



Hik-ProConnect Mobile Client

User Manual

Legal Information

©2021 Hikvision Europe B.V. All rights reserved.

About this Manual

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

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

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

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

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

Hik-ProConnect Mobile Client User Manual

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	1
1.1 Target Audience	1
1.2 Running Environment	1
1.3 Region Availability for Hik-ProConnect Functions	2
1.3.1 Regions Only With Support for Free Functions	2
1.3.2 Functions Only Available in Certain Regions	3
1.4 Download the Mobile Client	4
Chapter 2 Account Management	7
2.1 Register by Hik-Connect Account	8
2.2 Register an Installer Admin Account	10
2.3 Complete Your Company Information	12
2.4 Authenticate Your Account	13
2.5 Link Your Account to a Distributor	14
Chapter 3 Login	15
Chapter 4 Hik-ProConnect Mobile Client Overview	17
Chapter 5 Manage Site	23
5.1 Site Page Introduction	23
5.2 Add New Site	24
5.3 Add Existing Site	26
5.4 Invite Site Owner	27
5.5 Apply for Site Authorization from Site Owner	29
Chapter 6 Device Management	31
6.1 Batch Configure Devices on LAN	31
6.1.1 Batch Activate Devices and Assign IP Addresses for Them	33
6.1.2 Batch Link Channels to NVR	34
6.1.3 Create Templates for Setting Parameters	34

6.1.4 Batch Set Parameters for Devices	35
6.2 Add Device	36
6.2.1 Add Devices After Batch Configuring Them on LAN	36
6.2.2 Connect Offline Device to Network	38
6.2.3 Add Device by Scanning QR Code	38
6.2.4 Add Device by Hik-Connect (P2P)	41
6.2.5 Add Device by IP Address or Domain Name	43
6.2.6 Add Devices Without Support for the Hik-Connect Service	45
6.3 Activate the Health Monitoring Service	47
6.4 Manage Device Permission	49
6.4.1 Apply for Device Permission	49
6.4.2 Release the Permission for Devices	49
6.5 Migrate Devices from Hik-Connect Account	50
6.6 Linkage Rule and Exception Rule	51
6.6.1 Add Linkage Rule	51
6.6.2 Add Exception Rule	59
6.6.3 Enable Device to Send Notifications	61
6.7 Reset Device Password	62
6.8 Manage Security Control Panel	64
6.8.1 Control AX Pro	64
6.8.2 Configure AX Pro	65
6.8.3 Batch Arm/Disarm AX Pro	66
6.8.4 Batch Configure AX PROs	68
6.9 Alarm Receiving Center (ARC) Service	71
6.10 View Video	73
6.10.1 View Live Video	73
6.10.2 Play Back Video Footage	73
6.11 Network Switch Management	74

6.11.1 Network Switch Operations	74
6.11.2 Network Topology	76
6.12 Other Management	78
6.12.1 Upgrade Device	78
6.12.2 Unbind a Device from Its Current Account	79
6.12.3 Configure DDNS for Devices	79
6.12.4 Remote Configuration	80
Chapter 7 Service Market	82
Chapter 8 Manage Cloud Storage	84
8.1 Set Cloud Storage for Hik-ProConnect Box	84
8.2 Set Cloud Storage for Cloud Storage DVR	86
8.3 Network Test	88
Chapter 9 Exception Center	89

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 solution provides different ways/clients for Installers and Installers' customers.

Table 1-1 Client Description

Client	Description
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 your customers to manage their devices, accept the Installer's invitation as the Site Owner, approve the Installer's application of site information management permission, etc.
Hik-Connect Portal	Portal for your customers to manage their employees' access level and attendance data after you set an attendance system for them via the Hik-ProConnect Portal.

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.

1.3 Region Availability for Hik-ProConnect Functions

Hik-ProConnect offers both free basic functions and value-added functions that cost certain fees. You can purchase certain services in the Service Market to get access to the value-added functions. Currently, certain value-added functions are only available in certain countries and regions. And users in some countries and regions can only access the free functions.



This document contains introductions of all Hik-ProConnect functions, therefore some functions illustrated in this document may NOT be supported in your country or region. And contents in figures in this document may be different from the actual interface, if so, the latter shall prevail.

1.3.1 Regions Only With Support for Free Functions

The following two tables show the free functions on the Mobile Client and the countries and regions only with support for free functions.

Table 1-2 Free Functions on the Mobile Client

Module	Function(s)
Account Management	<ul style="list-style-type: none">• <u>Register an Installer Admin Account</u>• <u>Complete Your Company Information</u>
Site Management	<ul style="list-style-type: none">• <u>Add New Site</u>• <u>Add Existing Site</u>• <u>Invite Site Owner</u>• <u>Apply for Site Authorization from Site Owner</u>
Device Management	<ul style="list-style-type: none">• Add Device<ul style="list-style-type: none">◦ <u>Add Device by Scanning QR Code</u>◦ <u>Add Device by Hik-Connect (P2P)</u>◦ <u>Add Device by IP Address or Domain Name</u>• <u>Apply for Device Permission</u>• <u>Release the Permission for Devices</u>

Module	Function(s)
	<ul style="list-style-type: none"> • <u>Migrate Devices from Hik-Connect Account</u> • <u>Enable Device to Send Notifications</u> • <u>Upgrade Device</u> • <u>Configure DDNS for Devices</u> • Manage AX Pro Security Control Panel (Hereafter Simplified as AX Pro) <ul style="list-style-type: none"> ◦ <u>Control AX Pro</u> ◦ <u>Configure AX Pro</u> ◦ <u>Batch Arm/Disarm AX Pro</u> • <u>Remote Configuration</u> • <u>Reset Device Password</u> • <u>Unbind a Device from Its Current Account</u> • <u>Network Switch Management</u>
Video	<ul style="list-style-type: none"> • <u>View Live Video</u> • <u>Play Back Video Footage</u>
Tool	Use Tools Including: <ul style="list-style-type: none"> • Disk Calculator • NVR Channel Calculator • Focal Length Calculator • Bandwidth Calculator

Table 1-3 Countries and Regions That Only Support Free Basic Functions

Continent	Country/Region (Listed in Alphabetical Order)
Africa	Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo(Brazzaville), Congo(Kinshasa), Cote D'Ivoire, Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Guinea, Guinea-Bissau, Liberia, Madagascar, Malawi, Mali, Mayotte, Mozambique, Namibia, Niger, Nigeria, Rwanda, Senegal, Seychelles, Sierra Leone, Somalia, Tanzania, Togo, Uganda, Zambia, Zimbabwe
Asia	Japan, Taiwan (China)

1.3.2 Functions Only Available in Certain Regions

The following table shows the value-added functions only available in certain countries and regions.

 **Note**

For details about whether your country or region supports functions contained in the value-added services listed below, refer to the after sales or local distributor.

Service	Function(s) Only Available in Certain Countries and Regions
Health Monitoring Service	<p><u>Add Linkage Rule</u></p> <p> Note Linkage Rule is not available in the United States and Canada.</p>
Cloud Storage Service	All Functions Contained in the Service
People Counting Service	All Functions Contained in the Service
Temperature Screening Service	All Functions Contained in the Service
Access & Attendance Service	All Functions Contained in the Service
Alarm Receiving Center (ARC) Service	All Functions Contained in the Service
Employee Account Add-On	All Functions Contained in the Service

1.4 Download the Mobile Client

You can download Hik-ProConnect Mobile Client via the Portal, QR code, and app stores.

iOS System

The ways listed below are available to iOS system.

- Portal: Visit <http://www.hik-proconnect.com> , click  at the top right of page, and use your mobile phone to scan the QR code in the box to download the Mobile Client.
- QR Code: Scan the QR code below to download the Mobile Client. Using a browser to scan the QR code is recommended.
- App Store: Search Hik-ProConnect Mobile Client in the App Store to download the Mobile Client.



Figure 1-1 QR Code

Android System

The ways listed below are available to Android system.

- Portal: Visit <http://www.hik-proconnect.com> , click  at the top right of page, and use your mobile phone to scan the QR code in the box to download the Mobile Client.
- QR Code: Scan the QR code below to download the Mobile Client. Using a browser to scan the QR code is recommended.
- Google Play: Search Hik-ProConnect Mobile Client in Google Play to download the Mobile Client.
- Galaxy Store: Search Hik-ProConnect Mobile Client in Galaxy Store to download the Mobile Client.
- HUAWEI AppGallery: Search Hik-ProConnect Mobile Client in HUAWEI AppGallery to download the Mobile Client.
- OPPO App Market: Search Hik-ProConnect Mobile Client in OPPO App Market to download the Mobile Client.
- VIVO App Store: Search Hik-ProConnect Mobile Client in VIVO App Store to download the Mobile Client.
- Xiaomi GetApps: Search Hik-ProConnect Mobile Client in Xiaomi GetApps to download the Mobile Client.



Figure 1-2 QR Code

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.

Note

For the countries and regions only with support for free functions, only Installer Admin is available. For details about free functions and these countries and regions, see **Regions Only With Support for Free Functions** .

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:** You should first register an Installer Admin account before accessing any functions of Hik-ProConnect. For details, refer to **Register an Installer Admin Account** .
- **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 by Hik-Connect Account

If you already have a Hik-Connect account, you can register a Hik-ProConnect account by the Hik-Connect account.

Before You Start

- Make sure you have registered a Hik-Connect account.
- Make sure the Hik-ProConnect account to be registered is in the same region with the Hik-Connect account.

Steps

1. Enter the login page of Hik-ProConnect Mobile Client.
2. Tap Hik-Connect on the lower side of the page.
You will enter authorizing and logging page.
3. Authorize Hik-ProConnect to get the account information of Hik-Connect.

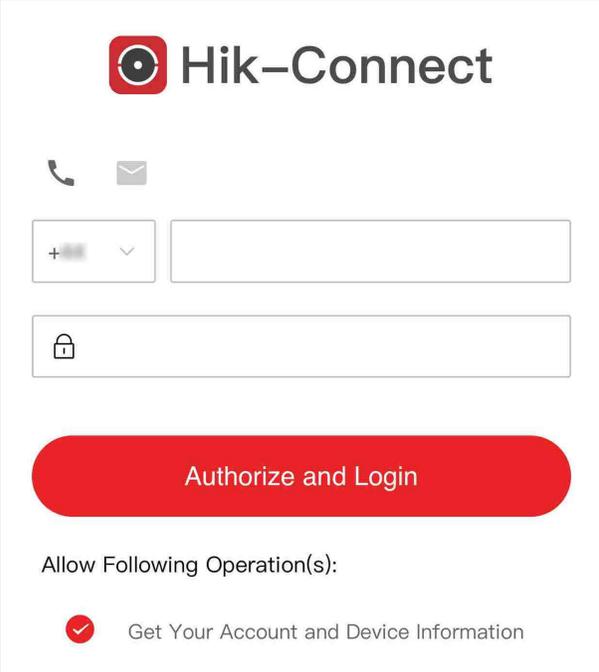


Figure 2-2 Authorize and Login

- Enter your phone number and password for authorization.
- Enter your email address/user name and password for authorization.

Note

You should check **Get Your Account and Device Information** to allow Hik-ProConnect to get these information.

-
4. Tap **Authorize and Login**.
 5. Register the Hik-ProConnect account.

Welcome to Hik-ProConnect

Please confirm the information below is completed.

Country/Region
Singapore

Email
Always Log in by this Email

Verification Code [Get Verification Code](#)

Password
Use a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.

Company Name

Phone Number
+86 > 18888188475

Start

Figure 2-3 Register Page

 **Note**

Country/Region information is filled by default.

1) **Optional:** Enter the email address.

 **Note**

- The email address will be filled by default if you have entered previously during authorization.
 - You can use this email address for logging in to Hik-ProConnect Mobile Client.
-

2) **Optional:** Tap **Get Verification Code**, and enter the received 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.

3) Enter the password 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.

4) Enter your phone number.

 **Note**

The phone number will be filled by default if you have entered it in Step 3 during authorization.

5) Enter your company name.

6) Enter the authentication code.

 **Note**

If you don't know how to get authentication code, you can tap **How to get authentication code?** for details.

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.**

8) Check **I agree to the Terms of Service and Privacy Policy** if you accept these agreements.

6. Tap **Start**.

7. **Optional:** Migrate devices in your Hik-Connect account to the Hik-ProConnect account.

 **Note**

For details, refer to ***Migrate Devices from Hik-Connect Account*** .

What to do next

On the login page, enter the email address and password to log in to Hik-ProConnect Mobile Client.

2.2 Register an Installer Admin Account

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

Steps

1. Tap  to start the Mobile Client.

The Login page will show.

2. If you start the Mobile Client for the first time, select the your country/region of your company and then tap **OK**.



Note

You cannot change the selected country/region after registration.

3. Tap **Enter Hik-ProConnect** to enter the Login/Register page.
4. Enter an email address to be bound with the Installer Admin account, and then tap **Next**.



Note

- If the account has not been registered, an email containing the verification code will be sent to the email address you entered.
- If the account has been registered, you will enter the Login page.

5. Enter the verification code you have received.



Note

- If you don't enter the verification code within the required time, you can tap **Resend** to get the verification code again.

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. Complete other required information, such as company name, address, and city.
8. **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*.

9. **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.

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

11. Tap **Start**.

Result

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

What to do next

- After registering an Installer Admin account, you should select your identity according to your actual role.
- 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. For details, refer to **[Complete Your Company Information](#)** .

2.3 Complete Your 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.

Steps

Note

If you didn't enter an authentication code when registering an Installer Admin account, you needn't to complete the company information.

- 1.** Enter the name of your company.
 - 2. Optional:** Enter the website of your company.
 - 3.** Enter your address line.
 - 4.** Enter the city of your company.
 - 5.** Enter an email address which will be bound with the Installer Admin account after registration.
 - 6.** Enter other information of your company, such as state/province/region, and postal code.
 - 7.** Enter your phone number.
 - 8.** Enter the VAT number.
-

Note

If you have entered the authentication code which is used for authenticating that you are a professional installer when you register an installer admin account, you should enter the VAT number.

9. Tap **Finish**.

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

2.4 Authenticate Your Account

When registering an Installer Admin account, you can enter an authentication code which is used for authenticating that you are a professional installer. If you did not enter an authentication code when registering your account, you can use the basic features in Hik-ProConnect first, and authenticate your account later. Before your account is authenticated, you cannot purchase value-added services.

One of the following ways for account authentication is supported, depending on your country or region.

By Entering Authentication Code

For this way, you need to get an authentication code from Hikvision or the distributor first, and then enter the authentication code to authenticate your account.

1. Go to **Me** → **Authenticate Now** .
2. (Optional) If you have no authentication code, tap **Get Authentication Code**, and send the application email with the predefined content template, including your email address (the one used when registering your Installer Admin account) and company information, such as company name, VAT No., and phone number, to Hikvision or the distributor to apply for an authentication code.

Note

If the email server is not configured or the recipient's address is not filled automatically, you can copy the content and send it to Hikvision or distributor by your own email box.

3. Enter the authentication code on account authentication page, and tap **Authenticate Now** to authenticate your account.

By Submitting Online Application

You can fill and submit the online application information to authenticate your account directly. After your application is approved, your account will be authenticated.

1. Go to **Me** → **Authenticate Now** .
2. Select your identity type.
3. (Optional) Edit your company information, such as company name, address, city, and province/state/region.
4. Tap **OK**.
5. Tap **Authenticate Now**.
The application information will be sent.

2.5 Link Your Account to a Distributor

You can use the Mobile Client to scan the Hik-ProConnect QR code shared by a distributor to link your account to the distributor. Once the two are linked, you can contact the distributor to get support if you have problems using Hik-ProConnect.

Note

- This function is only supported in certain countries and regions.
- If you registered your account via the registration link shared by a distributor, your account is linked to the distributor by default.

Before linking, contact the distributor to get the Hik-ProConnect QR code, and then tap  in the upper-right corner of the Home page to scan the QR code to complete linking. Or go to **Me → Distributor** , and then scan the QR code.

Once the linking is established, the distributor name will be displayed in the Distributor field on the Me page.

Chapter 3 Login

After logging in by an Installer Admin account, or 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. For the first time to start the Mobile Client, select the country/region where your account locates and tap **OK**.
3. Tap **Enter Hik-ProConnect** to enter the Login/Register page.
4. Enter the registered email address, and then tap **Next**.



Note

- If the account has not been registered, an email containing the verification code will be sent to the email address you entered. Refer to **Register an Installer Admin Account** for more details.
- If the account has been registered, it will go to the Login page.

-
5. Enter the password.
 6. **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.

7. Tap **Enter Hik-ProConnect**.

 **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 authentication 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 five 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 tools, recently visited Sites, 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.
Business	<p>There are four types of services in the Service Market. You can tap a specific service package to view its details, activate the service, or use the activated service.</p> <p> Note You should purchase the service package via the Hik-ProConnect Portal. For details, refer to <i>User Manual of Hik-ProConnect Portal</i>.</p>
Me	<p>View Account Information: You can view the information of the current account, including name and authentication status (Authenticated and Not Authenticated).</p> <p> Note You can edit the account information via the Hik-ProConnect Portal. For details, refer to <i>User Manual of Hik-ProConnect Portal</i>.</p>

Module	Description
	<p>More: You can view three services including Health Monitoring, Employee Management, and Access & Attendance. Tap a service to view the service details, and tap Send Email to get quick access to the service.</p> <p> Note These services are not available on the Mobile Client.</p> <hr/> <p> : Tap  to enter Settings page.</p> <ul style="list-style-type: none"> • Change Password: Change the password of the current account. <p> 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.</p> <ul style="list-style-type: none"> • About: You can view the version of the current platform, unsubscribe from marketing communications, and read the agreements including legal terms, privacy policy, and open source license. <p> Note After unsubscription, you will not receive any emails about marketing communications from Hikvision.</p> <ul style="list-style-type: none"> • Logout: Log out of the current account and return to the login page. <hr/> <ul style="list-style-type: none"> • Companies → Company Information: View company information, including company ID, country/region, address, email, etc. Tap  in the upper-right corner to edit company information if needed. <p> Note Some information cannot be edited such as company name or address.</p> <ul style="list-style-type: none"> • Companies → Co-Branding: This function helps to enhance brand awareness and improve your product and service. After enabled, the end users can view your company logo, address, and phone number via Hik-Connect Mobile Client. <hr/> <p>Tools: You can use online tools to improve your work efficiency.</p> <hr/> <p>Tutorial Center: You can view video tutorials to learn more about Hik-ProConnect and the proper ways of using the product.</p>

Module	Description
	<p>Marketing Communications: For Installer Admin, if you didn't subscribe to marketing communications when registering the account, you can subscribe here. After subscription, we will send emails about the 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 on the  → About page. After unsubscription, you will not receive any emails about marketing communications from us.</p>
	<p>Wizard: You can view the detailed explanations and operation guidance of some important functions of Hik-ProConnect Mobile Client. Follow the guidance as prompted to add a Site, add a device, configure a device remotely, view live view of the device, etc.</p>
	<p>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.</p>
	<p>Feedback: If you have any questions or suggestions about the platform, you can submit feedback to us.</p> <ol style="list-style-type: none">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. Tap Submit.

Home Page Introduction

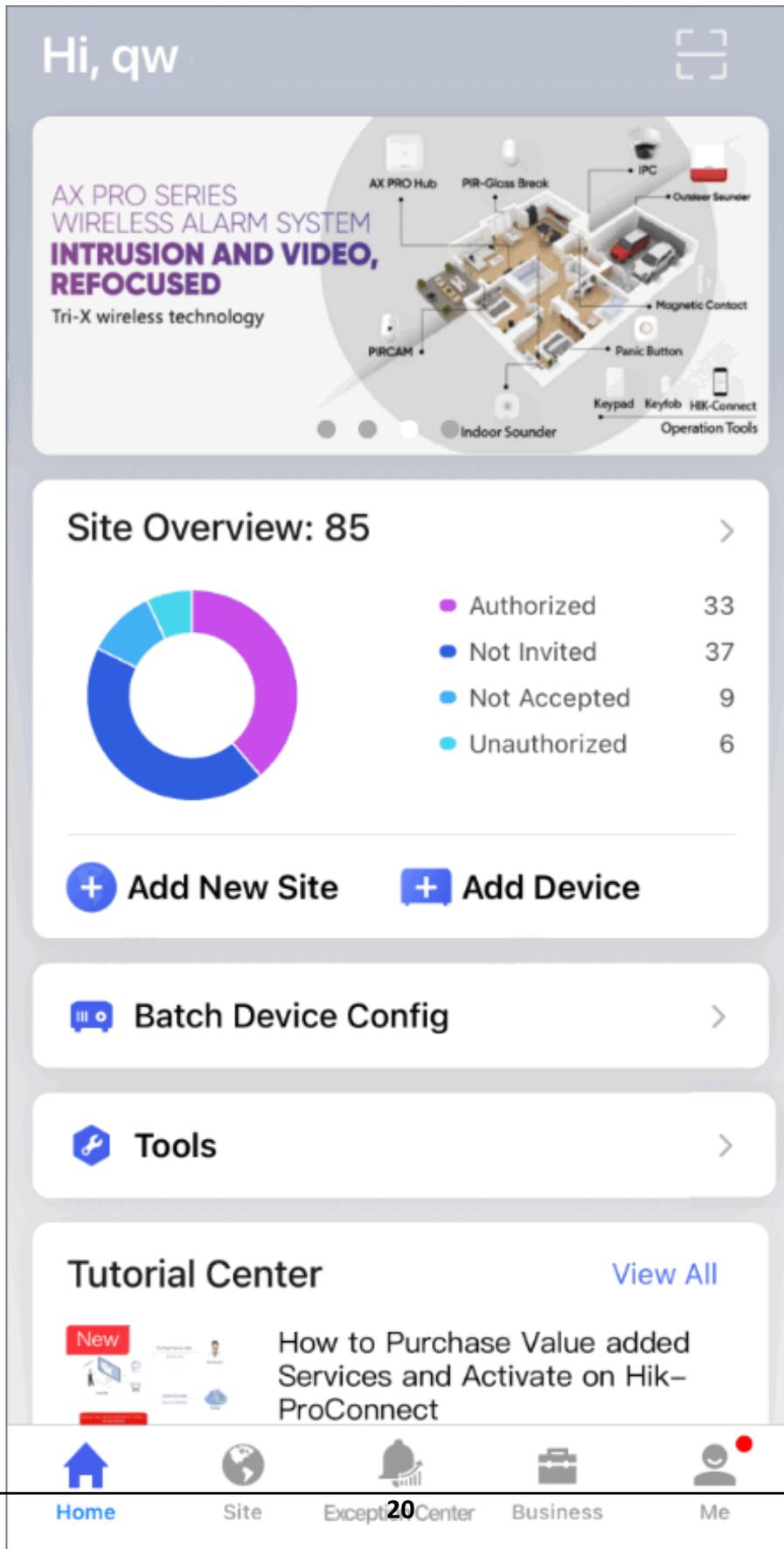


Figure 4-1 Home Page

Table 4-2 Home Page Description

Name	Introduction
	<p>You can scan the QR code to add a device, add a Site, view marketing communications information, etc. Tap  on the top right corner to view the details about different types of QR codes and their functions.</p> <ol style="list-style-type: none"> 1. Scan the QR code generated by Hik-Connect which contains the Site information to add a Site. For details about adding a Site, refer to <i>Add New Site</i> . 2. Scan the QR code on the device to add it. For details about adding device, refer to <i>Add Device by Scanning QR Code</i> . 3. Scan the QR code generated by iVMS-4200 or iVMS-4500 to add multiple devices. For details about adding devices, refer to <i>Add Device by Scanning QR Code</i> . 4. Scan other QR codes such as the QR code of marketing communications and enter the related webpage for more operations.
Banner	<p>There are some banners, showing the key features, functions, and important information of Hik-ProConnect.</p> <p> Note</p> <p>You can inform your end users to download or update the Hik-Connect Mobile Client (Version 4.13.0 and later) by sending the QR code or download link to them.</p>
e-Partner	<p>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:</p> <ul style="list-style-type: none"> • 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. <p> Note</p> <p>This function is only supported in some countries and regions.</p>
Site Overview	<p>You can view the total number of Sites and the corresponding number of Sites in different status which include:</p>

Name	Introduction
	<ul style="list-style-type: none"> • Authorized: The number of Sites which are authorized to you. • Not Invited: The number of Sites for which no Site owners are invited. • Not Accepted: The number of Sites of which the Site owners' invitations are not accepted. • Unauthorized: The number of Sites which have handed over to customers (i.e., the end users) but not get authorization from customers. <p> Note</p> <p>You can tap > to enter the Site list. For details about Site management, refer to <u>Manage Site</u> .</p> <p>You can tap Add New Site to add a new Site for managing the devices. For details, refer to <u>Add New Site</u> .</p> <p>You can tap Add Device to manually add devices to a Site or add by scanning the QR codes on the devices. For details, refer to <u>Add Device</u> .</p>
Batch Device Configuration	You can batch activate devices, batch add channels to NVR or DVR, and batch set device parameters. For details, refer to <u>Batch Configure Devices on LAN</u> .
Tools	You can use online tools to improve your work efficiency. Tap Tools to view all the provided tools.
Exception Notification	You can view the number of received exceptions and the proportions of each type of the exceptions.  Note
	<ul style="list-style-type: none"> • To receive exception notifications, you need to configure the recipient when setting the exception rule. For details, refer to <i>Hik-ProConnect Portal User Manual</i>. • The number of exceptions you view here may not be the same as that in Exception Center. You can tap > to enter Exception Center to check the received exceptions. For detailed instructions about Exception Center, refer to <u>Exception Center</u> .
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 been sent to end user who has not registered a Hik-Connect account.

Not Accepted

The invitation has been sent but not been 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.

< Add Site

Add Site

Add New Site >

*Site Name

New Site_20210107

*Time Zone

(UTC+08:00) Beijing, Chongqing, Hong Kong, Uru... >

Time zone cannot be edited after adding the site.

Scene

Not Selected >

Address

Enter street and number, P.O. box, c/o.

Enter apartment, suite, unit, building, floor, etc.

City

Enter city.

State/Province/Region

Enter state, province, or region.

Sync Time & Time Zone to Device

OK

Figure 5-1 Add New Site

 **Note**

- If an existing Site of end user is not authorized to any installation companies, you can tap **Add Existing Site** to add the existing Site.
- If you have no permission of adding new Site, when you tap **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, scene, 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.
- The Installer can select different configuration plan for the Site and devices according to the selected scene.

-
- 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.** Tap **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 [Device Management](#) .

5.3 Add Existing Site

If a Site was previously deauthorized from an Installer and currently not authorized to another, you can add it to the site list by using Site ID and applying for site authorization from the Site Owner.

Steps

1. Tap **Site** tab to enter Site page.
2. Tap  .
3. Select **Add Existing Site** as the adding method.

Figure 5-2 Add Existing Site

4. Enter the Site ID or scan the QR code of the Site.

 **Note**

- You can get the Site ID from the Site Owner, who can view and share the Site ID and QR code in Deauthorized Devices via Hik-Connect Mobile Client.
- Please inform your customer to download or update the Hik-Connect Mobile Client (Version 4.13.0 and later).

5. Click **OK**.

The Site will be added to the site list and the Site Owner will receive an application. After the Site Owner approves the application, the Site will be authorized to 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**.

If the check-box is checked, after you hand over the Site to your customer and your customer approves the request, you can disable Hik-Connect service for devices that you rent to your customer without her/his authorization. If Hik-Connect service is disabled, your customer cannot operate on these devices via the Hik-Connect Mobile Client.

Note

You can go to the **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 your customer's Hik-Connect account without her/his authorization.

-
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. **Optional:** Check **Apply for Activation of Time & Attendance Service**.

If the check-box is checked, after you hand over the Site to your customer, he/she will be able to use the Access & Attendance system provided by Hikvision or third-party manufactures.

Note

- If the Access & Attendance system provided by Hikvision has been added to the Site and activated, the check-box will appear on the Invite Site Owner page.
 - If the Access & Attendance service is provided by a third-party manufacturer, the check-box will be **Allow ### System to Access** or **Allow Third-Party Access & Attendance System to Access**. ### here refers to the name of the third-party manufacturer.
-

8. 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.
9. 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 4.13.0 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.
10. **Optional:** Before your customer 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.

3. Optional: On the Site Details page, tap  → **Discard Authorization** to discard authorization or the Site.

Note

For Sites with Allow Me to Disable Hik-ProConnect Service function enabled when handing over to Installer, discarding authorization is not supported.

Chapter 6 Device Management

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 parameters, 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 the Portal.

 **Note**

Some features may not be available in all countries or regions.

6.1 Batch Configure Devices on LAN

You can batch configure online devices on the same Local Area Network (LAN) with the phone on which the Hik-ProConnect Mobile Client runs. The available configurations include batch device activation and device IP address assignment, batch linking channels to NVR/DVR, and batch setting parameters for devices via templates. These functions allow you to complete basic configurations for multiple devices with much less efforts compared with configuring devices one by one.

 **Note**

- The functionality is only available for camera and NVR/DVR.
 - Before batch configuring devices, make sure you have connected them to the same LAN with the phone on which the Hik-ProConnect Mobile Client runs.
-

The flow chart for batch configuration of devices is shown below.

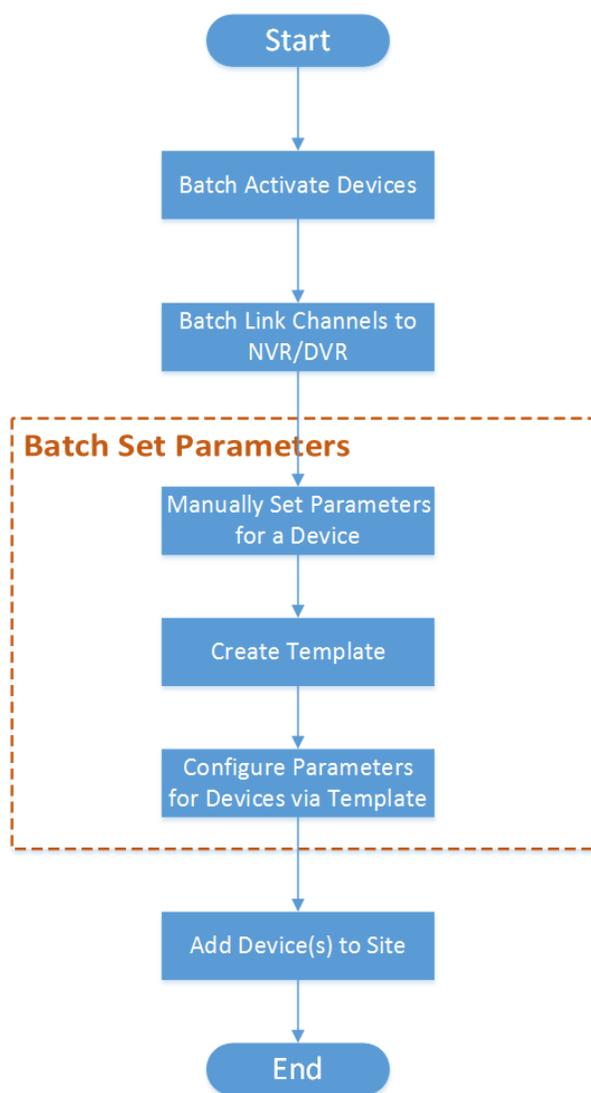


Figure 6-1 Flow Chart

Table 6-1 Flow Chart Description

Step	Sub-step	Description
Batch Activate Devices	N/A	Batch activate online devices on the same Local Area Network (LAN) with the phone on which the Hik-ProConnect Mobile Client runs, and assign IP addresses for the activated devices. See <i>Batch Activate Devices and Assign IP Addresses for Them</i> for details.
Batch Link Channels to NVR/DVR	N/A	If the activated devices include NVR/DVR, link channels to NVR/DVR. See <i>Batch Link Channels to NVR</i> for details.

Step	Sub-step	Description
Batch Set Device Parameters	Manually Set Parameters for a Device	Select an activated device and set its parameters manually. See <i>Create Templates for Setting Parameters</i> for details.
	Create Template	Created a template based on the manually configured device. See <i>Create Templates for Setting Parameters</i> for details.
	Configure Parameters for Devices via Template	Batch configure parameters for multiple devices via a selected template. See <i>Batch Set Parameters for Devices</i> for details.
Add Device(s) to Site	N/A	If required, add the activated and configured device(s) to a Site. See <i>Add Device by Scanning QR Code</i> , <i>Add Device by Hik-Connect (P2P)</i> , or <i>Add Device by IP Address or Domain Name</i> for details.

6.1.1 Batch Activate Devices and Assign IP Addresses for Them

The Mobile Client can detect available devices connected to the same network with the client, and you can activate devices and assign IP address for them.

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 **Batch Device Configuration** to enter the batch device configuration page.
2. Select the detected online devices to be activated.
3. Tap **Activate Devices & Assign IP** to open the Activate Devices & Assign IP window.
4. Enter the device admin password and confirm the password.
5. Tap **Activate Device & Assign IP**.

Note

- The unactivated device and the activated device but not be assigned with IP address will be displayed as **Not Obtained** in the **Device Name** column.
 - For the activated device and be assigned with IP address, if you hover the mouse on the IP address, **Auto** will be displayed to remind you the IP address is automatically assigned.
-

The devices are activated, and the device IP address, device port, HTTP port, subnet mask, gateway are assigned by the client.

The time of the mobile phone will be synchronized to the activated devices.

6. Optional: Enable **Time Synchronization** to synchronize the time from the mobile phone to the device.

7. Tap **OK**.

What to do next

After activating the devices, you should batch add channels to NVR. For details, refer to [**Batch Link Channels to NVR**](#) .

6.1.2 Batch Link Channels to NVR

If there are online NVR and network camera on the same LAN, you can batch link the network cameras to the NVR as channels. After linking, you can manage the linked channels according to your need.

Before You Start

Make sure you have activated the NVR and network cameras. See for details.

Steps



If there is no online NVR on the same LAN, skip this task.

1. On the Link Channel page, tap the NVR to enter its details page.



If you have not logged in to the device, enter the password to log in.

2. Enter the Link Channel page.

- Select the NVR and tap **Link Channel**.
- Tap the NVR name.

3. In the available device list, select a device and tap **+** to link the device.

The linked channel will be displayed in the linked channel list.

4. Optional: On the NVR details page, perform the following operations.

Edit NVR Name On the top of NVR details page, tap **Rename** to edit the NVR name.

Sort Channels Select a channel, press **≡** and drag to change its position.

Replace Device Select a channel and swipe left. Tap **Replace Device** to unlink this channel and link a new device.

Unlink Device Select a channel and swipe left. Tap **Delete** to unlink channel.

6.1.3 Create Templates for Setting Parameters

Before batch configuring parameters for devices, you should create a template. After creating a template, you can batch apply it to other devices.

Before You Start

Make sure you have activated devices and linked channels to NVR (if any). See [**Batch Activate Devices and Assign IP Addresses for Them**](#) and [**Batch Link Channels to NVR**](#) for details.

Steps

1. In the Parameter Template field of Configuration page, select an NVR and tap **⋮** → **Parameter Configuration** to enter the remote configuration page.
2. On the remote configuration page, set parameters for the device.
3. Tap **Save as Template** on the top right.
4. Select parameters you want to save in the template and tap **Next**.
5. Enter the template name and tap **Complete** to save the template.
6. **Optional:** Add a new template based on device with configured parameters.
 - 1) In the Parameter Template field of Configuration page, tap **Show All** to enter the Manage Template page.
 - 2) Tap **Create Template**.
 - 3) Select a device of which the parameters will be saved as the new template, and tap **Next**.
 - 4) Select the parameters you want to save in the template, and tap **OK**.
 - 5) Enter template name and tap **Complete** to create the template.
 - 6) **Optional:** On the Manage Template page, select a template and swipe left, and tap **Delete** to delete a template.

6.1.4 Batch Set Parameters for Devices

To configure devices with high efficiency, you can batch apply parameters in an existing template to devices.

Before You Start

Make sure you have created at least one template for setting parameters. See [**Create Templates for Setting Parameters**](#) for details.

Steps

1. Enter the Select Template page.
 - Select a device and tap **⊞**.
 - Select a device and tap **⋮** → **Set Parameters by Template**.
2. Select a template and tap **Apply Parameters**.

The application process and application results will be displayed.
3. **Optional:** Perform the following operations.

Add Device to Site Tap **Complete** on the top right and add devices to Sites. See [**Add Device**](#) for details.

Manage Template Tap **Show All** to enter the Manage Template page. You can add new template or delete template. See [**Create Templates for Setting Parameters**](#) for details.

Edit NVR Name Select an NVR, and tap **⋮** → **Rename** to edit name of NVR.

Synchronize Phone Time to Device On the top of Parameter Configuration page, tap **Synchronize** to synchronize the mobile phone time to all devices.

6.2 Add Device

Hik-ProConnect accesses devices by two modes: Hik-Connect (P2P) and Device IP Address/Domain Name. The former provides securer data communication (between the platform and devices) and full access to features based on the Hik-Connect service, such as device handover and exception notification; the latter provides faster data communication but no access to the features based on the Hik-Connect service.

The table below shows the device adding methods for the two access modes respectively.

Table 6-2 Device Adding Methods

Access Mode	Device Adding Method
Hik-Connect (P2P)	<ul style="list-style-type: none"> • <u>Add Device by Scanning QR Code</u> • <u>Add Device by Hik-Connect (P2P)</u> • <u>Add Devices Without Support for the Hik-Connect Service</u> <p> Note</p> <p>The last method in this table cell is for devices which do not support the Hik-Connect service. In this method, you can add them via the proxy of Hik-ProConnect Box to allow them access the features based on the Hik-Connect service.</p>
Device IP Address/Domain Name	<u>Add Device by IP Address or Domain Name</u>

6.2.1 Add Devices After Batch Configuring Them on LAN

After batch configuring devices, you can batch add these devices to the Mobile Client.

Before You Start

Make sure you have batch configured devices. For details, refer to **Batch Configure Devices on LAN**.

After you batch configured devices, a prompt pops up about whether to add devices or not. Tap **OK** to enter adding devices page.

Steps

1. Select a Site as the target to which devices will be added.

Note

You can select an existing Site, or you can add a new Site. For details about adding a new Site, refer to ***Add New Site*** .

2. Select the device(s) to be added.
 3. Tap **Next**.
 4. Batch enter the device password, and tap **Complete**.
-

Note

The password will be applied to all the devices to be added. You can also edit the password for single device.

5. Tap **Next**.

If there is a wrong password prompt, you can edit the password as prompted, or you can skip the prompt and go to the next step.
 6. Configure device verification code.
 - Tap **Configure Verification Code**, and batch configure a verification code for all the devices.
-

Note

You can customize the verification code as needed.

- Tap **Enter Verification Code**, and enter the verification code for each device to be added.
-

Note

You can get the verification code from the bottom of the device.

7. Tap **Next**.

Device compatibility test starts.
-

Note

Only when all devices' compatibilities have been tested, can you add them to Hik-ProConnect.

8. Add devices.
-

Note

For details about adding devices, see ***Add Device*** .

- If there are no upgradable devices, tap **Add** to add the selected devices.
 - If there are upgradable devices, tap **Add and Upgrade** to add all devices and upgrade the upgradable devices.
-

Note

- If there are devices that failed to be upgraded, you can tap **Details** to view failure details.
 - Devices that failed to be upgraded can also be added to the target Sites.
-

6.2.2 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.
-

6.2.3 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. Enter the scan page.
 - Tap **Add Device** in the Site Overview area on the home page.
 - Tap **Site** in the navigation, and then tap a Site to enter its details page and tap **Add Device**.
2. 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.

3. If you have not added the device(s) to a Site, tap **Add to Site** to select a Site to which the device(s) need to be added.

You can add device(s) to an existing Site, or enter Site ID or scan the Site QR code shared by your customer to add the device(s) to a new Site.

 **Note**

Skip this step if you have added these device(s) to a Site.

4. 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 4.13.0 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**

- After the device is added, 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.
- After you add an AX Pro device to Hik-ProConnect, you will be able to log into the AX Pro by your Hik-ProConnect account (i.e., Installer account or Installer Admin account) to configure and manage the device; if you delete the AX Pro device from Hik-ProConnect, you can no longer log into the AX Pro device by your Hik-ProConnect account.
- After your customer authorizes a Site with AX Pro devices to you, you can log into these AX Pro devices by your Hik-ProConnect account to configure and manage the device. In this case, if you are an Installer, the Installer Admin can also log into these AX Pro devices by her/his Hik-

ProConnect account; if you are the Installer Admin, your employees (i.e., Installers) have no permission to log into these devices by their Hik-ProConnect accounts.

- After you hand over a Site with AX Pro devices to your customer, your customer will be able to log into these devices by her/his Hik-Connect account, and you will no longer have the permission to log into these devices by your Hik-ProConnect account.

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

Activate Health Monitoring Service Tap **Activate Health Monitoring Service** on the adding result page to activate the health monitoring service. See ***Activate the Health Monitoring Service*** for details.



If the service is not activated, some features such as device health monitoring and device exception notification will be unavailable.

Remote Configuration Tap the device and then tap  to remotely configure its parameters.



- 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.



Deleting device is not supported if the site is authorized (except devices added by IP/Domain).

- 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**.
-



It is highly recommended that you encrypt the device QR code for security reasons.

- c. Tap **Save** to save the generated QR code in your phone.
-

Set Type for Unknown Device	<p>If the Hik-ProConnect cannot recognize a device's type after you add it, you can manually set a device type for it.</p> <ol style="list-style-type: none">Enter a device details page, tap  of the Device Type to enter the Device Type page.Select a type for the device. <p>You can edit it again after the selection.</p>
Edit Device Information	<p>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.</p> <p>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.</p>

6.2.4 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

- Enter the scan page.
 - Tap **Add Device** in the Site Overview area on the home page.
 - Tap **Site** in the navigation, and then tap a Site to enter its details page and tap **Add Device**.
- Tap **Manually Add** to enter the manual adding page.
- 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.

- If you have not added the device to a Site, tap **Add to Site** to select a Site to which the device needs to be added.

You can add the device to an existing Site, or enter Site ID or scan the Site QR code shared by your customer to add the device to a new Site.

Note

Skip this step if you have added these device(s) to a Site.

- Tap **Add**.

 **Note**

- 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.
- After you add an AX Pro device to Hik-ProConnect, you will be able to log into the AX Pro by your Hik-ProConnect account (i.e., Installer account or Installer Admin account) to configure and manage the device; if you delete the AX Pro device from Hik-ProConnect, you can no longer log into the AX Pro device by your Hik-ProConnect account.
- After your customer authorizes a Site with AX Pro devices to you, you can log into these AX Pro devices by your Hik-ProConnect account to configure and manage the device. In this case, if you are an Installer, the Installer Admin can also log into these AX Pro devices by her/his Hik-ProConnect account; if you are the Installer Admin, your employees (i.e., Installers) have no permission to log into these devices by their Hik-ProConnect accounts.
- After you hand over a Site with AX Pro devices to your customer, your customer will be able to log into these devices by her/his Hik-Connect account, and you will no longer have the permission to log into these devices by your Hik-ProConnect account.

6. 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.

7. Optional: Perform the following operations if you need.

Operations	Description
Activate Health Monitoring Service	Tap Activate Health Monitoring Service on the adding result page to activate the health monitoring service. See <u>Activate the Health Monitoring Service</u> for details.

 **Note**

If the service is not activated, some features such as device health monitoring and device exception notification will be unavailable.

Delete Device On the device page, tap ● ● ● → **Delete** to delete the device.



Deleting device is not supported if the site is authorized (except devices added by IP/Domain).

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.

- Enter a device details page, tap  of the Device Type to enter the Device Type page.
- 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.



- 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 (P2P) support configuring DDNS.
-

6.2.5 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 Hik-ProConnect by specifying its IP address/domain name, user name, password, etc. Once a device is added in this way, Hik-ProConnect will generate a QR code containing the device information. After completing device setup, you can share the QR code to your customer. And then your customer can scan the QR code via the Hik-Connect Mobile Client to add the device to her/his Hik-Connect account.

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



- Devices added in this method do NOT support the device handover process. If you need to hand over a device to your customer after completing the device setup work, please add it in one of

following two methods: ***Add Device by Scanning QR Code*** and ***Add Device by Hik-Connect (P2P)***.

- Only encoding devices mapped in WAN support this function.
 - Ask your customers to download or update the Hik-Connect Mobile Client (Version 4.13.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.
-

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. If you have not added the device to a Site, tap **Add to Site** to select a Site to which the device needs to be added.

You can add the device to an existing Site, or enter Site ID or scan the Site QR code shared by your customer to add the device to a new Site.



Skip this step if you have added these device(s) to a Site.

6. Tap **Add**.
-



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.

7. **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	<ul style="list-style-type: none">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.

 **Note**

It is highly recommended that you encrypt the device QR code for security reasons.

- 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** .

6.2.6 Add Devices Without Support for the Hik-Connect Service

Some devices do not support the Hik-Connect service, and therefore they cannot be accessed by Hik-ProConnect via Hik-Connect (P2P). If they are accessed via device IP address/domain name, some features (such as health monitoring and exception rule) will be unavailable. To solve this issue, you can add these devices to Hik-ProConnect via the proxy of Hik-ProConnect Boxes. In this way, the originally unavailable features will be available.

Before You Start

Make sure that you have added Hik-ProConnect Boxes to Hik-ProConnect. For details, see [Add Device by Scanning QR Code](#) or [Add Device by Hik-Connect \(P2P\)](#) .

Steps

 **Note**

- Currently only some encoding devices and access control devices can be proxied by Hik-ProConnect Boxes. For detailed device models, see *Hik-ProConnect Device Compatibility List*.
- The proxied devices do not support features including ARC service, access & attendance service, temperature screening service, people counting service, and ISAPI alarm. For the proxied encoding devices, in addition to the above-mentioned features, linkage rule is also not supported.

1. Tap **Site** in the navigation, and then tap a Hik-ProConnect Box to enter its device details page.
2. Tap **Proxied Device**, and then tap  to enter the Select Devices page.
3. Add devices in one of the following two methods.

Table 6-3 Add Devices

Method	Description
Add Online Devices	Add devices on the same LAN with the PC where the Portal runs.

Method	Description
	a. Select devices, and then tap Next . b. Tap Batch Enter , select multiple or all devices, and then click Batch Verification to set a user name and a password shared by all devices. Or enter the device user name and password for each device. c. Tap Next .
Add Manually	Add a device manually. a. Tap Add Device to enter the Add by IP Address/Port No. page. Enter the device IP address and port No. b. Tap Add to add the device to the device list. Or tap Add More to add more devices. c. Select device(s) from the device list, and then tap Password Verification to enter the device user name(s) and password(s). d. Click Next .

The adding result page shows.

- 4. Optional:** If adding failures exist, view failure reasons on the adding result page and do corresponding operations.

Take failure caused by incorrect password for an example, you can tap > and then enter the password again.

- 5.** Tap **Next**.
6. If there are encoding devices, enable proxy for their channels.



Note

If you do not enable proxy for channels of encoding devices, you cannot view live video and video footage of these channels.

-
- 1) Tap **Proxied Channel(s)** to enter the Select Channel page.
 - 2) Turn on the switches to enable proxy for the channels, and then tap **OK**.

- 7.** Tap **Complete**.
8. Optional: View the proxy information on the device details page of the Hik-ProConnect Box.

Related Information Add Device

6.3 Activate the Health Monitoring Service

After purchasing health monitoring packages, you can use them to activate the health monitoring service for specific devices. Once the service is activated, features such as device health monitoring and device exception notifications will be available for these devices.

Before You Start

Make sure you have purchased health monitoring packages.



Contact the local distributor for details about whether your country/region supports service keys. If supports, you can purchase a service key from the distributor, and then go to the Service Market on the Mobile Client to purchase health monitoring packages by the service key. If doesn't support, go to the Service Market on the Portal to purchase health monitoring packages online first (see *Hik-ProConnect Portal User Manual* for details).

Steps



Multiple entries are available for activating the service, including:

- The result page of adding a device by scanning QR code or by Hik-Connect (P2P).
- The result page of batch adding devices.
- The device details page.

Here we only introduce activating the service via the last entry, i.e., the device details page.

1. Tap a Site to enter the site details page.
2. Tap a device to enter the device details page.
3. Switch on **Health Monitoring Service** to enter the Select Activation Type page.



If the firmware version of a device is obsolete, or its device type cannot be recognized by Hik-ProConnect, activating health monitoring service for the device is not supported

4. Set the number of months/years that the service lasts for each selected device, and set other parameters.

Use All Device Package Only

When enabled, you can only select All Device Packages (All Device Monthly Package or All Device Annual Package) for network cameras to activate the service for them.

Auto Renewal

When enabled, if the service for a device expires, the service will be automatically renewed using the same service package in previous activation. For example, assume that you activated a 1-month health monitoring service for a NVR using an All Device Monthly Package

on 5/14/2021, the 1-month service will be automatically renewed using another All Device Monthly Package on 6/14/2021.

The following list shows the description of each package type.

All Device Monthly Package

An All Device Monthly Package can be used to activate the service for almost all types of devices. And the activated service lasts one month.

"All Device" here means that the service package is applicable to nearly all device types, including DVR, NVR, network cameras, PTZ cameras, access control devices, alarm devices, video intercom devices, doorbells, Hik-ProConnect Boxes, thermal devices, and network switches.

"Monthly" here means that the service term is one month. The service term starts when you activate the service.

All Device Annual Package

An All Device Annual Package can be used to activate the service for a device of nearly any type. And the activated service lasts one year.

"All Device" here means that the service package is applicable to nearly all device types, including DVR, NVR, network cameras, PTZ cameras, access control devices, alarm devices, video intercom devices, doorbells, Hik-ProConnect Boxes, thermal devices, and network switches.

"Annual" here means that the service term is one year. The service term starts when you activate the service.

Network Camera Monthly Package

A Network Camera Monthly Package can be used to activate the service for a network camera. And the activated service lasts one month.

"Network Camera" here means that the service package is only applicable to network cameras.

"Monthly" here means that the service term is one month. The service term starts when you activate the service.

Network Camera Annual Package

A Network Camera Annual Package can be used to activate the service for a network camera. And the activated service lasts one year.

"Network Camera" here means that the service package is only applicable to network cameras.

"Annual" here means that the service term is one year. The service term starts when you activate the service.

5. Tap **OK**.

6. **Optional:** Go to the device details page to perform the following operations if needed.

View Service Expiry Date

View the service expiry date shown beside **Health Monitoring Service**.

Renew the Service	Tap Health Monitoring Service to renew the service for the device.
Enable Auto Renewing the Service	Switch on Auto Renewal , and then select a type of service packages for auto renewal.
Transfer the Service	Tap Transfer , and then select a device to transfer the remaining service time from the current device to the selected device.

6.4 Manage Device Permission

By inviting the Site Owner and applying for site authorization, you have already acquired some device permissions. You can still apply for additional device permissions afterward or release device permissions if needed.

6.4.1 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. Tap **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.

6.4.2 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**.
-

6.5 Migrate Devices from Hik-Connect Account

You can migrate the devices, including devices shared by others and the ones added by you, in your Hik-Connect account to the Hik-ProConnect account to provide better device management and maintenance services to your customers.

Steps

1. Go to **Site** → **Device Migration** .
2. Log in to your Hik-Connect account.

Note

Make sure to check **Get Your Account and Device Information** to allow Hik-ProConnect to acquire necessary information for device migration.

3. Select the devices you want to migrate and tap **Next**.
4. Configure Sites for the devices.
 - 1) Tap **Site Time Zone** to set the default time zone for Sites.
 - 2) Tap **My Devices** or **Others' Devices**.
 - 3) Tap **Allocate Device** to select device allocation mode.

Auto Allocate to Sites

For My Devices, this will create different Sites by the names of the accounts that you share devices with, and then allocate devices to these Sites accordingly.

For Others' Devices, this will create different Sites by the name of the accounts that share devices to you, and then allocate devices to these Sites accordingly.

Same Site

Allocate all devices to a single Site named by your Hik-Connect account.

- 4) View and edit the configurations of each Site. Tap on each Site to view or edit information such as Site name, time zone, devices to be migrated, and device permissions.
- 5) Tap **Finish** to save the settings.
5. Tap **Migrate** to start device migration.

Note

- For Others' Devices, the platform will send an application to the belonging accounts for device authorization. You will obtain device permissions and be able to configure, operate, and manage these devices in Hik-ProConnect upon approval.
- After migration, you can still manage the devices in your Hik-Connect account and access Hik-Connect services.

6. Optional: Tap **Activate Health Monitoring Service** to activate the health monitoring service for the migrated devices.

6.6 Linkage Rule and Exception Rule

You can set up a linkage rule to trigger certain device actions when the triggering event occurs. You can configure an exception rule to specify how, when, and where you want to receive exception notifications of a device or channel.

Note

Make sure you have enabled the Notification functionality of the source device of the linkage/exception rule. If the function is disabled, events detected by the device cannot be reported and thus the linkage/exception rule cannot be triggered.

6.6.1 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 predefined 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...), and 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, and saving evidence, when specific events happen.

The picture below shows the process of the linkage.

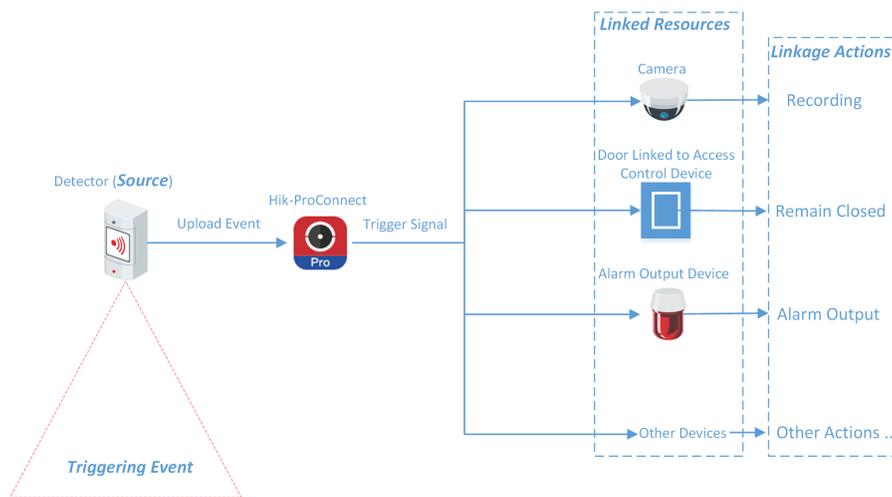


Figure 6-2 Linkage

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 sounder 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 following elements need to be defined in the linkage rule:

- Source: The PIR detector in the store.
- Triggering Event: Motion detection event.
- Linked Resources: The alarm output (the sounder in this case) and the network cameras in the store.
- Linkage Actions:
 - For sounder: The sounder sends out audible alarm.
 - For network cameras: The network cameras starts recording.
- Linkage Schedule: Non-work hours every day.

Add Custom Linkage Rule

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

Steps

Note

- 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 6-4 Available Triggering Events for Different Resource Types

Source	Triggering Event
Camera	<ul style="list-style-type: none"> • Motion Detection • Face Detection • Intrusion • Line Crossing Detection
Access Control Device	<ul style="list-style-type: none"> • Network Disconnected • Tampering Alarm
Door Linked to Access Control Device	<ul style="list-style-type: none"> • Door Opened Abnormally • Tampering Alarm
Door Station	<ul style="list-style-type: none"> • Calling
Area of Security Control Panel	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm.
Doorbell	<ul style="list-style-type: none"> 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 6-5 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	<p>The camera will record video footage when the Triggering Event is detected.</p> <p> Note</p> <p>The recorded video footage starts from 5 s before the detection of the Triggering Event, and lasts 30 s.</p>
	Call Preset	<p>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.</p> <p>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.</p> <p> Note</p> <p>Make sure you have configured presets for the PTZ camera. For details, see the user manual of the PTZ camera.</p>

Linked Resource	Linkage Action	Description
	Call Patrol	<p>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.</p> <p>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.</p> <p> Note Make sure you have configured patrols for the PTZ camera. For details, see the user manual of the PTZ camera.</p>
	Call Pattern	<p>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.</p> <p>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.</p> <p> Note Make sure you have configured patterns for the PTZ camera. For details, see the user manual of the PTZ camera.</p>
	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	<p>Privacy mask will be displayed on the live images of the camera when the Triggering Event is detected.</p> <p> Note Make sure you have configured privacy mask for the camera. For details, see the user manual of the camera.</p>
	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 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 4.13.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.
-

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 6-6 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 a door is opened abnormally.
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.
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.

Template	Description
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 tap **Add**.

Note

- You can only select only one linkage action.
 - For details about the linkage actions, see **Table 6-5**.
-

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.



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***.



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

Video Tutorial

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

6.6.2 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.

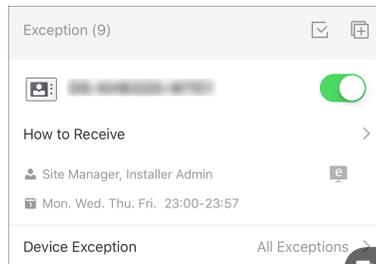


Figure 6-3 Add Exception Rule

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

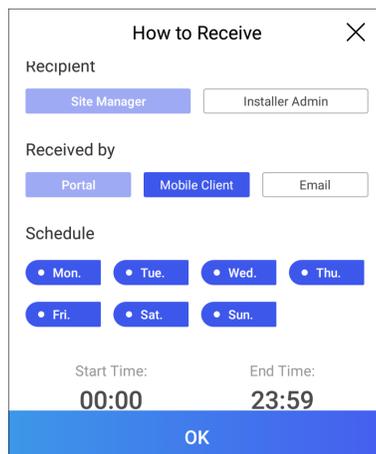


Figure 6-4 How to Receive

- 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) Tap **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) Tap **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) Tap **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 corner 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.

6.6.3 Enable Device to Send Notifications

After adding and enabling a linkage rule or exception rule, you need to 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. This 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 4.13.0 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.
-

6.7 Reset Device Password

You can reset the password of a device when you and the Site Owner both lost the password. Two methods of resetting device password are available: resetting password offsite and resetting password onsite.



Note

- Resetting password via Hik-ProConnect platform is not supported by every device type/model. For example, AX PRO 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*** .
-

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

Tap the device and then tap ● ● ● → **Reset Password** . There are two methods to reset the password.

- **Reset Password Offsite:** You needn't go to the Site where the device is located to reset the device password.

 **Note**

Make sure that Hik-Connect (the Mobile Client for your customers) and the device are on the same LAN and that the version of Hik-Connect is Version 4.13.0 and later.

Refer to the flow chart below for resetting the password offsite.

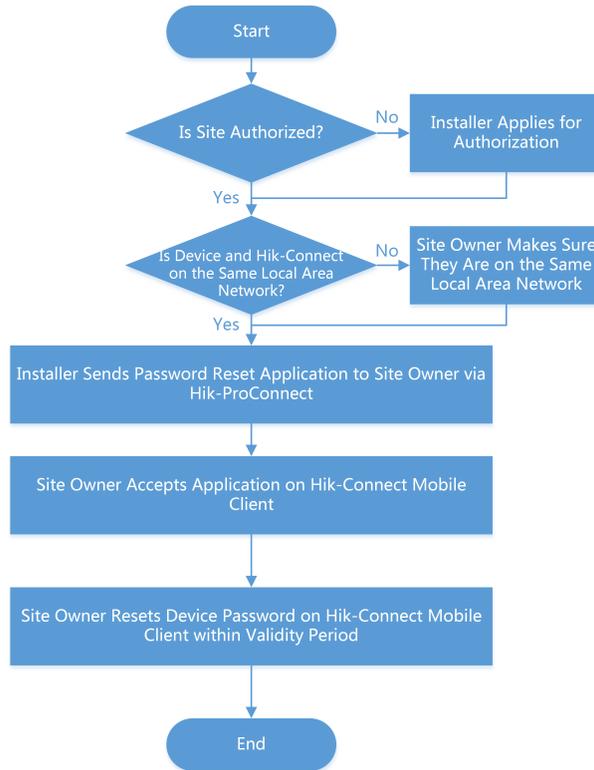


Figure 6-5 Flow Chart of Resetting Device Password Offsite

- **Reset Password Onsite:** You need to go to the Site where the device is located.
-

 **Note**

Make sure that Hik-ProConnect (the Installer platform) and the device are on the same LAN.

Refer to the flow chart below for resetting the password onsite.

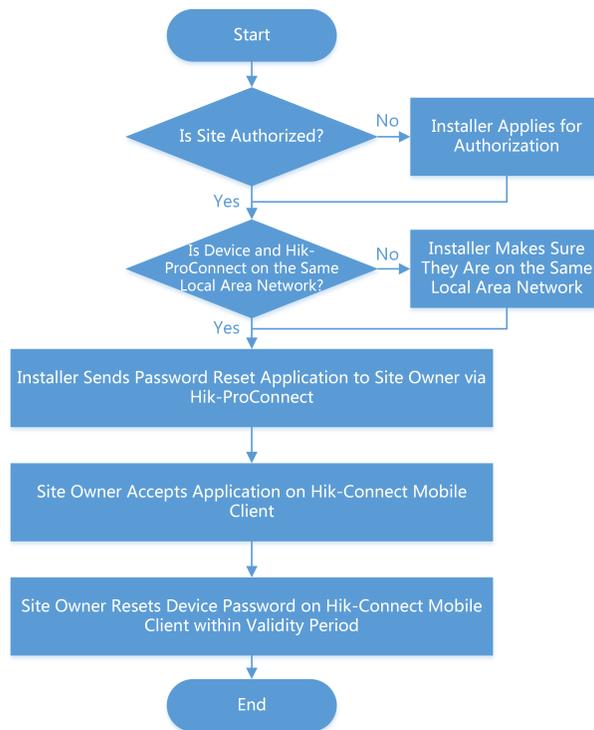


Figure 6-6 Flow Chart of Resetting Device Password Onsite

6.8 Manage Security Control Panel

You can add and manage AX Pro, AX Hub, and AX Hybrid security control panels on Hik-ProConnect.

Note

- The following chapter introduces functionality supported by AX Pro security control panel (hereinafter referred to as "AX Pro device"), such as batch arming/disarming.
 - AX Hub or AX Hybrid security control panel does not support the functionality introduced in the following chapter. AX Hub and AX Hybrid support generic device management, such as setting rules for linkage or exception reporting and enabling ARC service. For details, refer to ***Linkage Rule and Exception Rule*** and ***Alarm Receiving Center (ARC) Service***.
-

6.8.1 Control AX Pro

For AX Pro device, you can perform operations including adding area, arming/disarming area, clearing alarm, and bypassing zone.

Tap on an AX Pro device in a Site to enter its details page. On the device details page, you can perform the following operations.

Function	Operation
Add Area	Select the Area tab, and then tap  to add an area.
Stay Arm an Area	Select the Area tab, and then tap  to stay arm the area.
Away Arm an Area	Select the Area tab and then tap  to away arm the area.
Disarm an 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 <i>Add Device</i> .
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.

6.8.2 Configure AX Pro

On the Mobile Client, you can conduct remote operations on AX Pro device, such as starting walk test, setting DST (Daylight Saving Time), switching language, and upgrading device.

Tap on an AX Pro device in a Site to enter its details page. On the device details page, tap  to enter the settings page to remotely configure the device.

Configuration	Description
Start 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

Configuration	Description
	End Walk Test to view the test results: the status (normal or abnormal) will be displayed.
Set DST (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 device.
Upgrade and Switch Language	<p> Note Make sure you have the permission to access the device upgrade functionality. For details about permission settings for AX Pro, see the user manual of the device.</p> <p>Tap Project Maintenance → Device Upgrade to enter the device upgrade page. Then, select language and enter PIN code. Tap Upgrade to switch language for AX Pro and upgrade it.</p> <p> Note Tap Apply for PIN to apply for a PIN code.</p>
Other Configurations	<p>You can do other configurations including user management, system options configuration, linking network cameras, communication settings, etc.</p> <p> Note For details about other AX Pro configurations, see the user manual of the device.</p>

6.8.3 Batch Arm/Disarm AX Pro

You can batch arm or disarm multiple AX Pro devices in various Sites by grouping the devices.

Follow the steps to create a group of AX Pro devices and then control the group.

Steps

 **Note**

This function is available in Spain only.

1. Tap the **Site** tab.
2. Tap **Batch Arm/Disarm**.
3. Tap + .

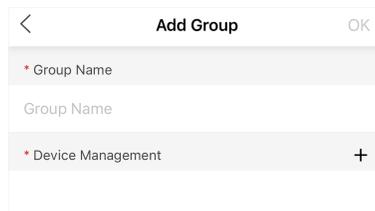


Figure 6-7 Add Group Page

4. Create a name for the group.
5. Add devices to the group.
 - 1) Tap **+** and select the devices in different Sites.

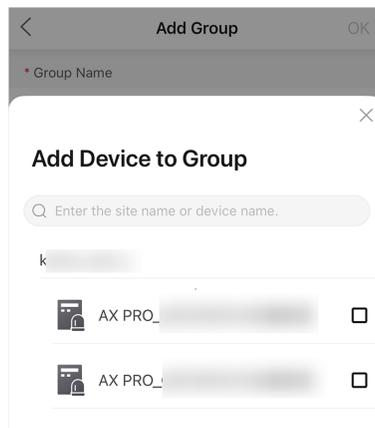


Figure 6-8 Add Device Page

Note

- Only devices of which you have the **Configuration** permission can be added.
- Up to 500 devices can be added to one group.

2) Tap **OK**.

6. Tap **OK**.

7. **Optional:** Perform further operations.

View Group Details Tap on the group to view its details, including devices in the group and their arming/disarming status.

Arm/Disarm Group Tap to arm in Stay mode; tap to arm in Away mode. Or tap to disarm all devices in the group.

You will be notified when the arming/disarming process is completed.

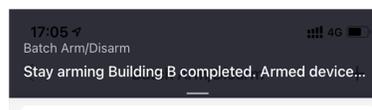


Figure 6-9 Result Notice

Check Last Result Tap → **Record** to check the last arming/disarming results. If there are devices that failed, you can arm/disarm the failed ones again.

- Edit Group Name** Tap ● ● ● → **Edit Group** to edit group name.
- Delete Device** Swipe left on a device and tap **Delete**.
- Add More Devices** Tap ● ● ● → **Add Device** to add more devices to the group.
- Delete Group** Tap ● ● ● → **Delete Group** to delete the group.

6.8.4 Batch Configure AX PROs

You can batch configure parameters for the added AX PROs by creating template(s) on the Mobile Client.



- Available for AX PROs with firmware V1.1.0 or later.
 - The function is only supported in certain countries and regions.
-

Create a Template

You should create a template which will be used for batch configuring parameters of AX PROs.

1. On the navigation panel, tap **Batch Device Config** → **Remote Batch Config**.
2. Tap **Templates** → **Add Template** to add a template.
3. Select the template content and configure the parameters as needed. These configured parameters can be batch applied to AX PROs.
4. Tap **Confirm** to save the template.

The following are the detailed parameters explanations.

Alarm Receiving Center

Protocol Type

Select **ADM-CID**, **SIA-DCS**, ***SIA-DCS**, ***ADM-CID**, **CVS-IP**, or **FSK Module** as the protocol type.



When selecting ***SIA-DCS** or ***ADM-CID**, you should configure the Encryption Arithmetic and Secret Key.

Address Type(Alarm Receiver Server)

Select **IP** or **Domain** as the address type, and enter the IP address or domain name of the alarm receiver server accordingly.

Port(Alarm Receiver Server)

Enter the port No., of the alarm receiver server.

Account Code

Enter the assigned account provided by the alarm receiving center.

Transmission Mode

Select **TCP** or **UDP** as the transmission mode.

Impulse Counting Time

Set the timeout period waiting for the receiver to respond. Re-transmission will be arranged if the transceiver of receiving center is timed out.

Attempts

Set the maximum number that re-transmission will be tried.

Polling Rate

Enable the function and set the interval between two live polling.

Periodic Test

Enable the function and set the interval between two periodic tests.

Companies

Select a company from the drop-down list.

Event Types Notification - ARC

Select which alarm receiving center to receive event notifications and the corresponding event types, including Zone Alarm/Lid Opened, Peripherals Lid Opened, Panel Lid Opened, Panic Alarm, etc.

Notification by Email

Enable the function of sending video verification event and configure the related parameters including the sender's name and email address, the SMTP server's IP address and port No., and the receiver's name and email address, etc.

Server Authentication

If enabled, you should enter the sender's user name and password for authentication.

FTP Settings

Address Type

Select **IP** or **Domain** as the address type, and enter the IP address or domain name of the FTP server accordingly.

Port

Enter the port No. of the FTP server.

Protocol Type

Select **FTP** or **SFTP** as the protocol type.

User Name

Enter the user name of the FTP server.

Password

Enter the password of the FTP server.

Enable Anonymity

If enabled, you do not need to enter the user name and password of the FTP server.



Note

This function is only available when selecting FTP as the protocol type.

Directory Structure

The saving path of snapshots in the FTP server.

Arming Schedule

Auto Arm

Enable the function and set the arming start time. The area will be automatically armed according to the configured time.

Auto Disarm

Enable the function and set the disarming start time. The area will be automatically disarmed according to the configured time.



Note

The auto arming time and the auto disarming time cannot be the same.

Late to Disarm

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

Weekend Exception

Enable the function and set the specific day(s) as weekend. The area will not be armed or disarmed on the weekend.

Holiday Settings

Enable the function and add holiday(s) as needed. The area will not be armed or disarmed on the holiday(s).



Note

You can set up to 6 holiday groups.

Alarm Duration

The duration of the alarm.

Batch Configure AX PROs by Template

You can batch configure parameters for AX PROs by the templates you added on the Mobile Client.

Before You Start

Make sure you have added template(s) for AX PROs. For details, refer to [Create a Template](#).

Steps

1. On the Home page, tap **Batch Device Config** → **Remote Batch Config**.
2. Select multiple AX PROs to be configured.
3. **Optional:** Tap **Templates** in the lower-right corner, and select a template to view and edit its content.
4. Tap **Set Parameters by Template**.
The Select Template panel pops up on the lower side.
5. Select a template from the list.
6. Tap **Apply Parameters** to start applying parameters to the devices.



You can view the applying process and results. After applying finished, you can tap **Details** to view the detailed applying results. For applying failed device(s), you can view the failure reasons.

6.9 Alarm Receiving Center (ARC) Service

Hik-ProConnect offers multiple Alarm Receiving Centers (ARC), which can provide remote 24/7 alarm receiving service for your selection. You can authorize a Site to an ARC, and then enable ARC service for devices on the Site to allow the staff of the ARC to receive events from the devices, respond to the events, and send out emergency dispatches (if needed) around the clock each day.

Steps



- ARC service is only supported by the devices added by Hik-Connect (P2P). The supported device types include camera and NVR manufactured by Hikvision, and AX Pro/Hub/Hybrid security control panel.
 - ARC service is not available in all countries or regions.
-

1. Tap **Site** to enter the site list page.
 2. Select a Site to enter the site details page, and then select **ARC Service**.
-



If the **ARC Service** tab is hidden, you can swipe to the left on the tab bar to show the tab.

3. Tap > to enter the ARC list page and then select an ARC.
 4. Tap an ARC to enter its details page to view its details, including company name, logo, country, location, contacts, and official website.
-

5. **Optional:** Tap the official website of the ARC to view more information about it.

6. Tap **Authorize** on the ARC details page.

The device(s) available for enabling ARC service will be displayed.



Note

ARC service is only supported by Hikvision encoding devices and AX Pro device added by Hik-Connect (P2P).

7. Switch on to enable ARC service for a specific device.



Note

If the Site has been handed over to the end user, you should apply authorization permission from the end user first before you can enable ARC service for the device. For details about applying authorization permission, see [***Apply for Site Authorization from Site Owner***](#).

The events detected by the device and the device exceptions will be sent to ARC.

8. **Optional:** If you have enabled ARC service for an AX Pro device in the previous step and the device is accessed to ARC via Hik IP Receiver Pro, tap the device in the device list to enter the Configuration page, and then set the way to connect the device to Hik IP Receiver Pro.



Note

- Hik IP Receiver Pro functions as the medium for transmitting alarms and alarm-related videos from the device to the ARC.
- You need to acquire **Configuration** permission before you can configure the device.
- You might need to verify the installer account of the device to modify this parameter.
- If the device is armed, disarm it first.

Ways to Connect to Hik IP Receiver Pro

Connect Directly or by Hik-ProConnect Server

When the two connections are both available, direct connection will be used in priority, i.e., the device will be connected to Hik IP Receiver Pro directly. When direct connection is abnormal, the device will be connected to Hik IP Receiver Pro by Hik-ProConnect server. If direct connection is restored, the way will automatically switch back to direct connection.

Such a mechanism ensures the stability of data transmission from the device to the ARC.

Connect by Hik-ProConnect Server

The device will be connected to Hik IP Receiver Pro by Hik-ProConnect server constantly.



Note

The stability of data transmission is less stable compared with **Connect Directly or by Hik-ProConnect Server**.

9. **Optional:** Tap the authorized ARC to enter its details page, and then tap **Deauthorize** to deauthorize the ARC.

Note

After you deauthorize the ARC, the ARC service for devices on the Site will be automatically disabled.

6.10 View Video

You can view the live video and the recorded video footage of the added encoding device(s).

6.10.1 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 tap **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 4.13.0 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 tap **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.
-

6.10.2 Play Back Video Footage

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

Note

- Make sure you have permission for playback. Otherwise, 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 tap  to enter the playback page. You can also enter the playback page on the live view page.

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

On the playback tool bar, tap 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.

	Tap the icon to select a channel for playback.
	Tap the icon to download the video footage to your mobile phone.
	Tap the icon to turn on/off the playback sound.
	Tap the icon to pause the playback.
	Tap the icon to select a speed for playing video footage.
	Tap the icon to perform digital zoom.
	Tap the icon to capture a picture.
	Tap the icon to clip the video footage and download it to your PC.

6.11 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.

6.11.1 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, tap the switch name to enter the device details page.

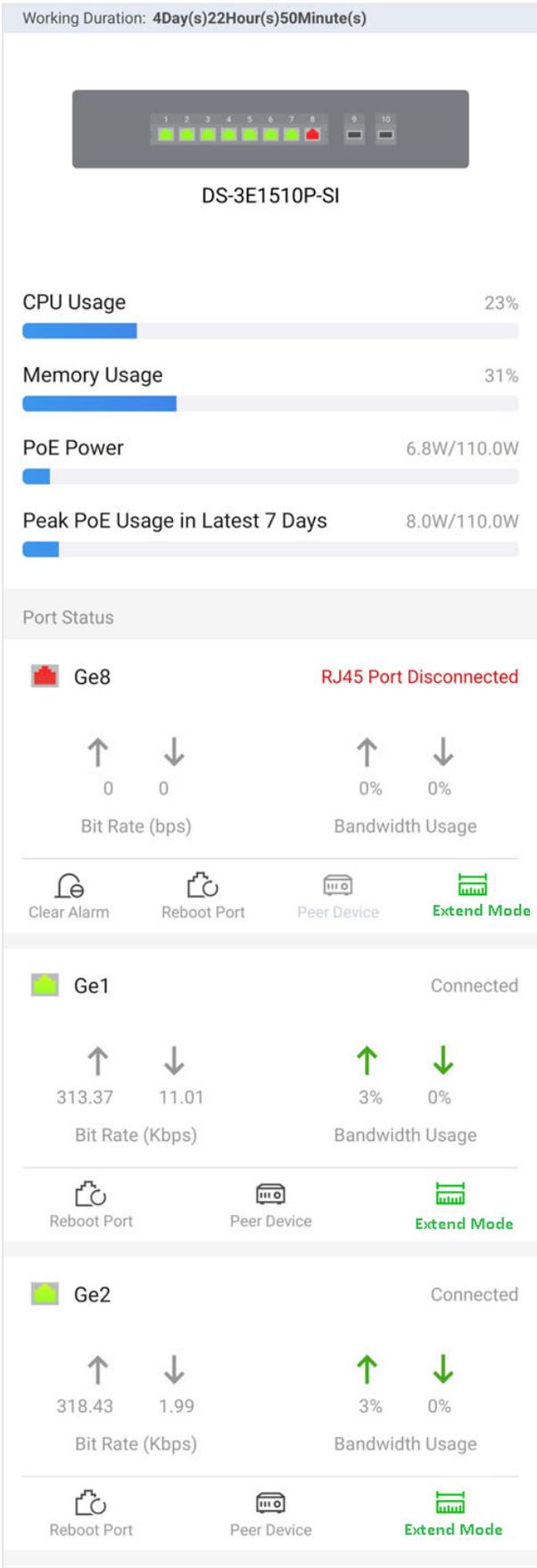


Figure 6-10 Switch Details

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	Tap Reboot to reboot the switch.
View Peer Device	Tap Peer Device to view the details of the device connected to this port.
Clear Alarm	For port with alarm(s), tap ... → Clear Alarm to clear the alarm(s) of this port.
Restart Port	For the abnormal port, tap ... → Restart Port to restart this port.
Enable/Disable Extend Mode for Port	<p>Tap Enable Extend Mode/Disable Extend Mode to extend or not to extend the transmission range of this port.</p> <p> Note</p> <p>After enabled, the transmission range of the port will be extended to 200 to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.</p>

6.11.2 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 site page, and then tap  next to a network switch to enter the network topology page. You can perform the following operations on the network topology.

Table 6-7 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 you want to change the root node, you can tap  to select a network switch as the root node.
View Network Switch Details	<p>You can tap a network switch on the topology to view its details, including basic information, device status, and port status.</p> <p>You can also perform operations such as rebooting the network switch and restarting port. For details, see Network Switch Operations.</p> <p> Note</p> <p>You cannot view details of a virtual network switch.</p>
View Details of Other Device	<p>Tap a device to view its details, such as device model and network status.</p> <p> Note</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>The color of the device icon indicates the running status of a device:</p>

Operation	Description
	<ul style="list-style-type: none"> • 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.

6.12 Other Management

You can perform more operations for device management, including upgrading device firmware, unbinding device from its current account, and configuring DDNS for devices added by Hik-Connect service.

6.12.1 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.

 will appear beside the name of an upgradable device on the site list.

Note

For AX Hub and AX Hybrid, you need to authenticate your identity by entering the password of the installer account of the device first if you have enabled EN50131 Compliant mode. If you do not authenticate, no new version will be detected without security authentication.

2. Tap the device name to enter the device page.

3. Tap **Upgrade**.

4. **Optional:** For security control panels enabled EN50131 Compliant mode, enter the device's password.

5. 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.
-

6.12.2 Unbind a 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 from its current account 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.
 - If you checked **Allow Me to Disable Hik-Connect Service** when you hand over a Site to your customer, you cannot unbind the devices added to this Site. For details about Site handover, see *[Invite Site Owner](#)* .
-

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.

6.12.3 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**.

6.12.4 Remote Configuration

You can configure parameters remotely for the added device such as doorbell and encoding device.

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.
- For AX Hub and AX Hybrid, you need to enter the installer account of the device and its password first if you have enabled EN50131 Compliant mode.

- If you have no permission for remote configuration, you can perform the following operations:
Connect your mobile phone to the same LAN with the device to be configured and then tap **Configuration in LAN** to log into the device and start remote configuration.
 - Make sure the device is online.
-

Chapter 7 Service Market

You can view the information of value-added services in the Service Market of the Mobile Client, including the health monitoring service, cloud storage service, access & attendance service, people counting service, temperature screening service, and employee account add-on. If your country or region supports service keys, you can purchase the health monitoring service and cloud storage service by service key directly on the Mobile Client. If not, you need to go to the Portal to purchase services.

Tap **Business** to enter the Service Market to view details of the value-added services.

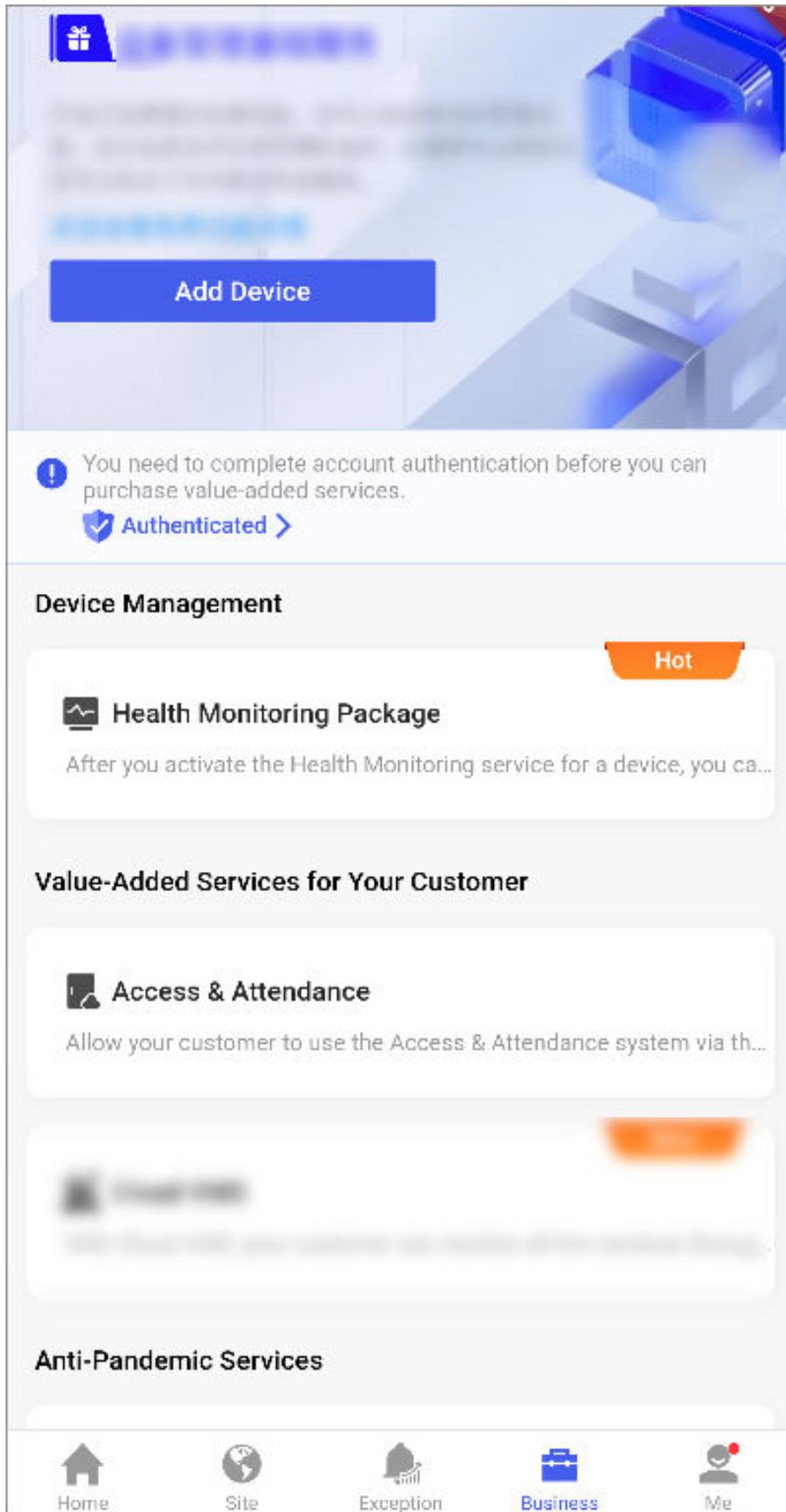


Figure 7-1 Service Market on the Mobile Client

Chapter 8 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.

8.1 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



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.
-



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.
-



- 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**, **Standard Definition** as the definition of the video footage uploaded to the cloud. Or customize a definition.

Custom

Select a resolution (1080P, 720P, 4CIF, or CIF), and then set the bit rate according to the recommendation shown on the interface.

Note

If you have tested your network, 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.

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.

8.2 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 tap 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.

8.3 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 tap **Network Test** → **Start** to start testing your network.

Chapter 9 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.

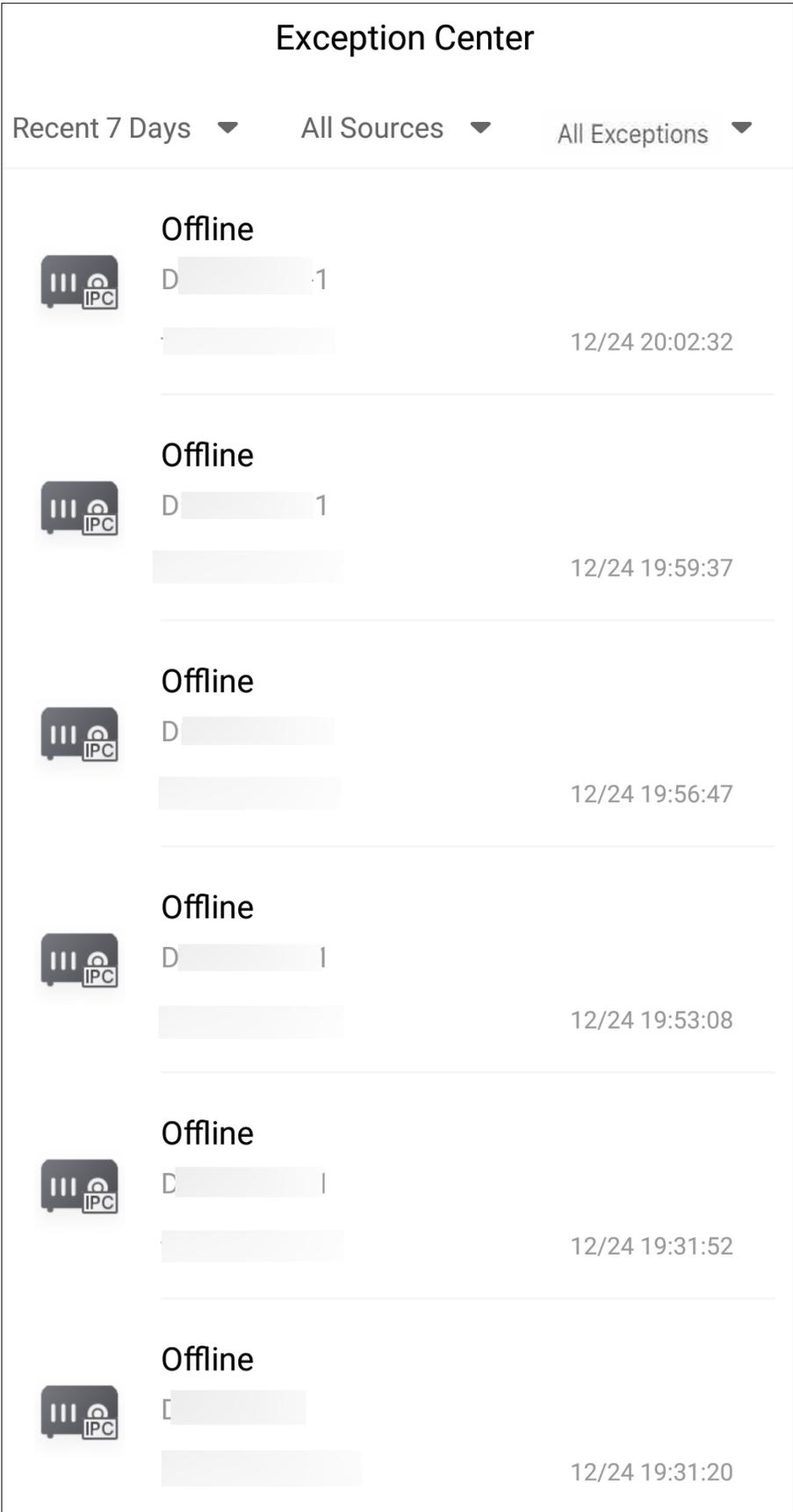


Figure 9-1 Exception Center

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.

