Hik-ProConnect Mobile Client (for Europe)

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

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

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

Contents

Chapter 1 Introduction

Hik-ProConnect is a convergent, cloud-based security solution that helps manage services for your customers and expand your business by subscription offers. You can monitor the system health status of your customers' sites (even resolving problems) remotely, using a simple and reliable platform. Hik-ProConnect solution enables you to customize security solutions for customers with fully-converged Hikvision devices, covering video, intrusion, access, intercom, and more.

Hik-ProConnect provides different ways/clients for Installers or end users to access the platform or manage resources.

- **Hik-ProConnect Portal:** Portal for Installer Admin and Installers logging into Hik-ProConnect to manage the security business, including permission and employees management, site management, devices management, and devices health monitoring, etc.
- **Hik-ProConnect Mobile Client:** Mobile Client for Installer Admin and Installers logging into Hik-ProConnect to manage site, apply for site information management permission from end user, manage and configure the devices, etc.
- **Hik-Connect Mobile Client:** Mobile Client for end users to manage their devices, accept the Installer's invitation as the site owner, approve the Installer's application of site information management permission, etc.

1.1 Target Audience

This manual provides the Installer with the essential information and instructions about how to use Hik-ProConnect Mobile Client to manage the security business.

This manual describes how to add new or existing site for management, apply for site authentication permission from end user, manage and configure the devices, etc.

1.2 Running Environment

The following is the recommended system requirement for running the mobile client.

System Requirement

For iOS: iOS 10 or later versions (since iPhone 6 or iPad Air).
For Android: Android 5.0 or later versions.

Memory

For iOS: 1 GB or above.
For Android: 2 GB or above.

Chapter 2 Account Management

There are two types of accounts: Installer Admin and Installer. Each company has only one Installer Admin but can have multiple Installers.

Installer Admin

The Installer Admin has full access to the functions in the system. Usually, the Installer Admin can be the manager of the installation company.

Installer

Installers are "sub-accounts" to the Installer Admin and are controlled by permission for what they can do. For example, they can only manage the sites that are assigned to them. Usually, the Installers are the employees in the installation company.

The installation company should first register an Installer Admin account, and then invite the employees to register Installer accounts.

The flow chart of the whole process is shown as follows.

Note

The latter three steps in the flow chart (Set Role and Permission, Invite Employees, and Accept Invitation and Register Installer Accounts) are only supported on the Portal currently. For detailed instructions about these three steps, refer to *User Manual of Hik-ProConnect Portal*.

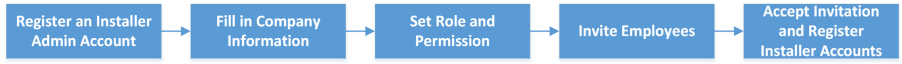

Figure 2-1 Flow Chart of Account Management

- **Register an Installer Admin Account:** The surveillance installation company should first register an Installer Admin account before accessing any functions of Hik-ProConnect. For details, refer to ***Register an Installer Admin Account*** .
- **Fill in Company Information:** After registering an Installer Admin account, you should bind your company information (including company name, country, logo, business license number, etc.) with this account for better service. For details, refer to ***Manage Company Information*** .
- **Set Role and Permission:** Before adding an employee to the system, you can create different roles with different permissions for accessing system resources.
- **Invite Employees:** You can invite employees to register Installer accounts and assign different roles to employees to grant the permissions to her/him.
- **Accept Invitation and Register Installer Accounts:** The employees can accept the invitation and register Installer accounts to manage sites and devices.

2.1 Register an Installer Admin Account

The surveillance installation company should first register an Installer Admin account before accessing any functions of Hik-ProConnect.

Steps

1. On the login page, tap **Register** to enter the registration page.

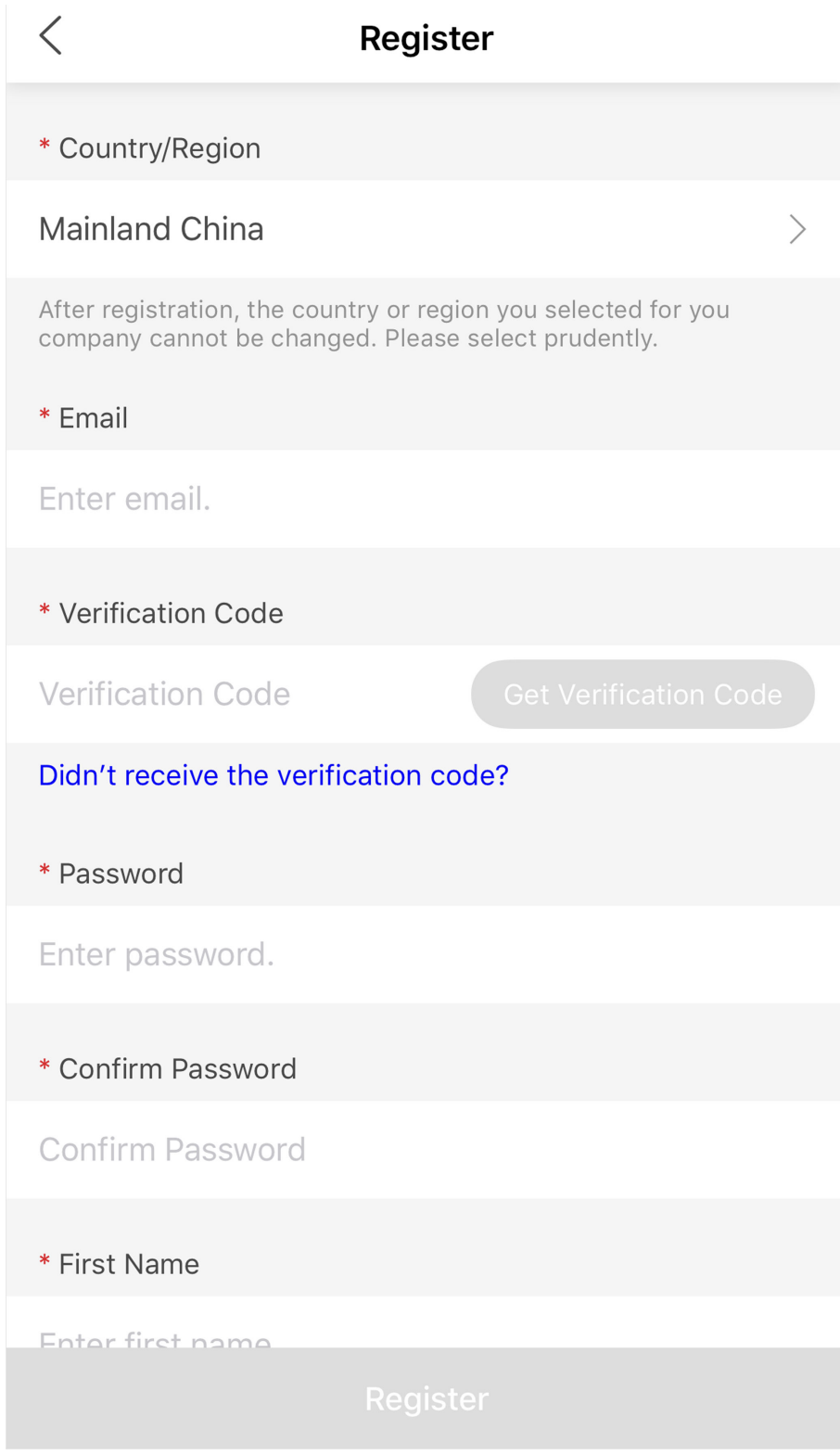

Figure 2-2 Register Page

2. Select the country/region of your company.

Note

After registration, the country or region you selected for your company cannot be changed.

3. Enter an email address which will be bound with the Installer Admin account.
4. Tap **Get Verification Code** to get the verification code.

Note

- If you don't enter the verification code within the required time, you can tap **Resend** to get the verification code again.
- If you fail to get the verification code, tap **Didn't receive the verification code?** for detailed reasons.

An email which contains the verification code will be sent to the email address you entered in the previous step.

5. Enter the verification code you have received.
6. Set the password of your account and confirm the 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. Enter your name and phone number.
8. Enter the company name.
9. **Optional:** Enter the authentication code which is used for authenticating that you are a professional Installer.

Note

- The authentication code should contain 10 digits. Follow the instruction on the interface to get the authentication code.
- If the authentication code is optional, you can leave it empty and authenticate your Installer Admin account later via the Hik-ProConnect Portal. For details about authenticating your account, refer to *User Manual of Hik-ProConnect Portal*.

10. **Optional:** Check **I would like to receive newsletters about new product introduction, service introduction, and questionnaires from Hikvision. I understand that at any time I can unsubscribe.** to subscribe. You can unsubscribe from it in the **Me → About** page.

- If subscription succeeded, you will receive a confirmation email in a few minutes. You can unsubscribe by clicking the URL in the email if needed.
- After subscription, we will send emails about latest product introduction, service introduction, questionnaires and special offers, to the email address which is used for your account registration.

11. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in these agreements.

12. Tap **Register**.

A registration confirmation email will be sent to the email address you entered in the above-mentioned step.

13. Tap **Verify Now** in the email you received.

After verification completed, you enter the login page of Hik-ProConnect.

Result

You can log into Hik-ProConnect with this account, and perform other operations such as site management, etc.

What to do next

After registering an Installer Admin account, you can log into Hik-ProConnect with your account. You need to fill in the information of your company to bind with your account. For details, refer to ***Manage Company Information*** .

2.2 Manage Company Information

After registering an Installer Admin account, you should bind your company information (including company name, phone number, email, etc.) with this account for better service.

After Installer Admin registration and login, you should complete company information according to actual situation. For details about registering an account and login, refer to ***Register an Installer Admin Account*** and ***Login*** .

Steps

1. Enter the name of your company.

2. Enter your phone number.

3. Enter an email address which will be bound with the Installer Admin account after registration.

4. Enter other information of your company, such as address, city, state/province/region, and postal code.

5. **Optional:** Enter the website of your company if any.

6. Tap **OK**.

After setting your company's information, you enter the Home page of the Hik-ProConnect Mobile Client.

Note

If you want to set VAT number, upload company's log, or edit your company information, log in to the Portal to edit. See the *User Manual Hik-ProConnect Portal* for details.

Chapter 3 Login

After logging in by an Installer Admin account, Installer account, or e-Partner account, you can manage sites and devices, and perform health monitoring, etc.

Before You Start

- Make sure you have registered an account. See *User Manual of Hik-ProConnect Portal* for details about registration.
- Make sure you have agreed the Terms of Service and Privacy Policy.

Steps

1. Tap to start the Mobile Client.

   The login page will show.
2. Select the country/region where your account locates and click **OK**.
3. Enter the registered email and password.
4. **Optional:** Reset the password if you have forgotten the password.
   1) Tap **Forgot Password** to enter the resetting password page.
   2) Tap **Get Verification Code**.

      You will receive a verification code sent by the portal in your email box.
   3) Enter the received verification code in the **Verification Code** field.
   4) Enter the new password and confirm 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.
   5) Tap **OK**.

      By default, you will be required to log in by the new password.
5. Tap **Login**.

Note

- For a newly registered user or a user who has registered an account before, if you have entered authentication code on the registration page, you should complete company authentication information when logging in to the Mobile Client, including occupation,

detailed company address (including street, state/province/region, and city), and company phone number.

- If you have registered an account before and did not enter the verification code on the register page, you should enter the company name to complete company authentication information when logging in to the Mobile Client.

Chapter 4 Hik-ProConnect Mobile Client Overview

Hik-ProConnect Mobile Client provides access to the Hik-ProConnect from your smart phone.

After logging into the Hik-ProConnect via Mobile Client, the Home page will show.

Main Modules

The Hik-ProConnect Mobile Client is divided into four main modules. You can access these modules via the navigation panel on the bottom.

Table 4-1 Main Modules of Hik-ProConnect Mobile Client

Module	Description
Home	On the Home page, you can view the overview of your sites, managed devices, received exceptions, and other quick entries such as key features, and tutorial center.
Site	In the Site module, the site list will show. A Site represents a physical location where devices are installed and through which the Installer Admin/ Installer can manage the devices.
Exception Center	After setting the exception rules, when an exception occurs on the device, the device will push a notification to the Mobile Client (if the **Received by** in the rule contains **Mobile Client**) and you can view all the notifications of exception received by the Mobile Client in the Exception Center.
Me	**View Account Information:** You can view the information of the current account, including name, email, profile, and phone number. **Note** You can edit the account information via the Hik-ProConnect Portal. For details, refer to *User Manual of Hik-ProConnect Portal*.
	Subscribe to Newsletters: For Installer Admin, if you didn't subscribe to newsletters when account registration, you can subscribe here. After subscription, we will send emails about latest product introduction, service introduction, questionnaires and special offers, to the email address which is used for your account registration. You can unsubscribe at any time in the **Me → About** page. After unsubscription, you will not receive any newsletter emails from us.
	Change Password: Change the password of the current account.

Module	Description
	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.
	About: You can view the version of the current platform, and read the agreements, including terms of service, privacy policy, and open source license. After subscribing to the newsletters, you can unsubscribe here at any time. After unsubscription, you will not receive any newsletter emails from us.
	Help: Open the user manual of the Hik-ProConnect Mobile Client. You can enter keywords to search the information you want in the user manual for help.
	Feedback: If you have any questions or suggestions about the system, you can submit feedback to us. 1. Select a type for your feedback and then enter your suggestions and questions in the pop-up window and attach a picture if necessary. 2. Enter an email address. After we receive your feedback, we will send an email to this address if we get an conclusion. 3. Click **Submit**.
	Logout: Log out of the current account and return to the login page.

Home Page Introduction

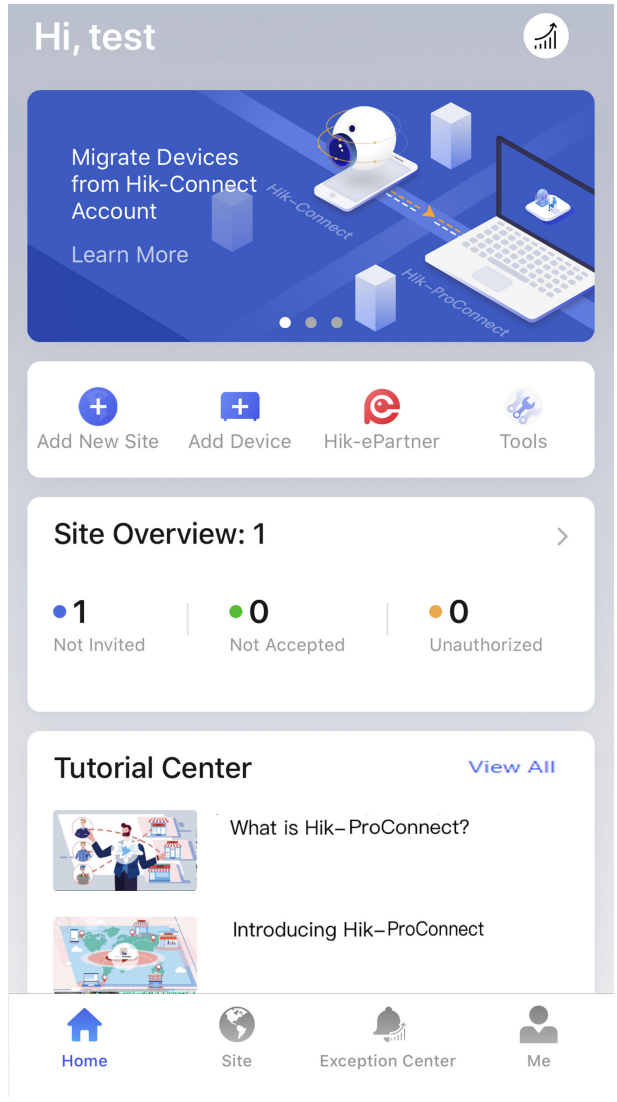

Figure 4-1 Home Page

Table 4-2 Home Page Description

Name	Introduction
Banner	There are some banners, showing the key features, functions, and important information of Hik-ProConnect.

Name	Introduction
	Note You can inform your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later) by sending the QR code or download link to them.

Shortcut	Shortcuts of the key features are provided on Hik-ProConnect Mobile Client.
	• **Add New Site:** Add a new site for managing the devices of end user. For detailed instructions, refer to ***Add New Site*** .
	• **Add Device:** Add devices to a site manually or add by scanning the QR codes on the devices. For detailed instructions, refer to ***Add Device*** .
	• **Linkage Rule:** Set a linkage rule which defines linked resource and linkage actions when the source detects the triggering event. For detailed instructions, refer to ***Add Linkage Rule*** .
	• **Hik-ePartner:** A mobile application specifically designed for Hikvision partners. Tap **Hik-ePartner** to open the App (if it has been downloaded) or download the App (If not downloaded). It is dedicated to provide a full range of services and support for Hikvision partners, including:
	  • Browsing and searching of Hikvision's product information, sales promotion, and scheduled events.
	  • Earning reward points and redeeming gifts.
	  • Installation Tools.
	  • Live-chatting with Hikvision support representatives.
	• **Tools:** Provides some online tools to improve your work efficiency.

Site Overview	You can view the number of sites managed in total. Besides, you can view: • **Not Invited:** The number of sites for which no site owners are invited. • **Not Accepted:** The number of sites of which the site owner invitation are not accepted. • **Unauthorized:** The number of sites which are not authorized to you. **Note** You can click > to enter the site list. For detailed instructions about site management, refer to ***Manage Site*** .
Exception Overview	You can view the number of received exceptions and the proportions of each type of the exceptions.

Name	Introduction
	Note You can click > to enter **Exception Center** to check the received exceptions. For detailed instructions about Exception Center, refer to ***Exception Center*** .
Tutorial Center	You can view video tutorials to learn more about Hik-ProConnect and the proper ways of using the product. Tap a video to open a webpage and start playing the video. Tap **View All** to view all the videos in Tutorial Center.

Chapter 5 Manage Site

A site can be regarded as an area or location with actual time zone and address, such as the end user's home, office, etc. The Installer can add the authorized devices of end user to the site and uses the site to manage and configure the devices remotely.

The Site Management function provides adding and deleting sites, inviting the end user as the site owner, applying for site authorization from site owner, etc.

5.1 Site Page Introduction

On the Site page, you can view the sites that are assigned to you (the Installer Admin as well as Installers with Manage All Sites permission can view all the sites of the company), and perform some operations for the sites, such as searching site, adding site, inviting site owner, etc.

There are different statuses for the sites in site list.

Not Invited

The site is newly added, and you have not invited the end user as the site owner, or the end user has not accepted the invitation.

Not Registered

The invitation has be sent to end user who has not registered a Hik-Connect account.

Not Accepted

The invitation has be sent but not be accepted by end user who has registered a Hik-Connect account.

Invited, Not Authorized (Shown as No Commission Authorization)

The end user accepts the invitation as the site owner, but the site is not authorized to the Installer.

Authorized and Monitoring (Shown as Email Address or Phone Number)

The Installer gets the authorization of the site from the end user.

Note

According to site status, the Installer Admin and Installers with site management permission can perform the following operations in the table below.

Table 5-1 Supported Operations in Different Statuses

Supported Operations	Not Invited	Not Accepted Not Registered	Invited, Not Authorized (Shown as No Commission Authorization	Authorized and Monitoring (Shown as Email Address or Phone Number)
Search Site	√	√	√	√
Invite Site Owner	√	√	×	×
Manage Device	√	√	×	√
Edit Site	√	√	×	√
Delete Site	√	√	×	×
Apply for Authorization	×	×	√	×

5.2 Add New Site

When the end user wants the installation company to provide installing service, the Installer Admin or Installer with related permissions needs to create a new site for managing these devices of end user.

Before You Start

Make sure you have the permission of adding new site.

Steps

1. Tap **Site** tab at the bottom to enter Site page.
2. Tap ⊕ to enter Add New Site page.

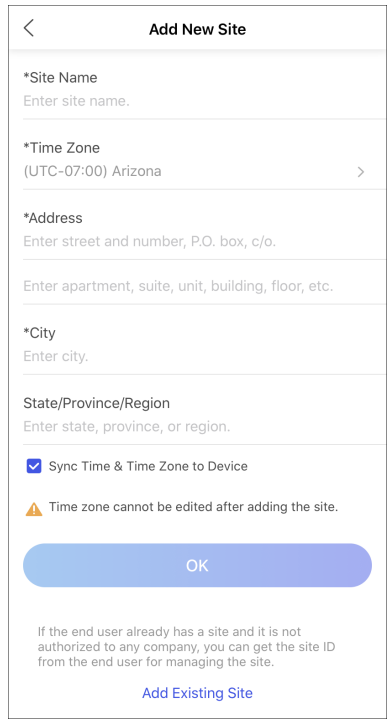

Figure 5-1 Add New Site

Note

- If an existing site of end user is not authorized to any installation companies, you can click **Add Existing Site** to add the existing site.
- If you have no permission of adding new site, when you click **Add New Site**, you will enter Add Existing Site page to add an existing site.

For more details, refer to ***Add Existing Site*** .

3. Set the site name, time zone, site address, city, and state/province/region.

Note

You should select the correct time zone where the devices locate and the time zone cannot be changed after the site is added.

4. **Optional:** Check **Sync Time & Time Zone to Device** to synchronize the time and time zone of the site to the devices added to the site.
5. Click **OK** to add a new site to the list.
6. **Optional:** According to the site's status and authorization, perform one of the following operations.

Note

For more details about supported operations in different site status, refer to ***Site Page Introduction*** .

Search Site	Enter keywords in search filed, and tap **Search** to display the search results in the list.
View Site Details	Tap the site to view the site details, including managed devices, site information, and so on.
Edit Site	Tap ··· in top right corner on Site Details page, and then tap **Manage Site Information** to edit site information. You can edit the site name, site address, city, and state/province/region. If you are authorized to manage the site, you can also edit whether enable **Sync Time & Time Zone to Device** or not.
Delete Site	Tap ··· in top right corner on Site Details page, and tap **Delete Site** to delete the site.
Invite Site Owner	For the site in the status of **Not Invited**, tap **Invite Now** on Site Details page to invite an end user as the owner of the site. **Note** For more details, refer to ***Invite Site Owner*** .
Manage Device	For the authorized site or the site with the status of **Not Invited**, **Not Registered**, or **Not Accepted**, enter Site Details page to manage the devices, such as adding device to the site, upgrading device, applying for live view or configuration permission, adding linkage rule,and adding exception rule, etc. **Note** For more details, refer to ***Manage Device*** .

5.3 Add Existing Site

When a site is either not assigned to a company or that was previously assigned to a company but was later released and is now not associated with a company, you can add it by applying for site authorization from the site owner.

Steps

1. Tap **Site** tab at the bottom to enter Site page.
2. Tap **Add New Site → Add Existing Site** .

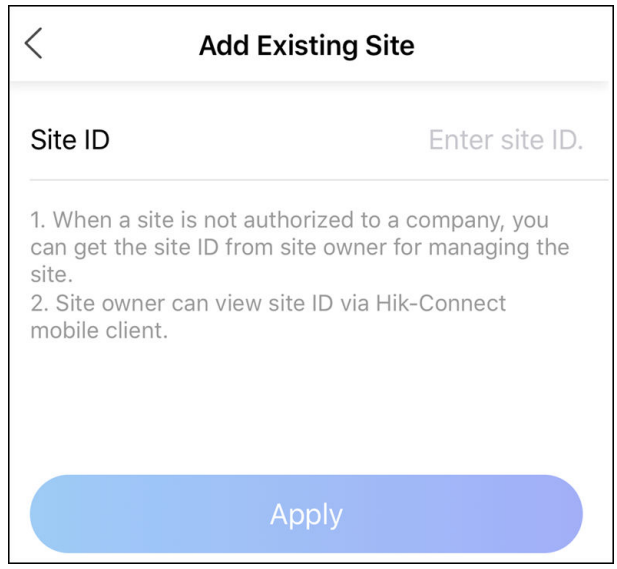

Figure 5-2 Add Existing Site

3. Enter the site ID.

Note

- You can get the site ID form the site owner, who can view the site ID via Hik-Connect Mobile Client.
- Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

4. Click **Apply**.

   The site will be added in the site list and the site owner will receive an application. After the site owner approves the application, the site will be authorized by the Installer.

5.4 Invite Site Owner

After installation company completed the installation, the Installer needs to invite Site Owner in order to hand over the site to end user. If required, the Installer can also apply for specified permissions for further device maintenance when inviting Site Owner.

Before You Start

Make sure the site status is **Not Invited** and you have the permission of site management, such as Manage All Sites and Manage Assigned Site.

Steps

1. In site list, tap a site to enter Site Details page.
2. Tap **Invite Now** to enter Invite Site Owner page.

3. **Optional:** Check **Allow Me to Disable Hik-Connect Service**. Then after handing over the site to end user, you can disable Hik-Connect service for the devices and the end user cannot perform device operations via Hik-Connect Mobile Client.

Note

When this function is enabled and the site is handed over, if required, you can enter Site Details page and tap **Device** tab to disable Hik-Connect service for one device or all devices in this site by tapping or setting **Hik-Connect Service** switch to off. You can also delete the devices from the end user's Hik-Connect account without authorization of end user.

4. Select **Email** or **Phone Number** as invitation mode.
5. Enter Site Owner's email address or phone number.
6. **Optional:** Select authorization permissions of the Installer after the site is handed over to the Site Owner.

Note

- You can tap > to set validity period for the permissions of configuration and live view and select the device(s).
- If you have no permission for managing device, or no devices are added in the site, you cannot select the permissions of configuration and live view when inviting Site Owner.
- If the following permissions are selected, when the end user accepts the invitation, the permission will be authorized to the Installer. The Installer does not need to apply for authorization from Site Owner again.

Site Information Management

The authorization for the permission of managing site information.

Configuration

The authorization for the configuration permissions of the selected devices in the site.

Live View

The authorization for the live view permissions of the selected devices in the site.

Playback

The authorization for the playback permissions of the selected devices in the site.

7. Enter the remarks, such as the reason of the invitation, which the invitee can view when he/she receives the invitation via Hik-Connect Mobile Client.
8. Tap **Invite** to send the invitation.
   - The invitee will receive an invitation email or message in email box or via short message with a download link of Hik-Connect Mobile Client. The invitee can download or open Hik-Connect Mobile Client via the link.
   - If the invitee has not registered a Hik-Connect account, he/she needs to register a Hik-Connect account first. After registering the account and accepting the invitation via Hik-Connect Mobile Client, the end user will become the Site Owner.

Note

Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page to them.

- If there are maintenance requirements for the devices added in Hik-Connect Mobile Client, but not added and managed in the site, after the end user accepts the invitation and becomes the Site Owner, he/she can authorize the permissions about these devices to the Installer.

9. **Optional:** Before the end user accepts the invitation, tap **Not Registered** or **Not Accepted** to send invitation again.

Note

You can send at most five invitations in one day and the previous invitations will be invalid if you send a new invitation again.

5.5 Apply for Site Authorization from Site Owner

When the site (no permissions selected when inviting Site Owner) has been handed over to Site Owner, and then there are maintenance requirements for the devices in the site, the Installer needs to send an application to Site Owner for the authorization. After the authorization is approved, the Installer can get the permission to manage and configure the devices of the site. Besides this, the Site Owner can add a device on Hik-Connect Mobile Client and authorize it to the Installer for further management and configuration.

Steps

1. Choose one of the followings to apply for authorization.
   - Tab the blue prompt about no authorization in site list.
   - Tap site to enter Site Details page. Tap ··· in top right corner, and tap **Apply for Authorization**.
2. Tap **OK** to confirm the operation.

   The Site Owner will receive and handle the application via Hik-Connect Mobile Client. After the Site Owner approves the application, the Installer will have the authorization of the site and perform some operations.

   If there are maintenance requirements for the devices added in Hik-Connect Mobile Client, but not added and managed in the site by the Installer yet, after consensus, the Site Owner can select the devices and authorize the permissions of the devices to the Installer.

Note

- Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.5.0 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.
- For AX Pro, after adding an AX Pro to Hik-ProConnect, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; these accounts will be deleted after the Installer deletes the AX Pro from Hik-ProConnect. If you edit an Installer's login password, the password for logging in to the AX Pro by this account will also change.
- After authorizing a site with AX Pro to an Installer, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; besides, the account with the permission of managing all sites will also become the account of the AX Pro.
- If an Installer hands over the site with this AX Pro to an end user, the end user's Hik-Connect account will also become an account of the AX Pro, while the Installer's account will be deleted from the AX Pro. This is also applicable to an Installer Admin.
- For more details about operations on Hik-Connect Mobile Client, refer to the User Manual of Hik-Connect Mobile Client.

Chapter 6 Manage Device

Hik-ProConnect supports multiple device types, including encoding device, security control panel, video intercom device, access control device, NVR/DVR, and doorbell. After adding them to the system, you can manage them and configure required settings, including remotely configuring device parameters, configuring exception rule and linkage rule, etc. After adding people counting cameras and temperature screening devices, you can also activate these services and set related parameters on Portal (some functions may not be available in specific countries and regions).

6.1 Add Device

Three ways for adding devices to site are provided. 1. Add devices by scanning the QR codes. By scanning the QR code on a device, you can add a single device to a site; by scanning the QR code generated by iVMS-4500 or iVMS-4200, you can add multiple devices to a site in a batch. 2. Add devices by Hik-Connect (P2P). 3. Add a device by IP or domain name.

6.1.1 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.

Steps

1. Add a device to the Mobile Client.
2. Tap **Connect to Network** on the pop-up prompt.
3. Select the device type and then follow the instructions on the interface to perform related operations.

Note

- Make sure that the device is powered on.
- For connecting wireless security control panel to network, if your phone OS is of Android, allow the Mobile Client to access your location, or the Wi-Fi which your phone connects to will NOT be obtained by the Mobile Client.

6.1.2 Add Device by Scanning QR Code

You can add a device to a site by scanning the QR code on the device, or add multiple devices to a site by scanning the QR code generated by iVMS-4200 or iVMS-4500.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.

Steps

1. Tap a site on the site list to enter the site details page.
2. Tap **Add Device** to enter the Add Device page.
3. Scan QR code to add device(s) to site.
   - Scan a QR code on a device. You can scan the QR code by aligning the QR code with the scanning frame; If there is a device QR code in phone album, tap **Album** to extract QR code from local album. By this mode, you can add only one device to site at a time.

     Note

     - Usually, the QR code is printed on the label, which is on the back cover of the device.
     - Tap to enable the flashlight if the scanning environment is too dark.
     - Please allow the Mobile Client to access the photo album of the phone.

   - Scan a QR code generated by iVMS-4200 or iVMS-4500. After scanning the QR code, you will enter the page for selecting to-be-added devices. Check devices and tap **OK** to add the selected devices to site. By this mode, you can add multiple devices to site at a time.
4. **Optional:** Perform the following operations if the following situations occur.
   - If the QR code only contains the information of device serial No., you will enter the manually adding page. Add the device manually in this case. See ***Add Device by Hik-Connect (P2P)*** 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, tap **Activate** on the pop-up window, and then create a device admin password and tap **Activate** to activate the device.

     Note

     During activation, Dynamic Host Configuration Protocol (DHCP) will be automatically enabled for allocating IP addresses for the device.

   - If the Hik-Connect service is disabled for the device, tap **Enable** on the pop-up window, and then create a device verification code and tap **Enable** to enable the service.

     Note

     Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

   The device will appear on the device list.

Note

- By default, Health Monitoring Service is enabled for the added devices. For devices with health monitoring service disabled, you cannot upgrade device firmware, set linkage rules

(the existing linkage rules will be invalid), set and receive exceptions, and check device health status.

- After adding the device, the Hik-ProConnect starts detecting whether the device firmware version is compatible. Some functions (including health monitoring, linkage rule, and remote configuration) are unavailable if the device is not compatible with the Hik-ProConnect.
- For AX Pro, after adding an AX Pro to Hik-ProConnect, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; these accounts will be deleted after the Installer deletes the AX Pro from Hik-ProConnect. If you edit an Installer's login password, the password for logging in to the AX Pro by this account will also change.
- After authorizing a site with AX Pro to an Installer, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; besides, the account with the permission of managing all sites will also become the account of the AX Pro.
- If an Installer hands over the site with this AX Pro to an end user, the end user's Hik-Connect account will also become an account of the AX Pro, while the Installer's account will be deleted from the AX Pro. This is also applicable to an Installer Admin.

5. **Optional:** Perform the following operations after adding the device if required.

Remote Configuration	Tap the device and then tap ⚙ to remotely configure its parameters. **Note** • For details, see the user manual of the device. • Only encoding devices, doorbells, and security control panels support remote configuration.
Delete Device	On the device page, tap • • • → **Delete Device** to delete the device.
Generate Device QR Code	• If a device is added by scanning the QR code generated by iVMS-4200/ iVMS-4500, you can generate a QR code of the device. If an end user did not add the device to his/her Hik-Connect account, he/she can add it to the Hik-Connect account by scanning this QR code using Hik-Connect Mobile Client. • a. On the top right of a device page, tap • • • → **Generate QR Code** to open the Generate QR Code window. b. (Optional) Enter the password to encrypt the QR code, and then tap **Next**. c. Tap **Save** to save the generated QR code in your phone.
Set Type for Unknown Device	If the Hik-ProConnect cannot recognize a device's type after you add it, you can manually set a device type for it. a. Enter a device details page, tap ✎ of the Device Type to enter the Device Type page. b. Select a type for the device. You can edit it again after the selection.

Edit Device Information	For devices added by scanning QR code generated by iVMS-4200/ iVMS-4500, if the device's information changed, or a network exception occurs, you can edit its information accordingly. Enter a device page, and tap **IP/Domain** to edit the device's name, IP address, port number, user name, or password, and then tap **Save**.

Note

- It is highly recommended to encrypt the device QR code for security reasons.
- Deleting device is not supported if the site is authorized (except for devices added by IP/ Domain).

6.1.3 Add Device by Hik-Connect (P2P)

If a device is connected to Hik-Connect Service, you can manually add it to a site by entering the device serial number and device verification code.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.

Steps

1. Tap a site on the site list to enter the site details page.
2. Tap **Add Device** to enter the scan page, and then tap **Manually Add** to enter the manual adding page.
3. Enter the device serial number and device verification code.

   Note

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

4. Tap **Add**.

   Note

   - By default, Health Monitoring Service is enabled for the added devices. For devices with health monitoring service disabled, you cannot upgrade device firmware, set linkage rules (the existing linkage rules will be invalid), set and receive exceptions, and check device health status.
   - After adding the device, the Hik-ProConnect starts detecting whether the device firmware version is compatible. Some functions (including health monitoring, linkage rule, and remote configuration) are unavailable if the device is not compatible with the Hik-ProConnect. For devices incompatible with the Hik-ProConnect, you need to upgrade them. Tap **Add and**

Upgrade to upgrade and add the device. For some devices, you need to enter the device user name and password. You can also upgrade the device on the device page.

- For AX Pro, after adding an AX Pro to Hik-ProConnect, the Installer/Installer Admin account will become the account of the AX Pro; the accounts will be deleted after the Installer/ Installer Admin deletes the AX Pro from Hik-ProConnect. If you edit an Installer's login password, the password for logging in to the AX Pro by this account will also change.
- If an Installer/Installer Admin hands over the site with this AX Pro to an end user, the end user's Hik-Connect account will also become an account of the AX Pro, while the Installer Admin's/Installer's account will be deleted from the AX Pro.

5. **Optional:** Perform the following operations if the following situations occur.
   - 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, tap **Activate** on the pop-up window, and then create a device admin password and tap **Activate** to activate the device.

     Note

     During activation, Dynamic Host Configuration Protocol (DHCP) will be automatically enabled for allocating IP addresses for the device.
   - If the Hik-Connect service is disabled for the device, tap **Enable** on the pop-up window, and then create a device verification code and tap **Enable** to enable the service.

   The device will appear on the device list.
6. **Optional:** Perform the following operations if you need.

Operations	Description
Delete Device	On the device page, tap • • • → **Delete** to delete the device.
Set Type for Unknown Device	If the Hik-ProConnect cannot recognize a device's type after you add it, you can manually set a device type for it. a. Enter a device details page, tap ✎ of the Device Type to enter the Device Type page. b. Select a type for the device. You can edit it again after the selection.
Configure DDNS	After adding the device, the DDNS status will be displayed in the device area. If the DDNS needs to be configured, tap **Configure**. See ***Configure DDNS for Devices*** for details about configuring DDNS.

Note

- Deleting device is not supported if the site is authorized (except for devices added by IP/Domain).
- For devices with invalid or old firmware version, you can configure DDNS for them to make sure they can be managed by Hik-ProConnect properly.
- Only encoding devices added by Hik-Connect Service support configuring DDNS.

6.1.4 Add Device by IP Address or Domain Name

If you know the IP address or domain name of a device, you can add it to the Hik-ProConnect by specifying its IP address/domain name, user name, password, etc.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.

Steps

Note

Only encoding devices mapped in WAN support this function.

1. Tap a site on the site list to enter the site details page.
2. Tap **Add Device → Manually Add** to enter the Add Device page.
3. Select **IP/Domain** as the register mode.
4. Enter the device name, device's IP address, port number, user name, and password.
5. Tap **Add**.

   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.

   Note

   By default, Health Monitoring Service is enabled for the added devices. For devices with health monitoring service disabled, you cannot upgrade device firmware, set linkage rules (the existing linkage rules will be invalid), set and receive exceptions, and check device health status.

6. **Optional:** Perform the following operations if you need.

Operations	Description
Edit Device Information	For devices added by IP/Domain, if the device's information changed, or a network exception occurs, you can edit its information accordingly. Enter a device page, and tap **IP/Domain** to edit the device's name, IP address, port number, user name, or password, and then tap **Save**.
Generate Device QR Code	• You can generate a QR code of the added device. If an end user did not add the device to his/her Hik-Connect account, he/she can add it to the Hik-Connect account by scanning this QR code using Hik-Connect Mobile Client. • a. On the top right of a device page, tap • • • → **Generate QR Code** to open the Generate QR Code window. b. (Optional) Enter the password to encrypt the QR code, and then tap **Next**. c. Tap **Save** to save the generated QR code in your phone.
Set Type for Unknown Device	If the Hik-ProConnect cannot recognize a device's type after you add it, you can manually set a device type for it. a. Enter a device details page, tap ✎ of the Device Type to enter the Device Type page. b. Select a type for the device. You can edit it again after the selection.
Delete Device	On the device page, tap • • • → **Delete Device** .

Note

- It is highly recommended to encrypt the device QR code for security reasons.
- For AX Pro, after adding an AX Pro to Hik-ProConnect, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; these accounts will be deleted after the Installer deletes the AX Pro from Hik-ProConnect. If you edit an Installer's login password, the password for logging in to the AX Pro by this account will also change.
- After authorizing a site with AX Pro to an Installer, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; besides, the account with the permission of managing all sites will also become the account of the AX Pro.
- If an Installer hands over the site with this AX Pro to an end user, the end user's Hik-Connect account will also become an account of the AX Pro, while the Installer's account will be deleted from the AX Pro. This is also applicable to an Installer Admin.
- Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.
- Deleting device is not supported if the site is authorized (except for devices added by IP/Domain).

6.2 Apply for Device Permission

After handing over a site to the end user, if you need to view the live view/recorded videos of devices added to the site or configure the devices added to the site, you can apply for the permission accordingly from the end user.

Steps

1. Tap a site to enter the site details page.
2. Tap a device to enter the device details page.
3. In the Device Permission area, select **Configuration** or **Live View** or **Playback** and tap to enter the Apply for Permission page.
4. Select a validity period for the permission.

   Note

   You can select **Permanent**, **1 Hour**, **2 Hours**, **4 Hours**, or **8 Hours** as the validity period.

5. **Optional:** Enter the remarks for the permission.
6. Click **Send** to send the application to end user.

   If the end user approves your application, you will be able to view the live video and (or) configure devices.

6.3 Release the Permission for Devices

If you do not need the permissions of configuration and live view for devices, or you finish the device configuration task earlier than the planned time, you can release the permissions manually.

Before You Start

Make sure the site of the devices has been authorized to you.

Steps

1. Tap a site in the site list to enter the site details page.
2. Tap a device on the site details page to enter the device details page.
3. In the Permission area, select a permission, and tap → **Release Permission** → **Release Permission** to release the permission.

   Note

   - After releasing, the permission will be unavailable for you. You need to apply for it again if needed.
   - You do not have to release permission if the permission validity is **Permanent**.

6.4 Add Linkage Rule

A linkage (see the picture below for reference) refers to the process in which an event detected by resource A triggers actions of resource B, resource C, resource D, etc. You can add a rule using the pre-defined template or customize a rule to define such a linkage. The rule contains five elements, including Source (resource A), Triggering Event (the event detected by device A), Linked Resources (resource B, resource C, resource D...), Linkage Actions (actions of resource B, resource C, resource D...), as well as Linkage Schedule (the scheduled time during which the linkage is activated). The linkages can be used for purposes such as notifying security personnel, upgrading security level, saving evidence, etc., when specific events happen.

The picture below shows the process of the linkage.

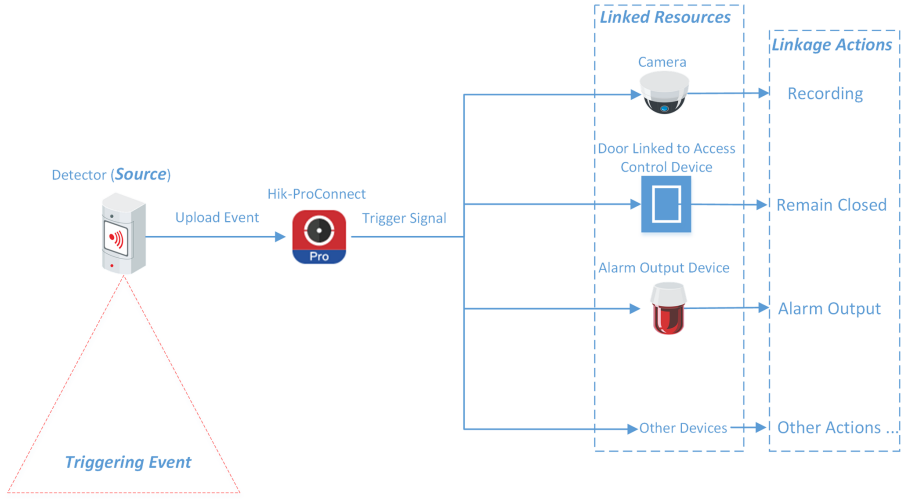

Figure 6-1 Linkage

Example

Sample Application

Assume that the end user is the manager of a jewelry store, and the store needs to upgrade security level during non-work hours. And the store has been installed with a PIR detector linked to a security control panel, a siren linked to the security control panel, and several network cameras. In this case, you can set a linkage rule for him/her to trigger alarm output and recording in the store when object(s) in motion are detected in the store during non-work hours. The followings should be defined in the linkage rule:

- Source: The PIR detector in the store.
- Triggering Event: Motion detection event.
- Linked Resources: The alarm output (the siren in this case) and the network cameras in the store.
- Linkage Actions:

- For siren: The triggering of the alarm output (i.e., the siren) sends out audible alarm.
- For network cameras: The network cameras starts recording.

- Linkage Schedule: Non-work hours every day.

6.4.1 Add Custom Linkage Rule

If the pre-defined templates cannot meet your needs, you can customize linkage rules as desired.

Steps

Note

- If the trial period of your company expires, the added linkage rule(s) will remain for 3 month but the linkage will not be activated. After 3 months, the linkage rule(s) will be cleared.
- Make sure you have the permission for the configuration of the devices. Or you should apply for the permission first. For details about applying for the permission, see ***Apply for Device Permission*** .
- The Source and the Linked Resource cannot be the same device.
- You cannot configure two totally same linkage rules. In other words, you cannot configure two rules with the same Source, Triggering Event, Linked Resource, and Linkage Action.
- When the Source is a device added by IP/domain, the device added by Hik-Connect cannot be set as the Linked Resource for triggering capture.

1. Tap a site in the site list to enter the site details page.
2. Tap **Linkage Rule** to enter the Linkage Rule page.
3. Tap **Add Linkage Rule** to enter the Add Linkage Rule page.
4. Select the Source and Triggering event, and then tap **Next**.

Note

Make sure that the selected triggering event has already been configured on the device. For details about configuring event on device, see the user manual of the device.

Table 6-1 Available Triggering Events for Different Resource Types

Source	Triggering Event
Camera	• Motion Detection • Face Detection • Intrusion • Line Crossing Detection
Access Control Device	• Network Disconnected • Tampering Alarm
Door Linked to Access Control Device	• Door Opened Abnormally • Tampering Alarm

Source	Triggering Event
Door Station	• Calling
Area of Security Control Panel	• Away Arming • Disarmed • Stay Arming • Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm.
Zone (Detector) Linked to Security Control Panel	• Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm.
Doorbell	• Calling • PIR Detection

5. Tap **Add Linkage** to select the Linkage Action(s) and Linked Resource(s), and then tap **Next**.

Note

- For configuring Linkage Actions for a same Source, if its Linked Resources are cameras (i.e., channels), you can set at most four Linkage Actions. For example, if you have set capturing picture and recording (the two are considered as two Linkage Actions) as the Linkage Actions for camera 1, you can only set two more Linkage Actions, i.e., capturing picture and recording for camera 2, or capturing picture for channel 2 and recording for channel 3, or recording for channel 2 and capturing picture for channel 3.
- Up to 128 Linkage Actions or 10 Linked Resources can be selected.

Table 6-2 Linkage Action Description

Linked Resource	Linkage Action	Description
Camera (Channel)	Capture Picture	The camera will capture a picture when the Triggering Event is detected.
	Recording	The camera will record video footage when the Triggering Event is detected. **Note** The recorded video footage starts from 5 s before the detection of the Triggering Event, and lasts 30 s.
	Call Preset	Select a preset from the Preset drop-down list to specify it as the preset which will be called when the Triggering Event is detected. A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other

Linked Resource	Linkage Action	Description
		parameters. By calling a preset, the PTZ camera will move to the predefined image position. **Note** Make sure you have configured presets for the PTZ camera. For details, see the user manual of the PTZ camera.
	Call Patrol	Select a patrol from the Patrol drop-down list to specify it as the patrol which will be called when the Triggering Event is detected. A patrol is a predefined PTZ movement path consisted of a series of key points (i.e., presets) that have their own designated sequence. By calling a patrol, the PTZ camera will travels to all the key points in set speed so as to provide a dynamic view. **Note** Make sure you have configured patrols for the PTZ camera. For details, see the user manual of the PTZ camera.
	Call Pattern	Select a pattern from the Pattern drop-down list tot specify it as the pattern which will be called when the Triggering Event is detected. A pattern is a predefined PTZ movement path with a certain dwell-time configured for a certain position. By calling a pattern, the PTZ camera moves according the predefined path. **Note** Make sure you have configured patterns for the PTZ camera. For details, see the user manual of the PTZ camera.
	Arm	The camera will be armed and hence the events related to the camera will be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected.
	Disarm	The camera will be disarmed and hence the events related to the camera will not be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected.
	Enable Privacy Mask	Privacy mask will be displayed on the live images of the camera when the Triggering Event is detected.

Linked Resource	Linkage Action	Description
		Note Make sure you have configured privacy mask for the camera. For details, see the user manual of the camera.
	Disable Privacy Mask	Privacy mask will NOT be displayed on the live images of the camera when the Triggering Event is detected.
Alarm Output	Alarm Output	The alarm output of the Linked Resource will be triggered when the Triggering Event is detected.
Area of Security Control Panel	Stay Arm	The arming status of the area of the security control panel will switch to Stay when the Triggering Event is detected.
	Away Arm	The arming status of the area of the security control panel will switch to Away when the Triggering Event is detected.
	Disarm	The area of the security control panel will be disarmed when the Triggering Event is detected.
Door Linked to Access Control Device	Open Door	The door related to the access control device will be opened when the Triggering Event is detected.
	Remain Open	The door related to the access control device will remain open when the Triggering Event is detected.
	Remain Closed	The door related to the access control device will remain closed when the Triggering Event is detected.
Door Station	Open Door	The door linked to the door station will be automatically opened when the Triggering Event is detected.
Alarm Input	Arm Alarm Input	The alarm input will be armed and hence events related to it will be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected.
	Disarm Alarm Input	The alarm input will be disarmed and hence events related to it will NOT be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected.

6. Configure the scheduled time during which the linkage is activated.
   1) Select date(s) in a week.
   2) Set the start time and end time of the scheduled time for each selected date(s).
   3) Tap **Next**.
7. Create a name for the linkage rule.
8. Tap **Enable**.

   The linkage rule will be displayed on the linkage rule list.

9. Optional: Set to to disable the linkage rule.

What to do next

If you have enabled the linkage rule, make sure the Notification functionality of the Source is enabled. For details about enable the functionality, see ***Enable Device to Send Notifications*** .

Note

- If the Notification functionality of the Source is disabled, the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not.
- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the Hik-Connect Mobile Client, or the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *Hik-Connect Mobile Client User Manual*.
- Please notify your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page to them.

6.4.2 Add Linkage Rule Based on Pre-defined Template

You can use six pre-defined templates to add linkage rules, including Intrusion, Forced Entry Alarm, Back to Home/Office, Away, Visitor Calling, and Perimeter Zone Alarm. Each of the six templates is designed for a typical applications (see the list below) of linkage rule.

Before You Start

You should have the permission for the configuration of the devices. Or you should apply for the permissions first. For details about applying for permission, see ***Apply for Device Permission*** .

Table 6-3 Template Description

Template	Description
Intrusion	The Intrusion Template: Used for improving security level by triggering the linkage actions including capture, recording, and alarm output, when the intrusion event (people, vehicles, or other objects enter a pre-defined area) occurs.
Forced Entry Alarm	The Forced Entry Alarm Template: Used for improving security level by triggering the linkage actions including capture, recording, remaining door closed, alarm output, and calling preset when line crossing detection (people, vehicles, or other objects cross a pre-defined virtual line) occurs.
Back to Home/Office	The Back to Home/Office Template: Used for lowering the security level and enabling privacy protection by triggering the linkage actions

Template	Description
	including disarming and enabling privacy mask, when you are back to home or office.
Away	The Away Template: Used for improving security level and canceling privacy protection by triggering the linkage actions including arming and disabling privacy mask when you leave your home or office.
Visitor Calling	The Visitor Calling Template: Used for improving security level by triggering the linkage actions including capture and recording when visitor(s) are calling from the door station.
Perimeter Zone Alarm	The Perimeter Zone Alarm Template: Used for improving security level by triggering the linkage actions including capture, recording, calling preset, alarm output, and remaining door closed, if people or other objects are detected in all accesses (including doors, windows, cellar doors, etc.) to a property.

Steps

Note

Due to the similarity of adding linkage rules based on different templates, here we only introduce how to add a linkage rule based on the Forced Entry Alarm template.

1. Tap a site on the site list to enter the site details page.
2. Tap **Linkage Rule** to enter the Linkage Rule page.
3. Tap a linkage template to enter the template configuration page.
4. Set the required information.

Linkage Rule Name

Create a linkage rule name.

When

Select a resource as the Source for detecting line crossing event from the drop-down list.

Trigger the Following Actions

Tap **Select** to select the Linked Resources used for triggering the linkage actions, and then click **Add**.

Note

- You can only select only one linkage action.
- For details about the linkage actions, see ***Table 6-2*** .

Linkage Schedule

Define the scheduled time during which the linkage is activated.

All Days

The linkage action is always activated from Monday to Sunday, 7 days × 24 hours.

Custom

Select date(s) within a week and then specify the start time and end time for each selected date.

Note

The date(s) marked blue is selected.

5. Tap **Enable**。

   The linkage rule will be displayed in the linkage rule list.

6. **Optional:** Set to to disable the linkage rule.

What to do next

If you have enabled the linkage rule, make sure the Notification functionality of the Source is enabled. For details about enabling the functionality, see ***Enable Device to Send Notifications*** .

Note

- If the Notification functionality of the Source is disabled, the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not.
- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the Hik-Connect Mobile Client, or the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *Hik-Connect Mobile Client User Manual*.
- Please notify your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page to them.

6.4.3 Video Tutorial

The following video shows that what is a linkage rule and how to set a linkage rule.

6.5 Add Exception Rule

An exception rule is used to monitor the status of managed resources in real-time. When the resource is exceptional, the resource will push a notification to the Hik-ProConnect to notify the specified Installer about this exception. Currently, the exceptions include two types: device exceptions and channel exceptions.

Before You Start

- Make sure you have the permission for configuration of the device (if the device supports). For applying for configuration permission, refer to ***Apply for Device Permission*** .
- Make sure you have enabled the device to send notifications to the system (if the device supports). For details, refer to ***Enable Device to Send Notifications*** .

You can add a rule to define such an exception. The rule contains five elements, including **Source** (device A or channel A), **Exception** (the exception occurred on device A or channel A), **Received by** (the source pushes a notification to notify the recipient via certain ways), **Recipient** (who can receive the notification), as well as **Schedule** (when the recipient can receive the notification).

Steps

1. Tap the name of a site to enter the site details page, and then tap **Exception** in the bottom.

   The exception rules of all the devices added in this site are displayed respectively.

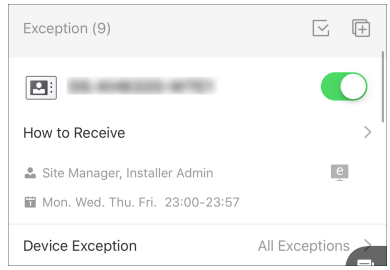

Figure 6-2 Add Exception Rule

2. Tap **How to Receive** in one device panel to set the **Recipient**, **Received by**, and **Schedule** in the rule.

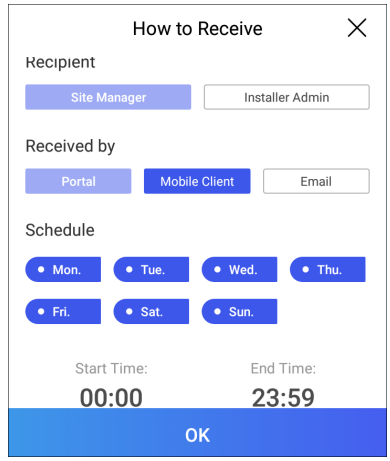

Figure 6-3 How to Receive

1) In the **Recipient** field, select **Site Manager** or **Installer Admin**. The recipient can receive the notification when the exception is detected in real-time.

   Note

   The Site Manager is selected by default and you cannot edit it.

2) In the **Received by** field, select the receiving mode(s) according to actual needs.

Portal

When an exception is detected, the device will push a notification to the Portal in real-time.

The Portal is selected by default and you cannot edit it.

Mobile Client

When an exception is detected, the device will push a notification to the Hik-ProConnect Mobile Client in real-time.

Note

For checking the exceptions received by the Mobile Client, refer to ***Exception Center*** .

Email

When an exception is detected, the device will push a notification to the Hik-ProConnect, and the system will send an email with the exception details to the email address(es) of the recipient(s) in real-time.

3) In the **Schedule** field, set when the recipient can receive the notification of the exception according to the actual needs, including days and time period on the selected days.
4) Click **OK**.

3. Tap **Device Exception** or **Channel Exception** to select types of exceptions which can trigger the notification.

Note

- For **Offline** exception, you can set the threshold of offline duration. When the device or channel is offline for longer than this threshold, an offline exception will be triggered.
- The threshold of offline duration should be between 5 and 120 minutes.

4. Optional: Set the exception rules of the devices in the site in a batch.
1) Tap .
2) Check the devices or channels you want to set the exception rules, and tap **Next**.
3) Set the exception types including device exception or channel exception, and tap **Next**.
4) Set the receiving mode, recipient, and time.
5) Click **Finish** to save the settings.

5. Optional: After setting one rule, you can copy the rule settings to other devices or channels for quick settings.
1) Tap .
2) Select device(s) or channel(s) as the sources to copy from.
3) Select the target resources of the same type as the selected sources.
4) Click **OK** to copy the rule settings of the sources to the target resources.

6. After setting the exception rule, you need to set the switch at the upper-right cornet of the rule to on to enable the device's exception rule.

After enabling the rule, it will be active and when an exception occurs, the device will push a notification according to the settings in the rule.

6.6 Enable Device to Send Notifications

After adding and enabling a linkage rule or exception rule, you should make sure the Notification functionality of the Source device is enabled so that the events detected by the device can be uploaded to the Hik-ProConnect system and the Hik-Connect Mobile Client, which is the prerequisite to trigger the linkage actions and exception rules defined in the Source-device-related linkage rule(s) and exception rule(s) respectively.

Steps

1. Tap a site to enter the site details page.
2. Select the **Device** tab.
3. Tap a device to enter the site details page.
4. Tap → **Notification** to enter the Notification Settings page.
5. Set the parameters.

   Notification

   Make sure the functionality is enabled.

   Notification Schedule

   After enable the Notification functionality, set a time schedule for uploading the events detected by the Source.

   You can select date(s) and then set the start time and end time for each selected date.
6. Tap **OK**.

Note

- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the Hik-Connect Mobile Client, or the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *Hik-Connect Mobile Client User Manual*.
- Please notify your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

6.7 Upgrade Device

If the Hik-ProConnect Mobile Client detects new firmware versions of devices including security control panels, doorbells, Hik-ProConnect box, Cloud Storage DVR, and certain models of network cameras, you can upgrade the devices by the Mobile Client.

Steps

Note

- Device upgrade needs to be supported by device firmware. Contact our technical supports for details.
- You can also upgrade the device when you add it. See ***Add Device by Hik-Connect (P2P)*** for details.

1. On the site list page, tap a site name to enter the site's page.
2. If you did not perform security authentication, tap **Authenticate** to perform this operation. See ***More Functions*** for details.

   Note

   - No new version will be detected without security authentication.
   - will appear beside the name of an upgradable device on the site list.

3. Tap the device name to enter the device page.
4. Tap **Upgrade**.
5. **Optional:** For security control panels enabled EN50131 Compliant mode, enter the device's password.
6. Tap **OK** to start upgrading.

   Note

   - Upgrading device may takes a few minutes. You can go back to the last page to perform other operations.
   - Once started, the upgrade cannot be stopped. Make sure a power failure or network outage does not happen during the upgrade.

6.8 Unbind Device from Its Current Account

When you add a device by scanning QR code or add it manually, if the adding result page shows it has been added to another account, you need to unbind it first before you can add it to your account. The device unbinding functionality is useful when you need to add a device to a new account but have no access to delete it from the old account (e.g., if you forgot the password of the old account).

Note

Make sure the phone on which the Mobile Client runs are on the same LAN with the device. Otherwise, this function will be unavailable.

Tap **Unbind** on the adding result page, and then enter the device password and tap **Finish** to unbind it from its currently-added account. When the device is unbound, you can add it to your account.

Note

If the device firmware does not support device unbinding, you are required to enter a CAPTCHA code after entering device password.

6.9 Reset Device Password

You can reset the password of a device when the Site Owner and the Installer both lost the password.

Note

- Resetting password via Hik-ProConnect platform is not supported by every device type/model. For example, AX Pro security control panel does not support this function.
- Make sure that the device is authorized by the Site Owner to you before resetting device password. For details, see ***Apply for Site Authorization from Site Owner*** .
- Make sure that the device is on the same local area network with the phone or tablet where your Hik-ProConnect Mobile Client runs.

Go to **Site** tab and enter the site where the device locates.

Tap the device and then tap • • • → **Reset Password** to send a password reset application to the Site Owner.

Refer to the flow chart below for the whole process of resetting the password of a device.

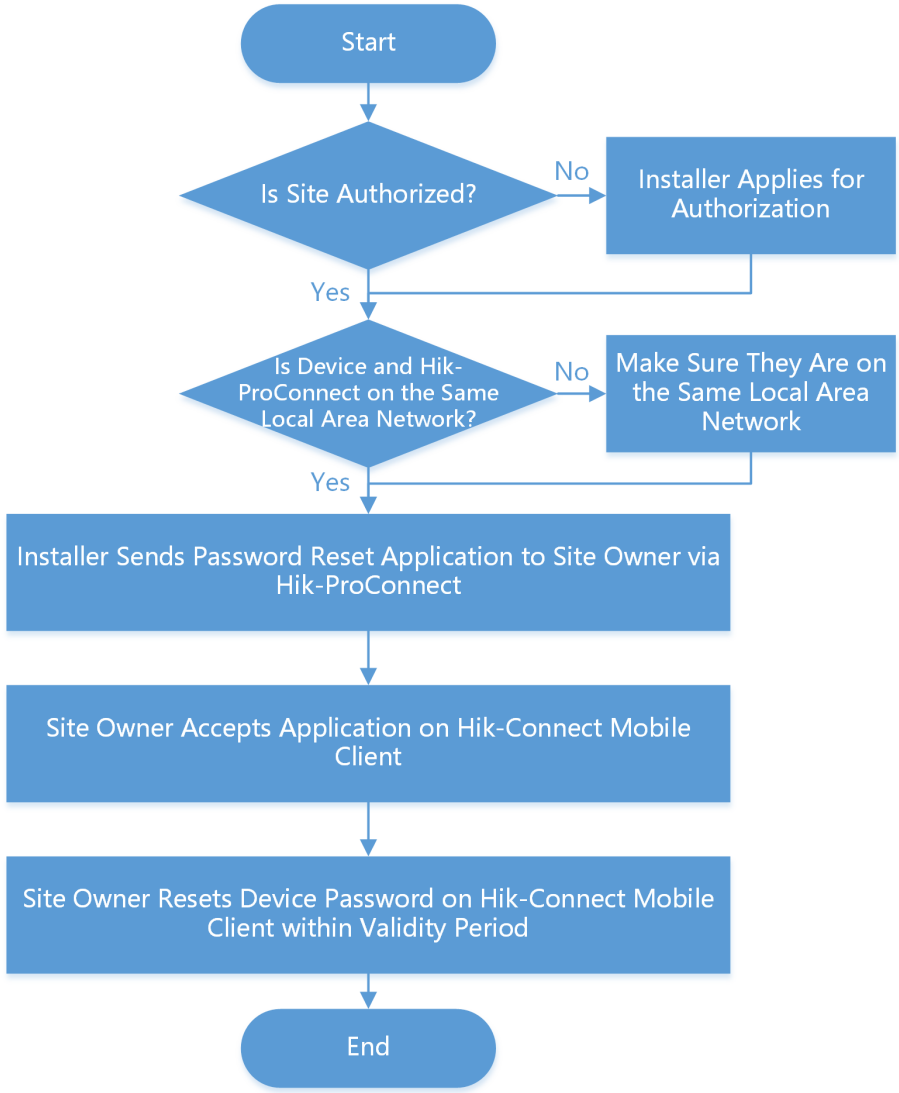

Figure 6-4 Flow Chart of Resetting Device Password

6.10 Configure DDNS for Devices

For devices with invalid or old firmware version, you can configure DDNS for them to make sure they can be managed by Hik-ProConnect properly.

Steps

Note

Only encoding devices added by Hik-Connect (P2P) support this function.

1. Tap a site on the site list to enter the site details page.

Note

For devices with invalid or old firmware version and without DDNS configured, a red dot will be displayed beside the device name.

2. Tap a device to enter the device page.
3. Tap **DDNS Settings** to enter the DDNS Settings page.

Note

You can tap **How to set port?** to learn the configuration.

4. Switch **Enable DDNS** on.
5. Enter the device's domain name.
6. Select **Port Mapping Mode**.

Auto

In this mode, the service port and HTTP port are obtained automatically, and you cannot edit them after obtaining them.

Manual

Enter the service port and HTTP port manually.

7. Enter the user name and 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.

8. Tap **Save**.

6.11 View Live Video

By Hik-ProConnect Mobile Client, you can view live view of managed cameras and perform related operations.

Tap to start live view of the latest 5 minutes of an encoding device. During live view, you can perform PTZ control (except Pattern), enable wiper to clean the camera lens, and click **High Definition** to switch image quality. For devices added by Hik-Connect Service without configuring DDNS, the live view will work for up to five minutes; for devices added by IP/Domain Name and devices added by Hik-Connect Service with DDNS configured, the live view duration is not limited.

Note

- If Image and Video Encryption has been enabled for the device on the Hik-Connect mobile client, you are required to enter the device verification code before starting live view. If you don't know the device verification code, ask the end user for it. For details about Image and Video Encryption, see *Hik-Connect Mobile Client User Manual*.
- Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.
- If you have no permission for live view, you can perform live view by a LAN: Connect your mobile phone to the same Wi-Fi with the encoding device, and then click **Live View in LAN** to log into the device and start live view.
- Make sure the device is online, otherwise the function cannot be used.

6.12 View Recorded Video Footage

You can start playback to view the recorded video footage of a device.

Note

- Make sure you have permission for playback. If you have no permission for playback, you cannot enter the playback page. See ***Apply for Device Permission*** for details about how to apply for playback permission.
- This function should be supported by the device.

Enter a site page, select a device and click to enter the playback page. You can also enter the playback page on the live view page.

Click the date below the playback window to select a date for playback.

On the playback tool bar, click the following icons to perform functions you need.

For devices added by Hik-Connect P2P, the video files are displayed by different color: the time-based video files are marked in blue in the time bar and the event-based video files are marked in yellow in the time bar.

	Click to select a channel for playback.
	Click to download the video footage to your PC.
/	Click to turn on/off the playback sound.
	Click to pause the playback.
	Click to select a speed for playing video footage.
	Click to perform digital zoom.

	Click to capture a picture.
	Click to clip the video footage and download it to your PC.

6.13 Operate and Configure AX Pro

On the Mobile Client, you can remotely operate AX Pro. The supported operations include adding area, arming/disarming area, clearing alarm, bypassing zone etc. You can also do remote configurations, such as walk test, DST settings, and device upgrade.

Tap a site to enter site details page, and then select the **Device** tab. On the device tab, tap an AX Pro security control panel to enter the device details page.

Remotely Operate AX Pro

On the device details page, you can perform the following operations.

Table 6-4 Operation Description

Operation	Description
Add Area	Select the **Area** tab, and then tap to add an area.
Stay Arm a Specific Area	Select the **Area** tab, and then tap to stay arm the area.
Away Arm a Specific Area	Select the **Area** tab and then tap to away arm the area.
Disarm a Specific Area	Select the **Area** tab and then tap to disarm the area.
Stay Arm All Areas	Select the **Area** tab, and then tap at the bottom of the page.
Away Arm All Areas	Select the **Area** tab, and then tap at the bottom of the page.
Disarm All Areas	Select the **Area** tab, and then tap at the bottom of the page.
Clear Alarms of All Areas	Select the **Area** tab, and then tap at the bottom of the page.
Filter Peripheral Device by Area	Select the **Device** tab, and then tap and select an area to only display the peripheral devices linked to the selected area, or select **All** to display all the peripheral devices linked to all the areas.
Add Peripheral Device	Select the **Device** tab, and then tap to add a peripheral device. **Note** For details about adding device, see ***Add Device*** .

Operation	Description
Bypass Zone	Select the **Device** tab, and then select a zone (i.e., detector) and turn on the **Bypass** switch to bypass the zone.
View Status	Select the **Status** tab to view the status information of the control panel, including external power supply status, Ethernet network status, Wi-Fi status, etc.

Remotely Configure AX Pro

Tap on the device details page to enter the settings page to remotely configure AX Pro.

Table 6-5 Configuration Description

Configuration	Description
Walk Test	Walk test is used to test if the detectors can detect target objects in the detection zones. Tap **Project Maintenance → Device Maintenance → Test → Start Walk Test** , and then walk in the detection zones, and finally tap **End Walk Test** to view the test results: the status (normal or abnormal) will be displayed.
Daylight Saving Time	Tap **System → Configuration → DST** to enter the DST settings page, and then turn on the switch to enable daylight saving time for AX Pro.
Upgrade and Language Switching	**Note** You should have the permission to access the device upgrade functionality. For details about permission settings for AX Pro, see the user manual of the device. Tap **Project Maintenance → Device Upgrade** to enter the device upgrade page, and then select language and enter the PIN, and finally tap **Upgrade** to switch language for AX Pro and upgrade it. **Note** If you don't have the PIN, you can tap **Apply for PIN** to apply for it.
Other Configurations	You can do other configurations including user management, system options configuration, linking network cameras, communication settings, etc. **Note** For details about other AX Pro configurations, see the user manual of the security control panel.

6.14 Network Switch Management

The network switch can be managed by the Mobile Client, including viewing topology and viewing the network switch details. Further more, you can remotely reboot the switch.

6.14.1 Network Switch Operations

On the network switch details page, you can view the CPU usage, memory usage, view the status of the port, reboot the device.

On the device list, click the switch name to enter the device details page.

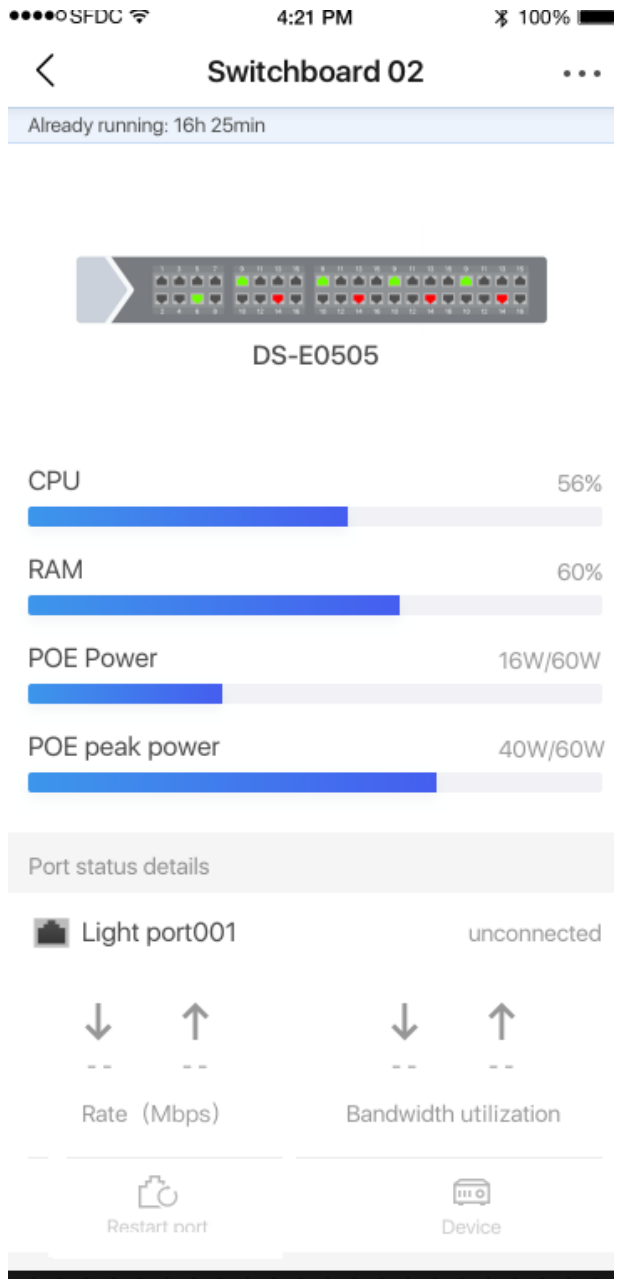

Figure 6-5 Switch Details

On the upper area of the page, you can view the CPU usage, memory usage, POE power and POE power peak.

On the middle area of the page, you can view the port status of each port, including the port type (Ethernet port, Fiber optical port), rate, bandwidth.

Perform the following operations according to your requirements.

Operation	Description
Reboot Switch	Click **Reboot** to reboot the switch.
View Peer Device	Click **Peer Device** to view the details of the device connected to this port.
Clear Alarm	For port with alarm, click **Clear Alarm** to clear the alarm of this port.
Restart Port	For the abnormal port, click **Restart Port** in the port status details to restart the port.

6.14.2 Network Topology

If you have added network switch(es) to a site and connected devices to the network switch(es), you can view these devices' network topology. Network topology displays network links between devices and shows the link exceptions and abnormal devices, helping you to locate exception source and troubleshoot faults in a visualized way.

Note

Make sure you have configuration permission for the network switch, otherwise network topology is unavailable. For details about applying for the permission, see ***Apply for Device Permission*** .

Tap a site on the site list to enter the device list page, and then click next to a network switch to enter the network topology page. You can perform the following operations on the network topology.

Table 6-6 Available Operations

Operation	Description
View Legend	You can tap **More** to view all the legends.
Edit Root Node	When multiple network switches are added to a site, the platform will randomly select one of them as the root node by default for the network topology. If the randomly-selected network switch is not the real root node, you can tap to select a network switch as the root node.
View Network Switch Details	You can tap a network switch on the topology to view its details, including basic information, device status, and port status. You can also perform operations such as rebooting the network switch and restarting

Operation	Description
	port. For details, see ***Network Switch Operations*** . **Note** You cannot view details of a virtual network switch.
View Details of Other Device	Tap a device to view its details, such as device model and network status. **Note** • Make sure you have the configuration permission for the device, otherwise you need to apply for the permission first. • You cannot view details of a virtual network switch. • If the device is not added to the same site with the network switch, you cannot view its details.
Expand Devices in a Node	Devices of the same type are folded in a node of the network topology. You can tap ⌄ on the node to expand all the devices and view whether their running status is normal. The color of the device icon indicates the running status of a device: • Gray: Normal • Red: Abnormal • Yellow: Device Busy
Move/Zoom In/Zoom Out	You can drag the network topology to move it; Pinch fingers together to zoom out, and spread them apart to zoom in.

6.15 More Functions

You can perform operations including security authentication and remote configuration if you need.

Note

Only site manager can perform the following operations and configurations of a site. See *User Manual of Hik-ProConnect Portal* for details about assigning site.

On the site list page, tap a site name to enter the site's page, and the site's information and devices will be displayed.

Security Authentication

For Axiom security control panel, a notification will appear in a site's device list or a device page to remind you to perform security authentication if you have enabled EN50131 Compliant mode on the device's configuration page. For security's sake, you need to click **Authenticate** and then enter the device password. Otherwise, device-related functions including health monitoring, device configuration, linkage rule, and new device versions will be unavailable. See device user manual for details about enabling EN50131 Compliant mode on the device's configuration page.

Remote Configuration

Tap ⚙ to set the device (including doorbell, encoding device, NVR, DVR, and security control panel) parameters. See device user manual for details about remote configuration.

Note

- For doorbell's remote configuration, you can only set the chime type.
- Make sure you have performed security authentication before starting remote configuration.
- If you have no permission for remote configuration, you can perform this operation by a LAN: Connect your mobile phone to the same Wi-Fi with the to-be-configured devices, and then click **Configuration in LAN** to log into the device and start remote configuration.
- Make sure the device is online, otherwise the function cannot be used.

Chapter 7 Manage Cloud Storage

If you have purchased cloud storage service packages on the Portal, you can use the Mobile Client to remotely add cloud storage devices to the Hik-ProConnect platform, and do further settings to make the cloud storage device be able to upload event-related video footage from channels of encoding devices to the cloud.

7.1 Set Cloud Storage for Hik-ProConnect Box

When you complete adding a Hik-ProConnect box to a site, the result page will show the entry for setting cloud storage. You can skip the settings, but it is recommended that you tap the entry to start the settings, including network test (optional), adding channels, channel resolution settings, event settings, and activating cloud storage service. When you complete all these settings, the Hik-ProConnect box will be able to upload event-related video footage from its linked channels to the cloud.

Steps

Note

If you skip the cloud storage settings when completing adding the Hik-ProConnect Box you can tap it in the device list to enter its settings page and then tap **Linked Channel** to set cloud storage for the device later.

1. Add a Hik-ProConnect box to the platform by Hik-Connect P2P.

   Note

   For details, see ***Add Device by Scanning QR Code*** and ***Add Device by Hik-Connect (P2P)*** .

   When you completes adding the device, the entry for setting cloud storage will be displayed in the pop-up window which shows the result of device adding.
2. Tap **Cloud Storage Settings** to start setting cloud storage parameters.

   You enter the Network Test page.
3. **Optional:** Tap **Start** to test the network performance if the network bandwidth is limited, and then tap **Add Channel** when the test completes.

   Note

   - For details about network test, see ***Network Test*** .
   - You can tap **Skip** to skip the step.

   You enter the Select Device to Link page, on which the available devices are displayed.
4. Tap a device to enter the Select Channel to Enable Cloud Storage page.
5. Turn on the switch(es) to add channel(s) to the Hik-ProConnect box.

6. Tap **Next** to enter the Device Information page.
7. Set the device information, such as device IP address, user name, and password.
8. Tap **Finish** to enter the Linked Channel page.
9. Activate cloud storage service for a channel.
   - Tap **Activate → Activate by Service Key** , and then enter the service key and tap **Activate**.
   - Tap **Activate → Activate Purchased Package** , and then select a type of purchased package and set the number of the to-be-activated package(s), and finally tap **Activate**.

Note

- You can purchase the service key from the distributor. For details, contact the distributor in your country or region.
- You can purchase cloud storage service packages from the service market on the Portal. For details, see *Hik-ProConnect Portal User Manual*.

10. Tap the activated channel to enter the Channel Details page to set cloud storage related parameters.

Video Definition

Set **High Definition** or **Standard Definition** as the definition of the video footage uploaded to the cloud.

Note

Make sure the number of standard definition channel(s) or high definition channel(s) is no more than the recommended upper-limit displayed on the Add Channel window (if you have tested your network).

Cloud Storage

Edit the cloud storage service you have activated for the channel.

Motion Detection

Set motion detection as the event to trigger video recording action of the channel.

Note

The events support such a trigger include motion detection, intrusion, and line crossing. On the Mobile Client, you can only set motion detection as the event for such a trigger.

Enable Motion Detection

When enabled, objects in motion on the image of the channel will be detected.

Area Settings

Tap **Draw Area** to draw an area on the image, and then drag the slider to set the sensitivity of the detection.

Objects in motion will be detected within the drawn area.

Arming Schedule

Define the time period during which motion detection is activated.

Linkage Method

Make sure **Notify Surveillance Center** is enabled, otherwise the channel will not record event-related video footage even if the event is detected.

11. Optional: Perform the following operations if required.

Switch Channel to Use the Service	Tap an channel with activated service in the channel list to enter Cloud Storage Settings page, and then tap ⇌ to switch channel to use the activated cloud storage service.
Delete Channel	If cloud storage service is not activated for a channel, tap it in the channel list, and then tap **Delete** to delete it. **Note** You cannot delete a channel with activated service.

7.2 Set Cloud Storage for Cloud Storage DVR

When you complete adding a cloud storage DVR to a site, the result page will show the entry for setting cloud storage. You can skip the settings later, but it is recommended that you click the entry to start the settings, including network test (optional), definition settings, event settings, enabling cloud storage for the DVR's channels, and activating cloud storage service for the channels. When you complete all these settings, the cloud storage DVR will be able to upload event-related video footage from its linked channels to the cloud.

Steps

Note

If you skip the cloud storage settings when completing adding the cloud storage DVR, you can tap it in the device list to enter its settings page and then tap **Linked Channel** to set cloud storage for the device later.

1. Add a cloud storage DVR to the platform by Hik-Connect P2P.

Note

For details, see ***Add Device by Scanning QR Code*** and ***Add Device by Hik-Connect (P2P)*** .

When you completes adding the device, the entry for setting cloud storage will be displayed on the pop-up window which shows the result of device adding.

2. Tap **Cloud Storage Settings** to start setting cloud storage parameters.

You enter the Network Test page.

3. Optional: Tap **Start** to test the network performance if the network bandwidth is limited, and then tap **Next** when the test completes.

Note

- For details about network test, see ***Network Test*** .
- You can tap **Skip** to skip the step.

You enter the Select Channel to Enable Cloud Storage page, on which all the channels of the cloud storage DVR are displayed.

4. Turn on the switch(es) to enable cloud storage functionality for channel(s) of the device.
5. Tap **Next** to enter the channel list page.
6. **Optional:** Tap the thumbnail of a channel to view its live video.
7. Tap a channel to enter the Cloud Storage Settings page.
8. Activate cloud storage service for the channel.
   - Tap **Activate → Activate by Service Key** , and then enter the service key and tap **Activate**.
   - Tap **Activate → Activate Purchased Package** , and then select a type of purchased package and set the number of the to-be-activated package(s), and finally tap **Activate**.

Note

- You can purchase the service key from the distributor. For details, contact the distributor in your country or region.
- You can purchase cloud storage service packages from the service market on the Portal. For details, see *Hik-ProConnect Portal User Manual*.

You enter the Cloud Storage Settings page.

9. Set cloud storage related parameters on the Cloud Storage Settings page.

Video Definition

Set **High Definition** or **Standard Definition** as the definition of the video footage uploaded to the cloud.

Note

Make sure the number of standard definition channel(s) or high definition channel(s) is no more than the recommended upper-limit displayed on the Add Channel window (if you have tested your network).

Cloud Storage

Edit the cloud storage service activated for the channel.

Motion Detection

Set motion detection as the event for triggering video recording action of the channel.

Note

The events support such a trigger include motion detection, intrusion, and line crossing. On the Mobile Client, you can only set motion detection as the event for such a trigger.

Enable Motion Detection

When enabled, objects in motion on the image of the channel will be detected.

Area Settings

Tap **Draw Area** to draw an area on the image, and then drag the slider to set the sensitivity of the detection.

Objects in motion will be detected within the drawn area.

Arming Schedule

Define the time period during which motion detection is activated.

Linkage Method

Make sure **Notify Surveillance Center** is enabled, otherwise the channel will not record event-related video footage even if the event is detected.

7.3 Network Test

When your network bandwidth is limited, you can only enable cloud storage for a limited number of channels, otherwise video loss may occur. To avoid such a risk, you can perform network test. Based on your network conditions, the result of network test shows the maximum number of channel(s) with cloud storage enabled and the recommended resolution setting for each channel, helping you to set cloud storage in the way that utilize the limited network bandwidth to the largest extent.

You can tap the cloud storage device in the device list to enter its settings page, and then click **Network Test → Start** to start testing your network.

Chapter 8 Exception Center

The Exception Center module shows all the history notifications of device exceptions and channel exceptions.

Note

- For Installer Admin, you can view all the exceptions of the devices in all the added sites. For Installers, you can view the exceptions of the devices in the site which has been assigned to you.
- You need to set the exception rule first. For details, refer to ***Add Exception Rule*** .

Tap **Exception Center** to enter the Exception Center page as follows.

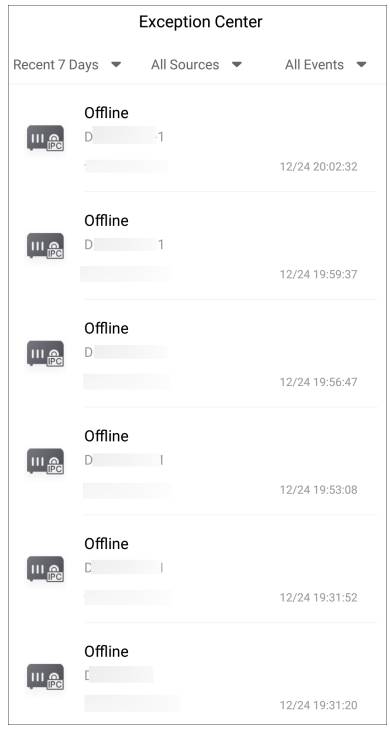

Figure 8-1 Exception Center

Check Exception Details

Perform the following steps to filter the exceptions according to actual needs.

1. Set the time period. The exceptions received during this time period will be displayed.
2. Select a source (including site, device, and channel) from the drop-down list to view the corresponding exceptions.
3. Select the exception types that you want to check. The exception types include device exception and channel exception.