

View Network Status

On the topology, you can know the type of the network connection between each node (i.e., an NVR or a network camera) by the type of the line between the two nodes: solid line represents wired connection, dotted line Wi-Fi connection.
You can also view network status of the cameras. If a camera icon is grayed out, the camera is offline.

Zoom In/Out

You can pinch fingers together to zoom in, and spread them apart to zoom out.

Refresh Topology Structure

Tap in the upper right corner to refresh the topology structure.

Show/Hide Cascaded Camera

You can enable the topology to display a specific camera's cascaded camera(s).

Note

The NVR should support this function.

1. On the device list page, tap to enter the Settings page of the device, and then tap **Linked Camera** to enter the Linked Camera page.
2. Tap a camera on the Linked Camera page to enter the Details page.
3. Turn on **Cascading Status** to display cascaded camera(s) of a specific camera in the topology. Turn off to hide.

5.8.9 Set Custom Audio

You can select a recorded audio file and set it as the custom audio prompt for the alarms sent from the channels linked to specific models of DVR.

Before You Start

Make sure you have recorded audio files on the Mobile Client. For details, see ***Manage Custom Audio*** .

Steps

Note

The device should support this function.

1. On the device list, tap to enter the Settings page of the device.
2. Tap **Custom Audio** to enter the Select Channel page.

3. Select channel(s), and then tap **Next Step**.

   The available audio file(s) will appear.
4. **Optional:** Tap the Play icon to play the audio file.
5. Select an audio file, and then tap **OK**.

5.8.10 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

Note

- 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. On the device list page, tap to enter the Settings page of the device.
2. Tap and tap **Remote Controller** to enter the following page.

Figure 5-4 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.

5.8.11 Remotely Configure Device

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

Note
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. On the device list page, tap to enter the Settings page of the device.
2. Enter the Remote Configuration page.
- For a device added via IP/Domain, tap → **Remote Configuration** .

  Note
  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.

  Note
  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. On the device list page, tap to enter the Settings page of the device.
2. Enter the Remote Configuration page.

- For a device added via IP/Domain, tap ⋯ → **Remote Configuration** .

Note

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.

Note

Make sure you 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.

Note

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.

Note

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

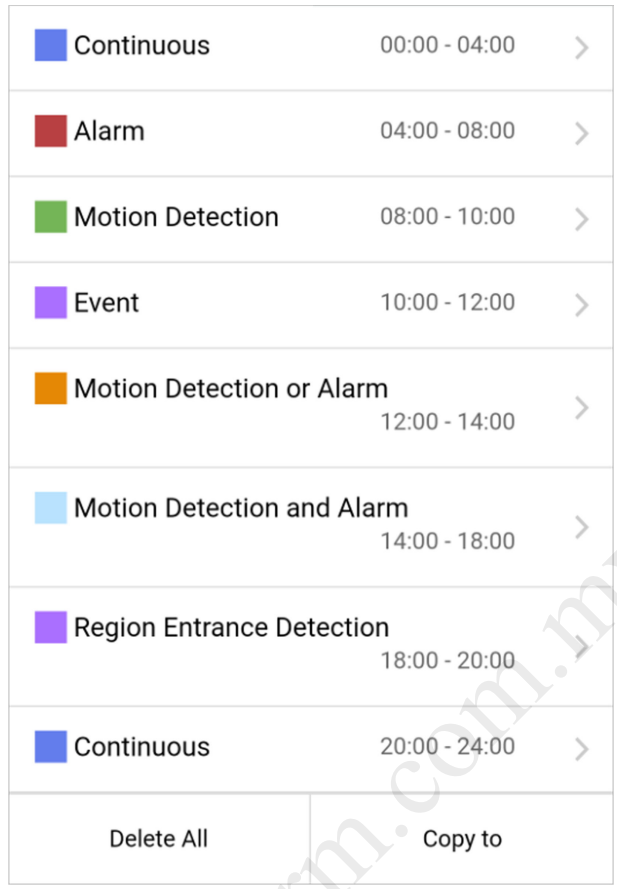

Figure 5-5 Setting Multiple Time Periods in a Day

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. On the device list page, tap to enter the Settings page of the device.

2. Enter the Remote Configuration page.

- For a device added via IP/Domain, tap → **Remote Configuration** .

Note

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.

Note

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.

     Note

     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. On the device list page, tap to enter the Settings page of the device.
2. Enter the Remote Configuration page.
   - For a device added via IP/Domain, tap → **Remote Configuration** .

     Note

     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.

     Note

     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. On the device list page, tap to enter the Settings page of the device.
2. Enter the Remote Configuration page.
   - For a device added via IP/Domain, tap → **Remote Configuration** .

     Note

     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.

     Note

     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. On the device list page, tap to enter the Settings page of the device.

2. Enter the Remote Configuration page.

- For a device added via IP/Domain, tap ⋯ → **Remote Configuration** .

Note

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.

Note

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

Note

This function is only available to the thermal camera.

1. On the device list page, tap ⚙ to enter the Settings page of the device.
2. Enter the Remote Configuration page.

- For a device added via IP/Domain, tap ⋯ → **Remote Configuration** .

Note

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.

Note

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.

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 Home 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 home page (Hik-Connect page), tap ⊕ .
2. Tap **Add to Favorites**.
3. Select devices and cameras on the Select Camera page.
4. Tap **OK**.
5. Create a name for the Favorites and then tap **OK**.

Note

- 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 home 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.

Note

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**.
   - Add to existing favorites.
     a. Tap **Add to Existing Favorites** in the pop-up window.
     b. Select a Favorites folder in the list.

Note

- 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. 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 select the device permissions granted to the recipient to determine which operations the recipient can do on the device.

Steps

1. Enter the Recipient page.

Option 1 Tap → **Share Device** → **Share Device** .

Option 2 On device list page, tap .

You will enter the Recipient 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.
- 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. The recipient will be able to view the device on the device list.

8. Optional: Edit the device permissions.

1) Go to **More** → **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** → **Manage Sharing Settings** .

2) Tap the device to enter the Sharing Details page and then tap **Delete**.

7.2 Share Multiple Devices by Scanning Recipient's Account QR Code

You can share multiple devices to another Hik-Connect user. You can also set the device permissions granted to the recipient to determine which operations the recipient can do on the device.

Steps

1. Enter the Recipient page.

Option 1 Tap ⊕ → **Share Device** → **Share Device** .

Option 2
a. Enter the Live View page.

Note

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

b. Select a live view window and than tap ••• .
c. Tap **Share**.

Option 3 For security control panel, tap the device on device list page to enter the device details page and then tap .

2. Tap **Scan QR Code**.

3. Scan the QR code of the recipient's account.

The recipient's account will be listed in the account list, and be automatically selected.

Note

The recipient can go to **More** → **Account Management** → **My QR Code** on his/her Mobile Client to get the QR code of his/her account.

4. Select device(s), and then tap **Next**.

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 notification about the sharing will appear on the recipient's Mobile Client. The recipient 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.

Tap ⚙ to enter the Settings page of the device and then enable the Silenced mode.

Chapter 8 Cloud Service

In Cloud Service, you can manage or access services related to Hik-ProConnect, which is a cloud service platform for Installers (installation companies). Installer can provide services such as device configuration and device maintenance for you if granted with device authorization and permissions. You can manage device authorization and permissions in Cloud Service.

Cloud Service page includes the following modules.

Service Notifications

Check cloud-related notifications and respond requests from Hik-ProConnect, such as applications from the Installer, including applications for device handover, device authorization and permissions, and device password reset.

Device Authorization

Manage device authorization, device permissions, and ARC authorization, check Installer information, and transfer devices to another user.

Deauthorized Devices

Check the devices that are deauthorized from the Installer and re-authorize to a new or existing Installer.

Cloud Features

Access the features activated by your Installer via Hik-ProConnect, including Access & Attendance, People Counting, and Temperature Screening.

Note

Cloud features are not available in all countries or regions.

8.1 Device Authorization Management

You can grant authorization and permissions of the devices in your Hik-Connect account to an Installer. With device authorization and permissions, the Installer is able to control and configure the devices, thereby managing and maintaining the devices for you.

You can manage device authorization in **Cloud Service → Device Authorization** .

Note

- If you have multiple Installers, you can tap on Installer's name at the top to switch between Installers.
- Authorized devices are grouped in "Sites" which are created by your Installer.

Grant Device Authorization and Permissions to Installer

- If your Installer has sent device authorization application to you, you can grant authorization by approving the application. See ***Approve Device Handover and Authorization Application*** for details.
- To authorize an Installer with more devices, follow the steps below.
  1. Tap ••• → **Authorize More Devices** .
  2. Select devices and permissions.
  3. Tap **OK** and the devices will be authorized to the Installer and added to the Site.

Edit Device Permissions

You can edit devices permissions for Installer in the following two ways.

- Bulk Edit the Permissions of Devices in a Site:
  Tap ••• → **Edit Device Permissions** . Select devices and edit the permissions.
- Edit the Permissions of a Single Device:
  Go to the Home page, in the device list, tap ⚙ of a device to enter the device settings page. Tap **Authorization Service → Edit Permission** to edit device permissions.

Cancel Device Authorization

Tap ••• → **Cancel Authorization** to cancel the authorization of all devices in the Site.
You can keep the Site if there are value-added services activated.
Deauthorized Sites and devices are in the Deauthorized Devices page. You can share Site ID or QR code to another Installer to resume the services.

8.2 Reset Password of Device in Authorization

You can reset the password of a device with the assistance of Installer.

Note

This feature requires device support.

Refer to the flow chart below for the whole process of resetting the password of a device that you authorized Installer with.

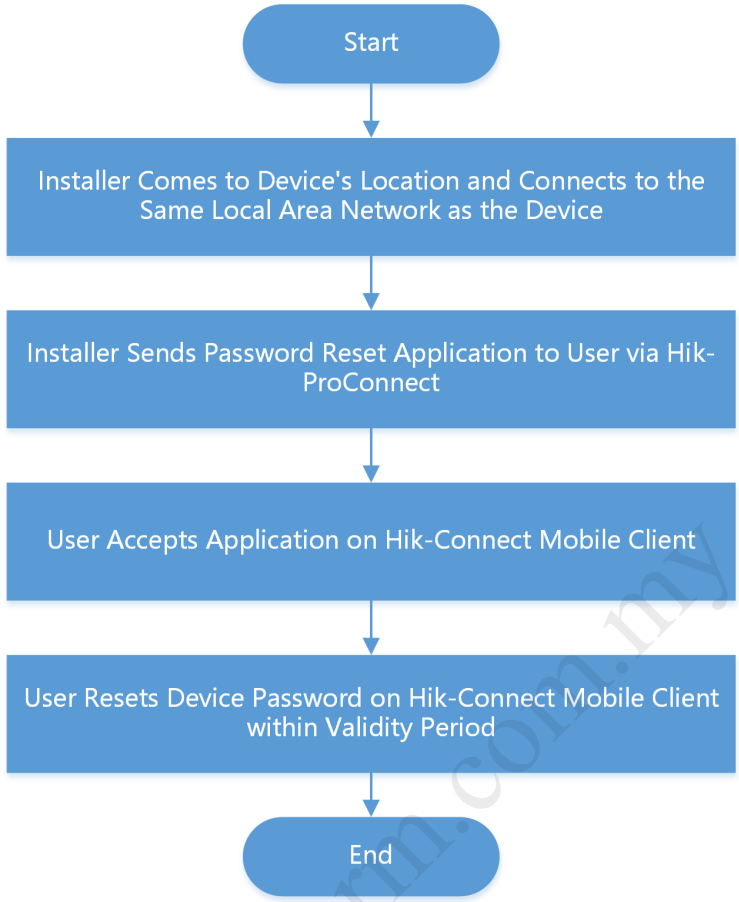

Figure 8-1 Flow Chart of Resetting Device Password

Note

- The validity period of password reset application is 5 minutes.
- You will be notified whether password reset is completed or failed.

Example

User can ask the Installer for a password reset if the password of an authorized device is lost. The Installer has to go to the device's location and connect to the same local area network before sending a password reset application to the user. After the Installer sends the password reset application, user can set a new password for the device.

8.3 Transfer Device to Others

You can transfer the devices in your account to another account. Once transferred, the devices will be unavailable to you, and the target account will have all configuration and operation permissions of the devices.

Steps

1. Go to **Cloud Service → Device Authorization** .
2. Tap ••• → **Transfer Device** .

Note

Only supports transferring devices in a Site altogether. Site is created by your Installer to group your devices.

3. Enter the mobile phone number or e-mail address of the target account.
4. Tap **OK** to start transferring.

Note

- The Site becomes unavailable during transfer process.
- The target user will receive a device transfer application. You can cancel device transfer before the target user accept the application. Once the target user accepts it, you will no longer have any access or permission towards the devices.

8.4 ARC Service

ARC stands for Alarm Receiving Center. ARC provides round-the-clock alarm monitoring and responding service for you. ARC can receive event notifications sent from your devices and respond to these events. In case of emergency, such as intrusions or fires, ARC sends out dispatches or contact the police on your behalf to address security issues to protect people and property.

Activate ARC Service

Note

ARC service is not available in all countries or regions.

Your Installer can enable ARC service for you with your approval.
To enable ARC service, the Installer needs to applies for ARC authorization and permissions. After the Installer sends an application, you need to accept it to activate the ARC service. See ***Approve Device Handover and Authorization Application*** for instructions.
To check the currently active ARC service, go to **Cloud Service → Device Authorization** .

Deactivate ARC Service

You can deactivate ARC service by deauthorizing ARC.
To deauthorize ARC, go to **Cloud Service → Device Authorization → Alarm Receiving Center (ARC)** and click **Deauthorize**.
After deauthorization, the ARC will lose all device permissions you granted previously and cease to provide ARC service for you.

8.5 Access & Attendance

Access & Attendance works with MinMoe access control devices. It is designed for bringing higher security and improved efficiency to access control and attendance tracking. Persons in an Access & Attendance system (usually employees in an organization) can use Access & Attendance on the Mobile Client to check attendance records, control doors and turnstiles, and check in/out.

Note

- Access & Attendance is not available in all countries or regions.
- If applicable, make sure you have evaluated the impact on data protection before using Access & Attendance.
- Select your role and read the part you need.
  - If you are the employee who needs to check attendance records and control doors, read the ***For Employee*** section.
  - If you are the administrator who needs to set up the Access & Attendance system, read the ***For Administrator*** section.

For Employee

Go to **Cloud Service → Access & Attendance** .

Note

If you cannot see Access & Attendance in the Cloud Service tab, you are not in an Access & Attendance system. Ask the administrator of the Access & Attendance system for help.

Access & Attendance has three tabs:

Attendance Report

Check your attendance status and records.

Check In

Check in or check out directly on the Mobile Client without actually presenting and authenticating at the attendance check devices. See details in ***Check In/Out Remotely*** .

Door Control

See the live view of an access control device and open door remotely. See details in ***Open Door Remotely*** .

For Administrator

If you are the administrator who manages employees' attendance, you need to set up the Access & Attendance system before the employees can use Access & Attendance via the Hik-Connect Mobile Client. The system contains the access control devices, person information, shift settings, and access permission settings.

Note

An Installer can create such a system, add access control devices into the system, and hand it over to you. Contact your Installer if you want to deploy Access & Attendance in your organization.

To set up the Access & Attendance system, you need to add persons (employees and sub-administrators) to the system, assign persons to access groups, allow check-in/out on app, and assign shift schedules to persons on the Hik-Connect Portal.
The following is the flow chart for deploying Access & Attendance:

Figure 8-2 Flow Chart for Deploying Access & Attendance

8.5.1 Check In/Out Remotely

You can check in or check out directly on the Mobile Client without actually presenting or authenticating at an attendance check device.

Ask Administrator to Enable Check-In/Out on Mobile Client

If you cannot see the **Check In** tab, it means that you do not have the permission to check in/out on the Mobile Client yet.

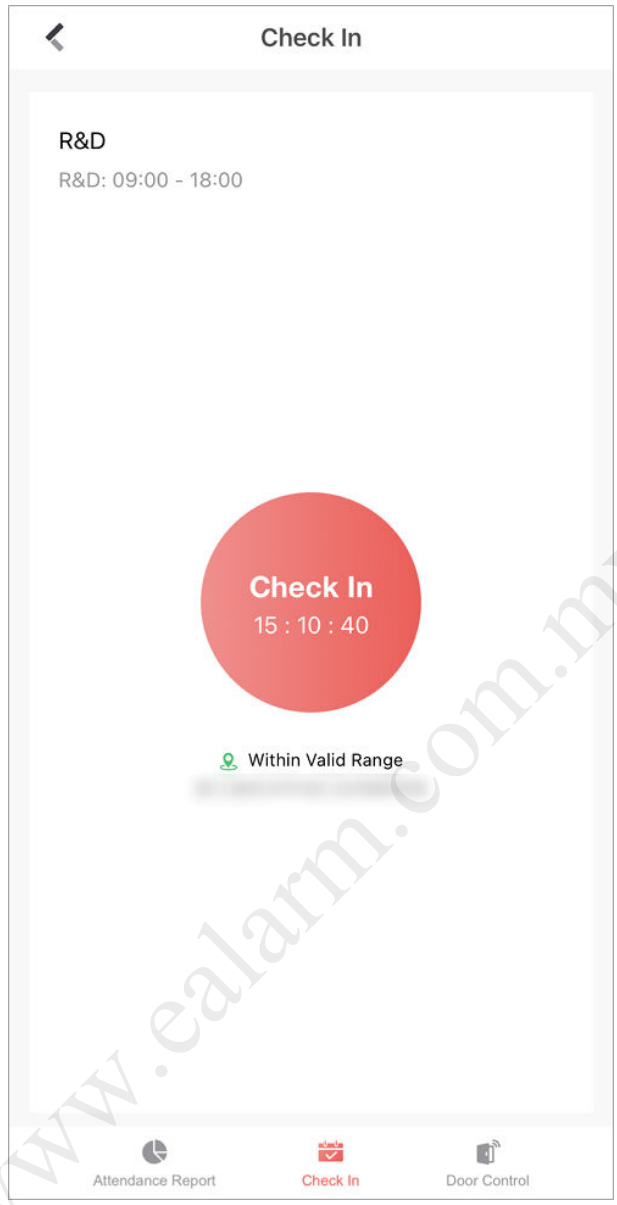

Figure 8-3 Check In Tab in Access & Attendance

You can ask the administrator of the attendance system to enable **Check-In/Out by Mobile Client** for you on the Hik-Connect Portal. The administrator also needs to set the locations of each attendance site and the valid check-in range.

If the attendance system has no attendance check device added, you cannot check in/out on the Mobile Client even if the feature is enabled for you.

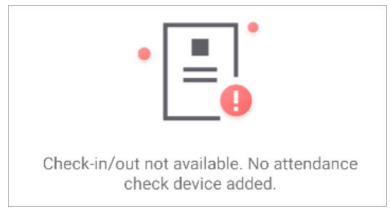

Figure 8-4 No Attendance Check Device

Check In/Out on the Mobile Client

If you have acquired the permission to check in on the Mobile Client, you can tap **Check In** whenever you are within the valid check-in range of any attendance site.
After checking in/out, you can view the recent attendance records.

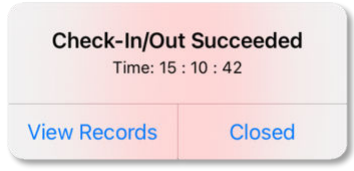

Figure 8-5 Pop-Up Notice on Recent Check-In/Out

If You are not Within Valid Range...

If you are not within the valid check-in range of any attendance site, check-in/out will be unavailable.

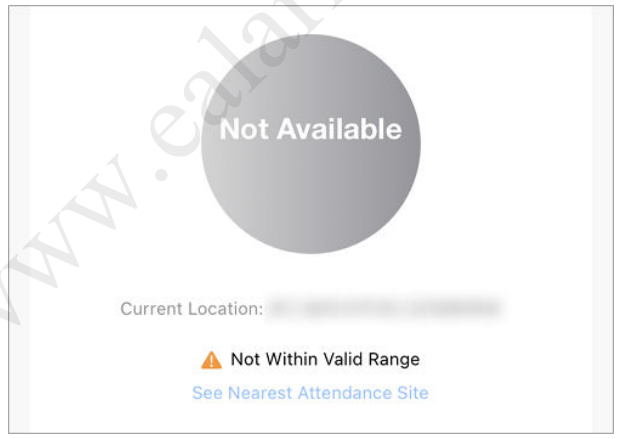

Figure 8-6 Check-In/Out Unavailable

You can tap **See Nearest Attendance Site** to check the nearest site for checking in/out.

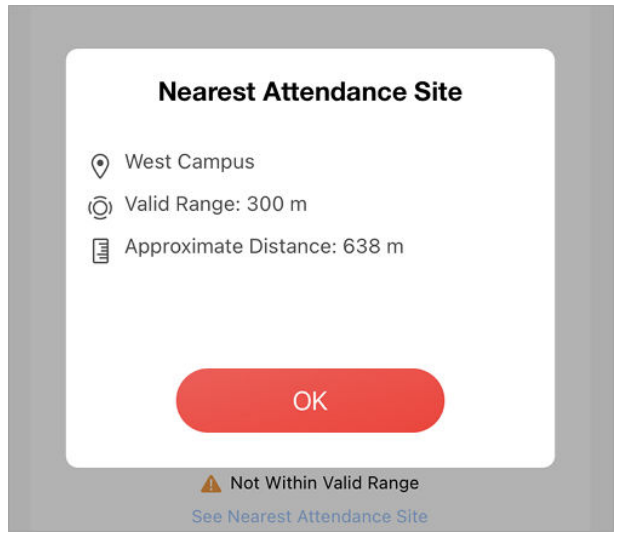

Figure 8-7 See Nearest Attendance Site

If You are Working from Home or on a Business Trip...

If you are not required to work at a fixed location, the administrator can enable **Allow Offsite Check-In** for you.
You can tap **Check In Offsite** to check in outside the valid check-in range of any attendance site.

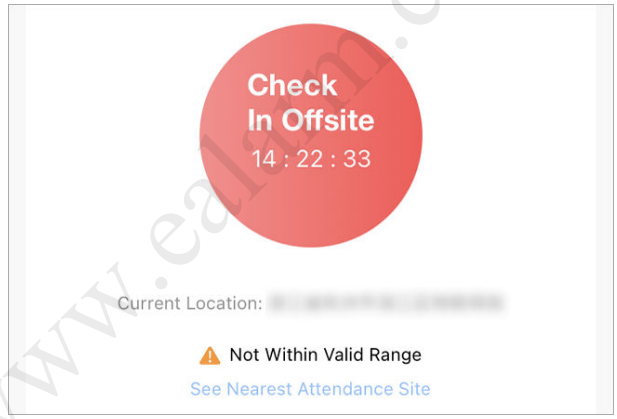

Figure 8-8 Check In Offsite

8.5.2 Open Door Remotely

You can control the status of doors in the Access & Attendance system. You can also see the live video of a door before you open it.

Before You Start
Make sure the administrator has granted the following permissions to you: Remotely Open Door and Remote Live View.

Steps

1. Go to **Cloud Service → Access & Attendance → Door Control** .
   You can see the live view of the access control devices.
2. Control door status.
   Remain Open
   Keep the door open.
   Open Door
   Open the door temporarily.
   Remain Closed
   Keep the door closed.

8.5.3 Add Face Picture for Face Recognition

The administrator of the Access & Attendance system can add a face picture in your person information, so that you can use face recognition for access control and time attendance. If the administrator did not add a face picture for you, you can add it by yourself.

Steps

Note

If you are the administrator of the Access & Attendance system, use Hik-Connect Portal to add employees' face pictures. You shall ensure that you have obtained the explicit consent from the data subject before you upload the face image and that you have performed the DPIA (Data Protection Impact Assessment) where applicable beforehand.

1. Go to **Cloud Service → Access & Attendance** .
2. Tap to enter person information page.
3. Tap **Add Face Picture** and follow the instructions on screen to finish the process.

8.6 People Counting

People Counting works with people counting cameras. It is designed for monitoring crowd density in order to achieve "social distancing" in workplaces, businesses, and public spaces. On the Hik-Connect Mobile Client, you can see the real-time number of people staying in an area, set the maximum number of people allowed to stay in the area, and get alerts when more people are present.

Note

Contact your Installer if you want to deploy People Counting in your space.

To check over-limit records, tap **Message and Report**. You can filter the records by dates and people counting groups.

Note

- An over-limit record contains information such as the name of people counting group, device name, alarm time, actual number of people, and the alarm threshold you set.
- Over-limit records can be kept for up to 30 days.

To send a copy of the records, tap and enter your email address.

Note

The records will be saved as an Excel file.

8.7 Temperature Screening

Temperature Screening works with temperature screening devices and thermographic cameras. It is designed for contact-less skin-surface temperature measurement and detection of protective face masks so as to achieve preliminary screening in public areas with high efficiency. On Hik-Connect Mobile Client, you can see the screening results in real-time, set a threshold temperature, and receive abnormal temperature alarms and no-mask alarms.

Figure 8-9 Temperature Screening and Mask Detection

Note

- Temperature Screening is not available in all countries or regions.
- Contact your Installer if you want to deploy Temperature Screening in your space.

To check the records of abnormal temperature alarms and no-mask alarms, tap **Message and Report**. You can filter the records by dates, alarm types, and devices.

Note

An alarm contains information such as device name, alarm time, alarm type, and body temperature.

To send a copy of the records, tap and enter your email address.

Note

The records will be saved into an Excel file.

8.8 Service Notification

In **Cloud Service → Service Notifications** , you can view the notifications related to services offered by your Installer via the Hik-ProConnect platform, including applications for device handover, device authorization and permissions, and device password reset. You can also view notifications about cross-device linkages and logs about Installer's operations on your devices.

Note

Hik-ProConnect is a cloud service platform for the Installers (installation companies) that configure and maintain your devices and provide value-added services for you.

8.8.1 Accept Invitation to Be Site Owner

You can accept the invitation from the Installer to be the owner of a specific site.

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.

8.8.2 Approve Device Handover and Authorization Application

If an Installer hands over devices to you or applies for device permissions on the Hik-ProConnect platform, you will receive an application notification. After you approve the application, the Installer will be able to provide device configuration and maintenance services based on the permissions you granted.

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

Steps

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

Note

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

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

Note

- In device authorization application, you can view details such as Installer information, permissions that the Installer applies for, and the Alarm Receiving Center (ARC) information.
- For more details on Alarm Receiving Center, see ***ARC Service*** .

5. Select the permissions you want to grant to the Installer.

Note

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

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

8.8.3 Notification about Availability of a Rent Device

If a device that you rent from the Installer is blocked or unblocked by the Installer, you will receive a notification about that.

Note

If a rent device is blocked by the Installer, you are not allowed to operate the device via the Mobile Client. In this case, you can contact the Installer and ask her/him to unblock the device if required.

For such a notification, you can view the Installer who block/unblock the device and the site where the device is added.

8.8.4 View Linkage Notification

Linkage refers to the process in which an event detected by a resource triggers actions in other resources. The linkage can be used for notifying security personnel, upgrading security level, saving

evidence, etc., when specific events happen. You can view notifications about linkages in Service Notifications.

Note

- This feature is not available in all countries or regions.
- The linkage can only be set by the Installer via the Hik-ProConnect platform.

Go to **Cloud Service → Service Notifications → Linkage** to view linkage notifications. You can tap on each notification to view the detected event, event time, devices in the linkage, and triggered actions.

Note

If the Installer has not set linkages for your devices, or the pre-defined linkage actions has not been triggered once, the Linkage tab will not show in Service Notifications.

Chapter 9 Video

With the Mobile Client, you can remotely view live videos of the added encoding devices (e.g., cameras) and play back their video footage.

9.1 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.

9.1.1 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. Tap a camera 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.

Note

- 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.
- 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	a. Tap to go back to the device list. b. Reselect cameras and then tap **OK**.

Note

You can select up to 256 cameras.

Switch to Playback Tap ••• → **Playback** to switch to playback.

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 at the top of the page.

9.1.2 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 left or right to see the rest.

9.1.3 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.

9.1.4 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.

Note

PTZ control should be supported by the camera.

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.

Note

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.

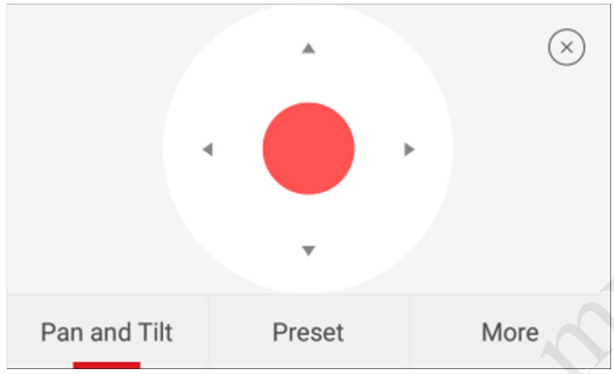

Figure 9-1 PTZ Control Panel

4. Tap **Pan and Tilt**.
5. Drag the circle button at the center of the PTZ Control panel to pan and tilt the camera.

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.

Note

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

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

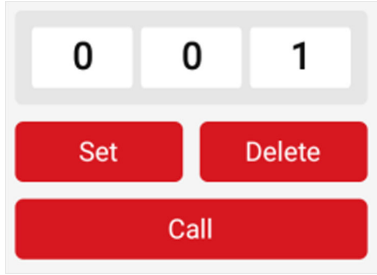

Figure 9-2 Set a Preset

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

Note

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.

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** → to open the PTZ speed panel.
4. Drag the slider to adjust the PTZ speed.

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.

Table 9-1 Other Functions

Icon	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-
	Focus control: Focus +/ Focus -
	Iris control: Iris +/ Iris -

Icon	Description
	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. **Note** The function should be supported by the device.

9.1.5 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

Note

- 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.

   Note

   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.

   Note

   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.

9.1.6 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.

Note

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

2. Capture a picture or record video footage.

Capture Picture Tap to capture a picture.

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

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

9.1.7 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

Note

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

1. Start live view of a device added via IP/Domain.

Note

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

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

Note

The icon vary with the actual video quality.

3. Set the image quality as desired.

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

Note

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

Table 9-2 Recommended Configuration

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

9.1.8 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

Note

The provided image quality types may vary with different devices.

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

   Note

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

2. Tap BASIC to enter the quality switching panel.

   Note

   The icon may vary with the actual image quality.

3. Set image quality.

   Basic

   Basic image quality.

   Note

   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).

9.1.9 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

Note

The function is only supported by fisheye camera.

1. Start live view of a fisheye camera.

Note

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

2. Tap to show the fisheye expansion panel.

3. Select mounting type.

Table 9-3 Mounting Type

Icon	Description
	Wall Mounting
	Ceiling Mounting

4. Select fisheye expansion mode.

Table 9-4 Fisheye Expansion Mode

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

Icon	Description
	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.

9.1.10 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.

Note

- 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 , and then enter the device verification code to open the door.

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

Note

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

9.2 Playback

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

9.2.1 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.

   Note

   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).

   Note

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

Play Video Footage Stored on Cloud	Tap at the top of the playback page to play back video footage stored on cloud. **Note** • The device should support cloud storage, or the icon will not appear. • Make sure you have purchased cloud storage service package for the camera (channel) from the Installer.
Adjust Playback Time	Slide the timeline to adjust the playback time. **Note** 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 Timeline	Spread two fingers apart to scale up the timeline or pinch them together to scale down.

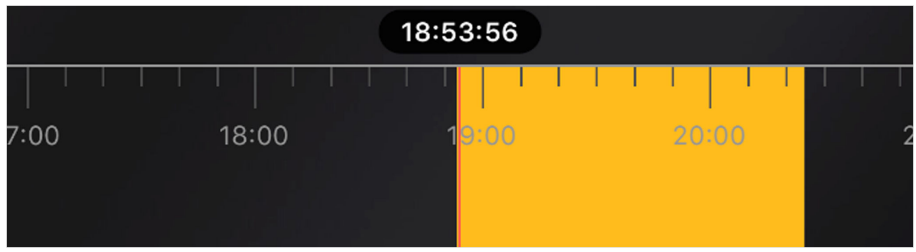

Figure 9-4 Timeline

9.2.2 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

Make sure you have configured events for the selected camera. For details, see ***Configure Normal Event*** and ***Configure Smart Event*** .

Steps

1. Start normal playback.

Note

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.

Figure 9-5 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.

Note

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

9.2.3 Capturing and Recording

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

Steps

1. Start playback.

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 → Pictures and Videos** . For details about managing pictures and videos, see ***Pictures and Videos*** .

9.2.4 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.

Note

For details about starting playback, see ***Normal Playback*** .

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

Note

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.

Note

- 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).

Table 9-5 Recommended Configuration

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

9.2.5 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 1X to set the playback speed to 1/8 X, 1/4 X, 1/2 X, 1X, 2X, 4X, and 8X. X here refers to the original playback speed.

9.2.6 Download Video Segment from Device

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

Note

The function should be supported by the device.

1. Start playback.
2. Tap if important information occurs on the image.

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

   Note

   In special occasions when 130-seconds duration is not available to be selected following the above-mentioned rule, the segment will extend 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.

   Note

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

   Note

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

Note

Downloading at the background is supported. Download task(s) continues if you exit the Download page or the Mobile Client.

6. **Optional:** Go to **More → Pictures and Videos** to view the downloaded video segment.

9.3 Download Video Footage from Cloud

The Mobile Client allows you to view video footage stored on cloud each day. And you can download these video footage if they contain important information about incidents such as violent crimes in case of the need for settling disputes or legal cases.

Before You Start

Make sure you have purchased cloud storage service package(s) for your cameras (channels) from the Installer.

Steps

1. Start playing back video footage stored on cloud.

Note

For details, see ***Normal Playback*** .

2. Tap to enter the Video Stored on Cloud page.
3. Select a date.

Note

The date marked with a blue dot is the date during which video footage is recorded.

4. Tap , and then select video footage.
5. Tap to download the selected video footage.

9.4 Enable/Disable Cloud Storage Service for a Channel

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

Steps

1. Enter the device settings page in the following ways.
   - On the device list page, if the page is in the list mode, swipe 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**.

Note

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

2. Tap **Cloud Storage** to enter the Cloud Storage page.

3. Turn on/off the switch to enable/disable cloud storage service a a specific channel.

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 Client supports 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

Note

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.

   Note

   The door icon varies with different door status.

2. Control the door status.

   Remain Open

   Keep the door open.

   Open Door

   Open the door for a configurable time period. When the time period expires, the door will close.

   Note

   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.

Note

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

3. Enter the super password.

Note

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

Make sure you have added an access control device to the Mobile Client.
See ***Add Device for Management*** for details.

Steps

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

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

Note

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

Note

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

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

   Note

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

   Note

   The password should contain 6 numbers.

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.

Note

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 function.

If you have ignored the above-mentioned prompt, you can tap ⚙ to enter the Settings page, and then switch on the function.

Chapter 11 Security Control

The Mobile Client supports video security control panel, AX security control panel (including AX PRO, AX Hub, and AX 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 AX PRO Security Control Panel

AX PRO security control panel is designed to protect premises required to be protected from intrusion. It supports LAN/Wi-Fi as the primary transmission network, and GRPS/3G/4G LTE as the secondary transmission network. It is applicable to the scenarios of market, store, house, factory, warehouse, office, etc.

- Innovative Tri-X 2-way wireless technology.
- Two-way communication with AES-128 encryption.
- Frequently-hopping spread spectrum (FHSS) is used to avoid interference, to prevent eavesdropping, and to enable code-division multiple access (CDMA) communications.
- Voice guide for alarm alert, system status indication, operation prompt, etc.
- Configuration via device web page, Hik-Connect Mobile Client, and Hik-ProConnect Portal and Mobile Client.
- Push alarm notifications via SMS or phone calls.
- Uploads alarm reports to ARC.
- SIA-DC09 protocol, and supports both Contract ID and SIA data format.
- 4520 mAh lithium backup battery with 12 H standby duration.

11.1.1 Connect to Wi-Fi

You can make the control panel connect to Wi-Fi via the Mobile Client.

Steps

1. On the device list page, tap the security control panel and then log in to the device to enter the page.
2. Tap → **Configure Wi-Fi Network** .
3. Follow the instructions on the page and change the control panel to the AP mode. Tap **Next**.
4. Select a stable Wi-Fi for the device to connect.
5. Back to configuration page to enter the Wi-Fi password and tap **Next**.
6. Tap **Connect to a Network** and wait for connection.

   After the connection is completed, the control panel will prompt to exit AP mode and automatically switch to STA mode.

11.1.2 Configure Cellular Network

You can configure the cellular settings via the Mobile Client.

Before You Start

- Make sure you have installed a SIM card in the device.
- If you have granted an Installer with device authorization, cellular network configuration is available for the Installer only.

Steps

1. On the device list page, tap on the security control panel.
2. Tap → **Cellular Data Network Settings** .
3. **Optional:** Turn on/off cellular network.
4. Tap on the SIM card item.

Note

You can set up for both SIM card slots for models with dual-SIM design.

5. **Optional:** Turn on **Data Usage Limit** to set an upper limit to avoid overage charges.
6. Tap **Parameter Configuration** to configure access number, APN, PIN, etc.
7. **Optional:** To check the balance of the SIM account, go back to the previous page and go to **Communication Parameters → Check Balance** .

11.1.3 Area Management

An area is a partition of a security control system that allows you to batch arm/disarm all zones in it. You can set area parameters such as area name, area background image, and auto arming/disarming schedule.

Go to the settings page of the AX PRO and tap **Area** to see the area list of your AX PRO.

By default, only Area 1 is enabled and cannot be disabled, and the rest are disabled.

Tap on an area to set the area parameters. See the descriptions of each parameter below.

Background Image

Set a unique background for the area.

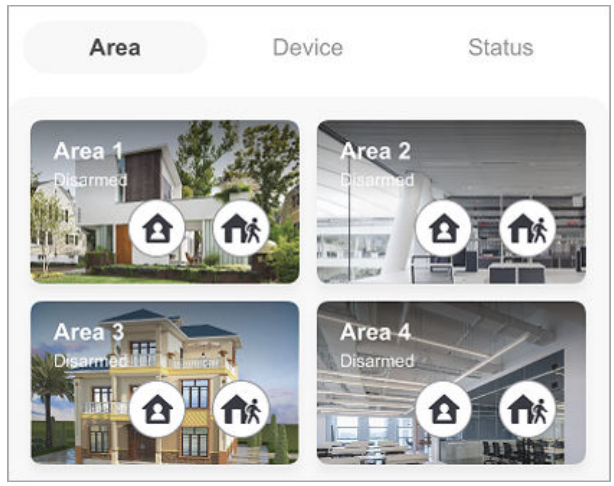

Figure 11-1 Area Background

Note

Background images are stored on your Mobile Client only. Therefore, your background settings will not be shared among other users of the AX PRO.

Enable Area

Switch on to enable the area. When enabled, the area can be linked to zones and users.

Area Name

Customize the name for the area.

Auto Arm

Set a schedule to automatically arm the area at a specific time.

Auto Disarm

Set a schedule to automatically disarm the area at a specific time.

Auto Arming Sound Prompt

If Auto Arming Sound Prompt is enabled, the AX PRO will sound a prompt when armed automatically.

Note

- The system will not be compliant with the EN50131-1 standards when Auto Arming Sound Prompt is disabled.
- This setting will take effect on all areas.

Late to Disarm

If Late to Disarm is enabled, the AX PRO will send a notification to remind you to disarm the area when the area is still armed after a specific time point.

Weekend Exception

If Weekend Exception is enabled, **Auto Arm**, **Auto Disarm**, and **Late to Disarm** will be disabled on weekends.

Note

You can set any day of a week as weekend.

Holiday Excepted

If Holiday Excepted is enabled, **Auto Arm**, **Auto Disarm**, and **Late to Disarm** will be disabled on holidays.

Note

You can set the start date and end date of each holiday.

11.1.4 Manage Users

AX PRO offers different permissions for different user types. The Administrator can add, edit, and delete users, and assign different permissions to the newly-added users.

Steps

Note

- There are four types of users in AX PRO, including Installer, Administrator, Operator, and Local User. Different types of users have different permissions for accessing the features of AX PRO.

Table 11-1 AX PRO User Roles

Role	Permission
Installer	Advanced configuration permissions* When the Installer hands over the AX PRO to you, you will become the Administrator of the device.
Administrator	Advanced configuration permissions*, full control permissions Administrator can share the AX PRO to invite Operators and control their permissions. Administrator can also add Local Users directly in User Management.
Operator	Limited configuration permissions, limited control permissions

Role	Permission
	Operators can use the Mobile Client to control the AX PRO.
Local User	No configuration permissions, limited control permissions Local Users can only use tags or keypads to control the AX PRO, such as arming or disarming the areas.

- * If you have granted an Installer with device authorization, advanced configurations are available for the Installer only. If device authorization is not granted to any Installer, advanced configurations are available for the Administrator of the device only.

1. On the device list page, tap the AX PRO.

2. Tap → **User Management** → **User** .

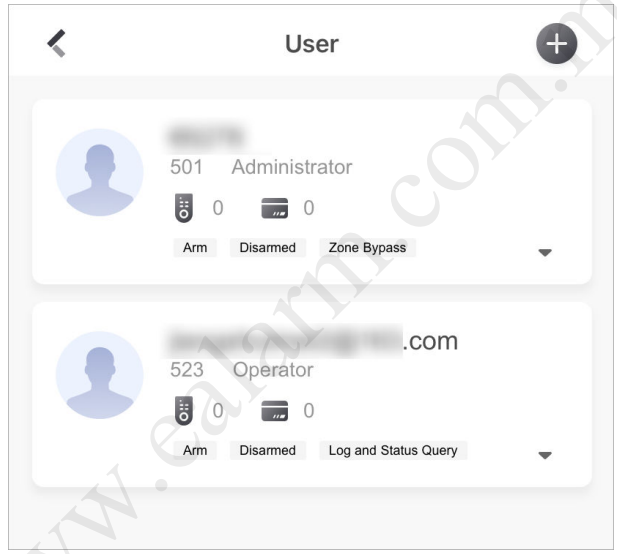

Figure 11-2 User Page

3. Optional: Perform further operations.

Check User ID AX PRO assigns a unique user ID to each user. When an alarm occurs, AX PRO will report the linked user ID along with other alarm information. If your Installer has enabled Alarm Receiving Center (ARC) service for the AX PRO, the alarm containing the user ID will be reported to ARC as well.

Note

For example, tenants in an apartment building co-use one AX PRO, and detectors (such as fire/smoke/CO/glass-break detectors) are set up for each room. The supervisor of the building needs to link each tenant's account

with the corresponding area, collect the room number, tenant contacts, and user ID in advance, and then provide these information to ARC. In case of emergency, whether detected by detectors or manually triggered by a tenant pressing a panic alarm (PA) button, an alarm including the related user ID will be reported to ARC. With such information, ARC can locate the alarm source in a targeted manner.

User Permission

Tap the user to grant or cancel the permissions.

Note

Only the Administrator can control the permissions.

Set Linked Areas

Tap the user and then tap **Linked Areas** to set the area linked to the target user.

Note

Only the Administrator can set linked areas.

Edit Keypad Password

Tap the user and then tap **Edit Keypad Password** to set the keypad password of the target user.

Edit Duress Password

Tap the user and then tap **Edit Duress Password** to set the duress password of the target user.

Note

If under duress, you can enter the duress code on the keyboard to arm and disarm area(s) and upload a duress alarm.

11.1.5 Manage Card/Tag

After adding cards/tags to the 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 to enter the page.
2. Tap → **User Management** → **Card/Tag** to enter the Card/Tag Management page.
3. Tap **+** to add a card/tag.
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.
   - The card/tag will be displayed on the Card/Tag page.
5. **Optional:** Tap a Card/Tag to enter the Setting Page.

6. Tap to edit the card/tag name.

Note

- 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.

7. Slide **Enable Card/Tag**..
8. Select a linked user.
9. Select the card/tag type

Note

Different linked users have different card/tag permissions.

Operation Tag/Card

You can swipe the tag/card to arm or disarm.

Patrol Tag/Card

When you swipe the tag/card, the system will upload a record.

10. Optional: Tap **Delete** to delete the card/tag.

11.1.6 Bypass a Zone

If you bypass a zone, the zone will NOT be armed (related alarms will not be triggered and faults will not be detected) even when the area is armed. Bypassing a zone is usually used in the following two scenarios: 1. If a zone is faulty, other zones of the same area can be armed only when the faulty zone is bypassed; 2. You want a specific zone not to trigger any alarms in special occasions.

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

11.1.7 Arm/Disarm Area

You can arm or disarm an area manually.

On the device list page, tap the security control panel to enter the Area page.

Arm or Disarm a Single Area

Figure 11-3 Arming Control for Each Area

- **Stay Arm**: Tap to arm an area in Stay mode. When people need to stay inside the area, you can use Stay Arm to enable all the perimeter burglary detection (such as perimeter detectors, magnetic contacts, and curtain detectors). In the meantime, the indoor detectors inside the area are bypassed (such as indoor PIR detectors). People can move inside the area freely and the alarm will not be triggered.
- **Away Arm**: Tap to arm an area in Away mode. You can activate Away Arm when you are leaving the area. The area will be armed after the last person exits the area and the exit delay time ends.
- **Disarm**: When the area is armed, you can tap or again to disarm the area. In Disarm mode, no zone in the area will trigger any alarm even when alarm events are detected.

Note

24-Hour zones will trigger alarms whenever alarm events are detected, even if the area is disarmed.

Arm/Disarm All Areas or Clear Alarm

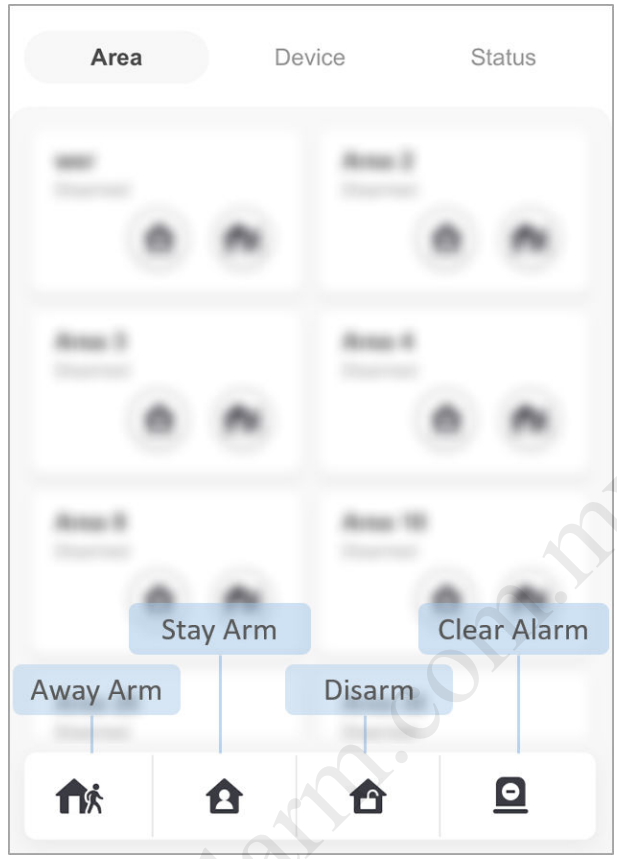

Figure 11-4 Arming Control for All Areas

- **Away Arm**: Tap to arm all areas in Away mode. You can activate Away Arm when you are leaving the premise. All areas will be armed after the last person exits the premise and the exit delay time ends.
- **Stay Arm**: Tap to arm all areas in Stay mode. When people need to stay inside the premise, you can use Stay Arm to enable all the perimeter burglary detection (such as perimeter detectors, magnetic contacts, and curtain detectors). In the meantime, the indoor detectors inside the premise are bypassed (such as indoor PIR detectors). People can move inside the premise freely and the alarm will not be triggered.
- **Disarm**: Tap to disarm all areas. In Disarm mode, no zone will trigger any alarm even when alarm events are detected.

Note

24-Hour zones will trigger alarms whenever alarm events are detected, even if the areas are disarmed.

- **Clear Alarm**: Tap to clear all the alarms triggered by any zones.

11.1.8 Virtual Panic Alarm (PA) Button

In case of emergency, you can tap the PA button for help. When you tap the PA button on the Mobile Client, the AX PRO will issue a panic alarm to alert the other users of the emergency. If the AX PRO has enabled with Alarm Receiving Center (ARC) service, the panic alarm will also be reported to the ARC.

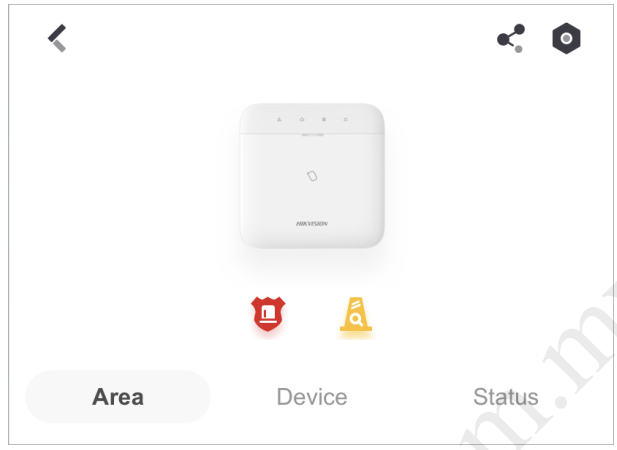

Figure 11-5 AX PRO Page

When an AX PRO user taps on the AX PRO page, the location will be included in the alarm information if the user has enabled location service for the Mobile Client.

If your Installer has enabled ARC service for the AX Pro, the alarm containing location will be reported to ARC as well.

11.1.9 Check System Faults

The system fault list gathers the information on the errors and faults in the security control system in one place.

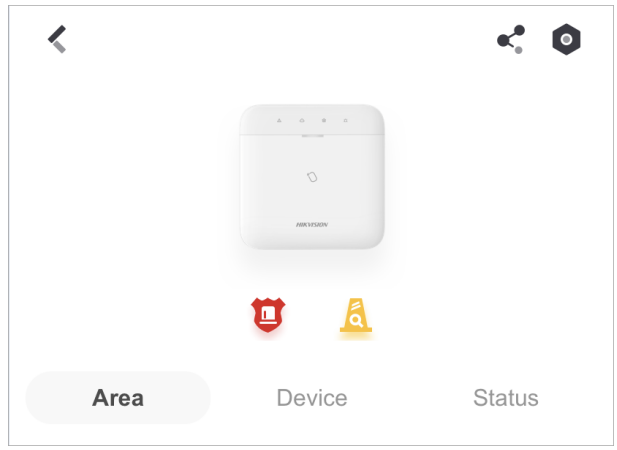

Figure 11-6 AX PRO Page

You can tap on the AX PRO page to check the system fault list.

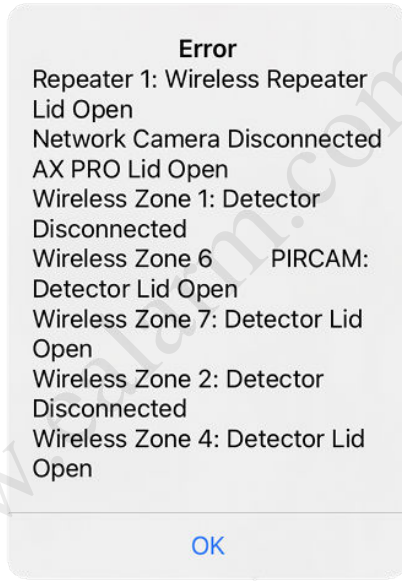

Figure 11-7 System Fault List

11.1.10 Reboot Device

You can reboot the device.

Steps

1. On the device list page, tap the security control panel.
2. Tap → **Maintenance** .
3. Tap **Reboot Device**.

The security control panel will reboot.

11.1.11 Find Device

After you enable Find Me mode of a peripheral device, the indicator of the device will flash. In this way, you can easily distinguish a peripheral device from other devices.

Enter the Settings page of the peripheral device, and then tap **Find Me** to start finding the device.

Note

- The function should be supported by the peripheral device.
- Make sure that the security control panel is not armed, and that it is not under zone test mode, zone test mode, or signal strength test mode.

11.2 AX Hub Security Control Panel

After adding an AX Hub security control panel to the Mobile Client, you can add wireless peripheral devices (including detectors, keyfobs, 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.

Note

- AX Hub security control panel only supports wireless peripheral devices.
- For details about how to add an AX security control panel to the Mobile Client, see ***Add Device(s) 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 AX 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.

Note

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 → **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.

Panel Lockup

If enabled, the installer user can still operate the security control panel, while the admin user will not be allowed to operate it.

Siren Delay Time (Perimeter Alarm)

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

Note

- 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.

Note

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 → **Area Management** to enter the Area Management page.

Note

If EN50131 Compliant mode is enabled, you should log in to the security control panel before you can configure it. For details about enabling EN 50131 Compliant mode, see ***EN50131 Compliant Mode*** .

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

Note

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.

   Note

   If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 mode, see ***EN50131 Compliant Mode*** .

2. Tap → **User Management** → **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.

   Note

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

   User Name

   Enter the user name.

   Password

   Create a password for the user.

Note

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.

Note

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.

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.

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.

Note

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.

Note

Only the administrator and installer can do such an operation.

Keyfob Management

You can add keyfobs to the 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.

   Note

   If EN50131 Compliant mode is enabled, you should log in to the security control panel before you can configure it. For details about enabling EN 50131 Compliant mode, see ***EN50131 Compliant Mode*** .
2. Tap + and then tap **Add Keyfob** on the Scan QR Code page.
3. Present the keyfob to the security control panel.
4. Press any button on the keyfob to learn.
5. Create a keyfob name.

   Note

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

   Note

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

   You can remotely control the selected area(s) by the keyfob based on the permission(s) configured in step 8.
7. Set the Enable Keyfob switch to on to enable the keyfob.

   Note

   If you log in as an installer, skip this step. Enabling keyfob is only available for the administrator.
8. Select permissions (such as the permission to disarm and clear alarm) for the keyfob to define what operations can be done via keyfob.

   Note

   If you log in as an installer, skip this step. Setting permissions for keyfob is only available for administrator.
9. Tap **Add**.
10. **Optional:** Enable silent panic alarm.

1. Go to the settings page of the keyfob.
2. Enable **Silent Panic Alarm**.

   When enabled, no linked alarm output (e.g., sound prompt) will be triggered when panic alarms of the keypad is triggered.

Card/Tag Management

After adding cards or tags to the 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, or 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.

   Note

   If EN50131 Compliant mode is enabled, you should log in to the security control panel before you can configure it. For details about enabling EN 50131 Compliant mode, see ***EN50131 Compliant Mode*** .

2. Tap → **User Management → Card/Tag Management → Add New Card/Tag** to enter the Card/Tag Management page.
3. 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.
4. Create a card/tag name.

   Note

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

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

   Note

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

   Note

   If you log in as an installer, skip this step. Enabling card/tag is only available for the administrator.
7. 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.

Note

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

8. 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.

Note

If EN50131 Complaint mode is enabled, you should log in to security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .

Tap → **Event Video Settings** to enter the page, and then configure the following parameters.

Video Channel

Set the channel for caching video.

Note

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 AX 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.

Note

If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .

2. Tap → **Communication Parameters** → **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

a. Tap **Phone Call**.
b. Set the **Phone Call** switch to on.
c. Tap **Numbers of Calling** to set the maximum calling times if the call is not accepted.
d. 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

a. Tap **SMS**.
b. Set **SMS** switch to on.
c. Select the event(s) for triggering the SMS notification.
d. 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.

Note

For details about control messages, see ***Table 11-2*** 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 11-2 Control Message Description

Command	Operation Type	Target
The number representing the command should be 2 digits. 00: Disarm 01: Away 02: Stay 03: Clear Alarm	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 ... 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 **EN50131 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.

Note

Only the Installer (or Setter) has the permission to enable/disable EN50131 Compliant mode.

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 ⚙ to enter the Settings page.

Note

If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN501313 Compliant mode, see ***EN50131 Compliant Mode*** .

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.

Note

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 → 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 wireless 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 →** ⊞ to enter the Scan QR Code page to add a detector.
   - Tap **Peripheral Device →** ⊞ to enter the Scan QR Code page to add other types of peripheral devices.
3. Scan the QR code of the device.

Note

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.

Note

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

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

Note

For AX 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 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.

Note

If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device.

2. Tap → **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.

Note

If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .

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.

Note

Make sure you have enabled Operation Event Notification on the web page of the security control panel, or the notification will not be pushed to the phone or tablet. For details about the web page, 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** will be disabled on the weekend.

Entry Delay 1
Entry Delay 2

Set a value for **Entry Delay 1** and **Entry Delay 2**. 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.

Entry delay is usually used for avoiding the triggering of false alarms when you enter a certain armed region. For example, you can set an entry delay after you arm your home. In this way, you can avoid the unnecessary triggering of intrusion alarm between the time point when you return home and the time point when you finally disarm your home.

Note

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.

Exit delay is usually used for avoiding the triggering of false alarms when you exit a certain armed region. For example, you can set an exit delay after you arm your home. In this way, you can avoid the unnecessary triggering of intrusion alarm between the time point when you arm your home and the time point when you exit your home.

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.

Note

- If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .
- You can also tap the arming status icon on the device list to arm or disarm the area(s).
- If EN50131 Compliant mode is enabled 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

Make sure you have linked detector(s) to the 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.

   Note

   If EN50131 Compliant mode is enabled, you should log in to the security control panel before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .

2. Tap **Zone** and then tap a detector (zone) on the zone list to enter the 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.

Note

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.

Note

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

Chime

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

Double Knock

If enabled, the detector only alarm when it is triggered for two times within the time interval (i.e., **Double Knock Time Interval**) you set.

This is useful for avoiding false alarms.

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).

Note

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 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

- Make sure you 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, make sure you have linked the network camera to the security control panel via the panel's Web Client. For details, see the user manual of the AX wireless security control panel.

Steps

Note

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.

   Note

   If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .
2. Tap **Zone** and then select a detector from the zone list.
3. Tap **Link Camera** to enter the Link Camera page.

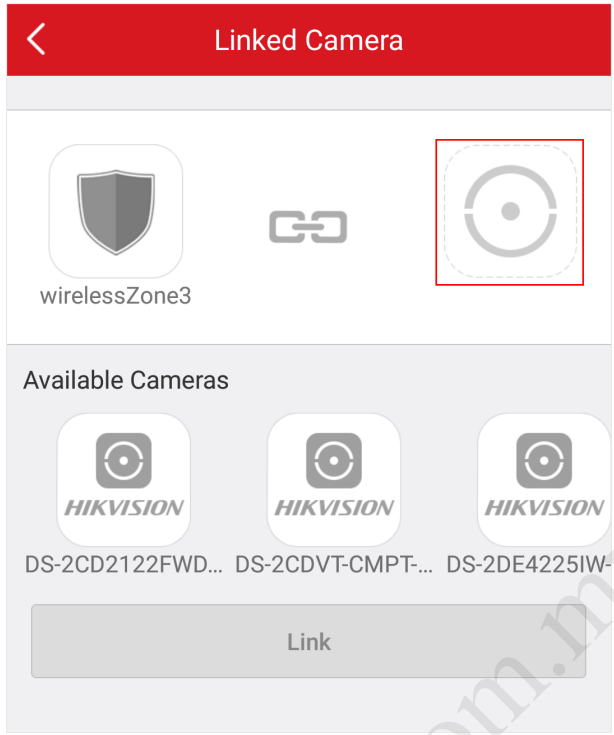

Figure 11-8 Link Camera Page

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

Make sure you have added wireless outputs expander(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.

   Note

   If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .

2. Tap **Peripheral Device** and then tap a wireless outputs expander on the device list.

   The name of the module and the relays of the expander will be displayed.

3. Click the name of the module to set its parameter.

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.

Note

The default offline duration is 1 hour.

4. Tap a relay to enter its settings page to set its parameters.

Continuous Output

If enabled, the relay will be normally closed or open.

Output Delay

The delay time for the relay to become closed. In other words, output delay refers to the duration of the alarm output.

Link Event

Set the type of the event linked to the relay.

Alarm

Alarm outputs will be activated when the zones in the selected area(s) alarm.

You can select a event sub-type (e.g, panic alarm) as the event that requires alarm output once it is detected within the zones.

Arming

Alarm outputs will be activated when the area(s) you select are armed.

Disarming

Alarm outputs will be activated when the selected area(s) are disarmed.

Manual Mapping

Set the switch icon to ON to manually activate alarm outputs of the relay.

Zone

Alarm outputs will be activated when the selected zone(s) are triggered or tampered.

11.2.10 Set Wireless Siren Parameters

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

Before You Start

Make sure you have added wireless siren(s) to the security control panel. For details, see ***Add Device 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.

   Note

   If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .

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.

   Note

   The function should be supported by the siren.

4. Set parameters.

   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.

   Arm/Disarm LED Indicator

   If enabled, the LED indicator of the siren will flash for one time when a area is armed, two times when disarmed.

   Note

   For sirens of the versions earlier than V1.0.6, the parameter is not supported.

   Arm/Disarm Buzzer

   If enabled, the buzzer of siren will buzz for one time when a area is armed, two times when disarmed.

   Note

   For sirens of the versions earlier than V1.0.6, the parameter is not supported.

   Volume Test

   Tap to test the volume of the siren.

   Note

   For sirens of the versions earlier than V1.0.6, the parameter is not supported.

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
Make sure you 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.

Note

If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .

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.

Silent Panic Alarm

When enabled, no linked alarm output (e.g., sound prompt) will be triggered when panic alarms of the keypad is triggered.

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

Make sure you 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.

Note

If EN50131 Compliant mode is enabled, you should log in to the security control panel first before you can configure the device. For details about enabling EN50131 Compliant mode, see ***EN50131 Compliant Mode*** .

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 AX Hybrid Security Control Panel

Compared with AX Hub security control panel, AX Hybrid security control panel supports not only wireless peripheral devices, but also wired ones. After adding an AX Hybrid security control panel to the Mobile Client, you can add peripheral devices (including detectors, keyfobs, 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.

Note

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

11.3.1 Configure Security Control Panel

Enter a short description of your concept here (optional).

This is the start of your concept.

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 to enter the Area page, and then tap → **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.

Note

- 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.

Note

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 → **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

Note

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 to enter the control panel page.
2. Tap → **User Management** → **User** .

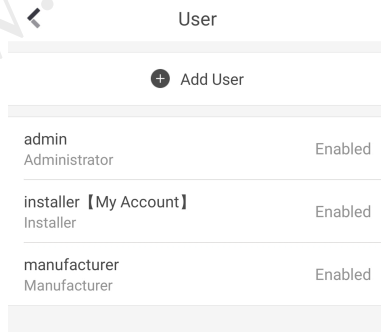

Figure 11-9 User Management

3. Tap **Add User**.

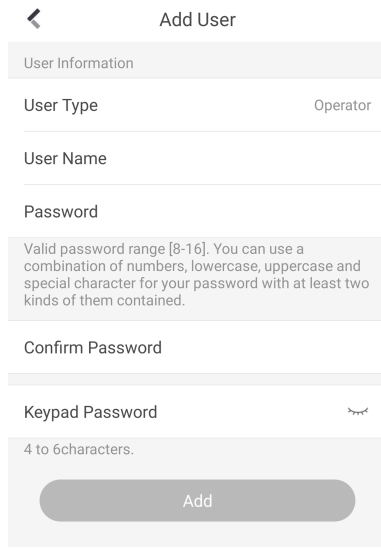

Figure 11-10 Add User

4. Select **User Type**. Enter **User Name** and **Password**.
5. Enter **Keypad Password**.

Note

The keypad password +1 or -1 is the duress code. Use the duress code can operate the keyboard to arm and disarm normally and upload a duress alarm. For example, if the keypad password is 123456, the duress code is 123455 or 123457.

6. Tap **Add** to add the user.
7. **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.

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.

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.

Note

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.

Note

Only the administrator and installer can do such an operation.

Keyfob Management

You can add keyfobs to the 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 to enter the area page.
2. Tap → **User Management** → **Keyfob Management** → **Add New Keyfob** to enter the Card/Tag Management page.
3. Select a wireless receiver or keypad.
4. Present the keyfob to the wireless receiver or keypad.
5. Press any button on the keyfob to learn.
6. Create a keyfob name.

Note

- 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.

Note

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

Note

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

Note

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

10. Tap **Add**.
11. **Optional:** Enable silent panic alarm.
    1) Go to the settings page of the keyfob.
    2) Enable **Silent Panic Alarm**.

    When enabled, no linked alarm output (e.g., sound prompt) will be triggered when panic alarms of the keypad is triggered.

Add Card/Tag

After adding cards or tags to the 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, or 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. Select a keypad.
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.

   Note

   - If you log in as an installer, skip this step. Editing card/tag name is only available to the 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.

   Note

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

   You can remotely control the selected area(s) by the card/tag based on the permission(s) configured in step 8.
7. Set the Enable Card/Tag switch to on to enable the card/tag.

Note

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

Note

If you log in as an installer, skip this step. Setting permissions for card/tag is only available for the 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 to enter the control panel page.

Tap → **Event Video Settings** to enter the page, and then configure the following parameters.

Video Channel

Set the channel for caching video.

Note

Make sure you 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 AX 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 to enter the Area page.
2. Tap → **Communication Parameters** → **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

a. Tap **Phone Call**.
b. Set the **Phone Call** switch to on.
c. Tap **Numbers of Calling** to set the maximum calling times if the call is not accepted.
d. 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

a. Tap **SMS**.
b. Set **SMS** switch to on.
c. Select the event(s) for triggering the SMS notification.
d. 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.

Note

For details about control messages, see ***Table 11-2*** 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 11-3 Control Message Description

Command	Operation Type	Target
The number representing the command should be 2 digits. 00: Disarm 01: Away 02: Stay 03: Clear Alarm	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 ... 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.

11.3.2 Add Device to Security Control Panel

You should add detectors (zones), other 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, sirens, keypad, 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** → to enter the Scan QR Code page to add a detector.
- Tap **Peripheral Device** → to enter the Scan QR Code page to add other types of peripheral devices.

3. Scan the QR code of the device.

Note

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.

Note

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

5. Tap **Select Wireless Receiver** to select a wireless receiver.
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 AX Hybrid security control panel. For details, see the user manual of the device.

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 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.

Note

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 → **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.

11.3.3 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.

On the device list, tap the security control panel and log in to the device to enter the Area page, and then tap **More** to enter the Settings page to set the following parameters.

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.

Note

Make sure you have enabled Operation Event Notification on the web page of the security control panel, or the notification will not be pushed to the phone or tablet. For details about the web page, 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** will be disabled on the weekend.

Entry Delay 1

Entry Delay 2

Set a value for **Entry Delay 1** and **Entry Delay 2**. 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.

Entry delay is usually used for avoiding the triggering of false alarms when you enter a certain armed region. For example, you can set an entry delay after you arm your home. In this way, you can avoid the unnecessary triggering of intrusion alarm between the time point when you return home and the time point when you finally disarm your home.

Note

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.

Exit delay is usually used for avoiding the triggering of false alarms when you exit a certain armed region. For example, you can set an exit delay after you arm your home. In this way, you can avoid the unnecessary triggering of intrusion alarm between the time point when you arm your home and the time point when you exit your home.

11.3.4 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 to enter the Area page and then control the area. You can swipe to the left or right to switch areas.

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.

11.3.5 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

Make sure you have linked detector(s) to the 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 to enter the control panel page.
2. Tap **Zone** and then tap a detector (zone) on the zone list to enter the Settings page.

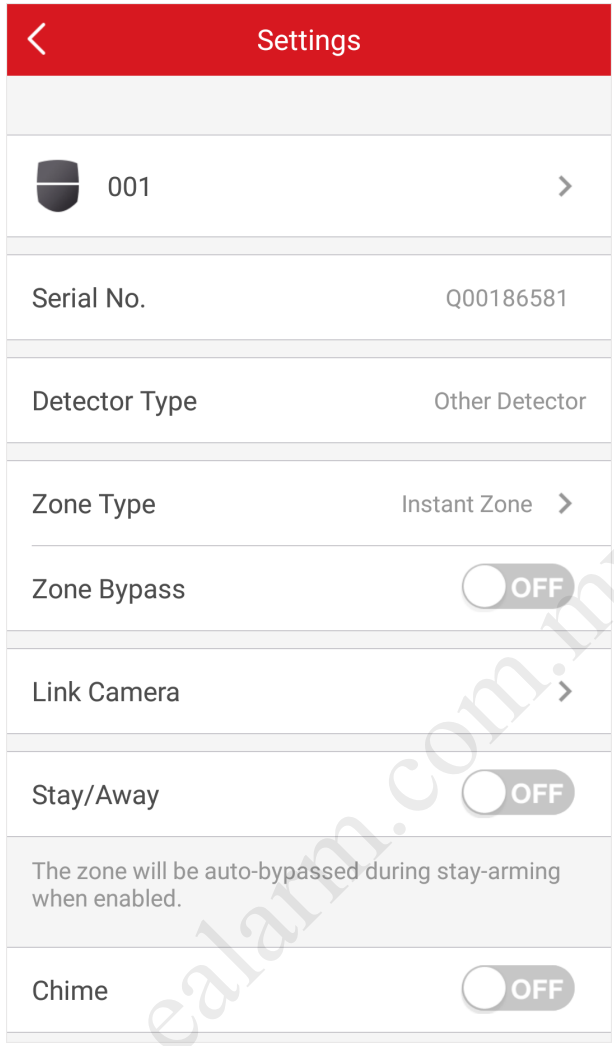

Figure 11-11 Zone Settings Page

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.

Note

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.

Note

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.

11.3.6 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).

Note

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

11.3.7 Link Camera to Zone

If a network camera has already been linked to the 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

- Make sure you 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, make sure you have linked the network camera to the security control panel via the panel's Web Client. For details, see the user manual of the AX wireless security control panel.

Steps

Note

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 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.

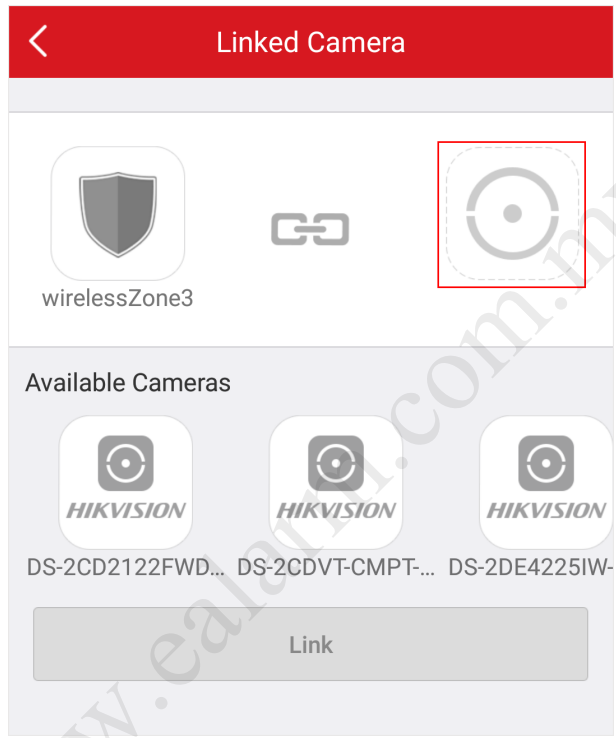

Figure 11-12 Link Camera Page

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

11.3.8 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

Make sure you have added wireless outputs expander(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 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.

   Note

   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. **Alarm** Alarm outputs will be activated when the zone alarms. **Arming** Alarm outputs will be activated when the area (system) is armed. **Disarming** Alarm outputs will be activated when the area is disarmed. **Manual** Set the switch icon to ON on the relay list to manually activate alarm outputs of the relay. **Zone** Alarm outputs will be activated when the selected zone is triggered or tampered.
Set Delay Time for the Relay to Close	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.

11.3.9 Set Wireless Siren Parameters

You can edit siren name and adjust siren's volume. And for a wired siren, you can also set siren type for it.

Before You Start

Make sure you have added wireless siren(s) to the security control panel. For details, see ***Add Device to Security Control Panel*** .

Steps

1. On the device list page, tap the security control panel and then log in to the device 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. **Note** The function should be supported by the siren.
Set Linked Event for Wired Siren	• **Alarm**: The siren will be activated when the zones in the selected area(s) alarms. You can select a event sub-type (e.g, panic alarm) as the event that requires alarm output once it is detected within the zones. • **Arming**: The siren will be activated when the selected area(s) are armed. • **Disarming**: The siren will be activated when the selected area(s) are disarmed. • **Manual Mapping**: Set the switch icon to ON to manually activate the siren. • **Zone**: The siren will be activated when the selected zone(s) are 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.

11.3.10 Set Keypad Parameters

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

Before You Start

Make sure you 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 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.

Silent Panic Alarm

If enabled, no linked alarm output (e.g., sound prompt) will be triggered when the device alarms.

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.

11.3.11 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

Make sure you 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 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.

11.4 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.

11.4.1 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.

Note

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 Hik-ProConnect 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

Note
- 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.

Figure 11-13 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.

Note

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.

11.4.2 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.

Note

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 to search for the detector.
4. Tap **Add** on the Result page.
5. Tap **Finish**.

11.4.3 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.

Note

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.

Note

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.

Note

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

11.4.4 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.

Note

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

11.4.5 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.

   Note

   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**

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

11.4.6 Enable Voice Prompt

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

Note

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.

11.4.7 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 → Delete** to delete the zone.

11.5 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.

Note

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.

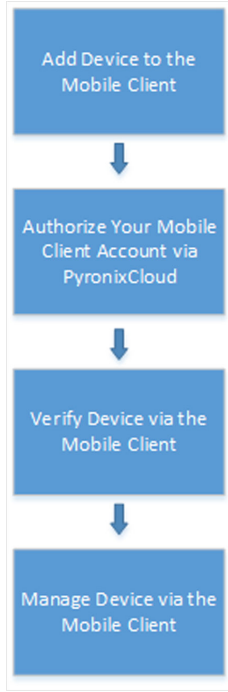

Figure 11-14 Flow Chart

11.5.1 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.

11.5.2 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:

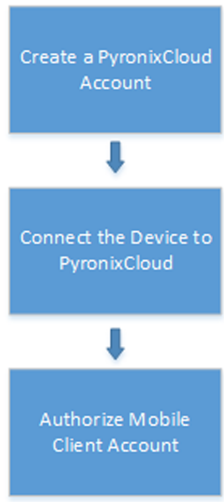

Figure 11-15 Flow Chart of the Authorization

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*** .

Figure 11-16 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**.

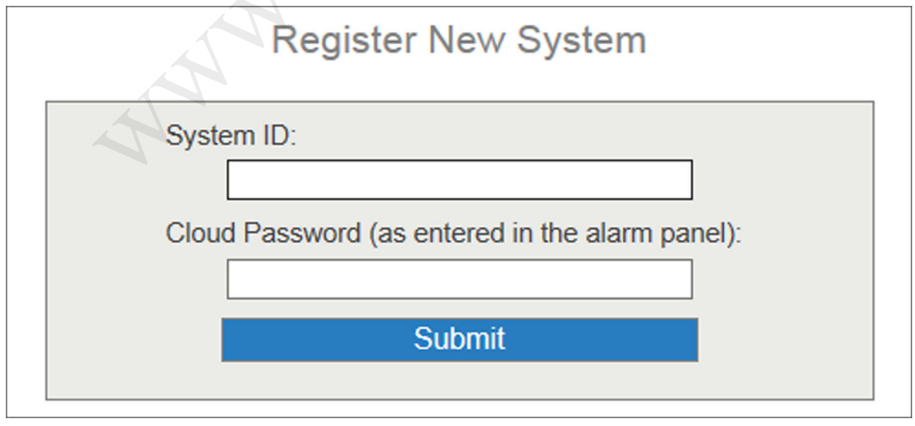

Figure 11-17 Register a New System

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.

Figure 11-18 Device User List Page

5. Click **Save Now**.

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

11.5.3 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**.

11.5.4 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

Note

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.

   Note

   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.

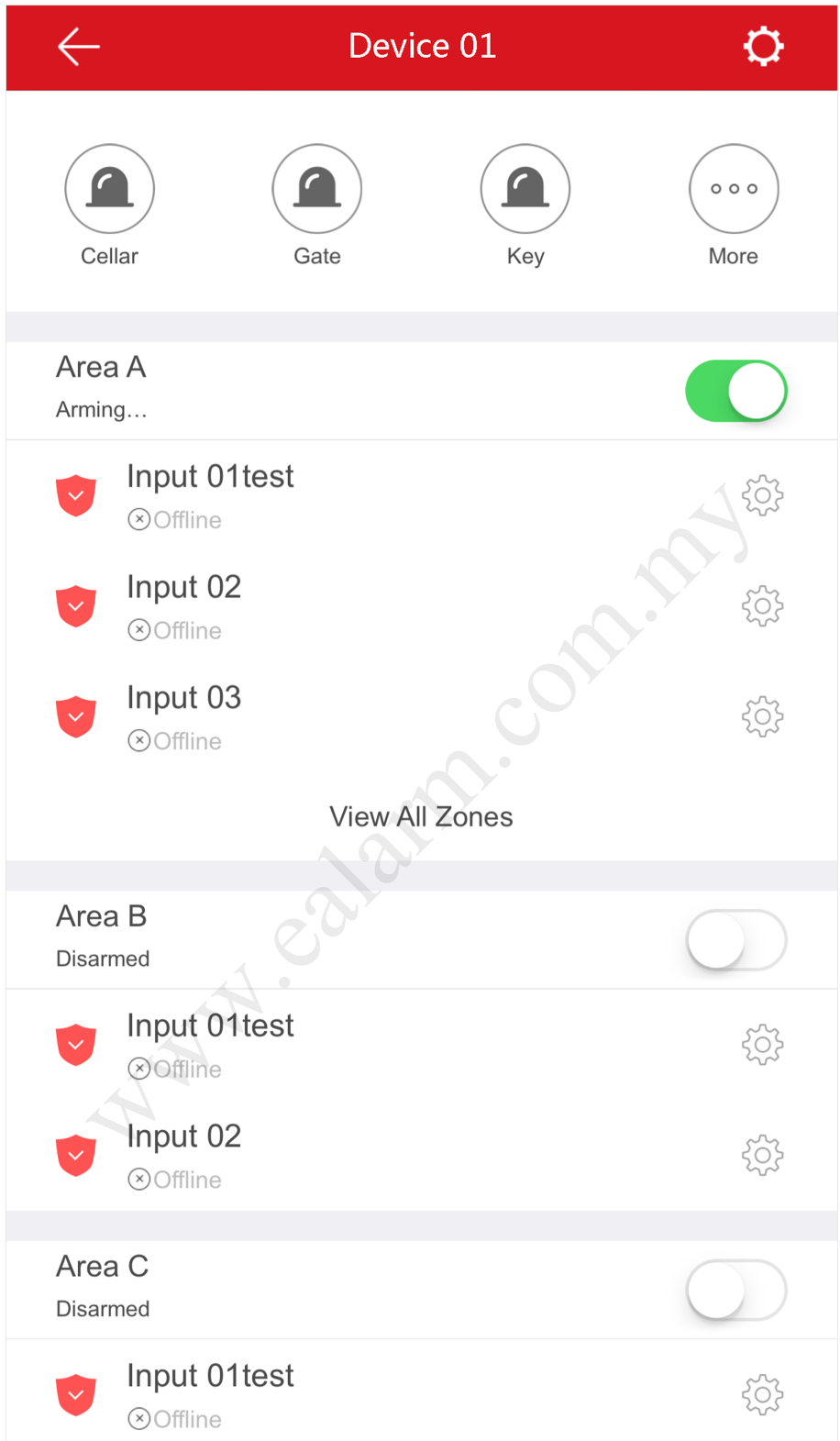

Figure 11-19 Area (Partition) Page

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

11.5.5 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.

   Note
   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.

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

11.5.6 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 to enter the Settings page of the zone, and then enable zone bypass.

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

Chapter 12 Panic Alarm Device

Panic alarm devices are designed to provide quick access of reporting emergencies and getting help when emergency situations occur and timely responses are required. You can quick respond to the emergency calls from the panic alarm devices on the Mobile Client.

  

When a person presses the panic button (or emergency button) on a panic alarm device (including panic alarm panel/box/station), you will receive a call from the device on the Mobile Client.

Therefore, you can respond to the emergency and get in touch with the person reporting the emergency in time.

- Before answering an emergency call, you can:
  - See the live video of the panic alarm device or linked camera.
  - Control the sounder, strobe light, and alarm outputs.

Note

You cannot control the sounder, strobe light, or alarm output if the panic alarm device is shared from another user.

- After answering an emergency call, you can:
  - Start two-way audio.
  - Control strobe light and alarm outputs.

Note

You cannot control sounder after answering the call.

You can see the history of incoming emergency calls in **Notification → Call** .

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

Make sure you have added an video intercom device to the Mobile Client. See ***Add Device for Management*** for details.

Steps

Note

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

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

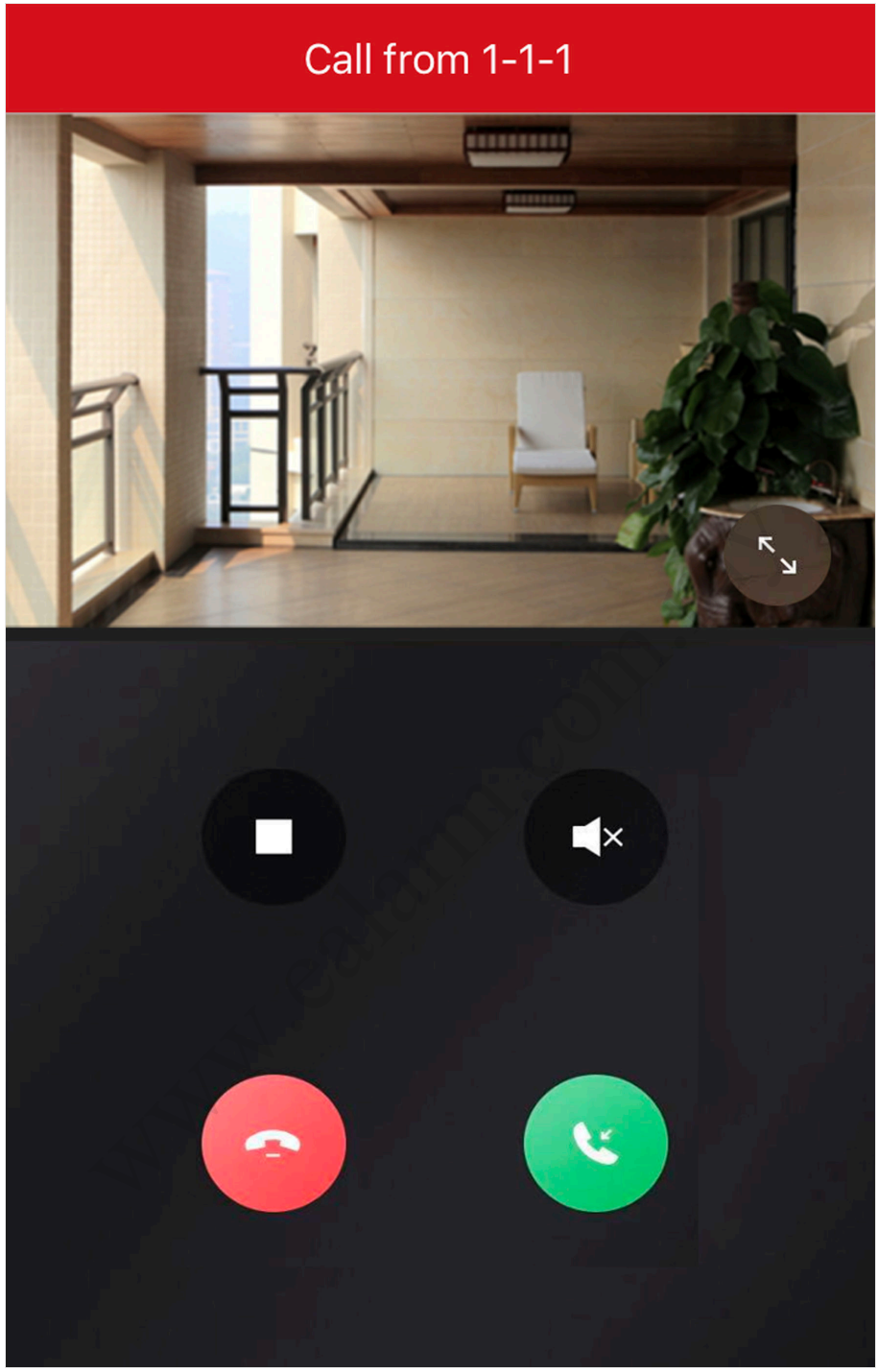

Figure 13-1 Call Page

2. Perform the following operations.

Answer the Call	Tap to answer the call.
Stop/Restart Live View	Tap to stop the live view. And tap to restart it.

Mute	Tap to mute the live video.
Open Door	Tap to open the door.
Digital Zoom	Pinch two fingers together to zoom in the live video image, and spread them apart to zoom out.

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, and controlling relays connected to the indoor station.

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

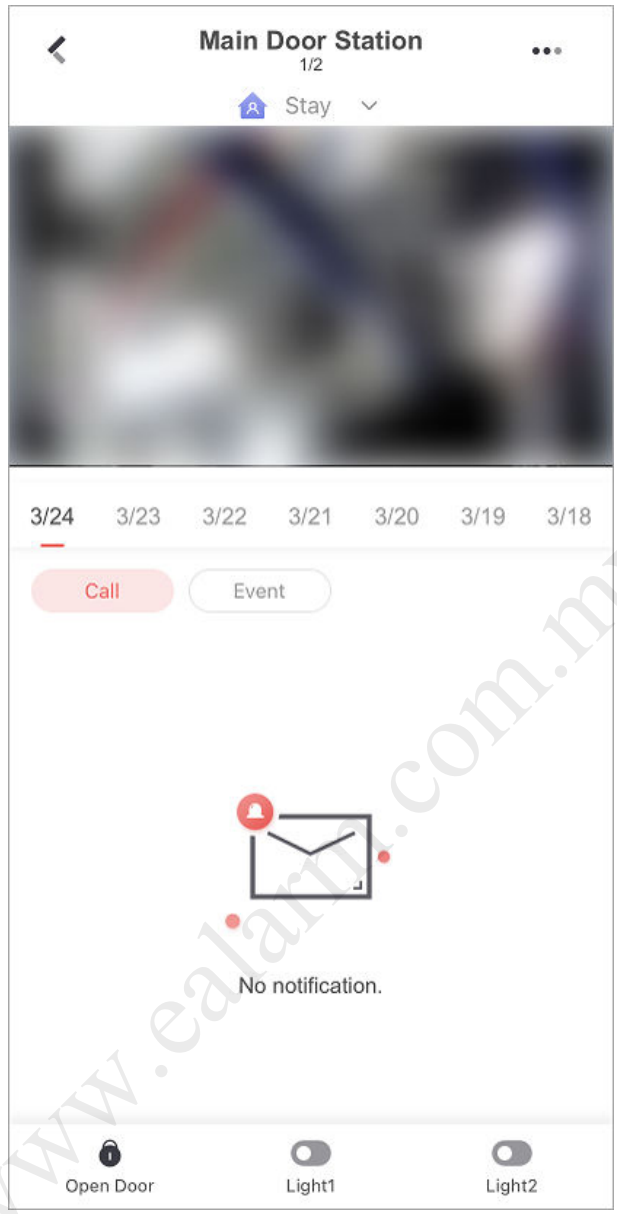

Figure 13-2 Video Intercom Device Page

Switch Scene

You can tap ⌄ to set **Stay**, **Away**, **Sleep**, or **Custom** as the scene for arming the detectors linked to the door station.

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.

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.

Sleep

The detectors in the bedroom is bypassed while the detectors in other rooms are armed. In this scene, all the perimeter burglary detection in other rooms are turned on, while no alarms will be triggered within the bedroom.

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.

Note

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 ••• → **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).

Control Door

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

Control Relay

You can tap to control the connected relays of an indoor station remotely.
To set up relay name and open duration, go to the Settings page of the video intercom device.
Open duration for a relay:

- Remain Open: The relay will not be closed automatically after you open it.
- 0-180s: The relay will be closed automatically after the open duration.

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 event notification about the motion detection alarm.

Before You Start

Make sure you have added a Wi-Fi doorbell to the Mobile Client. See ***Add Device for Management*** for details.

Steps

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

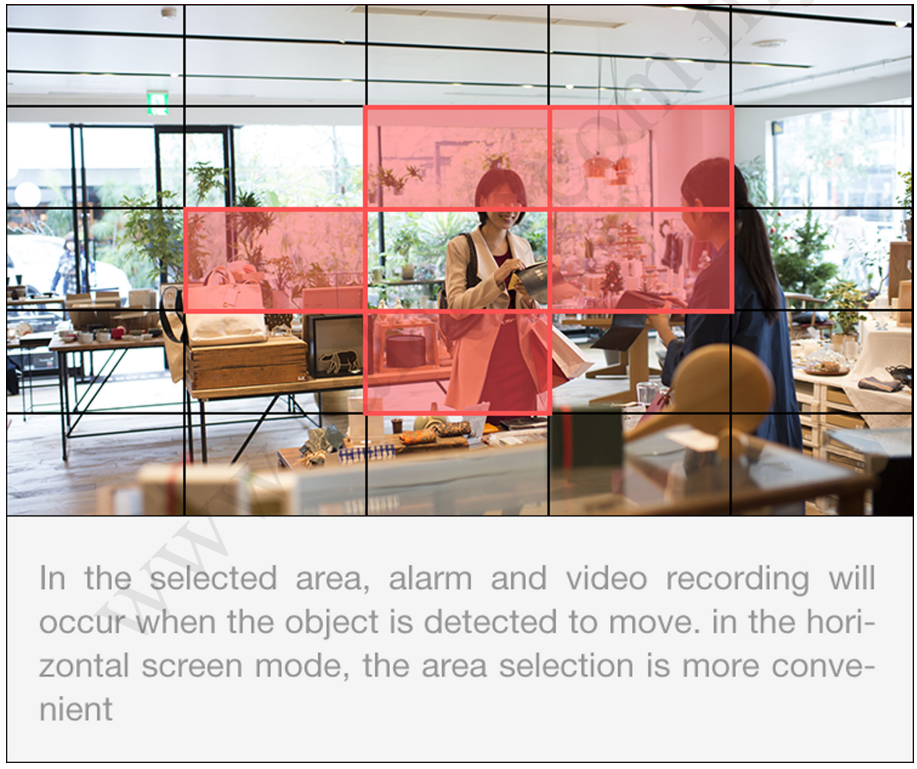

Figure 13-3 Draw Motion Detection Area

   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.

Note

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

13.4 Set Volume for Video Intercom

You can set video intercom volume as required.

Steps

Note

Only video intercom devices support this function.

1. On the device list page, tap ⚙ to enter the Settings page of a video intercom device.
2. Tap **Loudspeaker Volume** or **Microphone Volume** to adjust the loudspeaker and the microphone volume respectively.

Chapter 14 Router

You can establish a wireless network by setting up a Hikvision router.

Add and Set Up a Router

You can add a new router to the Mobile Client, so that you can set up your wireless network with just a few taps and manage the router right on your phone.
See details in ***Add and Set Up a Router*** .

Check the Network Speed and Connected Devices

After adding the router, it will show up in the device list.

Figure 14-1 Device List

You can tap on the router to see its network speed and connected devices.

Figure 14-2 Connection Details

Tap on a connected device, you can see its connection details, limit the connection speed, or add the device to the blocklist.
See details in ***Manage the Devices Connected to a Router*** .

Change the Wi-Fi Name, Security Mode, Password, and Bands

You can set the Wi-Fi name, security mode, and password of a router in Wi-Fi settings. You can also hide the Wi-Fi from other people's Wi-Fi list. If your router supports the 5 GHz Wi-Fi, you can also enable the 5 GHz Wi-Fi for higher data rates.
See details in ***Wi-Fi Settings of a Router*** .

Change the Internet Connection Type

You can set the Internet connection type to PPPoE, dynamic IP, or static IP in Internet Settings.
See details in ***Internet Settings of a Router*** .

Set Up a Guest Wi-Fi for Visitors

You can set up a guest Wi-Fi to securely separate visitors' Wi-Fi connection from yours. You can also control the validity period and bandwidth limit of the guest Wi-Fi.
See details in ***Set Up a Guest Wi-Fi for Visitors*** .

Improve the Network Quality with Wi-Fi Speedup

If the Wi-Fi connection is slowing down and becoming unstable, you can use Wi-Fi Speedup to improve the network quality.
See details in ***Wi-Fi Speedup*** .

Secure the Network with Security Checkup

Security Checkup examines the overall security level of your router and wireless network, and provides recommendations to guide you secure your network.
See details in ***Security Checkup*** .

Check the Internet Connection Details

Tap **Status** on the settings page of your router. You can see the overall status, speed, duration, connection type, IP address, subnet mask, network gateway, and DNS of the Internet connection.

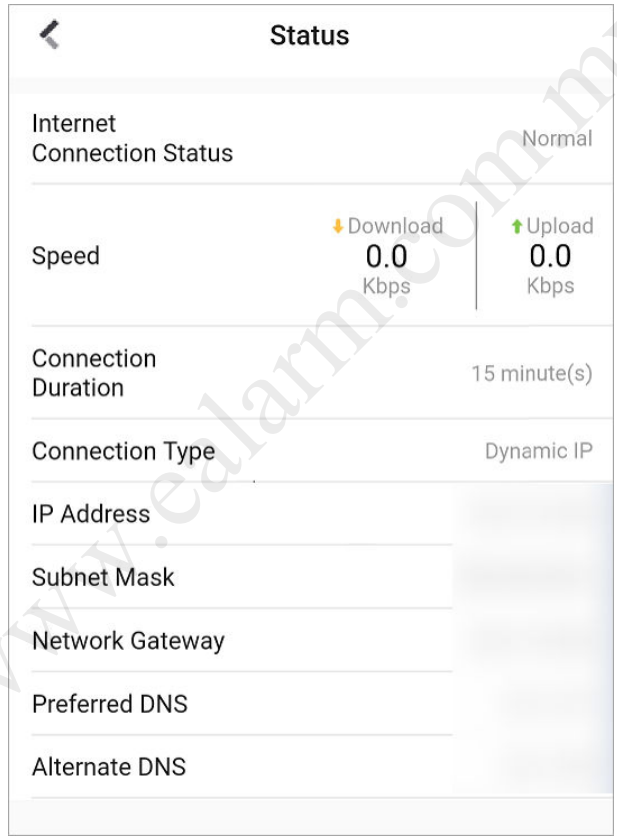

Figure 14-3 Status

Adjust the Wi-Fi Signal Strength

Tap **Wi-Fi Signal Strength** to select a signal strength mode: Power Saving, Standard, and High.

Set a Power-Off Schedule

Tap **Power-Off Schedule** on the settings page of your router to set a schedule to turn off the router during specific time periods in different days of a week.

Change the Admin Password

Tap **Change Admin Password** on the settings page of your router to set a new Admin password.

Restart the Router

Tap **Restart** on the settings page of your router to restart it.

Factory Reset the Router

Tap **Factory Reset** on the settings page of your router to reset the router to its factory state.

Note

A factory reset will erase all settings on the router. You have to add and activate the router again if you still want to manage the router on the Mobile Client.

14.1 Add and Set Up a Router

You can add a new router to the Mobile Client, so that you can set up your wireless network with just a few taps and manage the router right on your phone.

To add a Hikvision router, tap → **Manual Adding** .

Select **Router** as the **Adding Type** and then join the Wi-Fi of the router (whose name usually starts with "HIKVISION_").

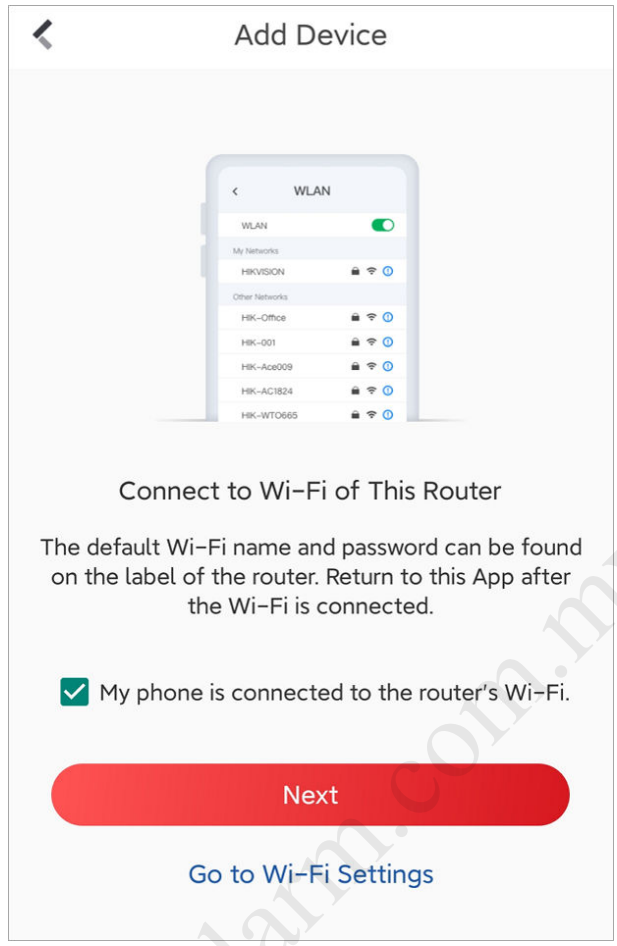

Figure 14-4 Add Device

During the process, you need to activate the router by setting an admin password, select the Internet connection mode (PPPoE, Static IP, or Dynamic IP), and set a Wi-Fi name and password.

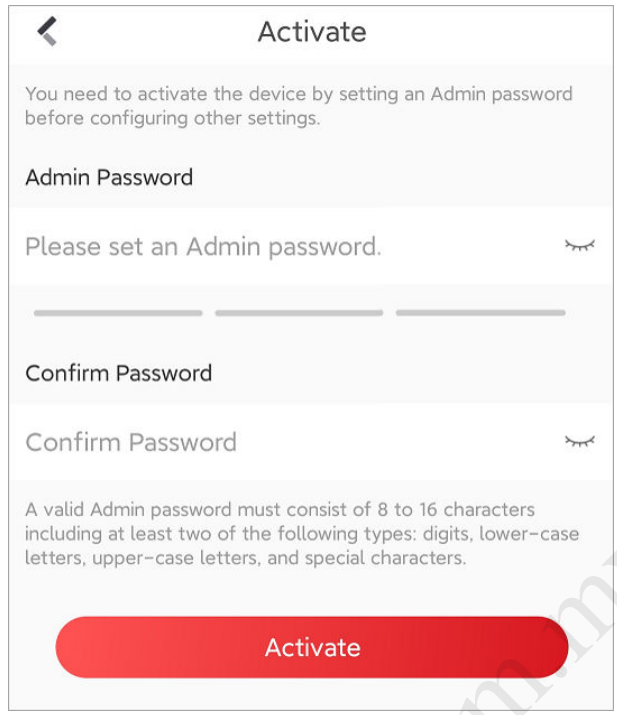

Figure 14-5 Activate Router

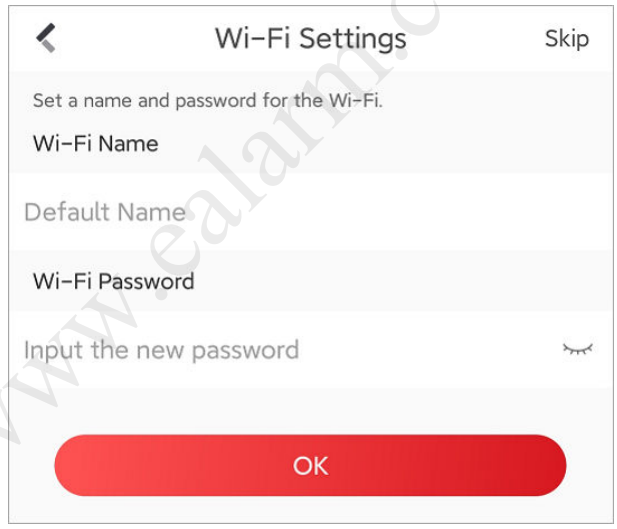

Figure 14-6 Set Wi-Fi Name and Password

Note

- Refer to ***Internet Settings of a Router*** if you need more information on Internet connection modes.
- After setting up the router, the router will restart. You need to re-connect to the Wi-Fi of the router before conducting further operations on the router.
- Routers are locally managed on the Mobile Client, so you can control or configure a router only when you connect your phone to the router's Wi-Fi.

14.2 Wi-Fi Settings of a Router

You can set the Wi-Fi name, security mode, password, and bands of a router in Wi-Fi settings. You can also hide the Wi-Fi from other people's Wi-Fi lists.

Where is the Wi-Fi Settings?

Tap **Wi-Fi Settings** on the settings page of the router.

Options in Wi-Fi Settings

Figure 14-7 Wi-Fi Settings

2.4 GHz Wi-Fi / 5 GHz Wi-Fi

Enable or disable different bands of Wi-Fi signal.

Some models are equipped with the 5 GHz band, which supports a higher maximum data rates. Tasks consuming a large amount of network traffic can benefit from the 5 GHz Wi-Fi network.

Wi-Fi Name

The Wi-Fi name will appear on the Wi-Fi list when you search for Wi-Fi connection.

The Wi-Fi name should contain 1 to 32 characters.

Security Mode

You can select None, WPA, WPA2, or WPA/WPA2 Mixed.

Caution

If you select **None**, your Wi-Fi network will be unprotected and open to anyone, which may cause security risks.

Password

Others must enter the password before connecting to the Wi-Fi.

The Wi-Fi password should contain 8 to 63 characters, excluding emoji or special characters.

Hide Wi-Fi

If you do not want your Wi-Fi network to appear on other people's Wi-Fi lists, you can hide the Wi-Fi.

14.3 Internet Settings of a Router

You can set the Internet connection type to PPPoE, dynamic IP, or static IP in Internet Settings.

Where is the Internet Settings?

Tap **Internet Settings** on the settings page of your router.

What Internet connection type should I select?

You need to select the type according to the current Internet service provided by your Internet Service Provider (ISP).

PPPoE

If your Internet service comes with an account name and password, select PPPoE.

ISP uses a PPPoE account to track the data traffic and bill each user. It is widely used in communities.

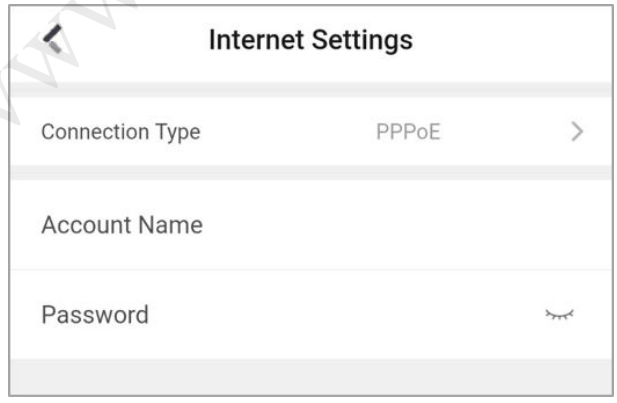

Figure 14-8 PPPoE

Dynamic IP

Also known as "DHCP". If your Internet service does not require any manual configurations to be connected, select Dynamic IP.

In this case, the ISP assigns a temporary IP address to you every time you try to connect to the Internet.

It is widely used in public spaces such as offices and hotels.

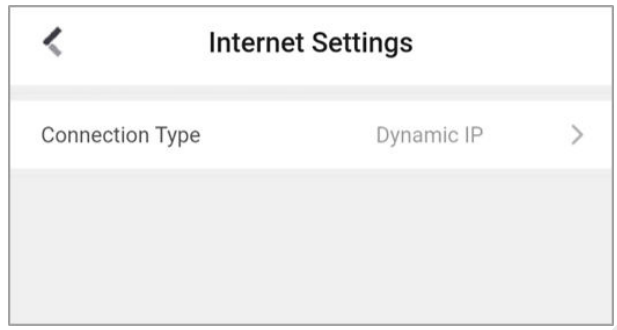

Figure 14-9 Dynamic IP

Static IP

If your ISP allocates a dedicated IP address to you, select **Static IP**.

Figure 14-10 Static IP

14.4 Manage the Devices Connected to a Router

You can check which devices are connected to your router, and view the connection details of a particular device. You can limit the speed of the connected devices and add unwanted devices to the blocklist.

Where can I see the connected devices?

In the **My Device** list, tap on the router to see all devices connected to it via the Wi-Fi or a network cable.

Figure 14-11 Connection Details

Check Device Connection Details

Tap on a connected device to see its connection details.

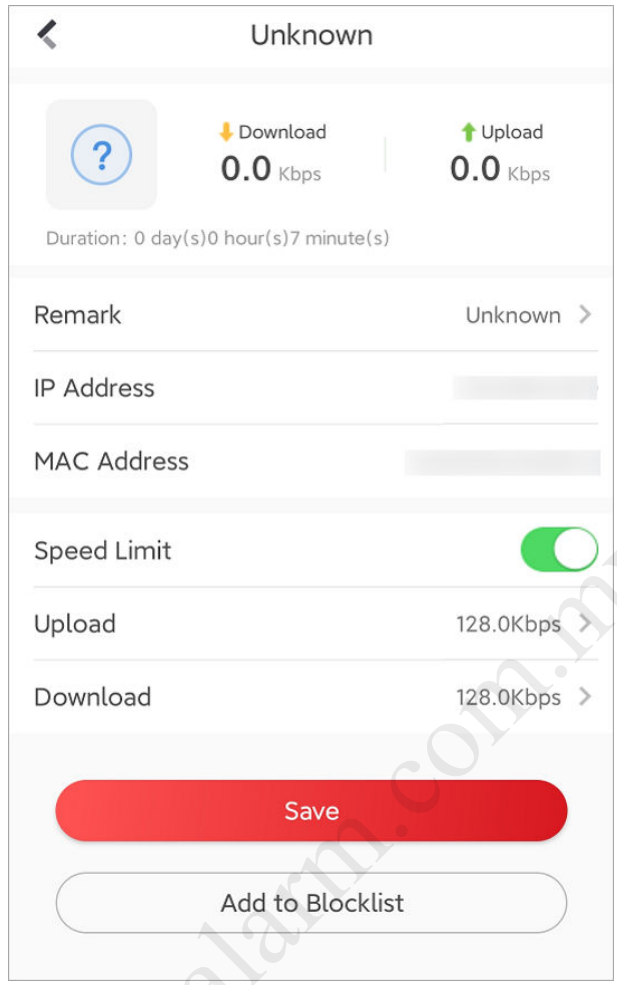

Figure 14-12 Device Connection Details

Limit a Device's Connection Speed

You can switch on **Speed Limit** and set a limit for the download/upload speed of the device.

Add Device to the Blocklist

Tap **Add to Blocklist** so that the device cannot be connected to the Wi-Fi again.
Tap **Remove from Blocklist** if you choose to allow the device to be connected to the router. You can also tap **Blocklist** on the settings page of the router to see all blocked devices.

14.5 Set Up a Guest Wi-Fi for Visitors

You can set up a guest Wi-Fi to securely separate visitors' Wi-Fi connection from yours.

Where can I set up the guest Wi-Fi?

To enable the guest Wi-Fi, go to the settings page of your router and tap **Guest Wi-Fi**.

Set Up the Guest Wi-Fi

In Guest Wi-Fi, you can set the name, password, validity period, and bandwidth limit of the guest Wi-Fi.

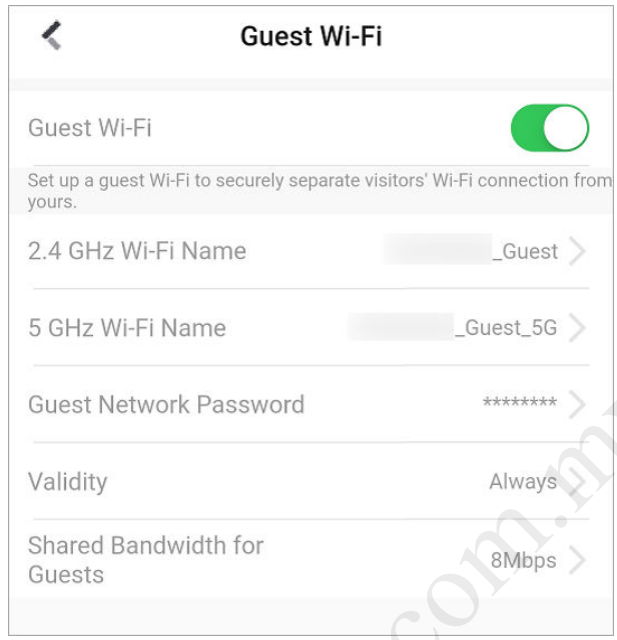

Figure 14-13 Guest Wi-Fi

14.6 Wi-Fi Speedup

If the Wi-Fi connection is slowing down and becoming unstable, you can use Wi-Fi Speedup to improve the network quality.

Where is Wi-Fi Speedup?

To use Wi-Fi Speedup, go to the settings page of your router and tap **Wi-Fi Speedup**.

How does Wi-Fi Speedup work?

Wi-Fi Speedup analyzes the signal interference, channel congestion, transmission speed, and signal quality of your Wi-Fi network.
When the network condition is poor, you can optimize your Wi-Fi network with just one tap.

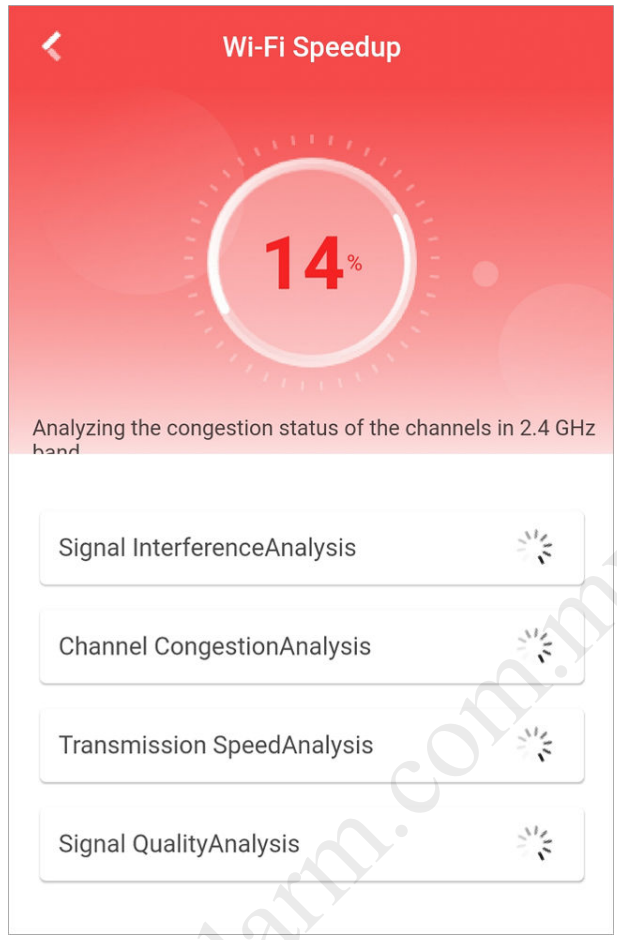

Figure 14-14 Wi-Fi Speedup

14.7 Security Checkup

Security Checkup examines the overall security level of your router and wireless network, and provides recommendations to guide you secure your network.

Where is Security Checkup?

To use Security Checkup, go to the settings page of your router and tap **Security Checkup**.

How does Security Checkup work?

Security Checkup examines your password settings to prevent brute-force attacks on the Wi-Fi password and admin password. Security Checkup also prevents system attacks, DNS hijacking, and redirection to phishing or malicious websites.

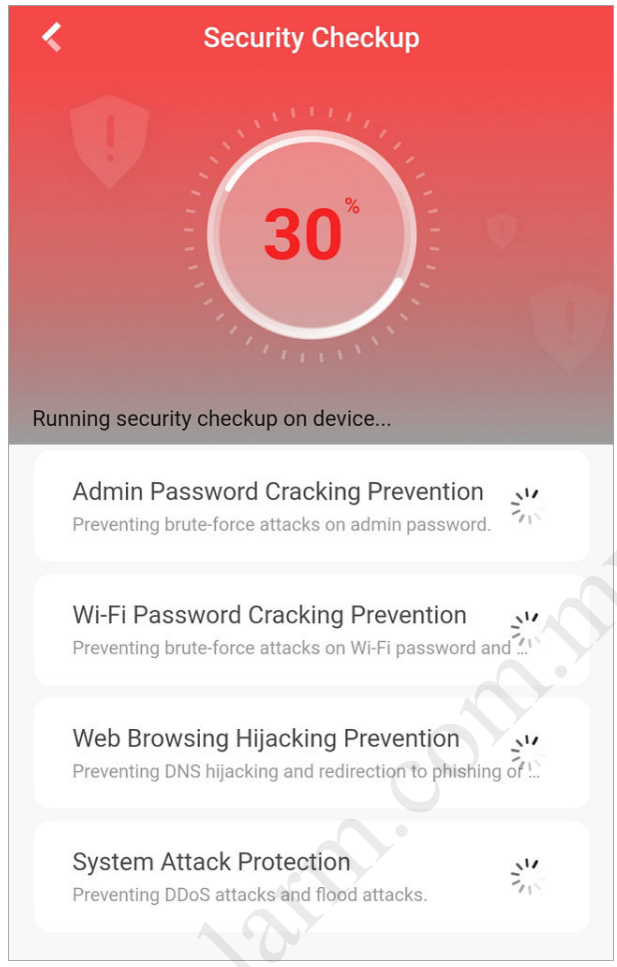

Figure 14-15 Security Checkup

If security threats are detected, Security Checkup will provide recommendations to guide you secure your network.

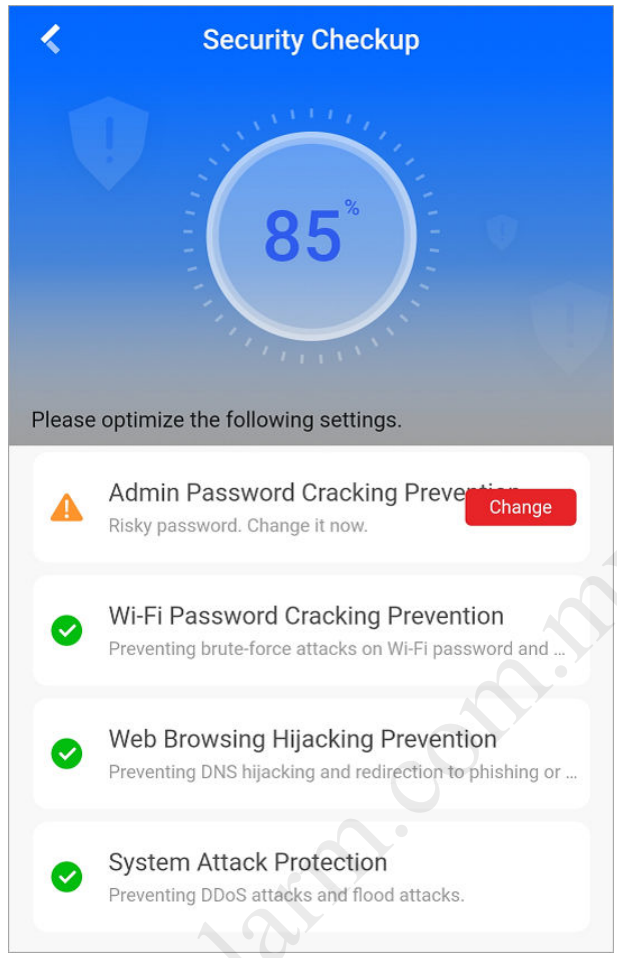

Figure 14-16 Result

Chapter 15 Network Switch

Network switch helps to expand device connectivity, improve data distribution efficiency, and reduce network bandwidth stress, thus streamlining the deployment and maintenance of larger-scale video security network. You can view the status of network switches in the Mobile Client.

Note

- Network switches need to be added on Hik-ProConnect by Installer and then handed over to you. You cannot add network switches by yourself via Hik-Connect.
- Refer to ***Cloud Service*** for details about what services an Installer can provide for you.

After your Installer hands over network switches to you, you can view them in the device list on the home page.

You can tap on a network switch to check its status.

When port connection changes or an exception occurs/restores, you will be notified. You can check the details on Notification tab.

Table 15-1 Supported Status and Operations of Network Switch

Status	Operation
• Device Uptime • Port Status • CPU Usage • Memory Usage • PoE Power	• Edit device name. • Check device firmware version. • Configure DDNS. • Change remote configuration. • Delete device.

Chapter 16 Notification

On the Notification tab, you can view event notifications, call logs of video intercom devices, and alarm information related to security control panels.

16.1 Enable Event 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 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

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

Steps

Note

- Make sure your phone supports Google Play service, or notifications may fail to be pushed to you.
- The Mobile Client will ignore alarm events triggered out of the time period defined by the notification schedule.
- The security control panel does not support setting notification schedule.
- For specific thermal device, you can also set custom voice prompt for the detected events, such as fire detection.

1. On the device list page, tap to enter the Settings page of the device.
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 Schedule** to enter the Schedule Settings page.

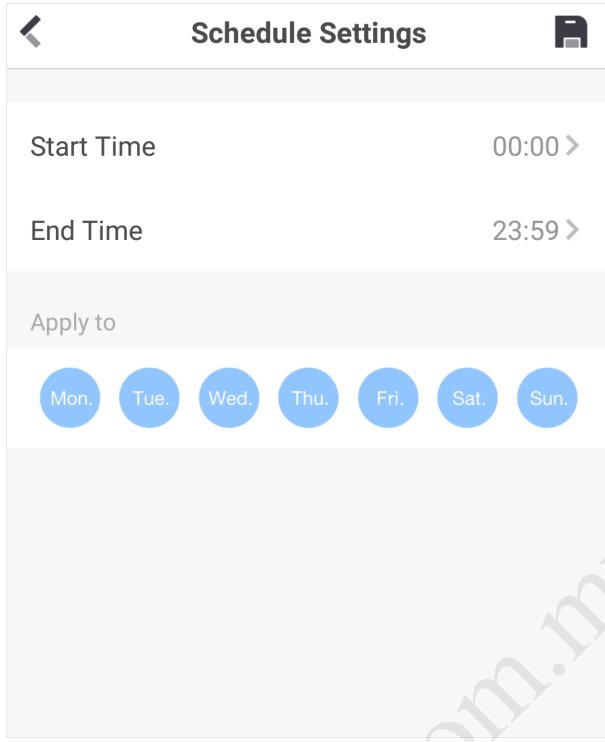

Figure 16-1 Schedule Settings Page

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

Note

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.

Note

The function should be supported by the device.

Intensive

Intense warning for the intrusion.

Soft

Soft warning for the intrusion.

Mute

No audible warning.

16.2 Check Event Notification

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

Before You Start

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

Steps

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

View and Download Event-related Picture	If there are multiple event-related pictures, you can swipe left/right to switch pictures. You can also tap a picture and then tap to download the picture.
Zoom In/Out Event-related Picture	Tap the picture, and then spread two fingers apart to zoom in the picture and pinch them together to zoom out, or double-tap the picture to zoom in or zoom out.
	Note • Make sure you have configured the event linkage action for capturing event-related picture for the device. See the user manual of the device for details. • If you have enabled Video and Image Encryption for the device, you need to enter the device verification code before you can view the picture. For details about Video and Image Encryption, see ***Set Video and Image Encryption*** for details.
View Event-related Video Footage	Tap **Playback** to view the video footage.
	Note Make sure you have configured the event linkage action for recording video for the device. See the user manual of the device for details.
View Live Video	Tap **Live View** to view the live video of the device.

Note

The device should support this function.

View External Linked Video

Tap **External Linked Video** to view the video footage recorded by the device's externally linked device.

For example, if a camera is linked to a detector, once the detector detects an event, the camera will record video footage.

Note

- Such a linkage (the configuration is called as "Configuring Linkage Rule) can be set by an Installer on Hik-ProConnect. For details, see the *Hik-ProConnect Portal User Manual*.
- 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 ••• , and then tap **Mark as All Read** to mark all event information as "already read".

Clear All Events

Tap ••• , and then tap **Clear All**.

Delete a Specific Event

Tap and hold an event notification until a prompt pops up, and then tap **Delete** to the prompt to delete the notification.

Chapter 17 Other Functions

The Mobile Client provides other functions, including fingerprint authentication and management of the recorded videos and captured pictures.

17.1 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 → 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 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.

17.2 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.

Note

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

Tap **More** and then tap on your account to enter the Account Management page and then enable the function.

17.3 Share Hik-Connect

You can show the QR Code for downloading the Mobile Client to others.

Tap **More → Share Hik-Connect** to view the QR code. After that, you can let others scan the QR code to download the Mobile Client.

Chapter 18 System Settings

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

18.1 Enable Push Notification

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

Note

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

Tap **More → Settings** to enter the Settings page, and then enable the push notification.

18.2 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.

Note

- 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 → Settings** to enter the Settings page, and then enable the function.

18.3 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 → Settings** to enter the Settings page and then enable the function.

Note

The power consumption of the phone or tablet may increase.

18.4 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

Note

Only devices added by IP/domain support this function.

1. Tap **More → 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.

18.5 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 → Settings** to enter the Settings page, and then enable the function.

Note

- 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.

18.6 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 → Settings** to enter the Settings page, and then tap **Traffic Statistics**.

18.7 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

Note

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

1. Tap **More → 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.

   Note

   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.

18.8 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).

Note

- 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 → Settings** to enter the Settings page and then enable the function.

18.9 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 → Settings** to enter the Settings page, and then enable the function.

18.10 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 → Settings** to enter the Settings page and then enable the function.

Note

After enabling tablet mode, you should restart the Mobile Client to make the settings effective.

18.11 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 → Settings** and then enable the Mobile Client to display channel-zero.

18.12 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.

Note

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

18.13 Manage Custom Audio

You can record audio files for setting them as the custom audio prompts for the alarms sent from the channels linked to specific models of DVR.

Perform this task to record an audio file.

Steps

1. Tap **More → Settings → Custom Audio Management** .
2. Tap **Start Recording** to start recording, and then tap **Stop Recording**.

   The Complete Recording dialog pops up.
3. **Optional:** Create a name for the audio file.

   Note

   By default, the file name is the time (accurate to second) when recording stops.
4. Tap **Confirm**.
5. **Optional:** Perform further operations.

Rename Audio	Long press and then tap **Rename** to rename the audio file.
Delete Audio	Long press and then tap **Delete** to delete the audio file.

What to do next

Set custom audio prompt for the alarms sent from the channels linked to specific models of DVR. For details, see ***Set Custom Audio*** .

Chapter 19 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.

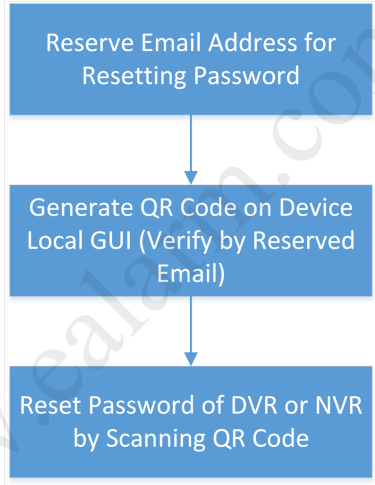

Figure 19-1 Flow Chart

- 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.

19.1 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.

19.2 Reserve Email Address for Resetting Password

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

Before You Start

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

Steps

Note

The DVR or NVR should support the function.

1. Go to **Configuration → User** on the local GUI of the device.
2. Select admin user and then click **Edit**.
3. Enter the password of the device in the Old Password field.
4. Click the Settings icon in Reserved E-mail Settings field.
5. Enter an email address for receiving verification code, and then click **OK**.

19.3 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

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

Steps

Note

The DVR or NVR should support this function.

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

   The QR code for resetting password pops up.

19.4 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

- Make sure you have allowed the Mobile Client to access your phone's camera.
- Make sure you 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 → Reset Device Password** to enter the Reset Device Password page.
2. Scan the QR code on the local GUI of the DVR or NVR.

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

   Note

   - The verification code will be valid for 48 hours.
   - If you reboot the device or change the reserved email address, the verification code would be invalid.
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.