Hik-ProConnect Mobile Client V1.1.1

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

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*.

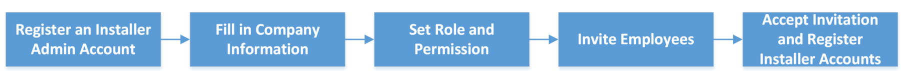


Figure 2-1 Flow Chart of Account Management

- **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 **Not Registered?** to enter the registration 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 after registration.
4. 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.

5. Enter your name and phone number.
6. Enter the authentication code which is used for authenticating that you are a professional Installer.

   Note

   - Send your email address to the regional distributor or national distributor, and apply for an 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*.
   - The authentication code should contain 10 digits.

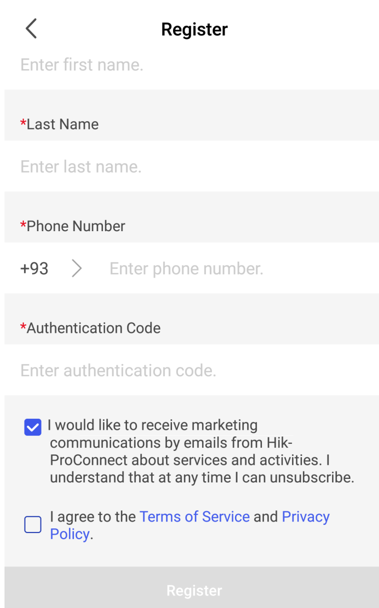


Figure 2-2 Register Page

7. **Optional:** Check **I would like to receive marketing communications by emails from Hik-ProConnect about services and activities. I understand that at any time I can unsubscribe.** to subscribe. You can unsubscribe from it in the Me 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 Hik-ProConnect activities, product updates, surveys, and special offers, to the email address which is used for your account registration.
8. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in these agreements.
9. Tap **Register**.

   A registration confirmation email will be sent to the email address you entered in the above-mentioned step.
10. 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, country, logo, business license number, etc.) with this account for better service.

Before You Start

Register an Installer Admin account first. For details, refer to ***Register an Installer Admin Account*** .

Steps

1. After Installer Admin registration and login, the Company Information page will pop up.

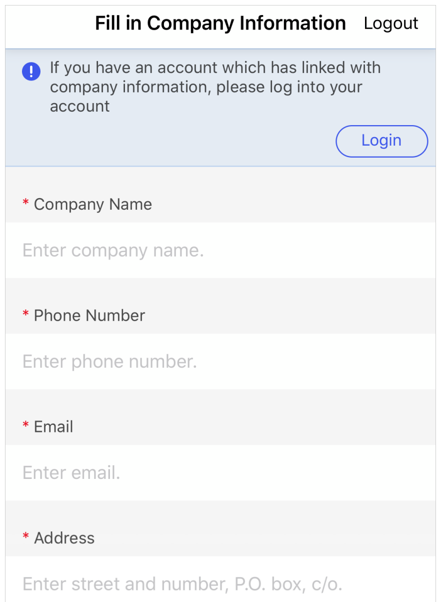


Figure 2-3 Bind Company Information Page

2. Enter the name of your company .
3. Enter your phone number.
4. Enter an email address which will be bound with the Installer Admin account after registration.
5. Enter other information of your company, such as address, city, state/province/region, and postal code.
6. Enter the business license number and VAT number of your company which will be used for qualification verification.
7. Tap **+** to upload a picture of the company's logo.

Note

- The picture should be in JPG, JPEG, or PNG format.
- Recommended picture size: Height = 200 px, 200 px ≤ Width ≤ 600 px.

8. **Optional:** Enter the website of your company if any.
9. Tap **OK**.

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

Note

If you want to edit your company information, log in to the Portal to edit. See the *User Manual Hik-ProConnect Portal* for details.

Chapter 3 Login

After login by an Installer Admin account or Installer account, you can manage sites and devices, and perform health monitoring and so on.

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.
2. Enter the registered email and password.
3. **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.
4. Tap **Login**.

   By default, you will enter the site list page.

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

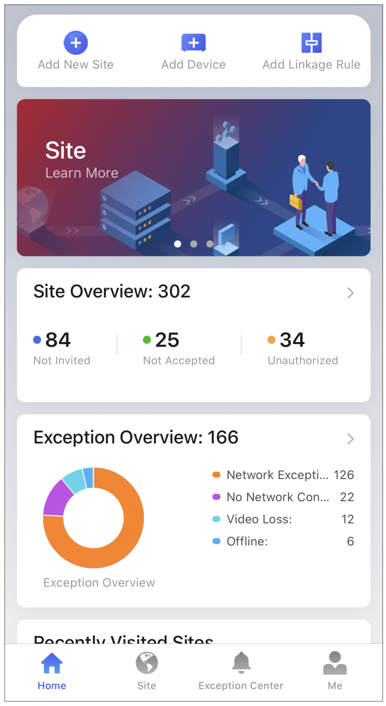
The Hik-ProConnect Mobile Client is divided into four main modules. You can access these modules via the navigation panel on the bottom.

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 recently visited sites.
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*.
	Marketing Communications: For Installer Admin, if you didn't subscribe marketing communications when account registration, you can subscribe to the marketing communications about Hik-ProConnect. After subscription, we will send emails about latest Hik-ProConnect activities, product updates, surveys, and special offers, to the email address which is used for your account registration. You can unsubscribe at any time here. After unsubscription, you will not receive any marketing communication 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.
	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



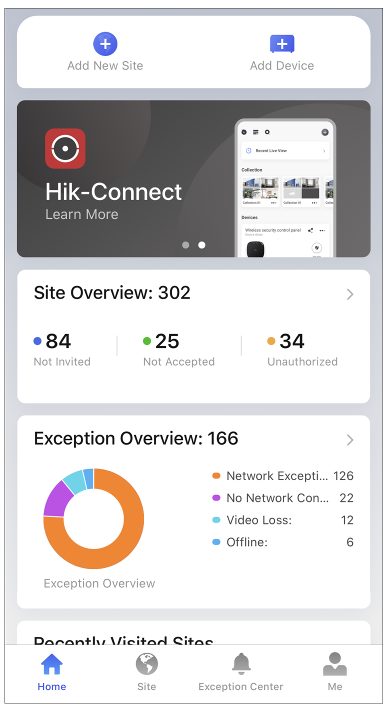


Figure 4-1 Home Page

Table 4-2 Home Page Description

No.	Name	Introduction
1	Shortcut	Three shortcuts of the key features 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*** .
2	Banner	There are some banners, showing the key features, functions, and important information of Hik-ProConnect. **Note** You can inform your end users to download or update the Hik-Connect Mobile Client (Version 4.3.0 and later) by sending the QR code or download link to them.
3	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*** .
4	Exception Overview	You can view the number of received exceptions and the proportions of each type of the exceptions. **Note** You can click > to enter **Exception Center** to check the received exceptions. For detailed instructions about Exception Center, refer to ***Exception Center*** .
5	Recently Visited Sites	You can view the five sites which you visited recently.

No.	Name	Introduction
		Click the site name to enter the site details page.

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 Assign Site 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.

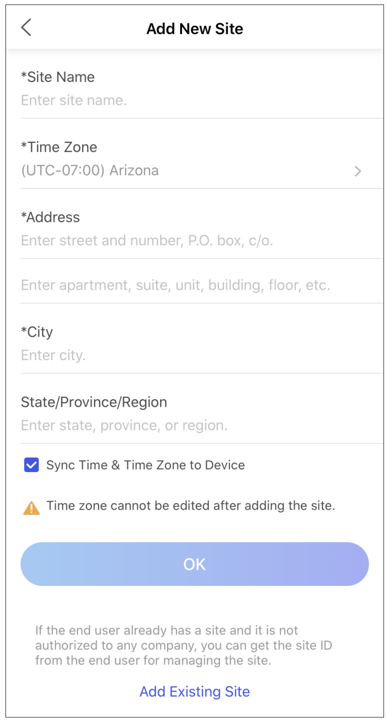


Figure 5-1 Add New Site

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** .

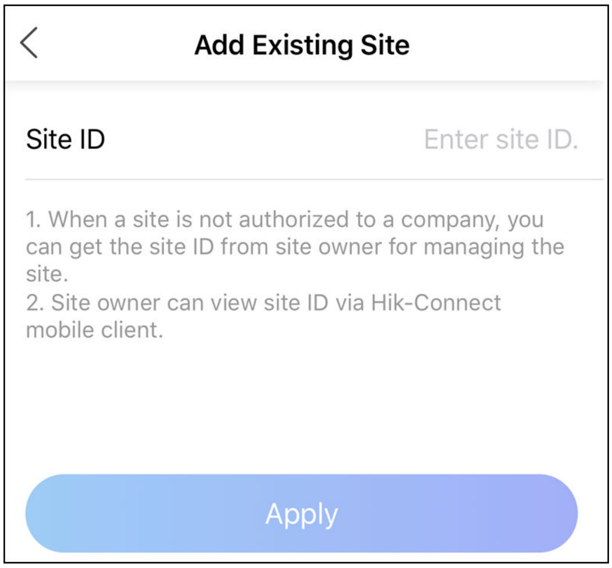


Figure 5-2 Add Existing Site

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 4.3.0 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.

Steps

1. In site list, tap a site to enter Site Details page.
2. Tap **Invite Now** to enter Invite Site Owner page.
3. Select **Email** or **Phone Number** as invitation mode.
4. Enter site owner's email address or phone number.

5. **Optional:** Select authorization permissions of the Installer after the site is handed over to the site owner.

Note

- If you have no device management permission or no devices are added in the site, the permissions of configuration and live view can not be selected.
- 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.

6. Tap **Invite** to send the invitation.
   - If the invitee has registered a Hik-Connect account, he/she will receive the invitation via Hik-Connect Mobile Client. After accepting the invitation, the end user will become the site owner.
   - If the invitee has not registered a Hik-Connect account, he/she will receive the registration email or message in email box or via short message. 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 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

7. **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 Authorization Permission 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.

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.

   Note

   Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

Chapter 6 Manage Device

Hik-ProConnect supports multiple device types, including encoding device, security control panel, video intercom device, and access control device, 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 configuring linkage rule, etc.

6.1 Add Device

You can add devices to a site manually or add by scanning the QR codes on the devices.

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.

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 the QR code on the device.
   - Scan the QR code by aligning the QR code with the scanning frame.

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.

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

Note

Please allow the Mobile Client to access the photo album of the phone.

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 ***Manually Add Device*** 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 click **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.

   Note

   - After adding the device, the Hik-ProConnect starts detecting whether the device firmware version is compatible with the Hik-ProConnect. Some functions (including health monitoring, linkage, and remote configuration) cannot be used if the device is not compatible with the Hik-ProConnect. Firmware version detection will not happen if a site is authorized.
   - Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

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	Tap the device and then tap → **Delete Device** to delete the device.

Note

Deleting device is not supported if the site is authorized.

6.1.3 Manually Add Device

You can manually add devices 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. Click **Add**.

   Note

   After adding the device, the Hik-ProConnect starts detecting whether the device firmware version is compatible with the Hik-ProConnect. Some functions (including health monitoring, linkage, and remote configuration) cannot be used if the device is not compatible with the Hik-ProConnect. Firmware version detection will not happen if a site is authorized.

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 click **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:** Tap the device and then tap ⋯ → **Delete** to delete the device.

Note

Deleting device is not supported if the site is authorized.

6.2 Apply for Live View & Configuration Permission

After handing over a site to the end user, if you needs to view the live video of devices added to the site or configure the devices added to the site, you can apply for the live view permission and (or) configuration permission from the end user.

Steps

1. Tap a site to enter the site details page.
2. Tap ⋯ → **Live View** or ⋯ → **Configuration** .
3. Tap **Apply for Permission** to apply for the permission.

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

6.3 Add Linkage Rule

An 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... 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 only shows the process of the linkage when its data transmission is done via Cloud (server).

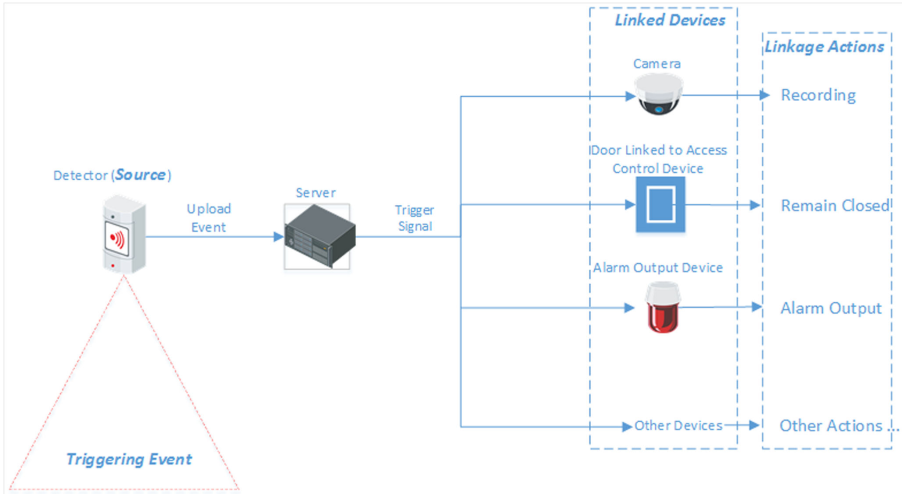


Figure 6-1 Linkage

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.

6.3.1 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.
- You should 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 Live View & Configuration 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.

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
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.

Source	Triggering Event
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 parameters. By calling a preset, the PTZ camera will move to the predefined image position. **Note** You should have configured presets for the PTZ camera. For details, see the user manual of the PTZ camera.

Linked Resource	Linkage Action	Description
	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** You should 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** You should 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 Surveillance Center 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 Surveillance Center 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. **Note** You should 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.

Linked Resource	Linkage Action	Description
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 Surveillance Center 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 Surveillance Center 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 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

6.3.2 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 Live View & Configuration 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 including disarming and enabling privacy mask, when you are back to home or office.

Template	Description
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 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

6.4 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 Live View & Configuration 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.

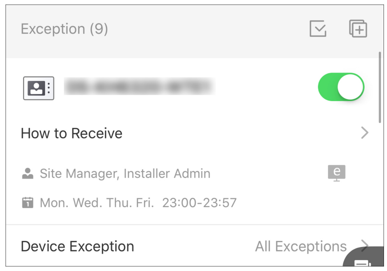


Figure 6-2 Add Exception Rule

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

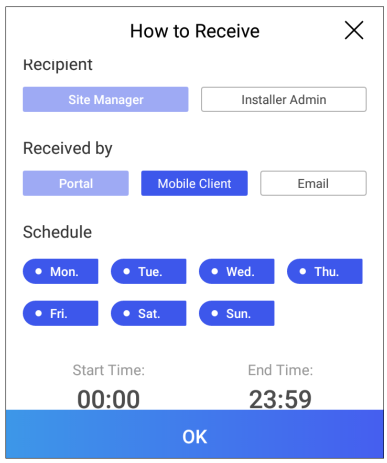


Figure 6-3 How to Receive

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 30 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.

6.5 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 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

6.6 Upgrade Device

If the Hik-ProConnect Mobile Client detects new firmware versions of devices including security control panels, doorbells, and certain models of network cameras (e.g. DS-2CV2Q23G0-IDW), 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.

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.

6.7 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.

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 4.3.0 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.

6.8 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, 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 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.

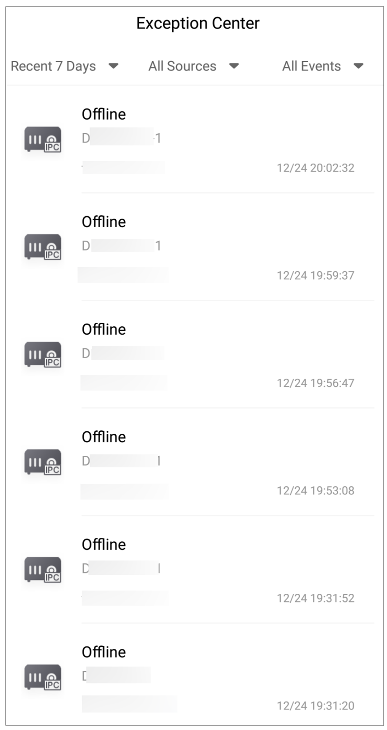


Figure 7-1 Exception Center

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.

UD19476N