Hik-Partner Pro Mobile Client

User Manual

Legal Information

©2023 Hikvision 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

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 LATTER 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 2
1.2 Entities in Hik-Partner Pro 2
1.3 Running Environment 4
1.4 Function Availability for Different Countries/Regions 4
1.4.1 Functions Only Available in Certain Regions 4
1.4.2 Regions Only With Support for Free Functions 5
1.5 Download the Mobile Client 8
Chapter 2 Account Management 9
2.1 Register by Hik-Connect Account 9
2.2 Register an Installer Admin Account 11
2.3 Manage Company Information 13
2.4 Authenticate Your Account 14
2.5 Company Merger 15
2.5.1 Initiate Company Merger 17
2.5.2 Accept Company Merger 19
2.6 Manage Role and Permission 20
2.7 Invite Employee 22
2.8 Manage My Agreements 24
2.9 Link Your Account to a Distributor 24
2.10 Edit Your Account Information 25
Chapter 3 Login 28
Chapter 4 Become a Hik-Partner Pro User After Product Upgrade 30
Chapter 5 Hik-Partner Pro Mobile Client Overview 33
Chapter 6 Site Management 43
6.1 Site Page Introduction 44

6.2 Add New Site 46
6.3 Add Existing Site 49
6.4 Assign Site to Installer 50
6.5 Hand Over Site 52
6.6 Typical Tenant Site Scenario 54
6.7 Apply for Site Authorization from Site Owner 56
6.8 Accept a Device Management Invitation from Your Customer 57
6.9 Site Sharing 60
6.9.1 Share a Site During Handover 63
6.9.2 Share a Site After Handover 65
6.9.3 Accept Site Sharing 66
6.9.4 Features Available to MSP/ISP on a Shared Site 67
Chapter 7 Device Management 69
7.1 Batch Configure Devices on LAN 69
7.1.1 Batch Activate Devices and Assign IP Addresses for Them 71
7.1.2 Batch Link Channels to NVR and DVR 72
7.1.3 Create Templates for Setting Parameters 73
7.1.4 Batch Set Parameters for Devices 73
7.2 Add Device 74
7.2.1 Add Devices After Batch Configuring Them on LAN 75
7.2.2 Connect Offline Device to Network 76
7.2.3 Add Device by Scanning QR Code 77
7.2.4 Add Device by Entering Serial No. 80
7.2.5 Add Devices on LAN 82
7.2.6 Add Device by IP Address or Domain Name 85
7.2.7 Synchronize Devices with Hik-Connect Account 86
7.2.8 Add Devices Without Support for the Hik-Connect Service 88
7.3 Activate the Health Monitoring Service 89

7.4 Manage Device Permission 91
7.4.1 Apply for Device Permission 92
7.4.2 Release the Permission for Devices 92
7.5 Move Devices 93
7.6 Linkage Rule and Exception Rule 96
7.6.1 Add Linkage Rule 96
7.6.2 Add Exception Rule 104
7.6.3 Enable Device to Send Notifications 109
7.7 Reset Device Password 110
7.8 Enable Remote Log Collection 112
7.9 Manage Security Control Panel 114
7.9.1 Control AX PRO and AX HYBIRD PRO 114
7.9.2 Configure AX PRO and AX HYBIRD PRO 115
7.9.3 Batch Arm/Disarm AX PRO and AX HYBRID PRO 117
7.9.4 Batch Configure AX PROs 118
7.10 Alarm Receiving Center (ARC) Service 122
7.11 View Video 123
7.11.1 View Live Video 123
7.11.2 Play Back Video Footage 124
7.12 Network Switch Management 125
7.12.1 Network Switch Operations 125
7.12.2 Network Topology 127
7.13 Other Management 129
7.13.1 Upgrade Device 129
7.13.2 Batch Upgrade Devices on LAN 130
7.13.3 Unbind a Device from Its Current Account 130
7.13.4 Configure DDNS for Devices 131
7.13.5 Remote Configuration 132

Chapter 8 Health Monitoring 133
8.1 View Status of Devices on All Sites 135
8.2 View Status of Devices on One Site 140
8.3 Send Reports Regularly 144
8.4 Network Topology 145
Chapter 9 Notification Center 148
9.1 Business Notifications 148
9.2 Exception Center 150
9.3 System Messages 154
9.4 Deals and Offers 155
Chapter 10 Case 156
10.1 Submit Case 156
10.1.1 Submit Hardware Product Case 156
10.1.2 Submit Software Product Case 158
10.1.3 Submit Hik-Partner Pro Case 160
10.1.4 Submit Device Password Reset Case 162
10.1.5 Submit Dedicated Customer Service Case 163
10.2 View and Handle Case Records 165
Chapter 11 Return Material Authorization 167
11.1 Submit RMA Requests 167
11.2 View and Handle RMA Requests 169
11.3 Find Repair Stations 169
Chapter 12 Value-Added Services 171
12.1 View and Purchase Value-Added Services 171
12.2 View and Manage My Services 171
12.3 Manage Cloud Storage 174
12.3.1 Set Cloud Storage for Hik-ProConnect Box 175
12.3.2 Set Cloud Storage for NVR 177

12.3.3 Set Cloud Storage for DVR 180
12.3.4 Network Test 182
12.3.5 Activate or Renew Service for a Channel 182
12.4 Co-Branding 183
Chapter 13 Products 185
13.1 View and Search Products 185
13.2 Compare Products 186
Chapter 14 Partner Program 189
Chapter 15 Rewards Store 195
Chapter 16 Quotation Tool 198
16.1 Add Products for Quotation 198
16.2 Create Quotation 200

Chapter 1 Introduction

Hik-Partner Pro 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-Partner Pro solution enables you to customize security solutions for customers with fully-converged Hikvision devices, covering video, intrusion, access, intercom, and more.

Hik-Partner Pro solution provides different ways/clients for service providers' customers.

Table 1-1 Client Description

Client	Description
Hik-Partner Pro Portal	Portal for Installer Admin and Installers logging into Hik-Partner Pro to manage the security business, such as permission and employees management, site management, device management, project registration, product selection, Hikvision product order management, solution search, and devices health monitoring, etc.
Hik-Partner Pro Mobile Client	Mobile Client for service providers logging into Hik-Partner Pro to manage site, apply for site information management permission from end user, manage and configure the devices, manage RMAs (Return Material Authorization) requests, create quotations, etc.
Hik-Connect Mobile Client	Mobile Client for customers to manage their devices, accept the site handover from the service provider as the site owner, approve the Installer's application of site information management permission, etc.
Hik-Connect Portal	Portal for customers to manage their employees' access level and attendance data after you set an attendance system for them via the Hik-Partner Pro Portal.
HikCentral Connect Portal	Portal for customers to manage resources, configure and use video management, on-board monitoring, alarm detection systems, etc.
HikCentral Connect Mobile Client	Mobile Client for customers to use video management, on-board monitoring, and alarm detection systems, such as live view, playback, driving monitoring, and track playback.

Client	Description
HikCentral ReGuard Web Client	Web Client for service providers to configure parameters for video alarm receiving center and manage work orders or statistics reports.
HikCentral ReGuard Control Client	Control Client for service providers to perform alarm monitoring, virtual guard, investigation and search, and so on.

1.1 Target Audience

This manual provides the service provider (i.e., Installer, System Integrator, Distributors, Resellers, OEM, and Alarm Receiving Centers(ARC)) with the essential information and instructions about how to use the Hik-Partner Pro Mobile Client to manage the security business.

This manual describes how to manage the permission and employees of your company, add new or existing site for management, apply for site authorization and device permissions from your customers, manage and configure the devices belonging to the site, select products, and check the device health status for further maintenance, etc.

1.2 Entities in Hik-Partner Pro

Here we introduce the entities (any physical or conceptual object) involved in Hik-Partner Pro.

Identity Related Entities

Service Provider

Those who provide services such as the design of security solutions, system/device installation, after-sales, and (or) device maintenance. There are several service provider types and the detailed descriptions are as follows.

Installer

Provides device installation and maintenance services for customers.

System Integrator

Integrates multiple systems to provide solutions for customers.

Distributor

Trades with Hikvision and supplies Hikvision devices to other businesses that sell to customers.

Reseller

Bulk purchases Hikvision devices from distributors and then sells the devices to installers.

Alarm Receiving Center (ARC)

Provides the alarm receiving and handling service for customers.

If you are to apply for joining Hik-Partner Pro as ARC, selecting **Alarm Receiving Center** as the type of service provider is recommended when registering.

OEM

OEM partners source products, parts or services from Hikvision and relabeling, rebranding or embedding them as a part to another product or system.

Maintenance Service Partner (MSP)

The MSP is a special type of security service providers. They offer technical support to installers who lack technical capabilities and skills. Usually, they collaborate with these installers to provide device management/maintenance services for end users. On Hik-Partner Pro, installers can share sites with their maintenance service partners to collaborate with them. For details, see ***Site Sharing*** .

Note

The MSP can select any of the five service provider types when they registering an account for logging in to Hik-Partner Pro.

Remote Monitoring Center (RMC)

Provides the alarm receiving and handling services remotely based on the video monitoring via HikCentral ReGuard.

Note

The RMC can select any of the service provider types when they registering an account for logging in to Hik-Partner Pro.

End User

Those who have purchased Hikvision devices (e.g., network cameras, DVRs, alarm devices, video intercom devices, and access control devices) and want to manage the devices via an easy-to-use mobile client. End users are customers of the service provider, and they use Hik-Connect to manage devices.

Site Related Entities

Site

A site represents a physical location where device(s) are installed and through which the Installer/ Installer Admin can manage and configure devices.

Site Manager

When a site is assigned to an Installer, the Installer becomes the site manager of the site, and can manage and configure the devices of the site.

Note

Assigning site to Installer is not supported in countries and regions only with support for free functions. For details about free functions and these countries and regions, see ***Regions Only With Support for Free Functions*** .

Site Owner

When an installer transfers ownership of a site to an end user, the end user becomes the site owner who is the holder of the site. The installer can also apply for site authorization from the site owner to manage the site.

1.3 Running Environment

The following is the recommended system requirement for running the Mobile Client.

System Requirement

For iOS: iOS 12 or later versions.
For Android: Android 5.0 or later versions.

Memory

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

1.4 Function Availability for Different Countries/Regions

Hik-Partner Pro 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.

Note

This document contains introductions of all Hik-Partner Pro 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.

1.4.1 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	***Add Linkage Rule*** **Note** Linkage Rule is not available in the United States and Canada.
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.
Cloud 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.
HikCentral Connect Services	All functions contained in the service.
HikCentral ReGuard Services	All functions contained in the services.

1.4.2 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	• ***Register an Installer Admin Account*** • ***Manage Company Information***
Site Management	• ***Add New Site*** • ***Add Existing Site*** • ***Hand Over Site*** • ***Apply for Site Authorization from Site Owner*** • ***Site Sharing***
Device Management	• Add Device

Module	Function(s)
	◦ ***Add Device by Scanning QR Code*** ◦ ***Add Device by Entering Serial No.*** ◦ ***Add Device by IP Address or Domain Name*** • ***Apply for Device Permission*** • ***Release the Permission for Devices*** • ***Synchronize Devices with Hik-Connect Account*** • ***Enable Device to Send Notifications*** • ***Upgrade Device*** • ***Batch Upgrade Devices on LAN*** • ***Configure DDNS for Devices*** • Manage AX PRO Security Control Panel (Hereafter Simplified as AX PRO) ◦ ***Control AX PRO and AX HYBIRD PRO*** ◦ ***Configure AX PRO and AX HYBIRD PRO*** ◦ ***Batch Configure AX PROs*** ◦ ***Batch Arm/Disarm AX PRO and AX HYBRID PRO*** • ***Remote Configuration*** • ***Reset Device Password*** • ***Unbind a Device from Its Current Account*** • ***Network Switch Management***
Video	• ***View Live Video*** • ***Play Back Video Footage***
Tool	Use Tools Including: • Disk Calculator • NVR Channel Calculator • Focal Length Calculator • Bandwidth Calculator • On-Site Batch Upgrade • Account Linking (Link with Hik-Connect Account) • Batch Device Search • Search for Important Firmware Update • On-Site Config • Remote Batch Config • Batch Arm/Disarm
Products	• View and Search for Products (See ***View and Search Products***) • Compare Products (See ***Compare Products***)

Module	Function(s)
Explore	• View, Search, Like, Share, and Comment on Feeds, and Add to Favorites • View, Search, Like, Share, and Comment on How To, and Add to Favorities • View, Search, Like, Share, and Comment on Videos, and Add to Favorities • Register for and Participate in Events
Incentive	• ***Rewards Store*** • ***Partner Program***
Support	• Tutorial Center • Chatbot • Case ◦ ***Submit Case*** ◦ ***View and Handle Case Records*** • Feedback • How To • Contact Us • RMA (Return Materials Authorization) ◦ ***Submit RMA Requests*** ◦ ***View and Handle RMA Requests*** **Note** This function is only available for accounts of authenticated channel partners.

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)

1.5 Download the Mobile Client

You can download Hik-Partner Pro Mobile Client via the Portal, QR code, and application stores.

The ways listed below are available to download the Mobile Client.

- Portal: Visit the landing page of ***https://www.hik-partner.com*** , use your mobile phone to scan the QR code at the bottom of the landing page to download the Mobile Client.

  Note

  For Russia, you can visit ***https://www.hik-partnerru.com*** .
- Portal: Log in and click the account name or profile photo in the top right corner of the Portal to open the drop-down list, click **About** to enter the About page and scan the QR code with your mobile phone to download the Hik-Partner Pro Mobile Client.
- QR Code: Scan the QR code below to download the Mobile Client. Using a browser to scan the QR code is recommended.



Figure 1-1 QR Code for iOS System



Figure 1-2 QR Code for Android System

- Application Store: Enter Hik-Partner Pro as the keyword to search in the application stores (e.g., App Store, Google Play, Galaxy Store, HUAWEI AppGallery, OPPO App Market, VIVO App Store, Xiaomi GetApps) of your mobile phone to download the Mobile Client.

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 the Installer Admin account is available and the Installer account is unavailable. 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.

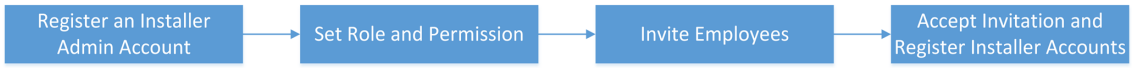


Figure 2-1 Flow Chart of Account Management

- **Register an Installer Admin Account:** You should first register an Installer Admin account before accessing any functions of Hik-Partner Pro. 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. For details, refer to ***Manage Role and Permission*** .
- **Invite Employees:** You can invite employees to register Installer accounts and assign different roles to employees to grant the permissions to her/him. For details, refer to ***Invite Employee*** .
- **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 an Installer Admin account by the Hik-Connect account.

Before You Start

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

Steps

1. Tap to start the Mobile Client.

   The Login page will show.
2. Tap Hik-Connect on the lower side of the page.

   You will enter authorizing and logging page.
3. Authorize Hik-Partner Pro to get the account information of Hik-Connect.

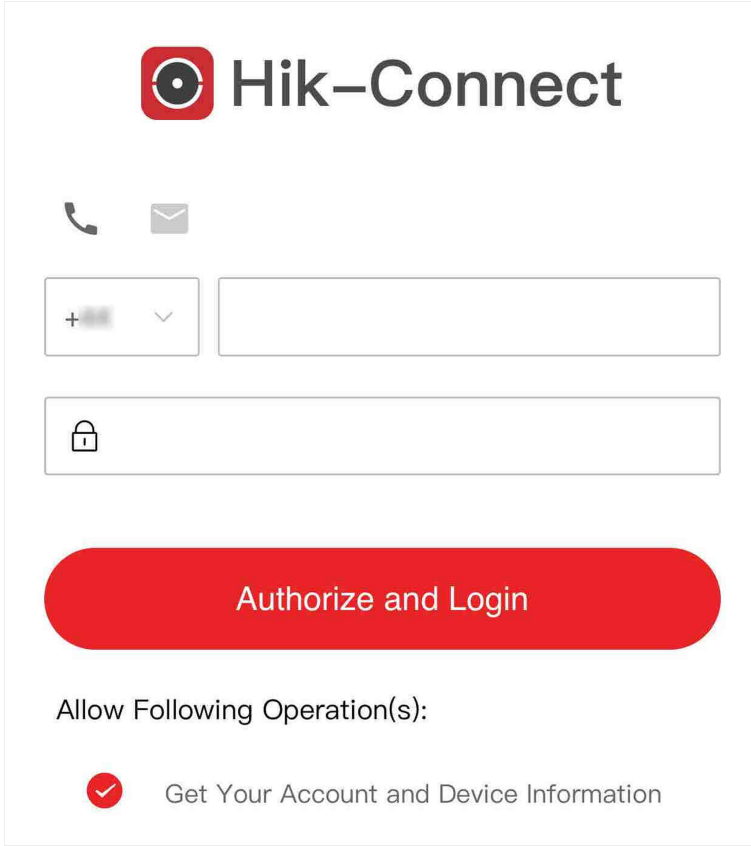


Figure 2-2 Authorize and Login

- 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-Partner Pro to get these information.

4. Tap **Authorize and Login**.
5. Register an Installer Admin account.

Note

For details about the registration process, refer to the ***Register an Installer Admin Account*** .

6. **Optional:** After you finish registration and log in to Hik-Partner Pro, synchronize devices in your Hik-Connect account with this account.

Note

For details, refer to ***Synchronize Devices with Hik-Connect Account*** .

What to do next

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

2.2 Register an Installer Admin Account

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

Steps

1. Tap to start the Mobile Client.
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. In the Login page, tap **Register** to register an account.

Note

If your account has been registered, you can tap **Log In** to log in to Hik-Partner Pro. For details about login, refer to ***Login*** .

4. Select your identity and service provider type (installer, system integrator, distributor, reseller, alarm receiving center (ARC), or OEM).

Note

For details about the identities and service provider types, refer to ***Entities in Hik-Partner Pro*** .

5. Select whether you are to register by email or by phone number.

Note

In some countries/regions, only the registration by email is supported.

6. Register an account.
   1) Set your name (first name and last name), company name, email, phone number, verification code (for verifying the email address) / SMS code (for verifying the phone number), and 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.

2) Check **I agree to Hikvision OneHikID's Privacy Policy.** if you accept the details in the **Privacy Policy**.
3) Tap **Register**.

You will be prompted that you have registered successfully, and the **Company Authentication** page will pop up.

7. Tap **Authenticate Now** or **Later** to enter either of the following processes.

- Tap **Authenticate Now** to submit the company authentication application.
  a. Set the required information and review the information already filled in (company name, address, email, phone, etc).

  Note

  For details, refer to ***Authenticate Your Account*** .

  b. (Optional) Check **I would like to receive marketing information about services and activities from Hik-Partner Pro via emails. I understand that I can unsubscribe at any time.**

  Note

  - 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 the latest product introduction, service introduction, questionnaires and special offers, to the email address which is used for your account registration.

  c. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in the agreements.
  d. Tap **Confirm** to submit the application and enter Hik-Partner Pro.
- Tap **Later** to go to the Complete Information page.
  a. Set the required information (address, etc.).
  b. (Optional) Check **I would like to receive marketing information about services and activities from Hik-Partner Pro via emails. I understand that I can unsubscribe at any time.**

Note

- 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 the latest product introduction, service introduction, questionnaires and special offers, to the email address which is used for your account registration.

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

d. Tap **Confirm** to enter Hik-Partner Pro.

Note

If you tap **Cancel**, the **Company Authentication** page will still pop up after you log in to the new account.

Result

You can log in to Hik-Partner Pro with this account, and perform other operations such as site management.

2.3 Manage Company Information

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

Steps

Note

When your company is not authenticated, the Installer Admin can manage and edit all the company information, and when your company authentication application is approved, the Installer Admin can submit the information change request and the information will be edited successfully after approval.

1. Go to the Company Information page.
2. Tap ✎ .
3. Enter the name of your company.
4. **Optional:** Enter the website of your company.
5. Enter your address.
6. Enter the city of your company.
7. Enter an email address which will be bound with the Installer Admin account after registration.
8. Enter other information of your company, such as state/province/region, and postal code.
9. Enter your phone number.
10. Enter the VAT number.
11. Tap **OK**.

Note

You can check the percentage of completed information after saving.

2.4 Authenticate Your Account

After you register an Installer Admin account, you can authenticate your account to purchase value-added services and use more features (besides the basic features) in Hik-Partner Pro.

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 the distributor by your own email box.
3. Enter the authentication code on the 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.

Note

If your company is not authenticated and you have the permission to submit the authentication application, you may be prompted and guided to authenticate your company by submitting the application after login.

1. Go to **Me → Authenticate Now** .
2. Review and edit the company information already filled in and set other required information, such as company name, address, city, etc.

Note

If your country/region is in Australia (continent), you should also enter your security license number and contact name.

3. Select the distributor if you have bought Hikvision products.

Note

This information is displayed and required only when your company type is installer, system integrator, or alarm receiving center (ARC).

4. Tap + to upload a picture (e.g., business license and business card) as evidence.
5. Tap **Authenticate Now**.
   The application information will be sent.

Note

After your application is approved, you will be notified with push notifications and emails.

2.5 Company Merger

If you and your employees or colleagues have created more than one Installer Admin account / company on Hik-Partner Pro, you can merge the companies into one for more efficient management and to carry on your business smoothly (you may have encountered the problem that your second registered account/company cannot be authenticated).

Refer to the following sections to learn more about the company merger.

- ***Benefits of the Company Merger***
- ***Effects on the Accounts/Companies After the Merger***
- ***Limitations***

Benefits of the Company Merger

- Manage your employees and the co-branding of your company via one account.
- Manage all your customers and their devices under one account.
- Get points faster to redeem for more gifts and value-added services.

Effects on the Accounts/Companies After the Merger

Installer Admin and Employee Accounts	• The Installer Admin who initiates the merger is still the Installer Admin. The Installer Admin of the invited company becomes an employee with the role of administrator under the initiating company. • All employee accounts of the invited company are migrated to the initiating

	company and become employees under the Installer Admin who initiates the merger. The disabled employees of the invited company will still be disabled after they are migrated. No matter whether the total number of free and purchased employee accounts (add-on) of the initiating company is insufficient or not, all employee accounts of the invited company will become limited accounts after the merger. If an employee has not become a Hik-Partner Pro user, they can still be migrated to the initiating company only if their previous Installer Admin has become a Hik-Partner Pro user. • If there is an account (email address) exists in both the initiating and invited companies before the merger, this account will exist only in the initiating company after the merger with its role the same as before.
Reward Points	Points of both companies will be combined and points history of both companies and all employees will be preserved.
Company Information	Only the information (company name, logo, address, authentication status, etc.) about the initiating company will be preserved.
Others	• The invited company will be deleted. • All accounts of the invited company will be logged out after the merger. After they log in again, they will be in the initiating company. • If there are invited employees of the invited company who have not registered right before the merger, the links for registration will become invalid after the merger. • Likes, favorites, and comments of all accounts will be preserved.

Limitations

- Both the account which initiates the company merger and the account which is invited to merge companies need to be Installer Admin accounts, should have been upgraded to OneHikID accounts, and should have upgraded and become Hik-Partner Pro users.
- The invited company cannot be an authenticated channel partner, or be authenticated already, or be added to the ARC list already.
- The initiator's account and the invited account need to be in the same country/region.
- The merger may also fail for the following reasons:
  - There are devices or handed-over sites under the invited account.
  - The invited account is linked with a Hik-Connect account.
  - The invited account has purchased value-added services and the services are still in use.

2.5.1 Initiate Company Merger

If you need to merge the data of another company into your company, you can initiate a company merger.

Before You Start

- Both the account which initiates the company merger and the account which is invited to merge companies need to be Installer Admin accounts, should have been upgraded to OneHikID accounts, and should have upgraded and become Hik-Partner Pro users.
- The invited company cannot be an authenticated channel partner, or be authenticated already, or be added to the ARC list already.
- The initiator's account and the invited account need to be in the same country/region.

Steps

1. Find the entry for initiating a company merger.
   - Go to the **Me** page.

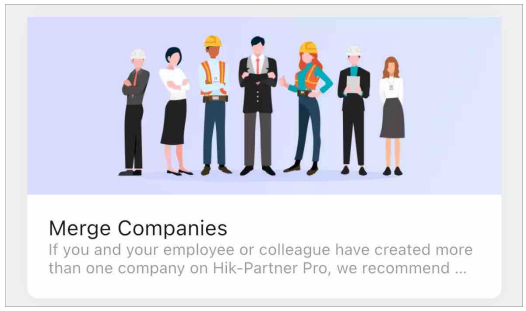


Figure 2-3 Entry on the Me Page

   - If other companies with information similar to your company's are detected, you will receive a company merger reminder in **System Message** of the Notification Center.

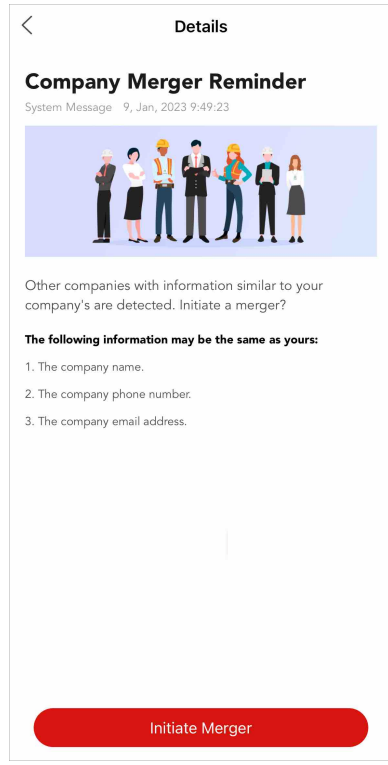


Figure 2-4 Entry in System Messages of Notification Center (Company Merger Reminder)

2. Tap the **Merge Companies** section or tap **Initiate Merger** to enter the Merge Companies page.

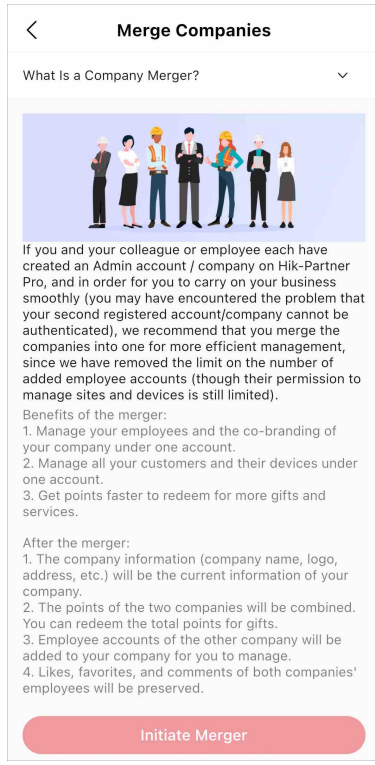


Figure 2-5 Merge Companies

3. Enter the Installer Admin account of the invited company.
4. Check **Agree to Information Sharing Protocol**.

Note

The invited company will be able to see your company name and your email address.

5. Tap **Initiate Merger** to send the company merger invitation.

What to do next

Contact the invited Installer Admin (who will receive an email and a message reminder) to log in to Hik-Partner Pro and accept the company merger request in **Notification Center**.

2.5.2 Accept Company Merger

If you are invited by another company to merge your company with theirs, you can receive and handle the company merger invitation in Notification Center on Hik-Partner Pro.

On the top right of the Home page, go to ✉ → **Business Notification** , and tap the company merger notification to view the details.

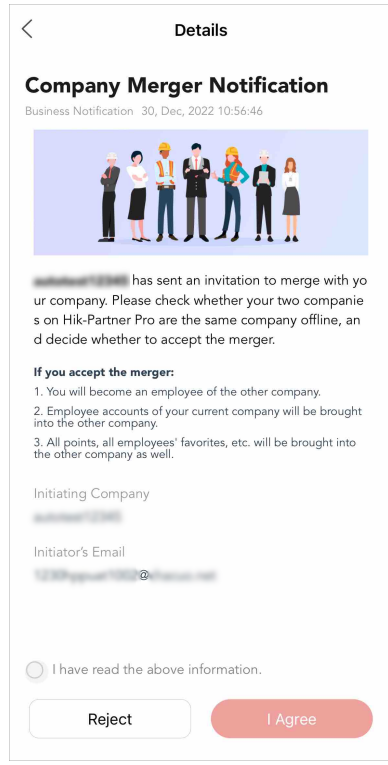


Figure 2-6 Company Merger Notification (Invitation)

You can view the information about what will happen if you accept the company merger, and also the initiating company's name and the initiator's email address.

To accept the company merger, check **I have read the above information.** and tap **I Agree**.

Note

The company merger may fail after you accept the merger for the following reasons:

- There are devices or handed-over sites under your account (the invited account).
- The invited account is authenticated.
- The invited account is linked with a Hik-Connect account.
- The invited account has purchased value-added services and the services are still in use.

To reject the company merger, tap **Reject**.

2.6 Manage Role and Permission

Before adding an employee to the system, you can create different roles with different permissions for accessing system resources and then assign roles to corresponding employees to grant the permissions to them. Or you can give a predefined role to an employee without creating one. An employee can have only one role.

Steps

Note

- For the countries and regions only with support for free functions, managing role and permission is not supported. For details about free functions and these countries and regions, see ***Regions Only With Support for Free Functions*** .
- There are three predefined roles in the system: Administrator, Site Manager, and IT Manager. The permissions of the three roles are as follows. The three roles cannot be deleted by anyone.
  - **Administrator**: Setting company information, managing employees, checking operation logs of all the employees, and managing all the sites.
  - **Site Manager**: Managing assigned sites, adding, configuring, and deleting devices, and enabling valued services for end users of assigned sites.
  - **IT Manager**: Managing all the sites, assigning sites to other employees, enabling or editing valued service for all the end users, and viewing operation logs of all the employees.

1. Tap **Me → Company Management → Role and Permission** .
2. Tap + in the upper-right corner of the Role and Permission page to open the Add Role page.
3. Enter the role name and select permission(s) for the role.

   Manage All Sites

   Managing all sites, including adding and editing site, assigning site to Site Manager, handing over sites, applying for site authorization, searching sites, managing devices in the site (adding, deleting, editing, upgrading), applying for device permission, and health monitoring. Up to 100 employees can be assigned with this permission.

   Manage Assigned Site

   Managing site(s) assigned to the employee, including editing site, handing over sites, applying for site information management permission, adding existing site, adding a new site, managing devices in the site (adding, deleting, editing, and upgrading), and deleting site.

   Note

   You need to give an employee this permission before assigning the employee a site.

   Manage Account and Role

   Accessing the Employee page and the Role and Permission page, adding and deleting accounts and roles. The Employee page and the Role and Permission page will not show without this permission.

   Manage Company Information

   Accessing company information page and edit company information (e.g. name, logo, addresses, etc.). Company information page will not show without this permission.

   Manage Service Package and Order

   Viewing orders, purchasing service packages such as health monitoring packages and employee packages.
4. **Optional:** Enter remarks of the role in the **Description** field.

5. Tap **OK**.
6. **Optional:** Perform the following operations after adding roles.

View Role Details	Tap an added role to enter the role details page to view the role information and permissions.
Edit Roles	Tap an added role to enter the role details page and tap ✎ to edit the role information and permissions.
Delete Roles	Tap 🗑 in the upper-right corner and select the added role(s) to delete them.

Note

You cannot delete a role which has been assigned to an employee.

2.7 Invite Employee

Installer Admin and Installer with the role permission for managing account and role can invite employees to manage resources in the system.

Steps

Note

For countries and regions only with support for free functions, inviting employee is not supported. For details about these countries, see ***Regions Only With Support for Free Functions*** .

1. Tap **Me → Company Management → Employee** .
2. Tap + in the upper-right corner of the Employee page to open the Add Employee page.
3. Enter the email of the to-be-invited employee.
4. Select a role for the employee.

   Note

   You can tap + in the upper-right corner of the Select Role page to create a new role. For details about managing roles, refer to ***Manage Role and Permission*** .

   The permissions of the role will be displayed.
5. Tap **Add**.

   The invited employee will receive an email delivering a link in the entered email box. The employee needs to tap the link to register an account, after which the employee's information will be displayed in the employee list.

   Note

   If you invite the employee via your OneHikID account, and if the Hik-ProConnect account of the to-be-invited employee has not been upgraded to the OneHikID account, the to-be-invited employee needs to upgrade the account according to the instructions on the interface.
6. **Optional:** Perform the following operations after adding employees.

Enable/ Disable Employee

Set the switch to on or off to enable or disable the employee account.

Note

- Once disabled, the employee cannot log in to the system via this account.
- You cannot disable your own account and the Installer Admin account.

Remove Account Limits

Note

- The status of employees is limited by default and some operations are unavailable to them such as creating sites, adding devices, viewing records in the Employee Efficiency Statistics module, and viewing operation logs.
- Installer Admin and Installers with employee management permission can remove account limits for employees, which requires the employee account add-on for each employee. See details in ***View and Purchase Value-Added Services*** .

Tap an employee to open the Employee Details pane, tap the account limit message on the top, and tap **Remove Limit** on the pop-up.

Delete Employees

Tap 🗑 in the upper-right corner and select the added employee(s) to delete them.

Note

- You cannot delete your own account, the Installer Admin account and the Site Manager account.
- If the employee has not merged account data or become a Hik-Partner Pro user, you cannot delete their account. Refer to ***Become a Hik-Partner Pro User After Product Upgrade*** for details.

View Employee Details

In the employee list, you can view the employee's contact number, email address, role permissions, and numbers of sites and devices the employee managed.

Edit Role Assigned to Employee

Tap an employee to open the Employee Details pane and tap ✎ in the role field to enter the Select Role page. Then you can tap + to add a new role or select another role for the employee.

Note

You cannot edit roles assigned to your own account and the Installer Admin account.

View Sites Managed by Employee	Tap numbers of sites and devices in the employee list or tap an employee to open the Employee Details page to view the list of all sites managed by the employee. You can tap a site to view the site details.

Note

The above operation is supported only when the employee has site(s) to be managed.

2.8 Manage My Agreements

As a distributor, you can manage and sign your contract agreements of partner programs with resellers and Hikvision on Hik-Partner Pro.

Note

- This function is not supported by some accounts or in some countries/regions.
- The contract agreements of partner programs are signed by three parties (the reseller, distributor, and Hikvision). The applications for partner programs can be submitted by resellers on Hik-Partner Pro. For details, refer to ***Partner Program*** .

Go to **Me → Agreement Management** to view your agreements.

You can view the program name, customer (i.e., reseller) name, agreement name, signing status (signed / to be signed), and the date when the signing process is initiated.

Tap **Sign** to sign the contract agreement online.

Tap an agreement to view its details.

2.9 Link Your Account to a Distributor

You can use the Mobile Client to scan the Hik-Partner Pro 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-Partner Pro.

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-Partner Pro QR code, and then tap on the top of the page to scan the QR code. Also, you can go to **Me → Distributor** , and then scan the QR code.

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

2.10 Edit Your Account Information

After login, you can edit your account information of the current account and change password if required.

Tap **Me** at the bottom and then tap the profile photo on the top-left corner to enter Me page. You can view and edit your account information of the current account, including the profile photo, name, email, phone number, etc. You can also view your HIK ID on this page, but you cannot edit it.

Note

For accounts registered in countries which support registration with phone number, the phone number information cannot be edited.

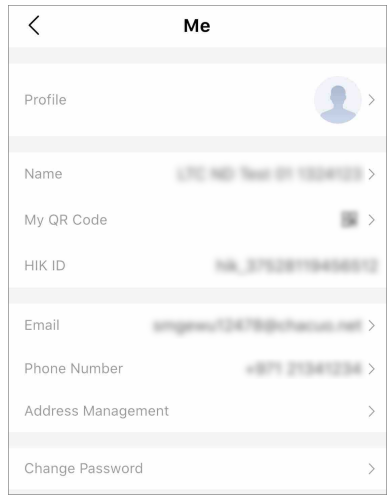


Figure 2-7 Edit Your Account Information

Change Profile Photo

You can change your profile photo to another one if required.

1. Tap the profile photo.
2. Choose a photo from the photo albums on your phone.
3. Optional: Drag, crop and rotate the photo to change the position and size of your profile photo.
4. Tap **OK**.

Edit Name

You can edit the name if required.

1. Tap the name to enter Edit Name page.
2. Enter the first name and last name.

Note

The last name and first name should contain 1 to 32 characters, excluding emoji and special characters including : * ? " < > |.

3. Tap **Save**.

Manage My QR Code

Tap to show My QR Code, which your customers can scan to add you as the service provider and authorize you to manage devices.
If you have uploaded your company logo, your company logo will be displayed in the center of the QR code. Or you can tap **Add Your Company Logo to the QR Code** to upload your company logo.
Tap to download the QR code.

Change Email

You can change the current bound email address of the account to another one if required.

Note

If the current bound account has been upgraded to OneHikID account, the page for editing OneHikID account information will be displayed. You can follow the instructions to change the email.

1. Tap the email to enter Change Email page.
2. Enter the password for the current account and tap **Confirm** to verify your identity.
3. Enter a new email address in the **Email** field.
4. Tap **Verify**.
   An email with a verification code will be sent to your new email address.
5. Enter the received verification code in the **Verification Code** field.
6. Enter the password of the current account.
7. Tap **Confirm**.

Edit Phone Number

You can edit the phone number if required.

1. Tap the phone number.
2. Choose the area code of your country/region, and enter a phone number.
3. Tap **Save**.

Change Password

Change the password of the current account.

Note

If your account has been upgraded to OneHikID account, the page for changing the password of your OneHikID account will be displayed. You can follow the instructions to finish change 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.

Add New Shipping Address

You can add, edit, and delete your shipping addresses, and set the default shipping address.

Note

This function is only supported in certain countries and regions.

Tap **Address Management → New Address** , fill in all required information (contact person, country/state, address, postal code, etc.), enable **Set as Default?** if you are to set it as the default shipping address, and tap **Save** to add a new shipping address.
You can also edit and delete your shipping addresses, and set another shipping address as default.

Upgrade Account

If your Hik-ProConnect account has not been upgraded to the OneHikID account, you can upgrade your account according to the instructions on the interface as needed. Whether you can upgrade the account or not is determined by the country and the region of your account.

Delete Installer Admin Account

For Installer Admin, if the account is no longer used, you can delete it on the Settings page.

Note

- Deleting Installer Admin account is irreversible. The company information and accounts CANNOT be restored once deleted. Back up the required data before deleting the account.
- If there are authorized site(s) or employee account(s) under the current account, you cannot delete it.
- If the current bound account has been upgraded to OneHikID account, the login page for OneHikID account will be displayed. You can follow the instructions to delete the account.

1. Tap **Me →** .
2. Tap **Delete Installer Admin Account**.
3. Tap **Delete Account**.
4. Enter the password of your Installer Admin account, and tap **Verify**.
5. Tap **Confirm** to confirm deleting.

Chapter 3 Login

After logging in by an Installer Admin account or Installer account, you can manage resources (including sites, devices, and roles, etc.) and perform health monitoring and so on.

Before You Start

Make sure you have registered an account. See ***Register by Hik-Connect Account*** or ***Register an Installer Admin Account*** for details about registration.

Steps

1. Tap to start the Mobile Client.

   Note

   For the first time to start the Hik-Partner Pro Mobile Client, select the country/region where your account locates and tap **OK**.

   The login page will show.
2. Select a country or region where the account locates at the top right of the page.
3. Tap **Log In → OneHikID (Hik-ePartner) Account / OneHikID Account** or **Log In → Hik-ProConnect Account** to log in by the OneHikID account or by the Hik-ProConnect account.

   Note

   - The display of "OneHikID" or "OneHikID (Hik-ePartner)" on the login page is determined by the country or region where you locate.
   - The login method available is determined by the country and the region of your account. If you select OneHikID as the login method, and your Hik-ProConnect account has not been upgraded to the OneHikID account, you need to upgrade your account according to the instructions on the interface.
   - If your Hik-ProConnect account has been upgraded to the OneHikID account, logging in to the platform by the Hik-ProConnect account is not supported.
4. Enter the registered email address and password.

   Note

   If the registration and login by phone number is supported in your country/region, you can also enter the registered phone number and password.
5. **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.

6. Tap **Sign In** or **Enter Hik-ProConnect**.

Note

- If the account has not been registered, an email containing the verification code will be sent to the email address your entered. Refer to ***Register an Installer Admin Account*** for more details.
- If you have completed company merging and your account still exists in more than one company, or if the companies in which your account exists are all kept on Hik-Partner Pro, you need to select one company for login. You can also tap **Switch Company** on the Me page to switch to another company. For details, refer to ***Become a Hik-Partner Pro User After Product Upgrade*** .

Chapter 4 Become a Hik-Partner Pro User After Product Upgrade

Hik-Partner Pro is upgraded from Hik-ProConnect, combining the features of Hik-ProConnect and another product named Hik-ePartner, so it provides services which are more diverse and more professional. If you have already registered for Hik-ProConnect and/or Hik-ePartner before the product upgrade, you can log in to Hik-Partner Pro using the existing account to become a Hik-Partner Pro user.

When you log in to Hik-Partner Pro for the first time using the existing account of Hik-ProConnect and/or Hik-ePartner, a window will pop up to notify you of the product upgrade.

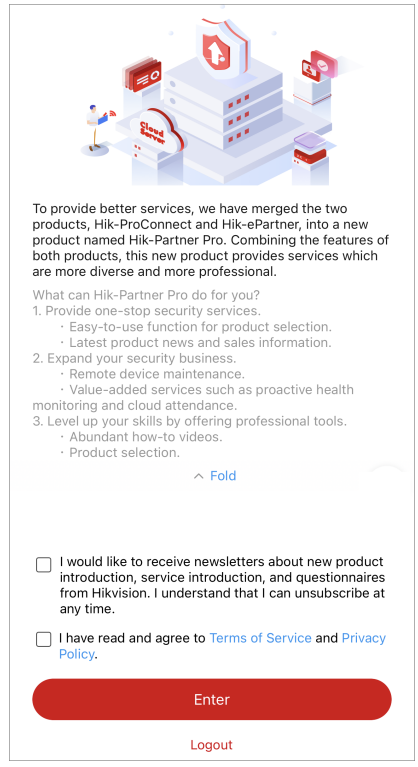


Figure 4-1 Product Upgrade

After you check **I would like to receive newsletters about new product introduction, service introduction, and questionnaires from Hikvision. I understand that I can unsubscribe at any time.** (which is optional) and **I have read and agree to Terms of Service and Privacy Policy.**, and tap **Enter**, you become a Hik-Partner Pro user and can continue to use Hik-Partner Pro.

Note

- In some countries/regions, the above-mentioned window will not pop up.
- If your existing account is an Admin account of Hik-ePartner, after you become a Hik-Partner Pro user, the employee account add-on will be given as a gift to you which can cover the existing employee accounts in your company and is valid for one year.
- In some countries/regions, the authenticated channel partners can complete the process of becoming a Hik-Partner Pro user offline.

Refer to the following sections for more details.

- ***Situations Where You Enter the Home Page Directly After You Tap Enter***
- ***Other Situations***
- ***After First-Time Login***

Situations Where You Enter the Home Page Directly After You Tap Enter

- Your account only exists in Hik-ProConnect.
- Your account exists in both Hik-ProConnect and Hik-ePartner, and is the Installer Admin / Admin account in both companies on Hik-ProConnect and Hik-ePartner, which means the two companies can be merged into one company, and the data (devices, employees, etc.) of both companies can also be merged and not lost. Moreover, the information about the two companies are the same so that you don't need to select the company information to be kept, or only one of the two companies is authenticated so that the information of the authenticated company will automatically be kept.
- Your account only exists in Hik-ePartner. And your account is the Admin account, or is an employee account but the Admin user has completed company merging.

Other Situations

- Your account exists in both Hik-ProConnect and Hik-ePartner, and is the Installer Admin / Admin account in both companies on Hik-ProConnect and Hik-ePartner, which means the two companies can be merged into one company, and the data (devices, employees, etc.) of both companies can also be merged and not lost. Moreover, the information about the two companies are the different, and both companies are authenticated / not authenticated. You have to select the company information you would like to keep after you tap **Enter**.
- Your account exists in both Hik-ProConnect and Hik-ePartner. The Installer Admin / Admin accounts of the two companies are different, so company merging is not supported, which means both companies are kept for you on Hik-Partner Pro. You have to select one for login after you tap **Enter**.
- Your account exists in both Hik-ProConnect and Hik-ePartner, and your account is an employee account in Hik-ePartner. You can log in to the company created on Hik-ePartner only after the Admin user completes merging companies. Or you can continue to log in to your company created on Hik-ProConnect for using.

- Your account only exists in Hik-ePartner and is an employee account. Moreover, the Admin user has not completed company merging. You can log in to use Hik-Partner Pro only after the Admin user completes merging companies.
- Your account exists in both Hik-ProConnect and Hik-ePartner. And your account exists in more than one company on Hik-ePartner. You have to select one from the companies on Hik-ePartner for company merging. You should also select the company information you would like to keep if needed.

After First-Time Login

If you have completed company merging and your account still exists in more than one company, or if the companies in which your account exists are all kept on Hik-Partner Pro, you need to select one company for login.
You can also tap **Switch Company** on the Me page to switch to another company.

Chapter 5 Hik-Partner Pro Mobile Client Overview

The Hik-Partner Pro Mobile Client provides access to Hik-Partner Pro from your smart phone.

After logging in to Hik-Partner Pro via the Mobile Client, the Home page will show.

Main Modules

The Hik-Partner Pro Mobile Client is divided into the following main modules. You can access these modules via the tab bar on the bottom.

Table 5-1 Main Modules of Hik-Partner Pro Mobile Client

Module	Description
Home	On the Home page, you can view the overview of your sites and devices, and other quick entries for health monitoring, on-site config, account linking, tools, recently visited sites, etc. You can also view feeds, hot products, how-to guides, videos, and events. **Note** Feeds, products, how to, videos, and events are not supported in some countries/regions.
Products	In the Products module, you can view, search for, download, and share the product information, including the product description, parameters, and documents. **Note** For countries/regions that do not support products, this module is not displayed.
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.
Explore	You can view feeds about Hikvision products and solutions, how-to guides, videos, and events. **Note** For countries/regions that do not support explore, this module is not displayed.

Module	Description
Health	**Note** For countries/regions that support the Explore and Products modules, this module cannot be accessed via the Health tab at the bottom, but can be accessed via **Health Monitoring** or **More → Health Monitoring** on the Home page, or via **Site → Health Monitoring** . Includes the following sub-modules: • **Health Status:** Provides near-real-time information about the status of devices (including the encoding device, alarm device, access control device, etc.,) added to the sites. You can view device status of a specific site or all sites. • **Exception Center:** Shows all the history notifications of device exceptions and channel exceptions. • **Scheduled Report:** Sends the health check reports of encoding devices and AX PRO devices to target recipients regularly.
Me	**View and Edit Account Information:** You can view the information of the current account, including name, authentication status (Authenticated and Not Authenticated), and your QR code. You can also tap the profile photo to view or edit the profile photo, name, email, phone number, QR code, password, etc. **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. **Switch Company:** If you have completed company merging and your account still exists in more than one company, or if the companies in which your account exists are all kept on Hik-Partner Pro, you can tap **Switch Company** to switch to another company. For details, refer to ***Become a Hik-Partner Pro User After Product Upgrade*** .
	: Tap to enter the Support page.

Module	Description
	Note Case, RMA, and How To are only available to some users in some countries/regions. For details, contact Hikvision. • **Case:** A center for you to report any issues generated when using Hik-Partner Pro. And our technical support will receive your issues and help you resolve them as soon as possible. For more about Case, refer to ***Case*** . • **RMA:** You can submit RMA requests to return products for exchanges or repairs, and view and handle your RMA requests. For details, refer to ***Return Material Authorization*** . • **Feedback:** If you have any suggestions about the platform, you can submit your suggestions to us. 1. Select a type for your suggestion and then enter your suggestions and upload pictures if necessary. 2. Tap **Submit**. • **How To:** You can view how-to guides (documents and videos) for helping you solve problems you encounter when using our products. You can also enter keywords in the search bar on the top of the Support page to search for how-to articles. • **Contact Us:** You can contact us by calling or sending emails to us, and our address is also shown in Contact Us. • **Chatbot:** You can seek online help if you have any questions about using the Mobile Client.
	: Tap to enter Settings page. • **Upgrade Account:** When you logged in by the Hik-ProConnect account, you can tap **Upgrade Account** and tap **Register** or tap **Login** to register an OneHikID account or log in by an existing OneHikID account. • **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. • **Logout:** Log out of the current account and return to the login page. • **Delete Installer Admin Account:** If you are the Installer Admin and the account is no longer used, you can delete the Installer Admin account.
	My Points: You can view your reward points or get more points to redeem for gifts. For more information about the reward point system, see ***Rewards Store*** .

Module	Description
	• **Service Market**: You can view services in the Service Market. You can tap a specific service package to view its details and purchase by service key. **Note** You should purchase the service package online (not by service key) via the Hik-Partner Pro Portal. For details, refer to *User Manual of Hik-Partner Pro Portal*. • **My Service**: View and manage all services you purchased and their details, including free packages.
	Company Management: Tap **Company Management** to enter the Company page. • **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. • **Co-Branding:** This function helps to enhance brand awareness. Once enabled, your customers can view your company logo, address, and phone number via the Hik-Connect Mobile Client. For details about how to get the co-branding service for free and enable the service, refer to ***Co-Branding*** . • **Employee:** Each company has only one Installer Admin but can have multiple Installers. The Installer Admin can invite the company's employees to register Installer accounts and assign different permissions to employees according to actual needs. Installer whose role contains permission **Manage Account and Role** can also invite other employees to be Installers by registering Installer accounts. • **Role and Permission:** A role defines one employee's rights to the functions in the system. After creating a role and specifying the role's permission, you can assign it to the employees according to actual needs. **Note** For countries and regions only with support for free functions, **Employee** and **Role and Permission** are not supported.
	My Favorites: You can view the news, how-to, and products which you added to your favorites. **My Comments:** You can view your comments on the news, how-to, and products.

Module	Description
	My Events: You can view all the events that you have registered and their detailed information.
	Verify Gifts: Distributors can verify the gifts redeemed offline and export the records. **Note** This function is available only to some users in some countries/regions. For details, contact Hikvision.
	Questionnaire: You can tap a questionnaire to jump to the website and answer the corresponding questions, which is important for better user experience and services.
	Help Center: • **Help:** Open the user manual of the Hik-Partner Pro Mobile Client. You can enter keywords to search the information you want in the user manual for help. • **Display Demo:** Displays brief introductions to the five features of the Mobile Client such as "What is Site?" and "What is Exception?". • **Wizard:** You can view the detailed explanations and operation guidance of some important functions of the Hik-Partner Pro 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. • **Tutorial Center:** You can view videos, solutions, technical guidance, user manuals, and so on to learn more about Hik-Partner Pro and the proper ways of using the product. • **After-Sales Authorization Code:** The after-sales authorization code is exclusive to the technical support staff for troubleshooting only. You can give your authorization code to the staff when it is necessary to log in to your account for troubleshooting. The staff can log in to your account via the authorization code to view or edit the information about the company (including name, type, etc.), manage sites, remotely devices (including AX PRO, etc.), perform health monitoring, etc. You can tap **Extend** to extend the validity period for the current authorization code or tap **Invalidate** to invalidate the code right away. • **FAQ:** Refer to FAQ to find the answers to your questions about Hik-Partner Pro quickly.

Module	Description
	Link with Hik-Connect Account: Link your account with Hik-Connect accounts to synchronize devices automatically from the linked Hik-Connect accounts.
	Hik-ePartner: If you have linked your account with your Hik-ePartner account, this section will be displayed for you to unlink from the Hik-ePartner account.
	Marketing Communications: For Installer Admin, if you did not 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. After unsubscription, you will not receive any emails about marketing communications from us. **Distributor:** You can view the distributor to which your account is linked. You can contact the distributor to get support if you encounter issues on Hik-Partner Pro. For details, see ***Link Your Account to a Distributor*** .

Home Page Introduction

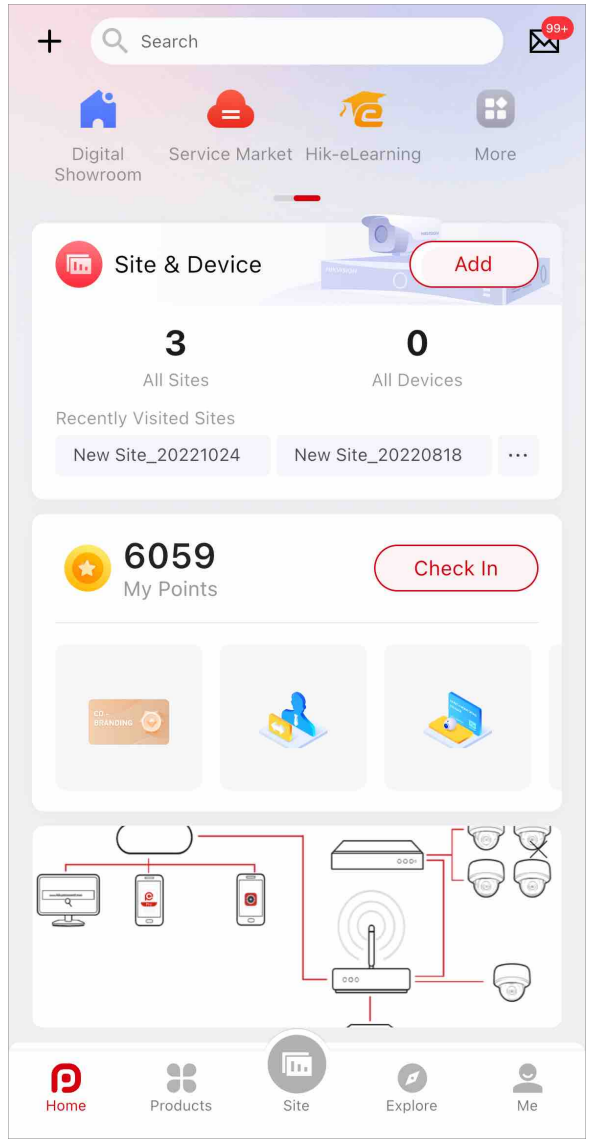


Figure 5-1 Home Page

Table 5-2 Home Page Description

Name	Introduction
+	**Scan QR Code** You can scan the QR code to add a device, view marketing communications, etc.

Name	Introduction
	Tap on the top right corner to view the details about different types of QR codes and their functions. 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 ***Add New Site*** . 2. Scan the QR code on the device to add it. For details about adding device, refer to ***Add Device by Scanning QR Code*** . 3. Scan the QR code generated by iVMS-4200 or iVMS-4500 to add multiple devices. For details about adding devices, refer to ***Add Device by Scanning QR Code*** . 4. Scan other QR codes such as the QR code of marketing communications to enter the related web pages for more operations. **Add Site & Device** Quick entries for adding devices and sites. For details, refer to , , and .
Search	You can search for feeds, how to, products, events, and sites and devices by entering keywords.
✉	In the Notification Center, you can view and handle all history business notifications (site sharing notifications, device management invitations, etc.), and view notifications of device and channel exceptions, system messages, and deals & offers.
Application Center	You can select 7 applications from the application center to display them on the Home page for quick access. • **Tools:** Quotation Tool, On-Site Config, Remote Batch Config, Batch Arm/Disarm, On-Site Batch Upgrade, Batch Device Search, Search for Important Firmware Update, and Account Linking ◦ **On-Site Config:** Batch configure online encoding devices on the same LAN with the Mobile Client via custom templates. See ***Batch Configure Devices on LAN*** for details. ◦ **Remote Batch Config:** Remotely batch configure AX PRO devices via custom templates. See ***Batch Configure AX PROs*** . ◦ **Batch Arm/Disarm:** Batch arm/disarm AX PRO devices on different Sites. See ***Batch Arm/Disarm AX PRO and AX HYBRID PRO*** . ◦ **On-Site Batch Upgrade:** Batch upgrade devices including encoding devices on the same LAN. See ***Batch Upgrade Devices on LAN*** . • **Calculators:** Disk Calculator, NVR Channel Calculator, Focal Length Calculator, and Bandwidth Calculator

Name	Introduction
	• **Learning:** Hikvision eLearning, Digital Showroom, Help, and Tutorial Center • **Rewards:** Rewards Store, Lottery **Note** Lottery is an event where you can upload sales receipts to get lottery tickets for chances of winning prizes, which is not available in some countries/regions or to some accounts. • **Support:** Chatbot, Case, RMA, Feedback, Contact Us, and FAQ • **Maintenance:** Health Monitoring • **Online Service:** Service Market
Sites and Devices Overview	You can view numbers of all/abnormal sites and all/abnormal devices. You can tap **Add** to add sites and devices. For details, refer to ***Add Device*** , ***Add New Site*** , and . You can view recently visited sites. Tap a site to enter the site details page.
Earn Points and Redeem for Gifts	You can check in, add devices, or do some other tasks to get the reward points redeemable for gifts. For more information about the reward point system. See ***Rewards Store*** for details.
Banner	Banners show the key features, functions, important information about Hik-Partner Pro, and events (including lottery draws where you can upload sales receipts to get lottery tickets for chances of winning prizes). **Note** Events such as lottery draws are not available in some countries/regions or to some accounts.
Feeds, Products, How To, and Event	• **Feeds:** You can view up-to-date news and information about Hikvision products and solutions. • **Products:** You can view information about hot products. • **How To:** You can view how-to guides (documents and videos) for helping you solve problems you encounter when using our products. • **Event:** You can view event details, and register for and participate in events, such as product promotions, trainings, lucky draws, and lottery.

Name	Introduction
	Note Lottery is an event where you can upload sales receipts to get lottery tickets for chances of winning prizes, which is not available in some countries/regions or to some accounts. **Note** For countries/regions that do not support Products and Explore, this section is not displayed; instead, the Tutorial Center section will be displayed.

Chapter 6 Site Management

A site can be regarded as an area or location with actual time zone and address, such as your customers' home, office, etc. You can create a site on Hik-Partner Pro to manage devices on it. Moreover, after you complete installing and setting up devices on a site, you can hand over the site and devices to your customer.

Read the following two sections to learn more about the key features related to site management.

- ***Real Sites and Sites on Hik-Partner Pro***
- ***Typical Scenario of Handing Over Site***

Real Sites and Sites on Hik-Partner Pro

The following diagram shows the relationship between the "real sites" and the "sites on Hik-Partner Pro".

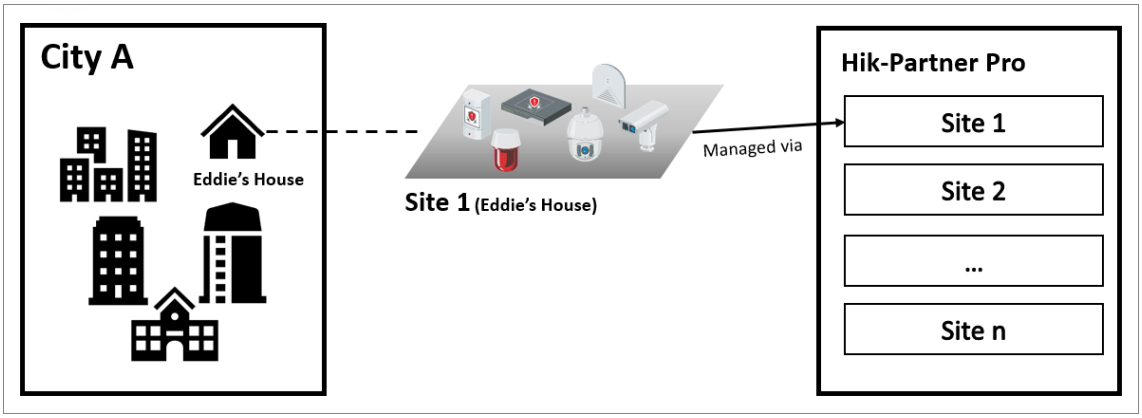


Figure 6-1 Manage Devices via "Site"

Typical Scenario of Handing Over Site

The following diagram shows a typical scenario related to device handover and authorization, as well as the overall process. For more information, see ***Hand Over Site*** .
In the diagram, HPP represents Hik-Partner Pro and HC represents Hik-Connect.

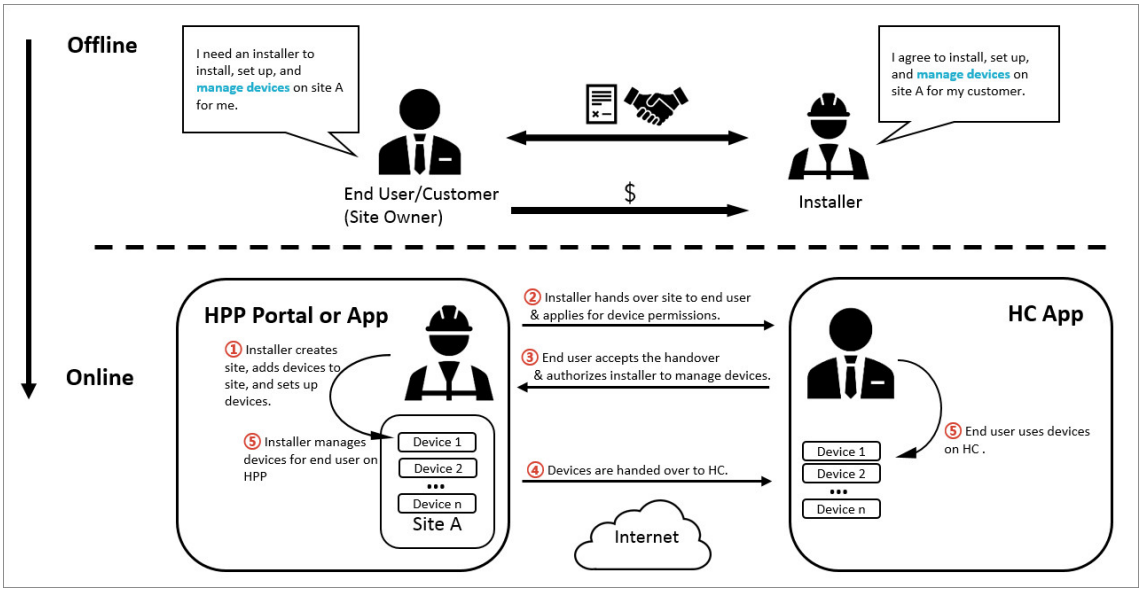


Figure 6-2 Scenario and Process

6.1 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 for sites, adding sites, and handing over sites.

There are different statuses for the sites in Site list.

Not Handed Over

The site is newly added, and you have not hand over it to the end user, or the end user has not accepted the handover.

Not Registered

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

To Be Accepted

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

Handed Over, Not Authorized (Shown as No Commission Authorization)

The end user accepts the handover, 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 6-1 Supported Operations in Different Status

Supported Operations	Not Handed Over	To Be Accepted Not Registered	Handed Over, Not Authorized (Shown as No Commission Authorization	Authorized and Monitoring (Shown as Email Address or Phone Number)
Search Site	√	√	√	√
Hand Over Site	√	√	×	×
Manage Device	√	√	×	√
Edit Site	√	√	×	√
Delete Site	√	√	×	×
Apply for Authorization	×	×	√	×
Share Site	×	×	×	√

Note

If there are abnormal devices on sites, you can view a red icon indicating the number of abnormal devices beside **Site**. If the number of abnormal devices equals or exceeds 100, you can view the icon . Also, you can click the Search box to view all abnormal devices.

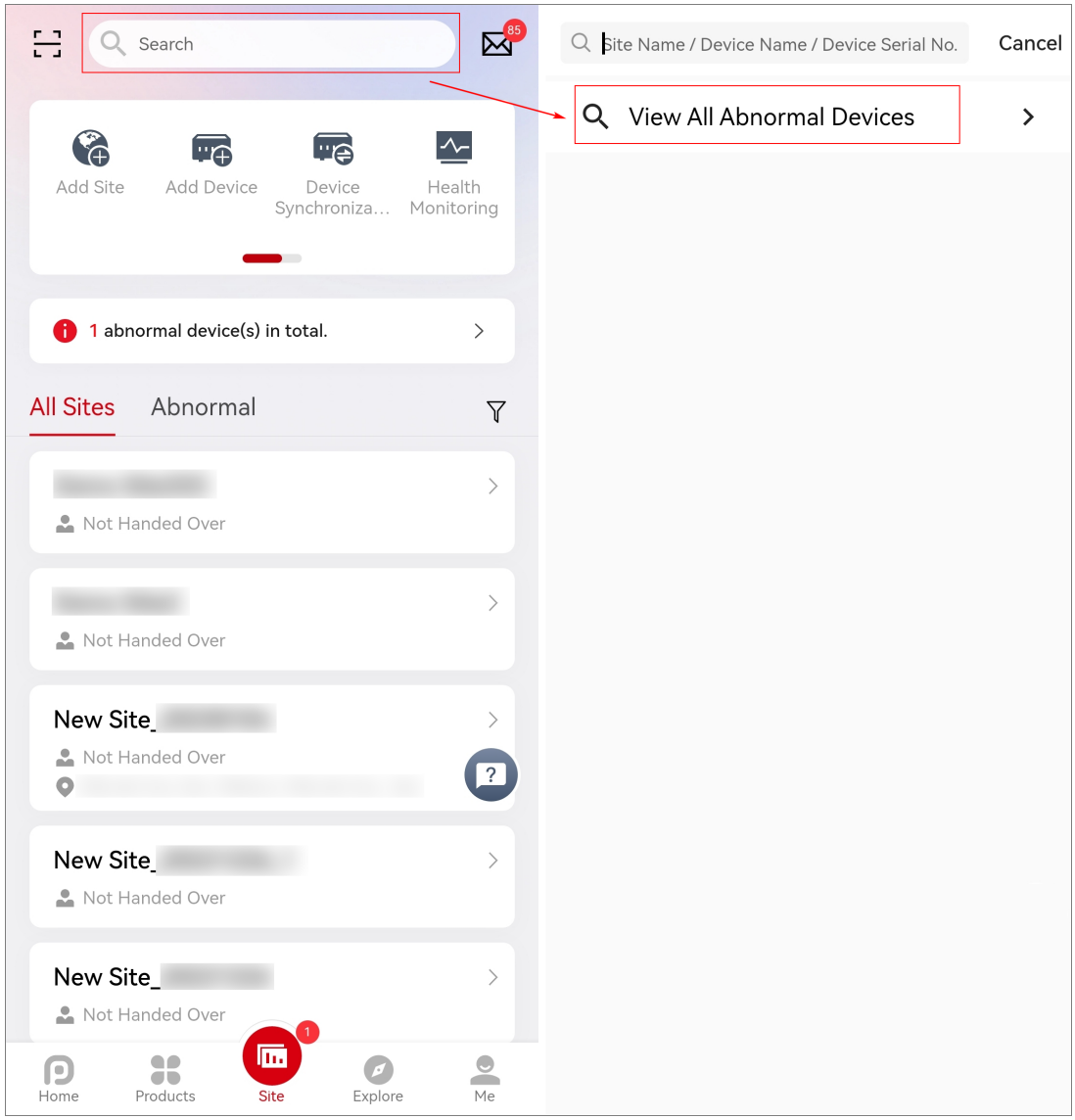


Figure 6-3 Search Sites Where Offline Devices Exist

6.2 Add New Site

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

Steps

1. Enter the Add New Site page.

- Tap the **Site** tab at the bottom to enter the Site page. Tap Add Site to enter Add New Site page.
- Tap **Add** in the Site area on the Home page.

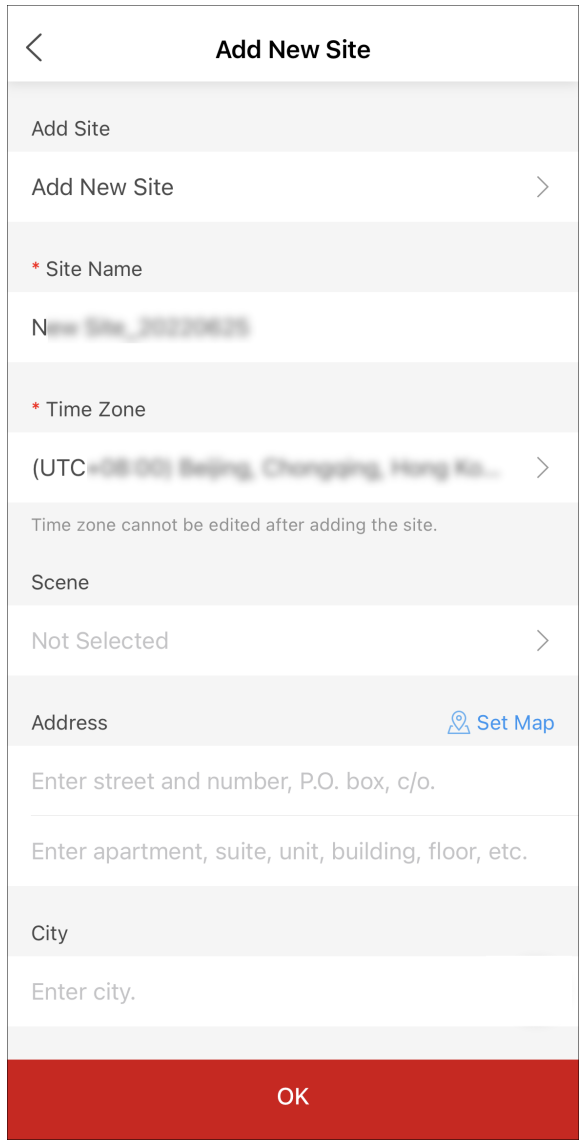


Figure 6-4 Add New Site

Note

If an existing site of customer is not authorized to any installation company, you can select **Add Existing Site** to add the existing site. For more details, refer to ***Add Existing Site*** .

2. 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 plans for the site and devices according to the selected scene.
- You can tap **Set Map** to set the location of the site on the map.

3. **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.
4. **Optional:** Enter the end user information, such as contact number and maintenance records as the remark.

Note

The end user can view the remarks via Hik-Connect Mobile Client.

5. Tap **OK**.

Note

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

6. **Optional:** Perform further operations.

Search Site	Enter keywords in search filed, and tap **Search** to display the results in the list.
View Site Details	Tap the site name to view the site details, including managed devices, site information, and so on.
Navigate with Map	Tap **Map** to enter the Map page, tap **Navigate** in the bottom to pop up the navigation tool(s) installed on the mobile phone, select a navigation tool to start navigation.
Edit Site	Tap ··· in the upper-right corner on the Site Details page, and then tap **Mange Site Information** to edit the site information. You can edit the site name, site address, city, state/province/region, GPC and remarks. If you are authorized to manage the site, you can also edit whether to enable **Sync Time & Time Zone to Device**.
Delete Site	Tap ··· in the upper-right corner on the Site Details page, and tap **Delete Site** to delete the site. **Note** If a site contains armed security control panel(s), it cannot be deleted.
Hand Over Site	For the site in the status of **Not Handed Over**, tap **Hand Over Now** on the Site Details page to hand over the site to your customer.

Note

For more details, refer to ***Hand Over Site*** .

Manage Device

For the authorized site or the site with the status of **Not Handed Over**, **Not Registered**, or **To Be Accepted**, enter the Site Details page to manage the devices, such as adding devices to the site, upgrading device, deleting devices, applying for live view or configuration permission, , adding linkage rule, adding exception rule, etc.

Note

If a security control panel is armed, it cannot be deleted unless being disarmed first.

6.3 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. Enter the Add New Site page.
   - Tap the **Site** tab at the bottom to enter the Site page. Tap Add Site to enter Add New Site page.
   - Tap **Add** in the Site area on the Home page.

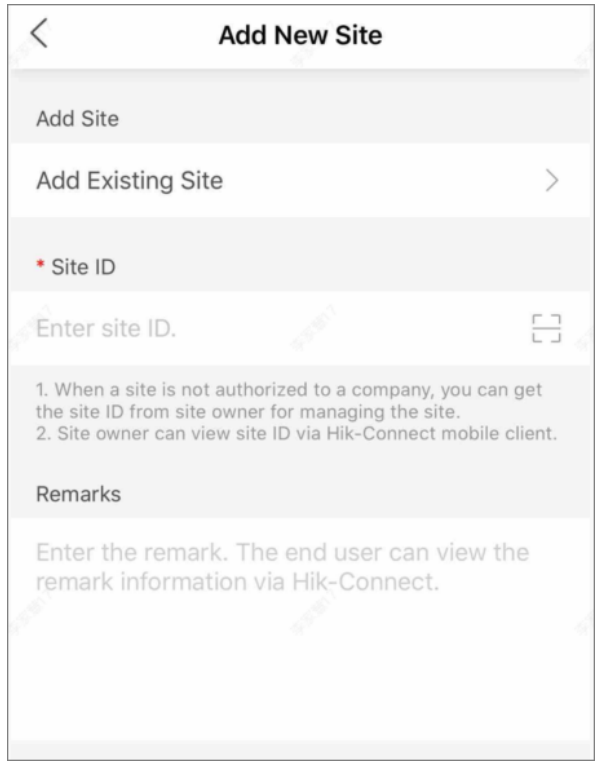


Figure 6-5 Add Existing Site

2. Select **Add Existing Site** as the adding method.
3. Enter the Site ID or scan the QR code of the Site.

Note

- You can get the Site ID form 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 (V 4.15.0 or later).

4. Tap **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.

6.4 Assign Site to Installer

The Installer Admin or the Installers with the Manage All Sites permission can assign a site to the specified Installer as site manager responsible for configurations of the devices on the site.

Before You Start

Make sure you have the Manage All Sites permission.

Steps

1. Tap the **Site** tab at the bottom to enter the Site page.
2. Tap to enter the Assign page.

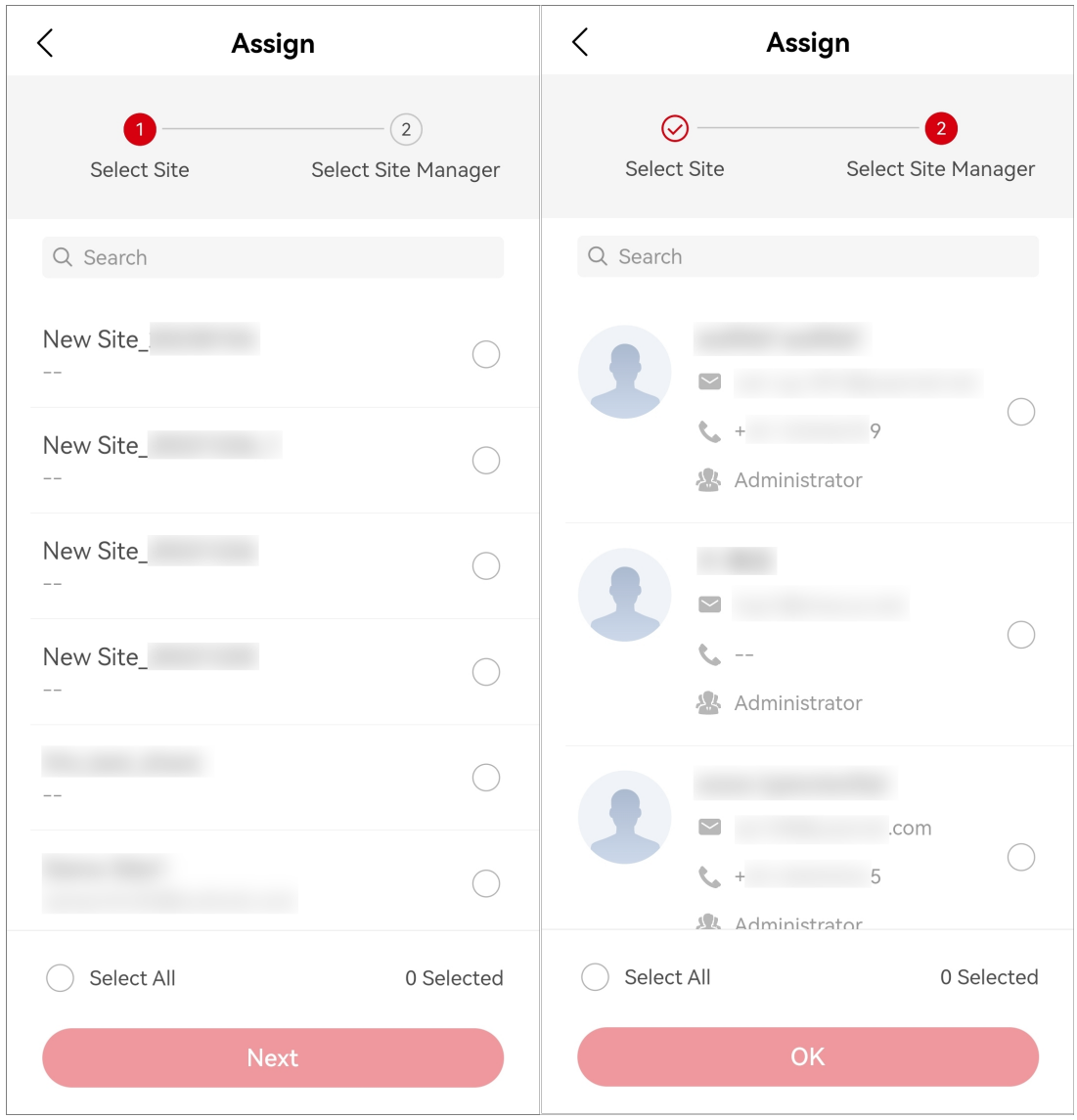


Figure 6-6 Assign Site to Installer

3. Select one or multiple sites for assignment, and tap **Next**.

Note

- You can check **Select All** to select all the sites.
- You can search for specific sites by entering keywords in the **Search** field.

4. Select one or multiple Installers as the site manager(s) of the selected site(s).

Note

- You can check **Select All** to select all the site managers.
- You can search for specific site managers by entering keywords in the **Search** field.
- No more than 100 site managers can be assigned to each site.

5. Tap **OK**.

   The site manager of assigned sites can enter site details and perform related operations, such as adding devices.

6.5 Hand Over Site

After the installation company completed the installation, the Installer needs to hand over the site to a customer. If required, the Installer can also apply for specified permissions for further device maintenance when handing over the site.

Before You Start

Make sure the site status is **Not Handed Over** and you have the permission of site management, such as managing all sites and assigned sites.

Steps

1. In the site list, tap a site to enter the Site Details page.
2. Tap **Hand Over** to enter the Hand Over Site page.
3. Select **Email** or **Phone Number** as handover mode.
4. Enter site owner's email address or phone number.
5. **Optional:** Check **Allow Me to Disable Hik-Connect Mobile Client Remote Use**.

Note

- If the check-box is checked, after you handed over the site to your customer and your customer approves the request, you can disable the Hik-Connect Mobile Client remote use for devices that you rent to your customer without their authorization. If the Hik-Connect Mobile Client remote use is disabled, your customer will not be able to use these devices via the Hik-Connect Mobile Client for live view, playback, receiving alarms, etc. The tenant site scenario is a typical scenario to which this feature is applicable (see ***Typical Tenant Site Scenario*** for details).
- You can go to the **Device** tab to disable the Hik-Connect Mobile Client remote use for one device or all devices in this site by tapping or setting the **Hik-ConnectMobile Client Remote Use** switch to off. You can also delete the devices from your customer's Hik-Connect account without her/his authorization.

6. **Optional:** If you have checked **Allow Me to Disable Hik-Connect Mobile Client Remote Use** in the previous step, check **Grant Me Highest Configuration Permissions for Devices on Site** to get the highest permissions for devices on the current site which your customer cannot edit.
7. **Optional:** Select permissions to apply for.

Note

- You can set the validity period for the permissions of configuration, live view, and playback, and select the device(s).
- If you have no permission for managing devices, or no devices are added to the site, you cannot select the permissions of configuration, live view, and playback when handing over the site.
- If the following permissions are selected, when the end user accepts the handover, the permissions will be authorized to the installer. The installer does not need to apply for authorization from the site owner again.

Site Information Management

The permission to manage the site information.

Configuration

The permission to configure selected devices on the site.

Live View

The permission to stream the live video from the selected devices on the site.

Playback

The permission to play back videos of the selected devices on the site.

8. **Optional:** Check **Apply for Activation of Cloud Attendance Service**.

Note

- If the check-box is checked, after you handed over the site to your customer, he/she will be able to use the cloud attendance system provided by Hikvision or third-party manufactures.
- If the cloud attendance system provided by Hikvision has been added to the site and activated, the check-box will appear on the Hand Over Site page.
- If the cloud attendance service is provided by a third-party manufacturer, the check-box will be **Allow ### System to Access** or **Allow Third-Party Attendance System to Access**. ### here refers to the name of the third-party manufacturer.

9. **Optional:** Check **Apply for Site Authorization for Maintenance Service Partner** to apply for site authorization for your maintenance service partner.

Note

For details, refer to ***Share a Site During Handover*** .

10. Enter the remarks, such as the reason of the handover, which your customer can view when he/she receives the handover via the Hik-Connect Mobile Client.
11. Tap **OK** to send the handover.

- Your customer will receive the handover email or message in email box or via short message with a download link of the Hik-Connect Mobile Client. Your customer can download or open Hik-Connect Mobile Client via the link.
- If your customer has not registered a Hik-Connect account, he/she needs to register a Hik-Connect account first. After registering the account and accepting the handover via the 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 (V 4.15.0 or later). You can send the QR code or download link shown in the banner on the Home page to them.

- If your customer wants you to manage and maintain his/her devices, after your customer accepts the handover via the Hik-Connect Mobile Client and becomes the site owner, he/she needs to authorize related permissions to you.

12. **Optional:** Before your customer accepts the handover, tap **Not Registered** or **To Be Accepted** to send handover again.

Note

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

6.6 Typical Tenant Site Scenario

In a typical tenant site scenario, you can help the property management company install and set up their security devices in their apartments, and help manage the devices so that the devices will be available for the tenants only during lease periods; as for the tenants, you can help them manage and configure the devices during lease periods.

To know more about the typical tenant site scenario, read the sections below:

- ***Two Agreements Reached***
- ***Online Operations***

Two Agreements Reached

Before you can hand over the devices in the apartment to the tenant via Hik-Partner Pro, the following two agreements have to be reached.

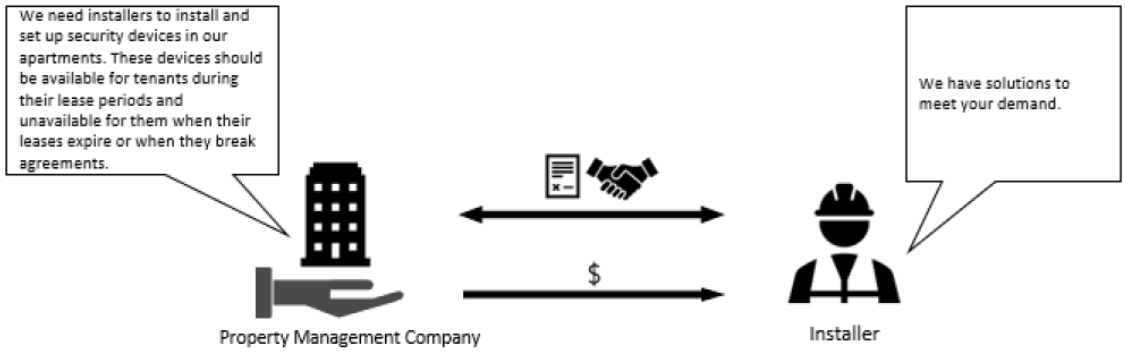


Figure 6-7 Agreement Reached Between the Property Management Company and Installer

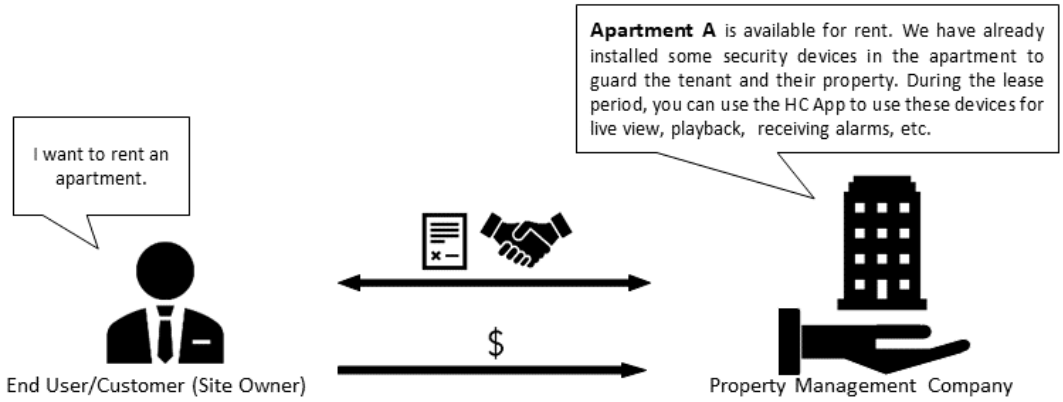


Figure 6-8 Agreement Reached Between the Tenant and Property Management Company

Online Operations

After the two agreements are reached, you will operate on Hik-Partner Pro to hand over the devices to the tenant, of which the process are shown below:

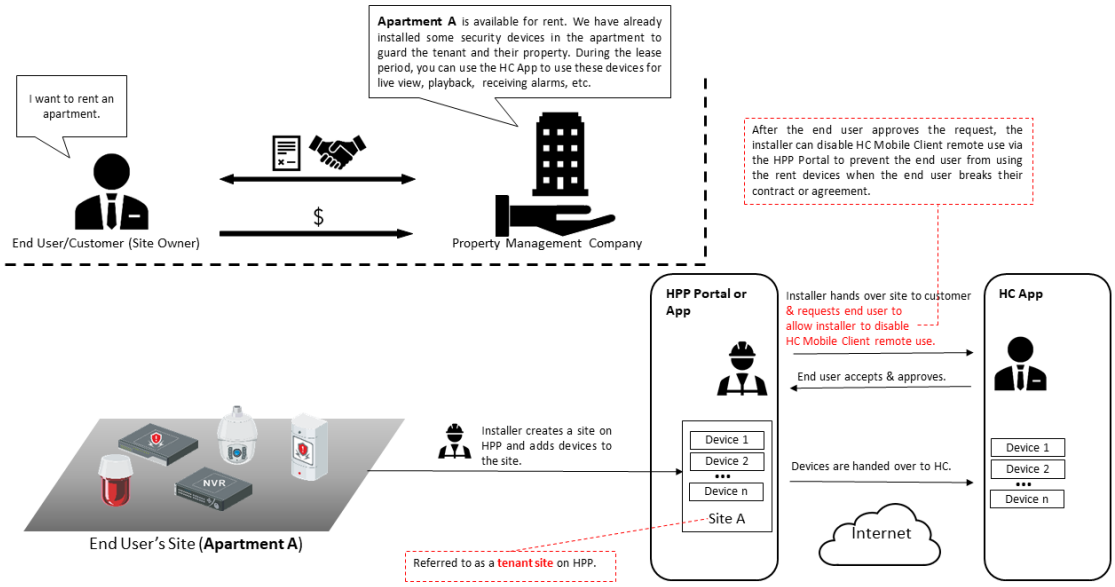


Figure 6-9 Hand Over Devices to the Tenant

1. Create a site. Refer to ***Add New Site*** for more details.
2. Add the devices to the site.
3. Batch configure the devices. Refer to ***Batch Configure Devices on LAN*** or ***Batch Configure AX PROs*** for more details.
4. Hand over the site to the tenant. Refer to ***Hand Over Site*** for more details.

Note

You should request the tenant to allow you to disable the Hik-Connect Mobile Client remote use, and if the tenant does not approve the request, the devices will not be handed over.

5. The tenant accepts the handover on the Hik-Connect Mobile Client, which means the tenant also approves your request to allow you to disable the Hik-Connect Mobile Client remote use and approves your application for permissions (if any).
6. The devices are handed over to the tenant's Hik-Connect account.

6.7 Apply for Site Authorization from Site Owner

When the Site (no permission selected when handing over site) 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. Select one of the followings to apply for authorization.
   - Tab the prompt about no authorization in Site list.
   - Tap Site to enter Site Details page. Tap ··· in top right corner, and tap **Batch Apply for Permissions**.
2. Select the permission type as required.
3. Select devices for batch applying for permission.
4. 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-Partner Pro, 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-Partner Pro. 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.

5. **Optional:** On the Site Details page, tap ··· → **Discard Authorization** to discard authorization of the Site.

Note

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

6.8 Accept a Device Management Invitation from Your Customer

You can accept a device management invitation from your customer (i.e., a Hik-Connect user) to manage a device that has already been added to a Hik-Connect account. In this way, the device,

along with its configuration and operation permissions, can be shared with you to allow you to manage it for your customer on Hik-Partner Pro. Compared with migrating the device from Hik-Connect to Hik-Partner Pro, which requires your customer to share their Hik-Connect account name and password with you, this way is much more privacy-friendly and easier to be accepted.

To know more about the device management invitation, read the sections below:

- ***Overall Process***
- ***How Your Customer Invites You to Manage Their Device***
- ***The Email of Device Management Invitation***
- ***The Notification of Device Management Invitation***

Overall Process

If your customer (i.e., the Hik-Connect user) has already added one device to their Hik-Connect account, the customer can use the Hik-Connect Mobile Client to invite you to manage this device. Once the customer completes the invitation, an email containing the invitation information (e.g., the Hik-Connect user name and device name) and the button/link for accepting the invitation will be sent to you, and then you can accept the invitation. Invitations for device management can also be accepted via ✉ → **Business Notification** . Once you accept the invitation, the device will show on the specified site (namely, the site mentioned in the email or the notification) on Hik-Partner Pro.

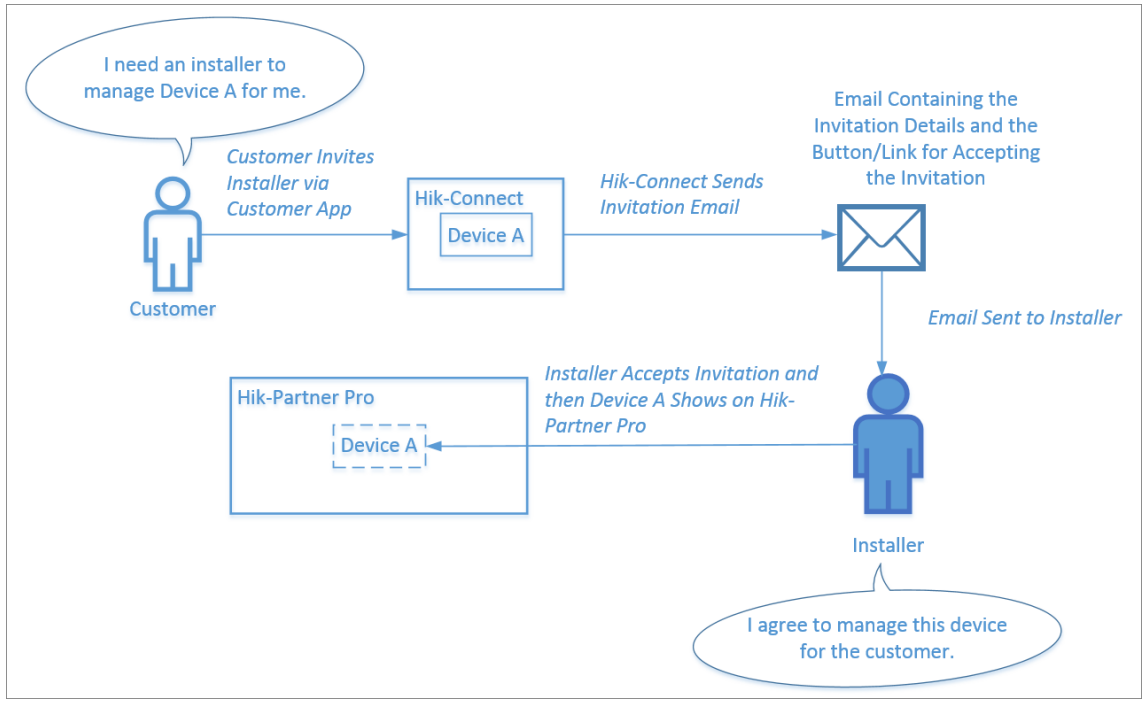


Figure 6-10 Overall Process Diagram

How Your Customer Invites You to Manage Their Device

You can go to the site list page, and then tap **Add Device → Learn More → Authorization Wizard** to open the following page to see how your customer uses the Hik-Connect Mobile Client to invite you to manage their device. It should be noted that you need to provide your Hik-Partner Pro account (email address) to your customer first to let them specify you as the Installer who manages their device.

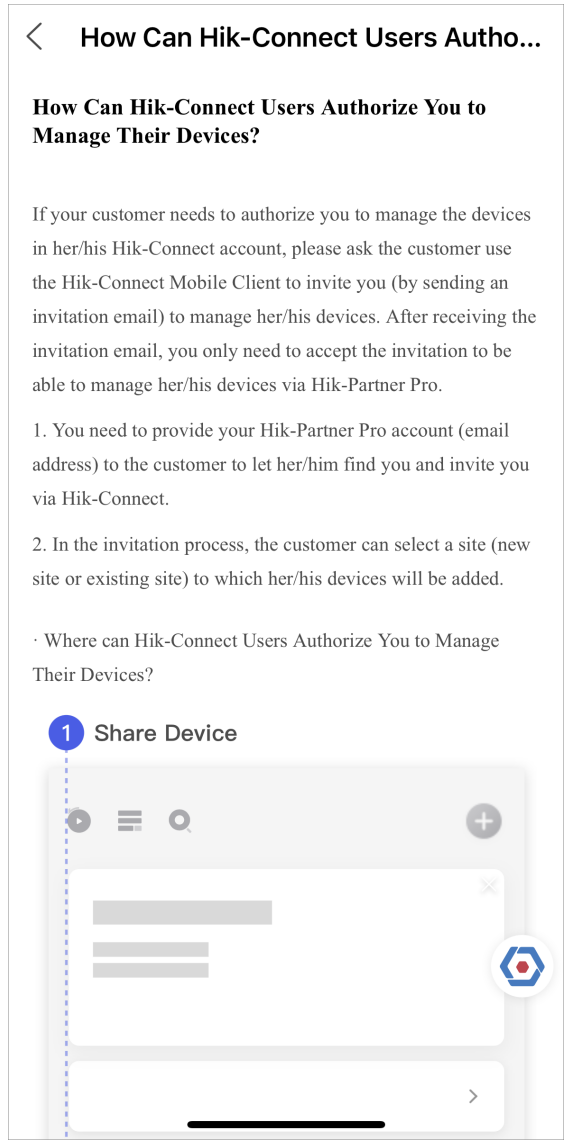


Figure 6-11 How Can Hik-Connect User Authorize You to Manage Their Device

The Email of Device Management Invitation

The email shows the invitation details including the device name, device serial number, name of the site where the device(s) is added, Hik-Connect user account, and the time of invitation. If you

agree to manage the device(s) for your customer, you need to accept the invitation in three days, otherwise the invitation will be invalid.

The Notification of Device Management Invitation

The notification shows the invitation details including name of the site where the device(s) is added, device name, device serial No., the Hik-Connect user account, and the time of invitation. If you agree to manage the device(s) for your customer, you need to accept the invitation in three days, otherwise the invitation will be invalid.

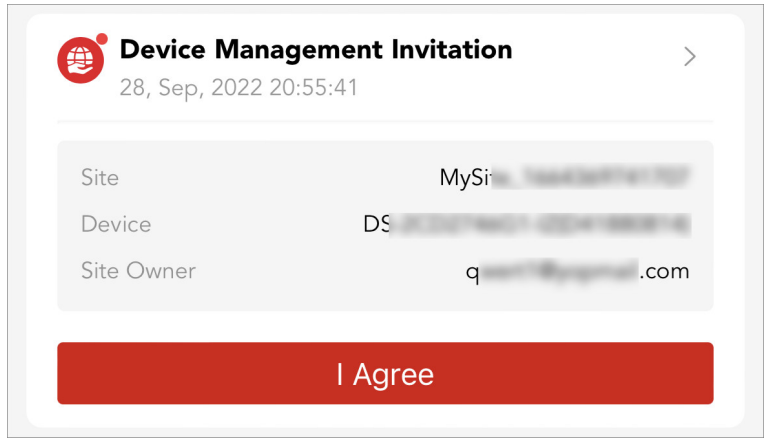


Figure 6-12 Sample Notification

6.9 Site Sharing

Before the site handover, you can share a site with your installation service partner (ISP) so that they can help you add and hand over devices. During and after the site handover, you can share a site with your maintenance service partner (MSP) to allow them to cooperate with you in providing device management/maintenance services for your customer, especially in offering technical support. For the ISP, they have all permissions for devices on a shared site before the site handover, and their device permissions will be removed after the site is handed over or the sharing is canceled. For the MSP, you can determine the permissions for them to access devices on the shared site, and after sharing a site, you can change the MSP's permissions.

Note

- If you change the maintenance service partner's permissions, your customer will receive a notification about it on the Hik-Connect Mobile Client.
- If the site is handed over by the ISP to your customer, the handover email/message your customer receives will only contain your company's information and will not contain any information about the ISP.
- You can initiate site sharing with your ISP before the site handover only on the Portal. The Mobile Client currently does not support initiating site sharing with the ISP. For details, refer to *Hik-Partner Pro Portal User Manual*.

Read the following sections to learn the overall process and limitations of site sharing.

Note

In the diagrams, HPP represents Hik-Partner Pro, HC represents Hik-Connect, MSP represents maintenance service partner, and ISP represents installation service partner.

- ***Share a Site Before Handover***
- ***Share a Site During Handover***
- ***Share a Site After Handover***
- ***Limitations***

Share a Site Before Handover

The diagram below shows the overall process of sharing a site before you hand it over to your customer, and in this scenario, suppose your company is an ARC company. For detailed steps, see *Hik-Partner Pro Portal User Manual*.

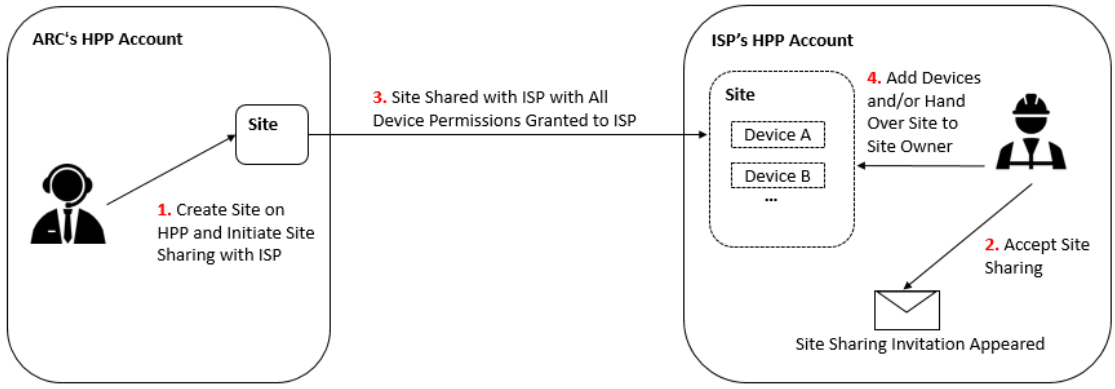


Figure 6-13 Overall Process

Share a Site During Handover

The diagram below shows the overall process of sharing a site when you hand it over to your customer, and in this scenario, suppose your company is an installation company. For detailed steps, see ***Share a Site During Handover*** .

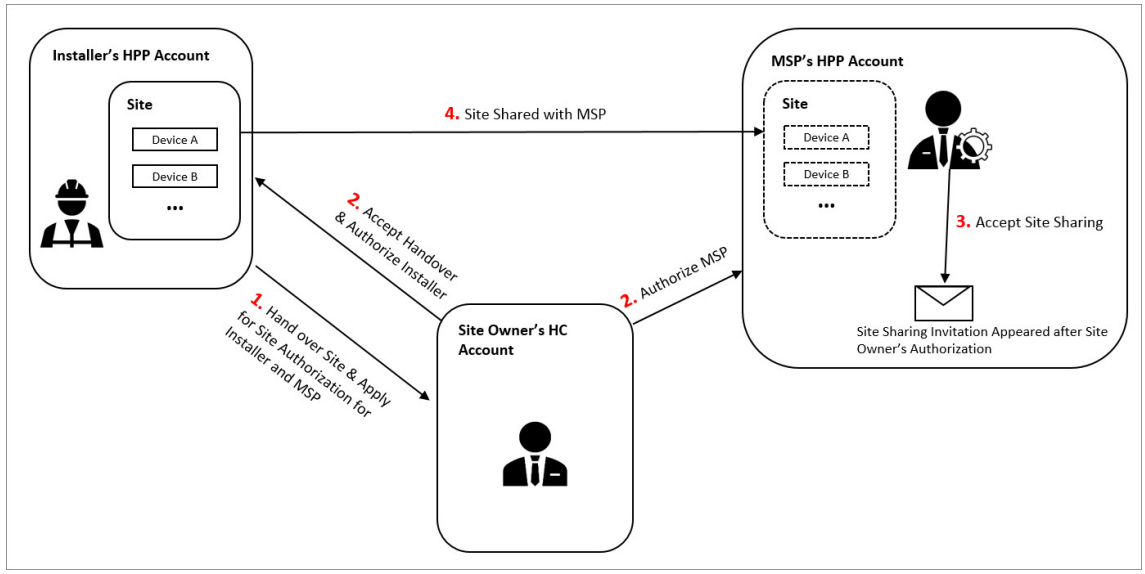


Figure 6-14 Overall Process

Share a Site After Handover

The diagram below shows the overall process of sharing a site that has been handed over to your customer, and in this scenario, suppose your company is an installation company. For detailed steps, see ***Share a Site After Handover*** .

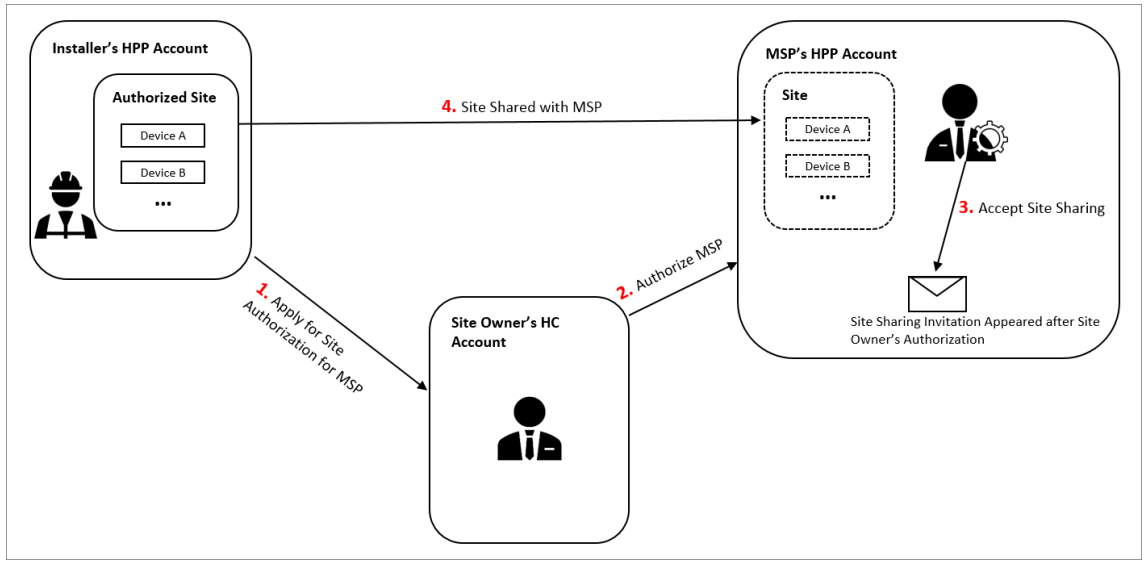


Figure 6-15 Overall Process

Limitations

- Site sharing is not supported in some countries/regions or by some accounts.
- You can only share a site with your MSP's Installer Admin account, or your ISP's account with the Manage All Sites or Manage Assigned Sites permission.
- Your account and the account with which you share a site need to be in the same country/region.
- You cannot share a site with any Installer account of your company.

6.9.1 Share a Site During Handover

You can apply for site authorization and select permissions for the maintenance service partner at the same time when you hand over the site, in order to share the site with your maintenance service partner for managing and maintaining the site together.

Before You Start

Make sure the site status is **Not Handed Over** and you have the permission to manage all sites or assigned sites.

Steps

Note

- The maintenance service partner's Hik-Partner Pro account should be an Installer Admin account, of which the country/region should be the same as that of your account.
- You cannot share the site with the account of any employee in your company.

1. Enter the Hand Over Site page. Refer to ***Hand Over Site*** for details.
2. In the Site Sharing section, switch on **Apply for Site Authorization for Maintenance Service Partner**.
3. Enter the maintenance service partner's Hik-Partner Pro account.

   Note

   If the account has been linked with two or more companies, you should select a company to share device permissions with.
4. Select permissions for the maintenance service partner.

Note

- You can set the validity period for the permissions of configuration, live view, and playback, and select the device(s).
- If you have no permission to manage devices, or no devices are added to the site, you cannot select the permissions of configuration, live view, and playback when handing over the site.
- If the following permissions are selected, when your customer accepts the handover and the maintenance service partner accepts site sharing, the permissions will be authorized to the maintenance service partner.

Site Information Management

The permission to manage the site information.

Configuration

The permission to configure selected devices on the site.

Live View

The permission to stream the live video from the selected devices on the site.

Playback

The permission to play back videos of the selected devices on the site.

5. Configure other settings on the Hand Over Site page. Refer to ***Hand Over Site*** for details.
6. Tap **OK**.
7. **Optional:** After your customer accepts the handover and the maintenance service partner accepts the site sharing, perform the operations below.

View Information About the Maintenance Service Partner	You can view the status of site sharing and the email address of the maintenance service partner on the site details page.
Cancel Site Sharing	You can cancel site sharing on the Site Sharing page.
Change Permissions for the Maintenance Service Partner	You can change permissions for the maintenance service partner on the Site Sharing page. **Note** You can only change the permissions that have already been granted to the maintenance service partner by your customer, and your customer will receive a notification on the Hik-Connect Mobile Client if the permissions are changed.

6.9.2 Share a Site After Handover

After a site is handed over, you can share the site with your maintenance service partner for managing and maintaining the site together.

Before You Start

Make sure the site status is **Authorized** and you have the permission to manage all sites or assigned sites.

Steps

Note

- The maintenance service partner's Hik-Partner Pro account should be an Installer Admin account, of which the country/region should be the same as that of your account.
- You cannot share the site with the account of any employee in your company.

1. On the site list, tap a site to enter the site details page.
2. Tap ··· → **Site Sharing** to enter the Site Sharing page.
3. Enter the maintenance service partner's Hik-Partner Pro account.

   Note

   If the account has been linked with two or more companies, you should select a company to share device permissions with.
4. Select permissions for the maintenance service partner.

   Note

   - You can set the validity period for the permissions of configuration, live view, and playback, and select the device(s).
   - If you have no permission to manage devices, or no devices are added to the site, you cannot select the permissions of configuration, live view, and playback when handing over the site.
   - If the following permissions are selected, when your customer accepts the handover and the maintenance service partner accepts site sharing, the permissions will be authorized to the maintenance service partner.

   Site Information Management

   The permission to manage the site information.

   Configuration

   The permission to configure selected devices on the site.

   Live View

   The permission to stream the live video from the selected devices on the site.

   Playback

   The permission to play back videos of the selected devices on the site.

5. Enter the remarks, such as the reason for site sharing.
6. Tap **OK**.
7. **Optional:** After your customer accepts the application and the maintenance service partner accepts the site sharing, perform the operations below.

View Information About the Maintenance Service Partner	You can view the status and email address of the Maintenance Service Partner on the site details page.
Cancel Site Sharing	You can cancel site sharing on the Site Sharing page.
Change Permissions for the Maintenance Service Partner	You can change permissions for the maintenance service partner on the Site Sharing page. **Note** You can only change the permissions that have already been granted to the maintenance service partner by your customer, and your customer will receive a notification on the Hik-Connect Mobile Client if the permissions are changed.

6.9.3 Accept Site Sharing

If you are the maintenance/installation service partner (MSP/ISP), you can receive and handle the site sharing application in the Notification Center on Hik-Partner Pro.

Before You Start

- If you are the MSP, make sure the site owner has agreed to the device authorization on the Hik-Connect Mobile Client.
- Make sure you (MSP/ISP) have logged in to the Hik-Partner Pro.

Steps

Note

If the site is shared with the ISP, all accounts of the ISP company can view the site sharing application in the Notification Center, but only the ISP account specified in the site sharing application and the accounts with the Manage All Sites permission can handle the application.

1. Tap ✉ in the upper-right corner of the page to enter the Notification Center page.
2. Tap the **Business Notification** tab.
3. Tap **I Agree** to accept the site sharing.

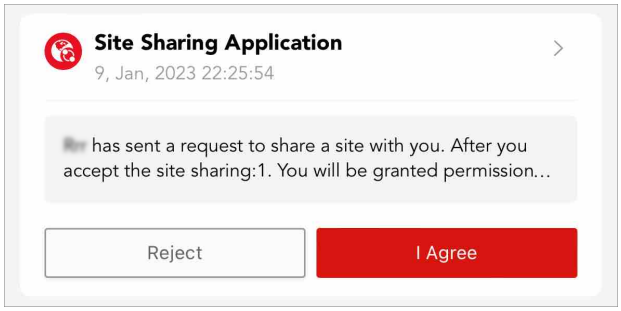


Figure 6-16 Site Sharing Application

For MSPs, you can manage and maintain devices on the shared site; for ISPs, you can add, configure, and hand over devices on the shared site.

6.9.4 Features Available to MSP/ISP on a Shared Site

After the maintenance/installation service partner (MSP/ISP) accepts the site sharing, the MSP can perform configurations and operations which the customer authorized on the shared site, and the ISP can add, configure, and hand over devices on the shared site. The MSP can also release device permissions, and both the MSP and ISP can cancel the site sharing. If the MSP is authorized to manage the site, the MSP can directly applying from the customer for device permissions.

Note

The MSP/ISP who accepted the site sharing cannot share the shared site with another MSP/ISP.

Customer Site

For MSP

Live view and playback, arming and disarming, remote configuration, device upgrade, linkage rule configuration, DDNS configuration, password reset, exception notification configuration, and deleting the site.

Note

If the MSP deletes the site, it indicates that the site authorization is discarded by the MSP, but the installer can still manage the sites and their devices.

For ISP

Adding and deleting devices, live view and playback, arming and disarming, remote configuration, linkage rule configuration, DDNS configuration, exception notification configuration, device upgrade, remote log collection, editing device names, editing site information (except the site name), ARC service configuration, and site handover.

Health Monitoring

Viewing the status of devices on the shared sites, device remote configuration, refreshing devices' status, live view, playback, manually inspecting devices, exporting health check reports, and device upgrade.

Exception Center

Receiving device exceptions and exporting exception records.

Send Report Regularly

Configuring report settings to send reports regularly.

Note

This feature is not available to the ISP.

My Service

Viewing the validity periods, expiration time, and status of activated services of the shared site and their corresponding resources.

Note

- The MSP cannot activate or transfer services on the shared site.
- This feature is not available to the ISP.

MSP Applies from Customer for Device Permissions

If the MSP is authorized to manage the site, the MSP can directly apply from the customer for device permissions. The installer who shared the site will receive the notification after the MSP sends the application for device permissions.
For how the MSP applies from the customer for device permissions, refer to ***Apply for Device Permission*** .

MSP Releases Device Permissions

If the MSP does not need device permissions, or the MSP finished the device configuration task earlier than the planned time, the MSP can release the permission.
For how the MSP releases device permissions, refer to ***Release the Permission for Devices*** .

MSP/ISP Cancels Site Sharing

The MSP/ISP can cancel the site sharing. After the site sharing is canceled, the site (and also the devices on the site) will be deleted from the MSP/ISP's Hik-Partner Pro account, and the granted permissions will be removed.

Chapter 7 Device Management

Hik-Partner Pro supports multiple device types, including encoding device (e.g., solar camera), 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.

7.1 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-Partner Pro 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

- This functionality is only available to certain models of cameras, NVRs, and DVRs.
- Before batch configuring devices, make sure you have connected them to the same LAN with the phone on which the Hik-Partner Pro Mobile Client runs.

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

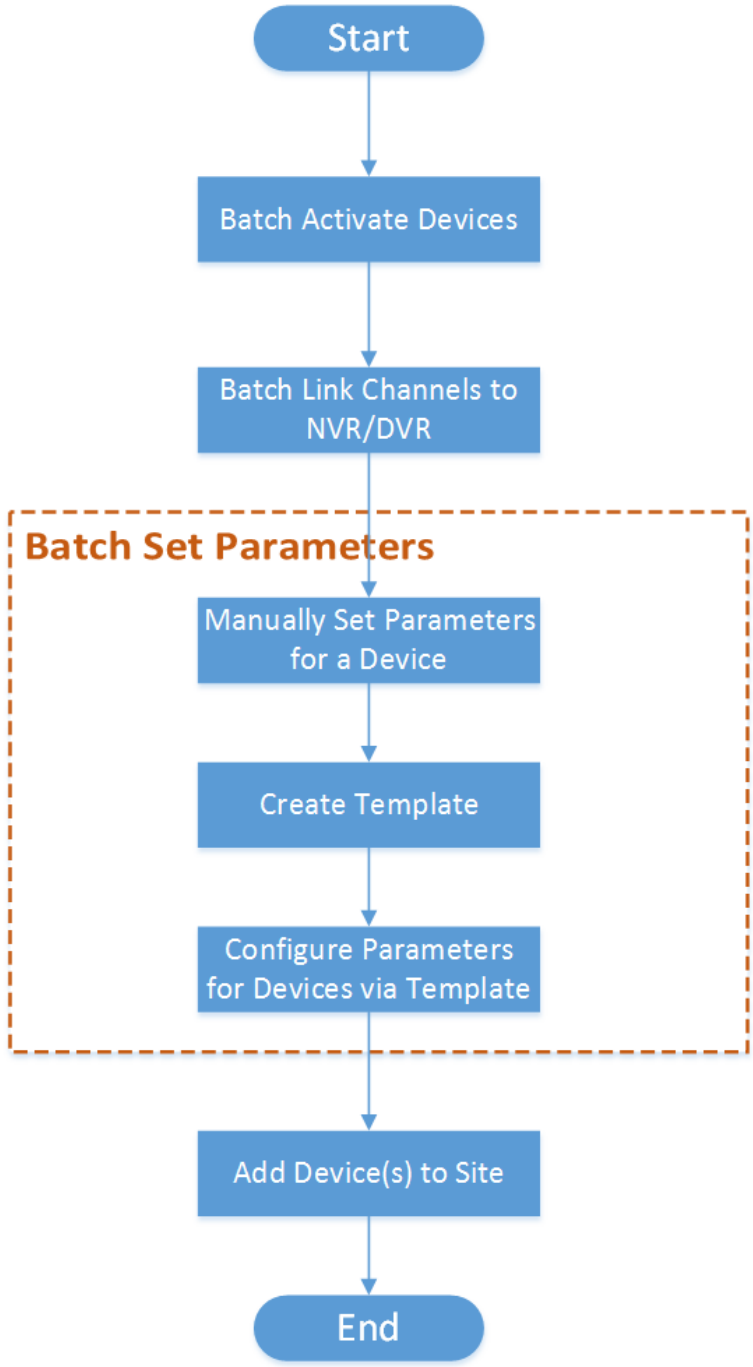


Figure 7-1 Flow Chart

Table 7-1 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-Partner Pro Mobile Client runs, and assign IP addresses for the activated devices. See ***Batch Activate Devices and Assign IP Addresses for Them*** for details.
Batch Link Channels to NVR/DVR	N/A	If the activated devices include NVR/DVR, link channels to NVR/DVR. See ***Batch Link Channels to NVR and DVR*** for details.
Batch Set Device Parameters	Manually Set Parameters for a Device	Select an activated device and set its parameters manually. See ***Create Templates for Setting Parameters*** for details.
	Create Template	Created a template based on the manually configured device. See ***Create Templates for Setting Parameters*** for details.
	Configure Parameters for Devices via Template	Batch configure parameters for multiple devices via a selected template. See ***Batch Set Parameters for Devices*** for details.
Add Device(s) to Site	N/A	If required, add the activated and configured device(s) to a Site. See ***Add Device by Scanning QR Code*** , ***Add Device by Entering Serial No.*** , or ***Add Device by IP Address or Domain Name*** for details.

7.1.1 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. On the Home page, tap **On-Site Config** or **More → Tools → On-Site Config** to enter the configuration page.
2. **Optional:** Tap **Show Inactivated Devices Only** to hide the activated devices.

3. Select the detected online devices to be activated.
4. Tap **Activate and Assign IP Address** to open the Activate and Assign IP Address window.
5. Enter the device admin password and confirm the password.
6. Tap **Activate and Assign IP Address**.

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.

7. **Optional:** Enable **Time Synchronization** to synchronize the time from the mobile phone to the device.
8. Tap **OK**.

What to do next

After activating the devices, you should batch add channels to NVR and DVR. For details, refer to ***Batch Link Channels to NVR and DVR*** .

7.1.2 Batch Link Channels to NVR and DVR

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

Before You Start

Make sure you have activated the NVR, DVR, and network cameras.

Steps

Note

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

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

Note

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

2. Enter the Link Channel page.
   - Select the NVR or DVR and tap **Link Channel**.
   - Tap the NVR or DVR 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 or DVR details page, perform the following operations.

Edit NVR/DVR Name	On the top of NVR / DVR 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.

7.1.3 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 and DVR (if any). See ***Batch Activate Devices and Assign IP Addresses for Them*** and ***Batch Link Channels to NVR and DVR*** 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.

7.1.4 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** .

   Note

   Before setting parameters for an NVR or DVR, you can tap → **Format** to format the disk of the selected device. Batch formatting is not supported.
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.

7.2 Add Device

Hik-Partner Pro accesses devices by two modes: Hik-Connect (P2P) and Device IP Address/Domain Name. The former provides securer data communications (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 communications 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 7-2 Device Adding Methods

Access Mode	Device Adding Method
Hik-Connect (P2P)	• ***Add Devices on LAN*** • ***Add Device by Scanning QR Code*** • ***Add Device by Entering Serial No.*** • ***Synchronize Devices with Hik-Connect Account*** • ***Add Devices Without Support for the Hik-Connect Service***

Access Mode	Device Adding Method
	Note 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 to access the features based on the Hik-Connect service.
Device IP Address/Domain Name	***Add Device by IP Address or Domain Name***

7.2.1 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 a 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**.

The device compatibility test starts.

Note

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

8. Add devices.

Note

For details about adding devices, see ***Add Device by Scanning QR Code*** or ***Add Device by Entering Serial No.*** .

- If there are no upgradeable 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.

7.2.2 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.

7.2.3 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.

You can tap in the upper-left corner to start scanning QR code to add device(s). If so, you can skip the first two steps.

Steps

1. Enter the adding device page.
   - Tap **Add** in the Device area on the Home page.
   - Tap **Site** in the bottom, and then tap **Add Device** above the site lite.
   - Tap **Site** in the bottom, and tap a Site to enter its details page and tap **Add Device**.
2. Select **Scan QR Code** as the adding mode.
3. Scan QR code to add device(s) to a 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 the phone album, tap **Album** to extract the QR code from the local album. In this mode, you can add only one device to a site at a time.

     Note

     - Usually, the QR code is printed on the label, which is on the back cover of the device.
     - Tap to enable the flashlight if the scanning environment is too dark.
     - Please allow the Mobile Client to access the photo album of the phone.
   - Scan a QR code generated by iVMS-4200 or iVMS-4500. After scanning the QR code, you will enter the page for selecting to-be-added devices. Check devices and tap **OK** to add the selected devices to site. By this mode, you can add multiple devices to site at a time.
4. **Optional:** 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.

   Note

   You can add device(s) to an existing Site, or tap **Add New Site** to add the device(s) to a new Site.
5. **Optional:** Perform the following operations if the following situations occur.
   - If the QR code only contains the information on device serial No., you will enter the manually adding page. Add the device manually in this case. See ***Add Device by Entering Serial No.*** for details.
   - If the device is offline, you should connect a network for the device. For details, see ***Connect Offline Device to Network*** .
   - 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 customers to download or update the Hik-Connect Mobile Client (V 4.15.0 or 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-Partner Pro 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-Partner Pro.
- After you add an AX PRO device to Hik-Partner Pro, you will be able to log into the AX PRO by your Hik-Partner Pro account (i.e., Installer account or Installer Admin account) to configure and manage the device; if you delete the AX PRO device from Hik-Partner Pro, you can no longer log into the AX PRO device by your Hik-Partner Pro account.
- After your customer authorizes a Site with AX PRO devices to you, you can log into these AX PRO devices by your Hik-Partner Pro 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-Partner Pro account; if you are the Installer Admin, your employees (i.e., Installers) have no permission to log into these devices by their Hik-Partner Pro 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-Partner Pro account, and you will no longer have the permission to log into these devices by your Hik-Partner Pro account.
- For the AX Hybrid Pro, after the device is added to the Hik-Partner Pro, its account and password which are configured on the Device Configuration page will be overwritten by those of the Hik-Partner Pro.

6. **Optional:** Perform the following operations after adding the device.

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. **Note** 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.

Note

- For details, see the user manual of the device.
- Only encoding devices, doorbells, and security control panels support remote configuration.

Delete Device

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

Note

- Deleting devices (except devices added by IP/Domain) is not supported if the site is authorized.
- For AX Hybrid Pro (V1.0.1 and above) which is connected to the Hik-Connect service and is online, if the device is in the armed status, you should disarm the device before deleting it.

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 the 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**.

  Note

  It is highly recommended that you encrypt the device QR code for security reasons.
  c. Tap **Save** to save the generated QR code to your phone.

Set Type for Unknown Device

If the Hik-Partner Pro cannot recognize a device's type after you add it, you can manually set a device type for it.

a. Enter a device details page, tap ✎ of the Device Type to enter the Device Type page.
b. Select a type for the device.

You can edit it again after the selection.

Edit Device Information

For devices added by scanning QR code generated by iVMS-4200/ iVMS-4500, if the device's information changed, or a network exception occurs, you can edit its information accordingly.

Enter a device page, and tap **IP/Domain** to edit the device's name, IP address, port number, user name, or password, and then tap **Save**.

7.2.4 Add Device by Entering Serial No.

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

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

Steps
1. Enter the dding device page.
   - Tap **Add** in the Device area on the Home page.
   - Tap **Site** in the bottom, and then tap **Add Device** above the site lite.
   - Tap **Site** in the bottom, and tap a Site to enter its details page and tap **Add Device**.
2. Tap **Enter Serial No.** to enter the adding by device serial number page.
3. Enter the device serial number.

   Note

   The device serial number is usually on the device label.
4. **Optional:** 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.

   Note

   You can add the device to an existing Site, or tap **Add New Site** to add the device to a new Site.
5. Tap **Add**.

   Note

   - After adding the device, the Hik-Partner Pro 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-Partner Pro. For devices incompatible with the Hik-Partner Pro, 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-Partner Pro, you will be able to log into the AX PRO by your Hik-Partner Pro account (i.e., Installer account or Installer Admin account) to configure and manage the device; if you delete the AX PRO device from Hik-Partner Pro, you can no longer log into the AX PRO device by your Hik-Partner Pro account.
   - After your customer authorizes a Site with AX PRO devices to you, you can log into these AX PRO devices by your Hik-Partner Pro 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-Partner Pro account; if you are the Installer Admin, your employees (i.e., Installers) have no permission to log into these devices by their Hik-Partner Pro 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-Partner Pro account.
- For the AX Hybrid Pro, after the device is added to the Hik-Partner Pro, its account and password which are configured on the Device Configuration page will be overwritten by those of the Hik-Partner Pro.

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*** .
   - 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.
   - If Enter Verification Code window pops up, enter the device verification code.

     Note

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

   The device will appear in the device list.
7. **Optional:** Perform the following operations.

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. **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. **Note** • Deleting devices (except devices added by IP/domain) is not supported if the site is authorized. • For AX Hybrid Pro (V1.0.1 and above) which is connected to the Hik-Connect service and is online, if the device is in the armed status, you should disarm the device before deleting it.

Set Type for Unknown Device

If the Hik-Partner Pro cannot recognize a device's type after you add it, you can manually set a device type for it.

a. Enter a device details page, tap ✎ of the Device Type to enter the Device Type page.
b. Select a type for the device.

You can edit it again after the selection.

Configure DDNS

After adding the device, the DDNS status will be displayed in the device area. If the DDNS needs to be configured, tap **Configure**. See ***Configure DDNS for Devices*** for details about configuring DDNS.

Note

- For devices with invalid or old firmware version, you can configure DDNS for them to make sure they can be managed by Hik-Partner Pro properly.
- Only encoding devices added by Hik-Connect (P2P) support configuring DDNS.

7.2.5 Add Devices on LAN

Hik-Partner Pro can detect the online devices on the same LAN with your phone, and you can add the detected online devices to Hik-Partner Pro.

Before You Start

Make sure the devices are connected to the same LAN with your phone.

Steps

1. Enter the adding device page.
   - Tap **Add** in the Device area on the Home page.
   - Tap **Site** in the bottom, and then tap **Add Device** above the site lite.
   - Tap **Site** in the bottom, and tap a Site to enter its details page and tap **Add Device**.
2. Select **Scan for Devices on LAN** as the adding mode.

   The device(s) connected to the same LAN with the Hik-Partner Pro will be displayed on the Add Device page. You can view information including device serial No., device IP address, and activation status (activated or not).
3. **Optional:** If you have not added the device to a Site, tap **Add to Site** and select a Site to which the device will be added.

   Note

   You can add the device to an existing Site, or tap **Add New Site** to add the device to a new Site.
4. **Optional:** Tap **Tap here to initialize the device in a few steps.** in the top side and perform the following operation(s) as needed.
   - Tap **Activate Device** to batch activate the devices. For details, refer to ***Batch Activate Devices and Assign IP Addresses for Them*** .

- Tap **Link Channel to NVR** to batch link the network cameras to the NVR or DVR as channels. For details, refer to ***Batch Link Channels to NVR and DVR*** .
- Tap **Batch Configure Devices by Template** to batch set parameters for devices by template. For details, refer to ***Batch Set Parameters for Devices*** .

5. Select the detected device(s) to be added and tap **Next**.
6. Perform part or all of the following 4 steps based on the status of the selected devices before adding them.

Note

- If the device is offline, you should connect the device to network. For details, see ***Connect Offline Device to Network*** .
- For the device which has been activated and assigned with the IP address, **Auto** will be displayed to show that the IP address of this device is automatically assigned.

Table 7-3 Step Description

Step	Description
Activate Device	If there are inactivated device(s) in the selected devices, create a shared device admin password for them in the pop-up window to activate them. **Note** If a device is activated, a fixed IP address will be automatically assigned for it.
Enter Device Password	For devices which are activated but not connected to the Hik-Connect service, you should enter its admin password on the pop-up window. The admin password is created when you activate the device.
Set Device Verification Code	If device(s) failed to be automatically connected to the Hik-Connect service, you need to set a shared device verification code for them to manually connect them to the service.
Test Compatibility	If a device is not compatible with Hik-Partner Pro, you need to upgrade its firmware.

The device added will appear on the device list.

Note

- After the device is added, the Hik-Partner Pro 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-Partner Pro. For

devices incompatible with the Hik-Partner Pro, 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-Partner Pro, you can log into the AX PRO by your Hik-Partner Pro account (i.e., Installer account or Installer Admin account) to configure and manage the device; if you delete the AX PRO device from Hik-Partner Pro, you can no longer log into the AX PRO device by your Hik-Partner Pro account.
- After your customer authorizes a Site with AX PRO devices to you, you can log into these AX PRO devices by your Hik-Partner Pro account to configure and manage them. In this case, if you are an Installer, the Installer Admin can also log into these AX PRO devices by her/his Hik-Partner Pro account; if you are the Installer Admin, your employees (i.e., Installers) have no permission to log into these devices by their Hik-Partner Pro 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-Partner Pro account.
- For the AX Hybrid Pro, after the device is added to the Hik-Partner Pro, its account and password which are configured on the Device Configuration page will be overwritten by those of the Hik-Partner Pro.

7. **Optional:** Perform the following operations.

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.

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.

Note

- Deleting devices (except devices added by IP/domain) is not supported if the Site is authorized.
- For AX Hybrid Pro (V1.0.1 and above) which is connected to the Hik-Connect service and is online, if the device is in the armed status, you should disarm the device before deleting it.

Set Type for Unknown Device

If the Hik-Partner Pro cannot recognize a device's type after you add it, you can manually set a device type for it.

a. Enter a device details page, tap ✎ of the Device Type to enter the Device Type page.
b. Select a type for the device.

You can edit it again after the selection.

Configure Device Quickly	Tap **Quick Configuration for Added Device → Link Channel to NVR** to batch link the network cameras to the NVR or DVR as channels. For details, refer to ***Batch Link Channels to NVR and DVR*** .
	Tap **Quick Configuration for Added Device → Batch Configure Devices by Template** to batch set parameters for devices by template. For details, refer to ***Batch Set Parameters for Devices*** .

7.2.6 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-Partner Pro by specifying its IP address/domain name, user name, password, etc. Once a device is added in this way, you can 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

Note

- 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 the following two methods: ***Add Device by Scanning QR Code*** and ***Add Device by Entering Serial No.*** .
- Only encoding devices mapped in WAN support this function.
- Ask your customers to download or update the Hik-Connect Mobile Client (V 4.15.0 or later). You can send the QR code or download link shown in the banner on the Home page to them.

1. Enter the adding device page.
   - Tap **Add** in the Device area on the Home page.
   - Tap **Site** in the bottom, and then tap **Add Device** above the site lite.
   - Tap **Site** in the bottom, and tap a Site to enter its details page and tap **Add Device**.
2. Select **Enter IP Address / Domain** as the adding method.
3. Enter the device name, device's IP address, port number, user name, and password.
4. **Optional:** 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.

   Note

   You can add the device to an existing Site, tap **Add New Site** to add the device to a new Site.
5. Tap **Add**.

Caution

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

6. **Optional:** Perform the following operations.

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	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 to your phone.
Set Type for Unknown Device	If the Hik-Partner Pro 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** .

7.2.7 Synchronize Devices with Hik-Connect Account

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

Steps

1. Go to logging into Hik-Connect page.

- Tap **Site → Device Synchronization** .
- Tap **Me → Link With Hik-Connect Account → Link With Account /** + .
- Tap **Account Linking** or **More → Tools → Account Linking /** + .

2. Log in to your Hik-Connect account.

Note

- Check **Get Your Account and Device Information** to allow Hik-Partner Pro to acquire necessary information for device synchronization.
- Check **Authorize Automatic Device Synchronization from Your Account to the Current Hik-ProConnect Account** to link your Hik-Connect account with your Hik-Partner Pro account. After linking, devices newly added to Hik-Connect will be synchronized automatically to Hik-Partner Pro for device management.

3. Tap **Authorize and Login**.
4. Select the devices you want to synchronize and tap **Next**.
5. 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 **Assign Site** 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 synchronized, and device permissions.
   5) Tap **Finish** to save the settings.
6. Tap **Synchronize** to start device synchronization.

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-Partner Pro upon approval.
- After synchronization, you can still manage the devices in your Hik-Connect account and access Hik-Connect services.

7. **Optional:** If you have authorized automatic device synchronization, view the linked account(s) and tap ··· **→ Unlink** to unlink an account if needed.
   - On the Home page, go to **Account Linking** or **More → Tools → Account Linking** .
   - Tap **Me → Link With Hik-Connect Account** .

7.2.8 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-Partner Pro 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-Partner Pro 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-Partner Pro. For details, see ***Add Device by Scanning QR Code*** or ***Add Device by Entering Serial No.*** .

Steps

Note

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

1. Tap **Site** in the bottom to enter site list page, 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 by one of the following two methods.

Table 7-4 Add Devices

Method	Description
Add Online Devices	Add devices on the same LAN with the PC where the Portal runs. a. Select devices, and then tap **Next**. b. Tap **Batch Enter**, select multiple or all devices, and then tap **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.

Method	Description
	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. Tap **Next**.

The adding result page shows.

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

Note

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

5. Tap **Next**.
6. **Optional:** 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.

7.3 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.

Note

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-Partner Pro Portal User Manual* for details).

Steps

Note

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.

   Note

   If the firmware version of a device is obsolete, or its device type cannot be recognized by Hik-Partner Pro, 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 the previous activation. For example, assume that you activated a 1-month health monitoring service for an 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.

7.4 Manage Device Permission

By handing over the site 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.

7.4.1 Apply for Device Permission

After handing over a site to the end user, if you need to view the live view or playback of device(s) added to the site or configure the device(s) added to the site, you can apply for the permission accordingly from the end user.

Steps

1. Tap **Site** in the bottom to enter the site list page.
2. Tap a site to enter the site details page.

   Note

   You can either apply for permission for one device (refer to Step 3) or apply for permission for multiple devices(refer to Step 4).

3. **Optional:** Apply for permission for one device.
   1) On the site list page, tap a device to enter the device details page.
   2) In the Device Permission area, select **Configuration** or **Live View** or **Playback** and tap to enter the Apply for Permission page.
4. **Optional:** Apply for permission for multiple devices.
   1) On the site list page, tap ... → **Apply for Device Permission** .
   2) Select **Apply for Configuration Permission** or **Apply for Live View Permission** or **Apply for Playback Permission**.
   3) Select the devices for applying for the permission.

      Note

      You can tap **Select All** to select all the devices in the list.

   4) Tap **OK**.
5. 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.

6. **Optional:** Enter the remarks for the permission.
7. Tap **OK** to send the application to the end user.

   If the end user approves your application, you will be able to view the live view, playback of the device(s) and configure device(s).

7.4.2 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**.

7.5 Move Devices

You can use the Device Movement feature to move devices from one site to another. By distributing devices to different Sites, you can manage both the sites and devices more efficiently.

Steps

Note

- The feature is only supported by a device matches the following conditions:
  - The original Site where the device belongs needs to have been authorized to you.
  - The device needs to be added by serial No. The devices added by IP address / domain name are not supported.
  - The original Site and the target Site should belong to the same Site Owner.
- Once a device is moved from its original Site, you need to configure the device again because all the original device configurations will be invalid. In addition, device related configurations including the linkage rules, exception rules, ARC settings, network switch settings, people counting service, temperature screening service, cloud storage service, and cloud attendance service, etc., will be affected. You also need to configure these related configurations again.

1. Tap **Site** in the bottom to enter the Site page.
2. Tap an authorized Site to enters its details page.
3. Tap ··· in the upper right corner, and then tap **Move Device** to open the following pane.
4. Tap **Select Device** to enter the Select Device page.

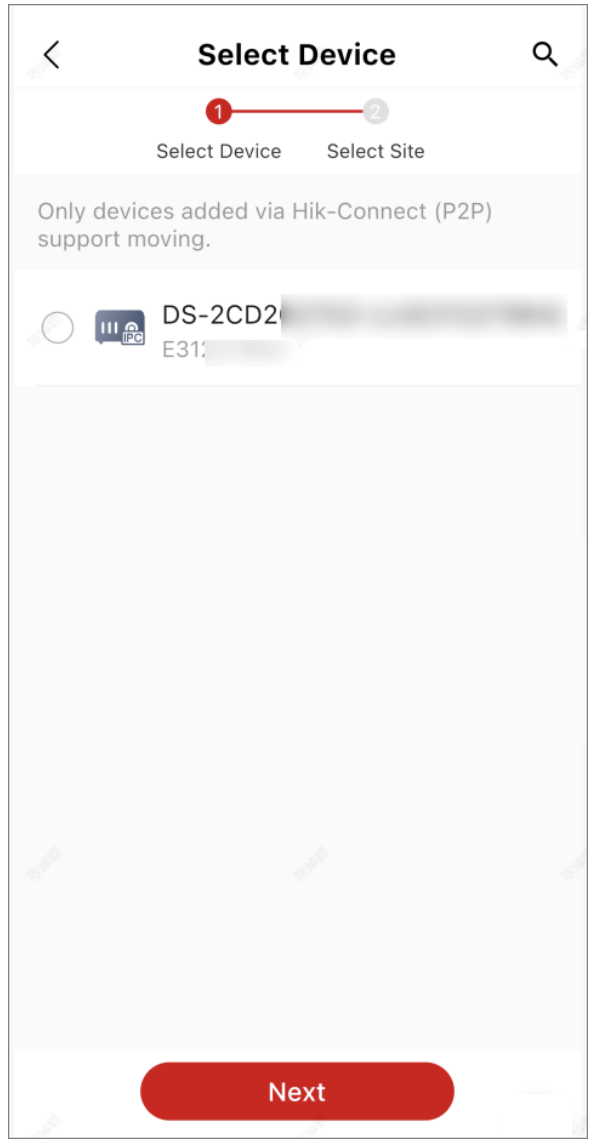


Figure 7-2 Select Device

5. Select device(s) and tap **Next** to enter the Select Site page.

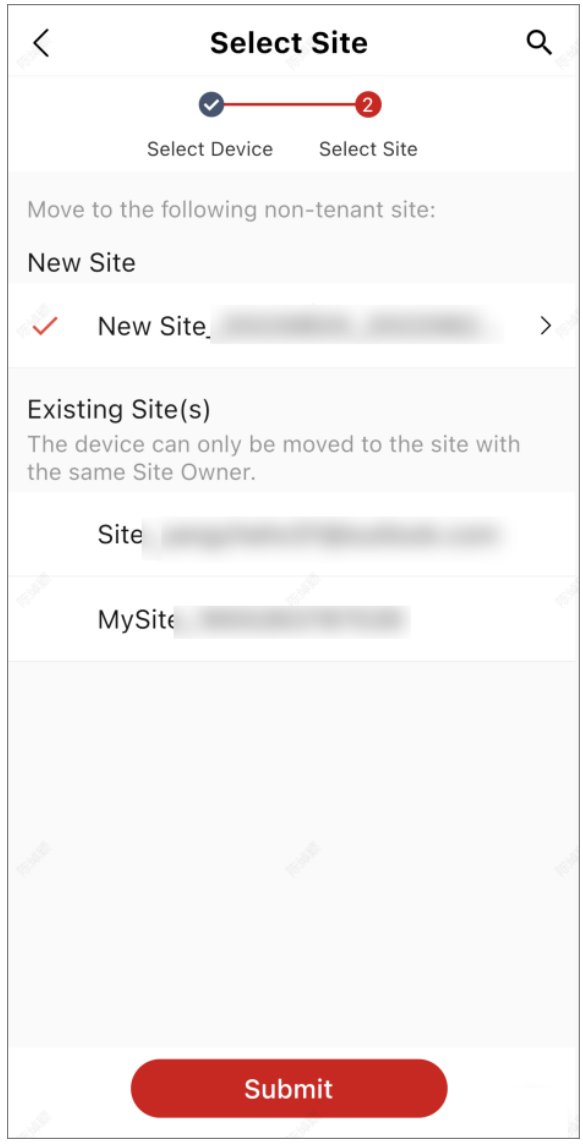


Figure 7-3 Select Site

6. Select a Site.

   New Site: If you select **New Site**, you need to create a name for the Site and set its time zone.

   Existing Site: If you select **Existing Site**, you need to select a Site that shares the same Site Owner with the current one. Under the condition that two sites are handed over to the same Hik-Connect user by email and phone number respectively, you can also move devices between the two sites.

7. Tap **Submit**.

   Note

   The application will expire if not handled within 7 days.

8. **Optional:** Tap **View Device Movement Records** and perform the following operation(s).

Apply Again	Tap an expired ( ) or rejected ( ) application to enter its details page, and then tap **Apply Again** to send the application again.
View Details	Tap an application record to enter its details page to see the details.
Move More	Tap an approved ( ) or sent ( ) application to enter its details page, and then tap **Move More** to move more devices.

7.6 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.

7.6.1 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 resource 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.

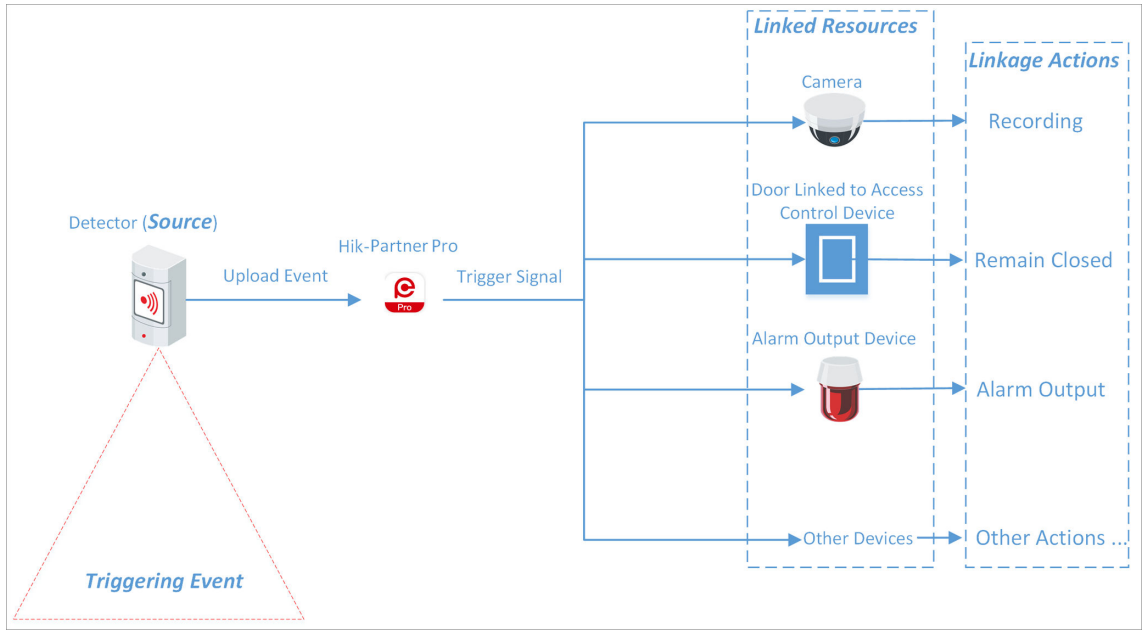


Figure 7-4 Linkage

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 7-5 Available Triggering Events for Different Resource Types

Source	Triggering Event
Camera	• Motion Detection • Face Detection • Intrusion • Line Crossing Detection
Access Control Device	• Network Disconnected • Tampering Alarm
Door Linked to Access Control Device	• Door Opened Normally **Note** Capture or Recording cannot be set as the linkage action for the triggering event Door Opened Normally. • Door Opened Abnormally • Tampering Alarm
Door Station	• Calling
Area of Security Control Panel	• Away Arming • Disarmed

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

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

Note

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

Table 7-6 Linkage Action Description

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

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

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

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

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

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

What to do next

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

Note

- If the Notification functionality of the Source is disabled, the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not.
- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the Hik-Connect Mobile Client, or the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *Hik-Connect Mobile Client User Manual*.
- Please notify your end users to download or update the Hik-Connect Mobile Client (V 4.15.0 or 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 7-7 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

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

Steps

Note

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

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

Linkage Rule Name

Create a linkage rule name.

When

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

Trigger the Following Actions

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

Note

- You can only select only one linkage action.
- For details about the linkage actions, see ***Table 7-6*** .

Linkage Schedule

Define the scheduled time during which the linkage is activated.

All Days

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

Custom

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

Note

The date(s) marked blue is selected.

5. Tap **Enable**。

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

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

What to do next

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

Note

- If the Notification functionality of the Source is disabled, the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not.
- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the Hik-Connect Mobile Client, or the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *Hik-Connect Mobile Client User Manual*.
- Please notify your end users to download or update the Hik-Connect Mobile Client (V 4.15.0 or 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.

7.6.2 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-Partner Pro to notify the specified Installer(s) 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

Note

This function is not supported by the solar camera.

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

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

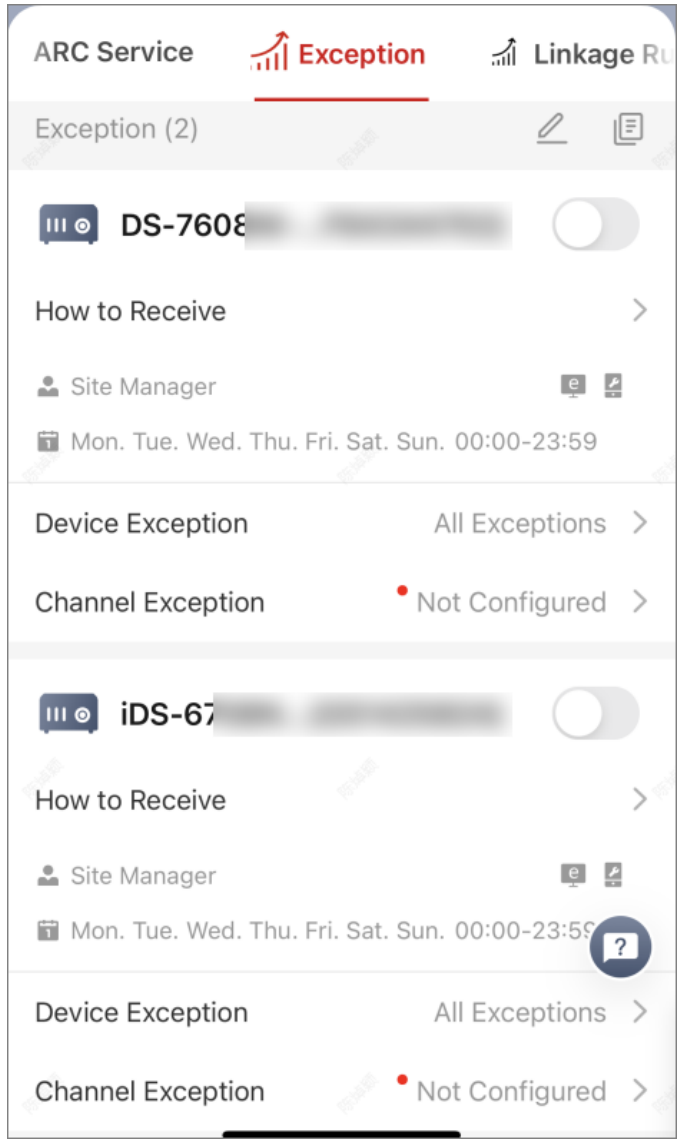


Figure 7-5 Add Exception Rule

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

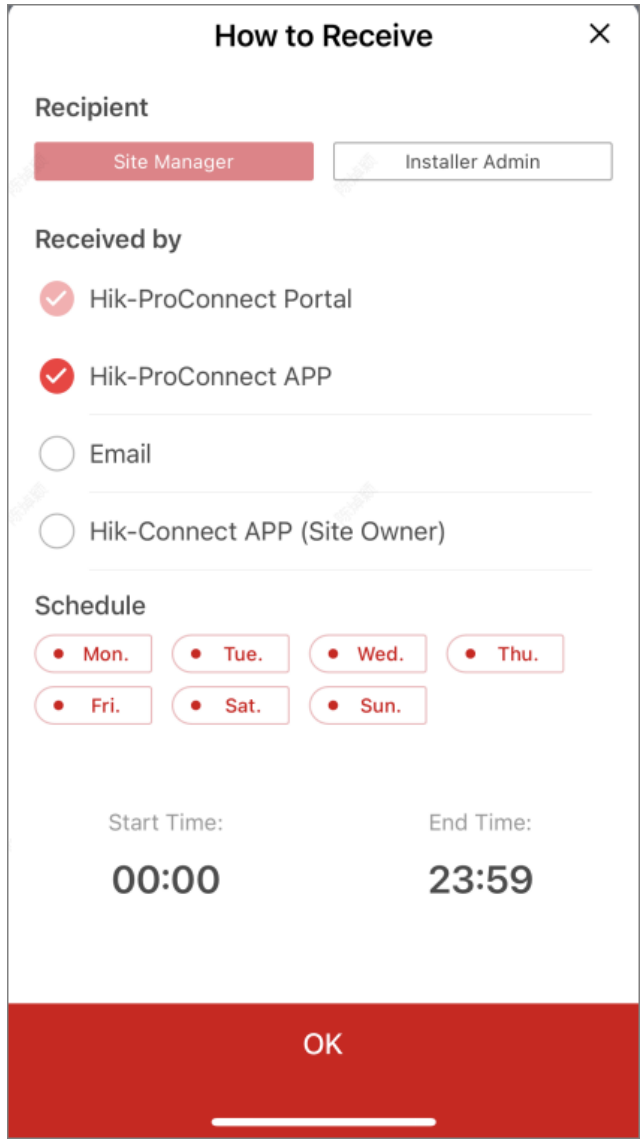


Figure 7-6 How to Receive

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.

Hik-Partner Pro App

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

Hik-Connect App (Site Owner)

When an exception is detected, the device will push an notification to the Hik-Connect Mobile Client, used by your customer in real time.

Note

For alarm devices, this option is enabled by default and you cannot disabled it.

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 in 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.

7.6.3 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-Partner Pro 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

Note

The device should support this functionality. If you have activated the health monitoring service for the device, the exception notification function of the device is enabled by default. For details about activating the health monitoring service, refer to ***Activate the Health Monitoring Service*** .

1. Tap a site to enter the site details page.
2. Select the **Device** tab.
3. Tap a device to enter the device 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 (V 4.15.0 or later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

7.7 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 (when you are not at the site) and resetting password onsite (when you are at the site).

Note

- Resetting password via Hik-Partner Pro 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*** .

Tap **Site** in the bottom 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. This method can be used when you are not at the site.

  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 V 4.15.0 or later.

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

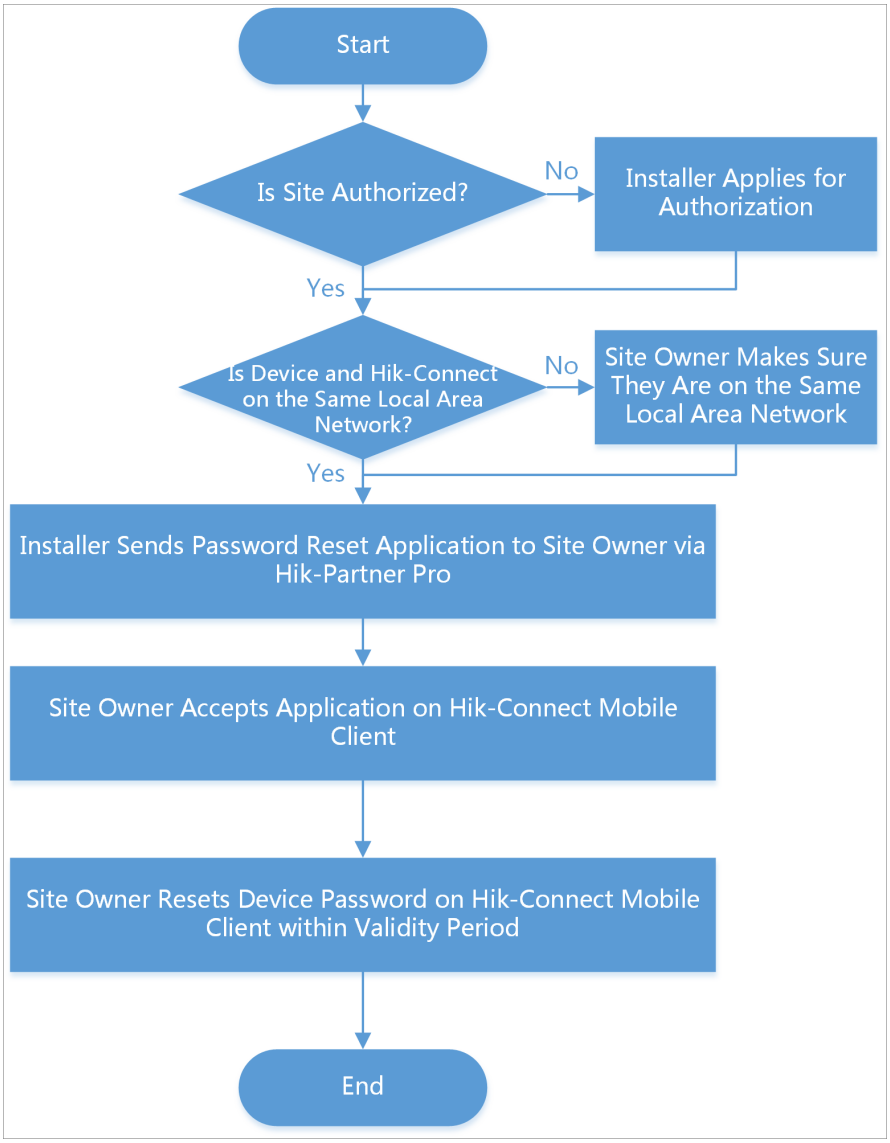


Figure 7-7 Flow Chart of Resetting Device Password Offsite

- **Reset Password Onsite:** You need to go to the Site where the device is located. This method can be used when you are at the site.

Note

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

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

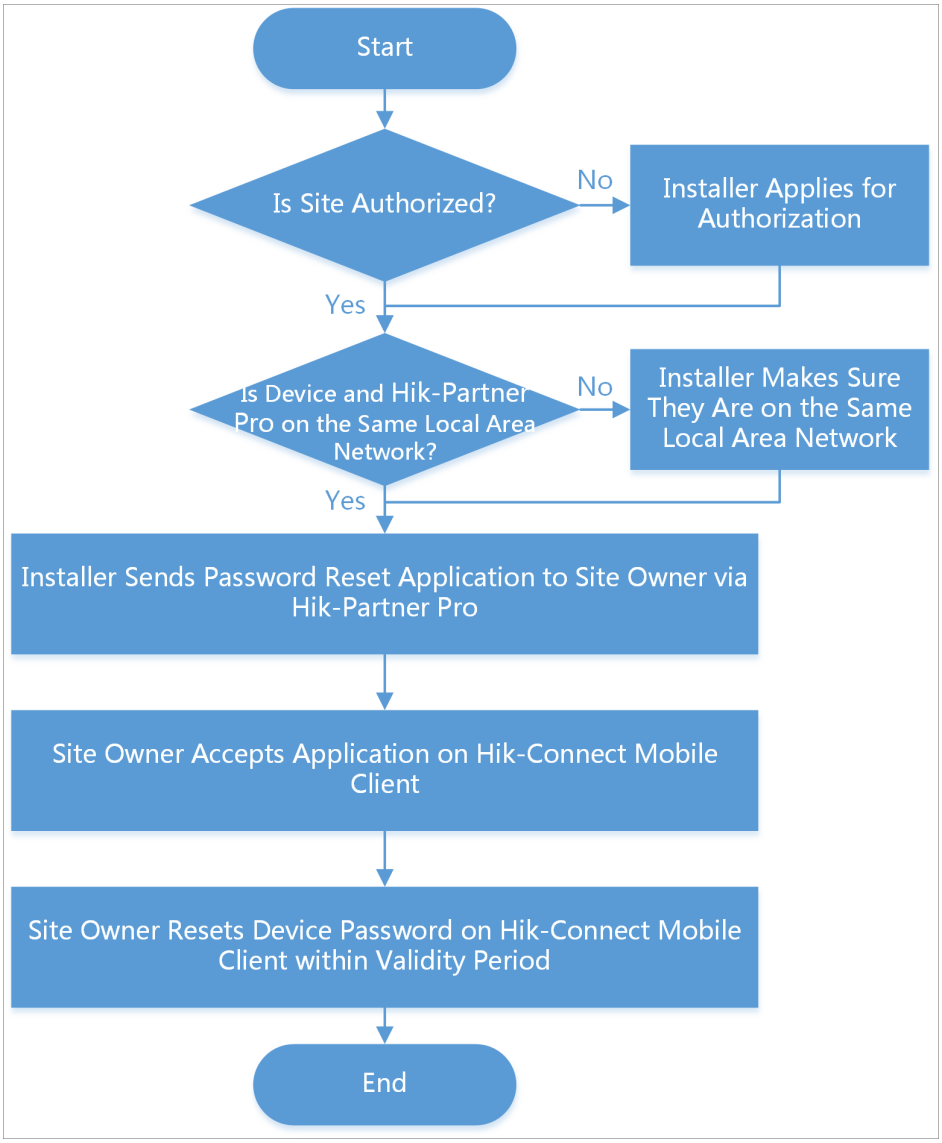


Figure 7-8 Flow Chart of Resetting Device Password Onsite

7.8 Enable Remote Log Collection

Remote Log Collection is for getting device logs. When this function is enabled, the technical support can collect device logs remotely for troubleshooting. You can set the validity period for collecting remote logs as needed, and this function will be automatically disabled when the validity period expires.

Before You Start

Make sure you have added the device which support remote log collection to the site, and the site has not been handed over to the end user. If the site has been handed over to the end user, you should contact with the end user to enable the Remote Log Collection function on Hik-Connect.

Steps

1. Tap a site to enter the site list page.
2. Tap a device to enter the device details page.
3. Tap ••• in the upper right corner.
4. Tap **Remote Log Collection** to enter Remote Log Collection page.
5. **Optional:** For enabling this function for the first time, tap **Enable** to confirm enabling the function.
6. Switch on **Log Collection**.

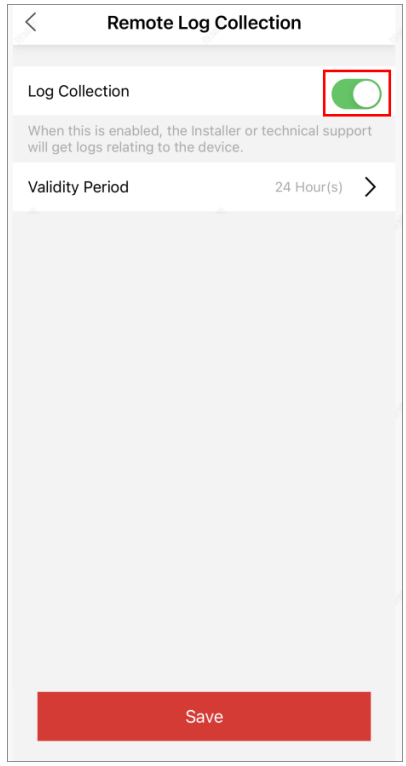


Figure 7-9 Remote Log Collection

7. Select the validity period.

Note

The function of remote log collection will be automatically disabled when the validity period expires. The default validity period is 24 hours.

8. Tap **Save**.
9. **Optional:** Disable the function.
   1) Tap **Remote Log Collection** to enter Remote Log Collection page.

2) Switch off **Log Collection**.
3) Tap **Save** to save the settings.
4) Tap **OK** to confirm the operation.

7.9 Manage Security Control Panel

You can add and manage AX PRO, AX HUB, AX HYBRID, and AX HYBIRD PRO security control panels on Hik-Partner Pro.

Note

- The following chapter introduces functionality supported by AX PRO / AX HYBIRD PRO security control panel (hereinafter referred to as "AX PRO / AX HYBIRD 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*** .

7.9.1 Control AX PRO and AX HYBIRD PRO

You can perform operations including adding area, arming/disarming area, clearing alarm, and bypassing zone.

Tap on an AX PRO or AX HYBIRD PRO device on 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 or to disarm the area.
Stay Arm All/Multiple Areas	Select the **Area** tab, and then tap at the bottom of the page to stay arm all areas; or tap to select multiple areas, and then tap at the bottom of the page to stay arm the selected areas.
Away Arm All/Multiple Areas	Select the **Area** tab, and then tap at the bottom of the page to away arm all areas; or tap to select multiple areas, and then tap at the bottom of the page to away arm the selected areas.

Function	Operation
Disarm All/Multiple Areas	Select the **Area** tab, and then tap at the bottom of the page to disarm all areas; or tap to select multiple areas, and then tap at the bottom of the page to disarm the selected areas.
Clear Alarms of All/Multiple Areas	Select the **Area** tab, and then tap at the bottom of the page to clear alarms of all areas; or tap to select multiple areas, and then tap at the bottom of the page to clear alarms triggered in these areas. **Note** This function is not supported by the AX HYBIRD PRO device.
Add Peripheral Device	Select the **Device** tab, and then tap to add a peripheral device. See details in ***Add Device*** . **Note** The AX HYBIRD PRO device only supports adding keyfobs as the peripheral device.
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.
Bypass Zone	Select the **Device** tab, and then select a zone (i.e., detector) and turn on the **Bypass** switch to bypass the zone. **Note** This function is not supported by the AX HYBIRD PRO device.
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.

7.9.2 Configure AX PRO and AX HYBIRD PRO

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

Tap on an AX PRO / AX HYBIRD 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 **Maintenance → Device Maintenance → Test → Start Walk Test** , and then walk in the detection zones, and finally tap **End Walk Test** to view the test results: the status (normal or abnormal) will be displayed.
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 Device	**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. Tap **Maintenance → Device Upgrade** to enter the Device Upgrade page. Tap **Upgrade** to upgrade it.
Switch Device Language	Tap **System → Configuration → Device Language** to enter the Device Language page. Select language, and you will be asked if you want to keep the names of the device and its areas. Tap **Yes** to keep the current names; tap **No** to switch the names to the default names in the switched language. Then tap **Yes** in the confirmation box to switch the device language. **Note** The switching process lasts for several minutes. During the process, please do NOT exit the Mobile Client, lock the screen, disconnect the device from network, or power off the device.
Other Configurations	You can do other configurations including user management, system options configuration, linking network cameras, communication settings, etc. **Note** For details about other AX PRO configurations, see the user manual of the device.

7.9.3 Batch Arm/Disarm AX PRO and AX HYBRID PRO

You can batch arm or disarm multiple AX PRO / AX HYBRID PRO devices on various sites by grouping the devices.

Follow the steps to create a group of AX PRO / AX HYBRID PRO devices and then control the group.

Steps

Note

This function is only supported in some countries/regions.

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

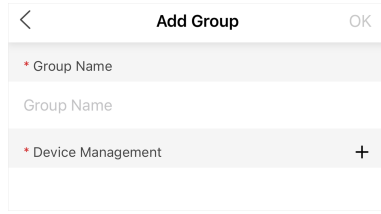


Figure 7-10 Add Group Page

4. Create a name for the group.
5. Add devices to the group.
   1) Tap + and select the devices on different sites.

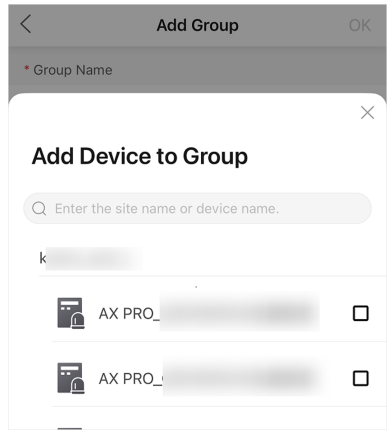


Figure 7-11 Add Device Page

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.

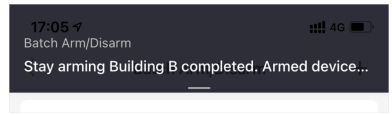


Figure 7-12 Result Notice

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.

7.9.4 Batch Configure AX PROs

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

Note

- Available for AX PRO devices (V1.1.0 and later) and AX HYBRID PRO devices.
- 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 Home page, tap **More → Remote Batch Config** , or tap **Remote Batch Config** on the Home page.
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**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, ***ADM-CID**, **CVS-IP**, **FSK Module**, **RDC Module**, or **IDS Module** as the protocol type.

Note

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 re-transmission attempts.

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 **More → Remote Batch Config** , or tap **Remote Batch Config** on the Home page.
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.

Note

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.

7.10 Alarm Receiving Center (ARC) Service

Hik-Partner Pro 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

Note

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

   Note

   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

   - After you authorize the ARC, an email will be sent to the **Email Address for Receiving Notification** to notify them, and the email content includes user account, device serial No., device model, installer logo, company name, company telephone number, and company address.
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-Partner Pro 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-Partner Pro 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-Partner Pro Server

The device will be connected to Hik IP Receiver Pro by Hik-Partner Pro 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.
- After you deauthorize the ARC, an email will be sent to the **Email Address for Receiving Notification** to notify them, and the email content includes user account, device serial No., device model, installer logo, company name, company telephone number, and company address.

7.11 View Video

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

7.11.1 View Live Video

By Hik-Partner Pro 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 (V 4.15.0 or later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.
- For those who have no permission for live view: If you are on site, tap **I Am at the Site** in the pop-up window of no-permission prompt, to connect your mobile phone to the same Wi-Fi with the encoding device and log into the device to start live view; if you are off site, tap **Apply for Permission** in the pop-up window to apply for permission for live view. See details in ***Apply for Device Permission*** .
- Make sure the device is online, otherwise the function cannot be used.

7.11.2 Play Back Video Footage

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

Note

- For those who have no permission for playback: If you are on site, tap **I Am at the Site** in the pop-up window of no-permission prompt, to connect your mobile phone to the same Wi-Fi with the encoding device and log into the device to start playback; if you are off site, tap **Apply for Permission** in the pop-up window to apply for permission for playback. See details in ***Apply for Device Permission*** .
- This function should be supported by the device.

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.

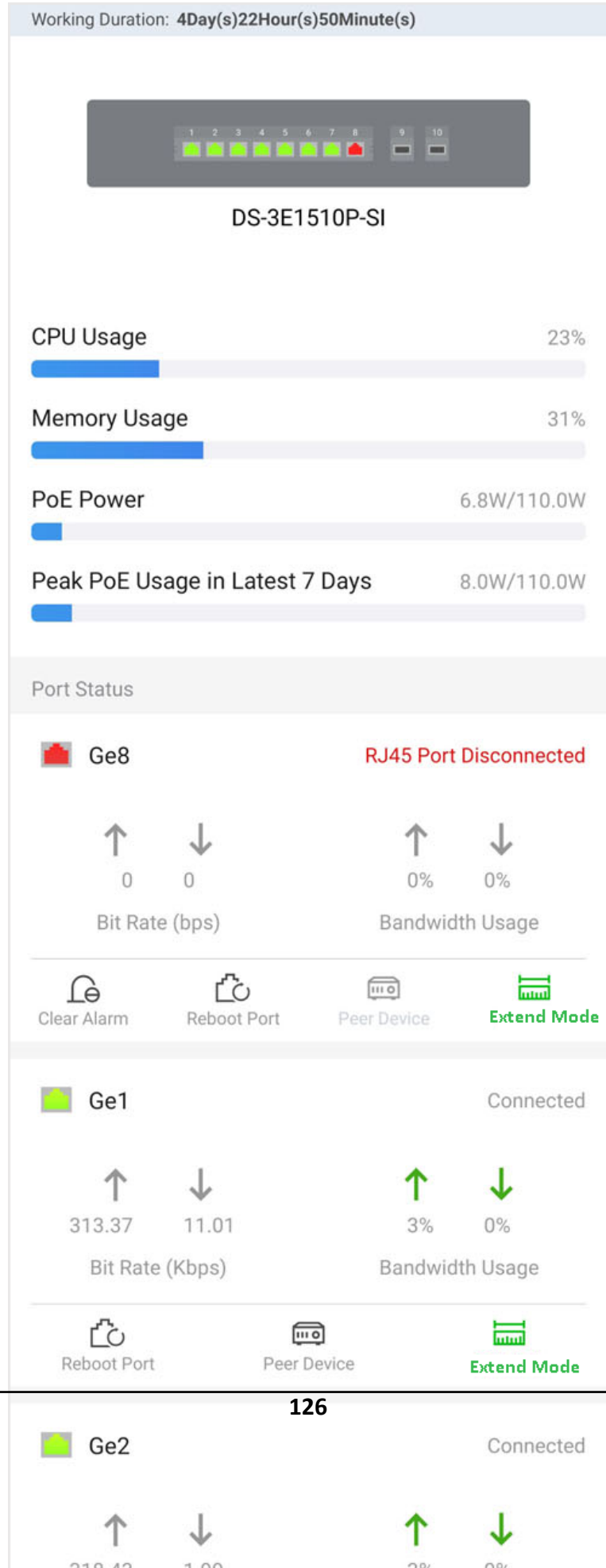
7.12 Network Switch Management

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.

7.12.1 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.


Working Duration: 4Day(s)22Hour(s)50Minute(s)
DS-3E1510P-SI
CPU Usage 23%
Memory Usage 31%
PoE Power 6.8W/110.0W
Peak PoE Usage in Latest 7 Days 8.0W/110.0W
Port Status
Ge8
RJ45 Port Disconnected
0 0
Bit Rate (bps)
0% 0%
Bandwidth Usage
Clear Alarm
Reboot Port
Peer Device
Extend Mode
Ge1
Connected
313.37 11.01
Bit Rate (Kbps)
3% 0%
Bandwidth Usage
Reboot Port
Peer Device
Extend Mode
Ge2
Connected

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	Tap **Enable Extend Mode/Disable Extend Mode** to extend or not to extend the transmission range of this port. **Note** 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.

7.12.2 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 7-8 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	You can tap a network switch on the topology to view its details, including basic information, device status, and port status. You can also perform operations such as rebooting the network switch and restarting port. For details, see ***Network Switch Operations*** . **Note** You cannot view details of a virtual network switch.
View Details of Other Device	Tap a device to view its details, such as device model and network status. **Note** • Make sure you have the configuration permission for the device, otherwise you need to apply for the permission first. • You cannot view details of a virtual network switch. • If the device is not added to the same site with the network switch, you cannot view its details.
Expand Devices in a Node	Devices of the same type are folded in a node of the network topology. You can tap on the node to expand all the devices and view whether their running status is normal. The color of the device icon indicates the running status of a device:

Operation	Description
	• 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.

7.13 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.

7.13.1 Upgrade Device

If the Hik-Partner Pro Mobile Client detects new firmware versions of devices including security control panels, doorbells, Hik-ProConnect boxes, DVRs/NVRs that support cloud storage, 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.
- The devices to be upgraded should be connected to the same LAN with the Mobile Client.
- You can also upgrade the device when you add it. See ***Add Device by Entering Serial No.*** for details.

1. On the site list page, tap a site name to enter the site's page.

   Note

   - will appear beside the name of an upgradable device on the site list.
   - 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. Hover over , and tap **Upgrade** in the popping window.
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 power failure or network disconnection does not happen during the upgrade.
- For the device failed to be upgraded, you can tap **Share Download Link** to share the download link via Email, Facebook, etc. You can then open the link to download the upgrade firmware and upgrade the device on the remote configuration page of the device or via other upgrade tools.

7.13.2 Batch Upgrade Devices on LAN

You can batch upgrade devices (security control panels, encoding devices, doorbells, etc.) on the same LAN to make the devices compatible with Hik-Partner Pro, if there are new firmware versions of the devices.

1. On Home page, tap **More → On-Site Batch Upgrade** , or tap **On-Site Batch Upgrade** on the Home page.
2. Select device(s) that need to be upgraded.
3. Tap **Upgrade Online** to upgrade the selected device(s).

7.13.3 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 Mobile Client Remote Use** when you hand over a site to your customer, you cannot unbind the devices added to this Site. For details about site handover, see ***Hand Over Site*** .

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.

7.13.4 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-Partner Pro 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**.

7.13.5 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.
- For those who have no permission for remote configuration: If you are on site, tap **I Am at the Site** in the pop-up window of no-permission prompt, to connect your mobile phone to the same Wi-Fi with the encoding device and log into the device to perform remote configuration; if you are off site, tap **Apply for Permission** in the pop-up window to apply for permission for remote configuration. See details in ***Apply for Device Permission*** .
- Make sure the device is online.

Chapter 8 Health Monitoring

The Health Monitoring module includes Exception Center, Scheduled Report and Health Status, where you can view the device exceptions, configure the report schedule, and check device health status.

Exception Center

When any exception occurs during health monitoring, the notification will appear in the Exception Center under the Notification Center module. See details in ***Exception Center*** .

Scheduled Report

With the scheduled report feature, the device status information will be sent to you or the corresponding user based on the configured schedule.

Health Status

Shows the near-real-time information about the status of the devices added to the sites. If you have added network switches to a site, you can view the device status and link status in a visualized way via network topology. The status information, which is important for the maintenance of devices managed across the Hik-Partner Pro platform as a whole, helps you locate the source of exceptions and determine troubleshooting methods in time, thus ensuring the smooth running of these devices.

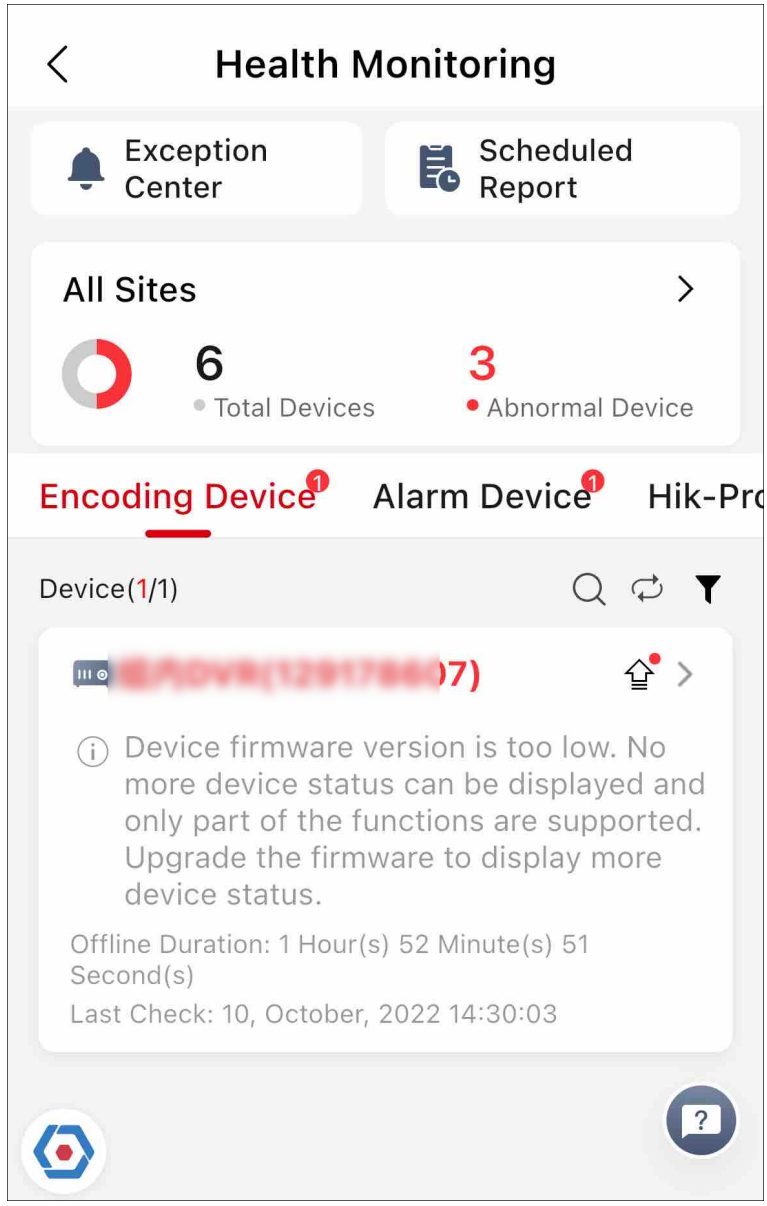


Figure 8-1 Health Monitoring Page

Note

- The link of video tutorial on how to check device health status will pop up on the bottom of the page when you first enter the Health Monitoring module.
  Tap to make the video link pop up when you enter Health Monitoring next time.
- For Installer, you can only view the status information of devices on the site assigned to you. For Installer Admin, you can view the status information of devices on all sites.

8.1 View Status of Devices on All Sites

For the Installer, you can view the status of each device type on all the sites which have been assigned to you. For the Installer Admin, you can view the status of each device type on all the sites.

On the Home page, tap **Health Monitoring** or **More → Maintenance → Health Monitoring** , or **Site → Health Monitoring** to enter the Health Monitoring page, and you can view the total number of devices and the number of abnormal devices on all sites.

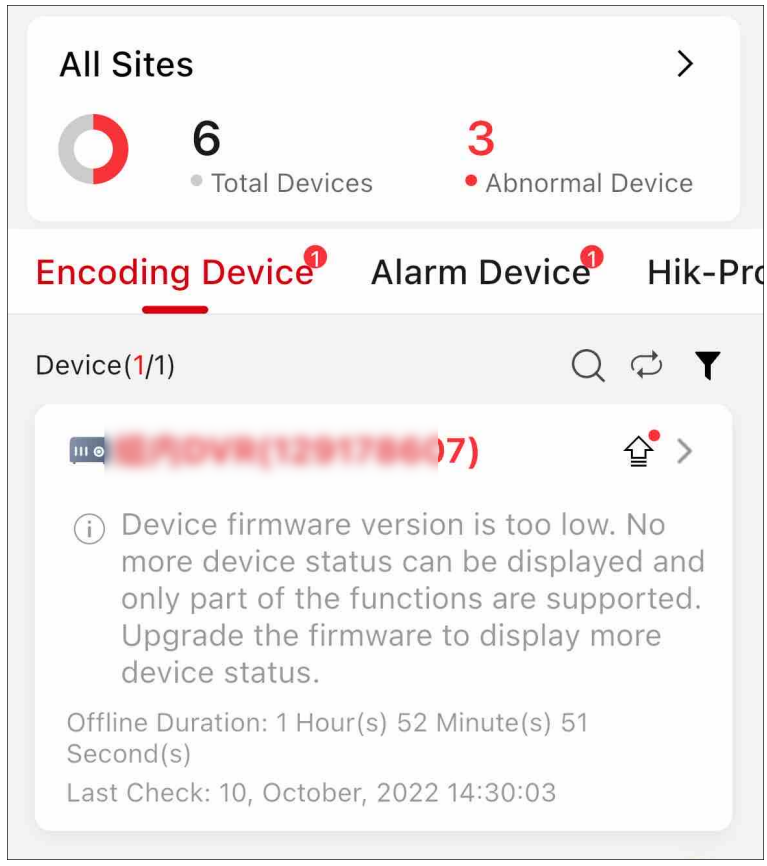


Figure 8-2 Device Status

Refer to the following to get the device descriptions and operations.

- For each device type, you can tap to inspect all the devices in the list; tap → **Display Abnormal Devices Only** to display the abnormal devices only; tap → **Display Authorized Devices Only** to display the devices whose configuration permission has been authorized to you.
- The Offline Duration column displays offline duration of devices in the format of "x Day(s) x Hour(s) x Minute(s)". If the offline duration is less than one day, the duration will be displayed as "x Hour(s) x Minute(s) x Second(s)".

- The icon beside the device name represents that you do not have the configuration permission for the device. You can tap the device and tap **Apply for Configuration Permission** to apply for the permission. For details, see ***Apply for Device Permission*** .
- The icon beside the device name represents that a new firmware is available. You can tap the device and tap **Upgrade** to upgrade the device. For details, see ***Upgrade Device*** .

Encoding Device

You can view the device information including network status, the number of offline linked cameras, storage status, HDD usage, last check time, overwritten recording status, etc.
The icon beside the device name represents that the IP address/domain set for the device is invalid or the DDNS is invalid, you can tap the device and tap **Edit Device Information** to edit the device information or tap **Configure DDNS** to reconfigure the device's DDNS.

Note

- For details about configuring device IP address/domain, see ***Add Device by IP Address or Domain Name*** .
- For details about configuring DDNS, see ***Configure DDNS for Devices*** .

Tap a device to enter the Device Details page to view more basic information about the device, and perform the following operations.

Operation	Description
Inspect Device	Tap to inspect the device manually.
Remotely Configure Device	Tap to remotely configure the device parameters. For details, see the device user manual.
Live View	Tap to view the live view of the device. **Note** • If you do not have the Live View permission, you can apply for the live view permission from the end user. For details, see ***Apply for Device Permission*** . • If the selected camera has been enabled with stream encryption, you should enter the device verification code before you can view its live view.
View Playback	Tap to view the playback of the device.

Operation	Description
View Site Owner and Site Manager Information	Tap beside site name to view the information about the Site Owner and Site Manager, such as name and phone number.
View Camera Status	Tap **Camera** to view the cameras linked to the device and their online/offline status.
View DVR HDD Information	Tap **HDD** to view the HDD information about the DVR, including self evaluation result, overall evaluation result, running status, running time, HDD temperature, and S.M.A.R.T information.

Alarm Device

You can view the device information including network status, remaining battery power, ARC ID, number of abnormal peripheral devices, etc.

Note

Displaying peripheral device's remaining power is not supported.

Tap a device to enter the Device Details page to view the basic information about the device, and perform the following operations.

Operation	Description
Remotely Configure Device	For security control panels, tap to remotely configure the device parameters. For details, see the device user manual. **Note** • Remote configuration is not supported if the device is armed. • Remote configuration is not supported if the device is a panic alarm device. • The icon beside the device name represents that EN50131 Compliant mode has been enabled on the device. You should tap **Authenticate** for authentication before you can configuring device remotely.
Control and Configure AX PRO Devices	For AX PRO devices, you can control and configure them. For details, refer to ***Control AX***

Operation	Description
	PRO and AX HYBIRD PRO and ***Configure AX PRO and AX HYBIRD PRO*** .

Hik-ProConnect Box

You can view the device information including network status, the number of offline linked cameras, and the last check time.
Tap a device to enter the Device Details page to view more basic information about the device, and perform the following operations.

Operation	Description
Inspect Device	Tap to inspect the device manually.
Remotely Configure Device	Tap to remotely configure the device parameters. For details, see the device user manual.
View Site Owner and Site Manager Information	Tap beside the site name to view the information about the Site Owner and Site Manager, such as name and phone number.
View Camera Status	Tap **Camera** to view the cameras linked to the device and their online/offline status.

Access Control Device

You can view the device information including device model, network status, last check time, etc.
Tap a device to enter Device Details page to view more basic information about the device, and perform the following operations.

Operation	Description
Inspect Device	Tap to inspect the device manually.
View Site Owner and Site Manager Information	Tap beside the site name to view the information about the Site Owner and Site Manager, such as name and phone number.

Video Intercom Device

You can view the device information including network status, last check time, etc.
Tap a device to enter Device Details page to view more basic information about the device, and perform the following operations.

Operation	Description
Inspect Device	Tap to inspect the device manually.
View Site Owner and Site Manager Information	Tap beside the site name to view the information about the Site Owner and Site Manager, such as name and phone number.

Doorbell

You can view the device information including device model, network status, SD card status, last check time, etc.
Tap a device to enter Device Details page to view the basic information about the device, and perform the following operations.

Operation	Description
Inspect Device	Tap to inspect the device manually.
Remotely Configure Device	Tap to remotely configure the device parameters. For details, see the device user manual.
Live View	Tap to view the live view of the device. **Note** • If you do not have the Live View permission, you can apply for the live view permission from the end user. For details, see ***Apply for Device Permission*** . • If the selected camera has been enabled stream encryption, you should enter the device verification code before you can view its live view.
View Playback	Tap to view the playback of the device.
View Site Owner and Site Manager Information	Tap beside the site name to view the information about the Site Owner and Site Manager, such as name and phone number.
View Camera Status	Tap **Camera** to view the cameras linked to the device and their online/offline status.

Network Switch

View information including network status of the switch (online/offline), the number of online ports of the switch, and the last check time.
Tap a network switch to view its information, including working duration, the thumbnail of the switch, PoE Power, peak PoE power in last 7 days, port status (alarm, normal, not connected). You can tap the thumbnail of switch to view its enlarged picture.

Note

Working duration refers to the time from when the switch is turned on till the current moment. If the switch is turned off, its working duration will be recounted when turned on again.

- Tap ··· → **Device Information** in the upper-right corner to view more basic information about the device, including device serial No., device model, device type, etc. You can tap **Reboot Device** at the bottom to reboot the device.
- Tap ··· → **Topology** in the upper-right corner to view the topology of this switch. For details about topology, refer to ***Network Topology*** .

For the port with alarms, tap **Clear Alarm** to clear the alarms of this port.
Tap **Extend Mode** to extend the transmission range of this port. Tap **Extend Mode** (displayed in green) to disable extending the transmission range of the port.

Note

When enabled, the transmission range of the port will be extended from 200 m to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.

8.2 View Status of Devices on One Site

You can view the status of devices on a specific site which has been assigned to you.

Steps

1. On the Home page, tap **Health Monitoring** or **More → Maintenance → Health Monitoring** , or **Site → Health Monitoring** to enter the Health Monitoring page, and you can view the total number of devices and the number of abnormal devices on all sites.
2. Tap › to enter the site list page, and select a site from the list.

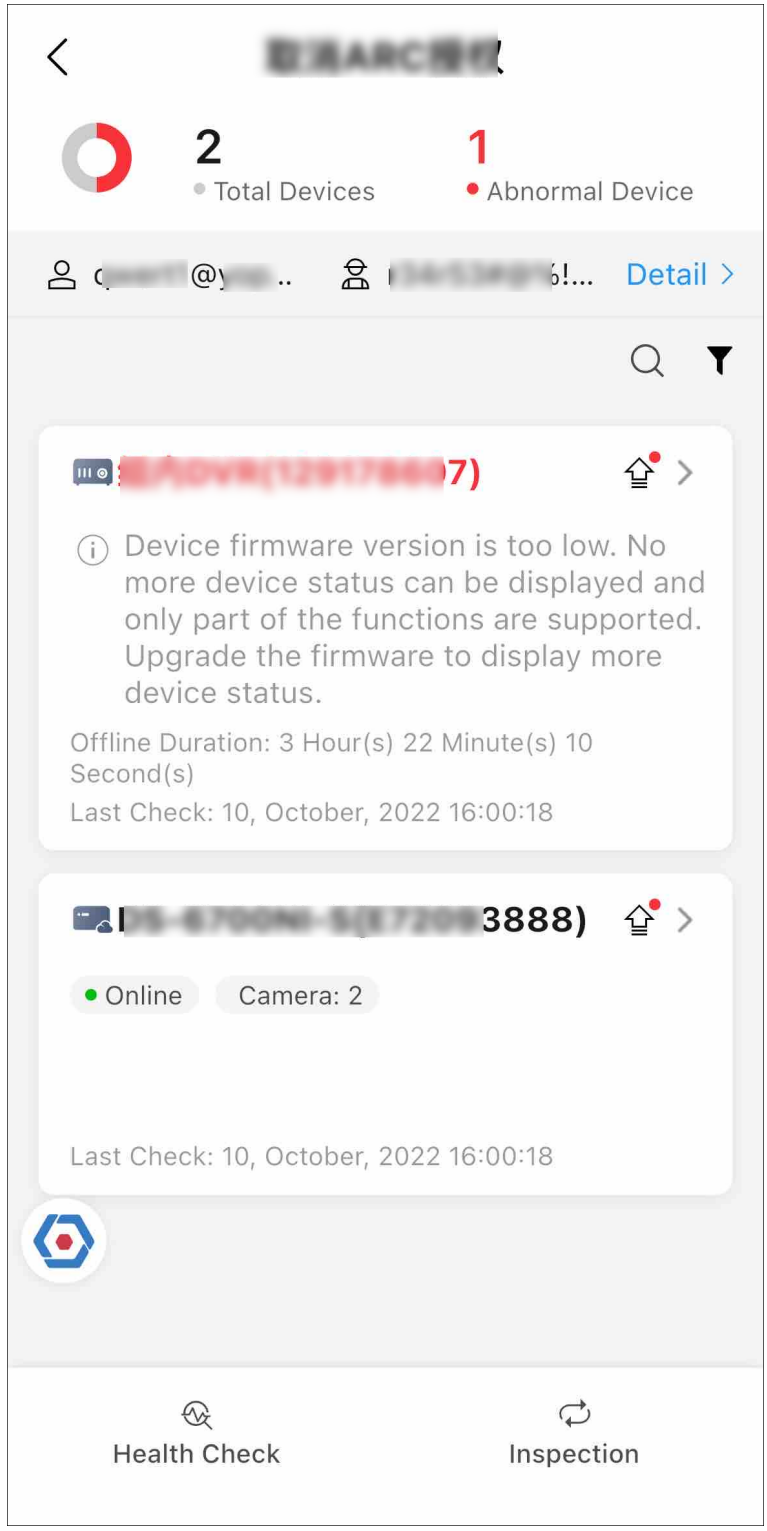


Figure 8-3 The Current Site

The status of the devices on the current site will be displayed.

3. **Optional:** Perform the following operations.

Filter Data	• Tap → **Display Abnormal Devices Only** to display the abnormal devices only. • Tap → **Display Authorized Devices Only** to display the devices whose configuration permission has been authorized to you.
View Information About Site Owner & Site Manager	Tap **Detail** to view the information about the Site Owner and Site Manager, including the name, email address, and phone number. Up to 100 site managers can be displayed.
Diagnose Devices	Tap **Health Check** at the bottom to open the Health Check window, and tap **Check Now** to check the health status of the devices on the site. When the checking is completed, you can view the status of each device on the site. You can tap to view the diagnostics report of each device. Tap **View All Reports** to view the diagnostic reports of all devices. **Note** Only AX PRO and AX Hybrid security control panels support this function.
Inspect Devices	Tap **Inspection** at the bottom to inspect all the devices on the site.
Upgrade Device Firmware	If there are devices available for upgrade, will appear. You can tap the device to enter its details page, and tap **Upgrade** to upgrade it. **Note** For details, see ***Upgrade Device*** .
Remote Configuration	Select a device and then tap to remotely configure the device parameters. **Note** • The device should be online. • For details, see the user manual of the device.
Inspect a Single Device	Select a device and then tap to inspect it.
Reconfigure IP/ Domain of Encoding Device	If the IP address/domain set for the device is invalid, will appear. You can tap the device to enter its details page, and tap **Edit Device Information** to reconfigure the device's IP/domain. For details about configuring IP/Domain, see ***Add Device by IP Address or Domain Name*** .
Reconfigure DDNS	If the DDNS of the device is invalid, will appear. You can tap the device to enter its details page, and tap **Configure DDNS** to reconfigure the device's DDNS. For details, see ***Configure DDNS for Devices*** .

View Encoding Device Details	You can view the network status, storage status, HDD usage, and overwritten recording status, etc. Also, you can tap the encoding device to view its details, including the basic information such as device type, serial No., and the network status of each linked camera. You can tap **Camera** to view all the linked cameras. If there is only one linked camera, tap to view its live view. If there are multiple cameras, tap , and select one camera to view its live view. If the encoding device is a DVR, you can also view its HDD information, including self evaluation result, overall evaluation result, running status, running time, HDD temperature, and S.M.A.R.T information. For the analog camera, you can view if video loss occurs. **Note** • If you do not have the Live View permission, you can apply for the live view permission from the end user. For details, see ***Apply for Device Permission*** . • If a camera has been enabled with stream encryption, you should enter its device verification code in the pop-up window before you can view its live view.
View Access Control Device Details	Tap an access control device to view its details, including basic information such as device type, serial No., and the device status including network status and the number of its linked doors.
View Security Control Panel Details	Tap a security control panel to view its details, including basic information about the security control panel, and status of the zones, the linked peripheral devices, and the linked cameras.
View Video Intercom Device Details	Tap a video intercom device to view its basic information and its network status.
View Doorbell Details	Tap a doorbell to view its basic information, including device model, device type, and device serial No. If the camera(s) are linked to the doorbell, you can tap a linked camera to view the live view.
View Hik-ProConnect Box Details	Tap a Hik-ProConnect box to view its basic information and the channel(s) added to it. You can also view the online status of the added channel(s).
View Network Switch Details	Tap a network switch to view its information, including working duration, the thumbnail of the switch, PoE Power, peak PoE power in

last 7 days, port status (alarm, normal, not connected). You can tap the thumbnail of switch to view its enlarged picture.

Note

Working duration refers to the time from when the switch is turned on till the current moment. If the switch is turned off, its working duration will be recounted when turned on again.

Tap ··· → **Device Information** in the upper-right corner to view more basic information about the device, including device serial No., device model, device type, etc. You can tap **Reboot Device** at the bottom to reboot the device.

Tap ··· → **Topology** in the upper-right corner to view the topology of this switch. For details about topology, refer to ***Network Topology*** .

For the port with alarms, tap **Clear Alarm** to clear the alarm(s) of this port.

Tap **Extend Mode** to extend the transmission range of this port. Tap **Extend Mode** (displayed in green) to disable extending the transmission range of the port.

Note

When enabled, the transmission range of the port will be extended from 200 m to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.

8.3 Send Reports Regularly

You can set up schedules for the platform to generate and send device health check reports to the specified email addresses automatically, so that the recipients can get regular updates on the health status of important devices and compare the report of each period.

Before You Start

Make sure you have activated the Health Monitoring service. For details, refer to ***Activate the Health Monitoring Service*** .

Steps

1. On the Home page, tap **Health Monitoring → Scheduled Report** or **More → Maintenance → Health Monitoring → Scheduled Report** , or **Site → Health Monitoring → Scheduled Report** .

Note

- All sites available for this feature are shown on the page automatically.
- The platform only supports automatically sending health check reports of encoding devices and AX PRO security control panels on authorized sites.
- Sites without the above-mentioned types of devices or sites that are not authorized to you will NOT be shown on the page.

2. Select site(s).
   - To configure the report sending schedule for a single site, tap a site.
   - To configure the report sending schedule for multiple sites, tap **Batch Configure** at the bottom of the page, and then select the sites you want to configure.
3. Configure the report sending settings.

   Device

   Select the device(s) to be health-checked and included in the report.

   Send At

   Specify the frequency, date, and time of sending the reports. You can set the frequency as Daily, Weekly, Monthly, Quarterly, Semiannually, or Annually.

   Recipient Email Address

   Add and edit the email addresses of the recipients.

   Note

   Up to 4 email addresses can be added.

   Report Language

   Choose a language for the report. The report is now available in 39 languages.
4. Tap **Save**.
5. Enable the settings.
   - To enable the settings for one site, switch on **Enable** for the site.
   - To enable the settings for all sites, switch on **Enable All** at the top of the page.

   The platform will generate and send reports according to the settings.

Note

If there are more than three site owners, only the first three can be displayed on the report while the others will be displayed as "...".

8.4 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 the exception source and troubleshoot faults in a visualized way.

Note

- Make sure you have the configuration permission of the network switch. Otherwise, network topology will be unavailable. For details about applying for configuration permission, see ***Apply for Device Permission*** .
- If you have not activated the health monitoring service for the network switch, some topology functions (e.g., viewing device status on the topology) will be unavailable. For details about activating the health monitoring service, see ***Activate the Health Monitoring Service***

On the Home page, tap **Health Monitoring → Scheduled Report** or **More → Maintenance → Health Monitoring → Scheduled Report** , or **Site → Health Monitoring → Scheduled Report** .

- Tap › beside All Sites, select a site from the list, and then tap **View Topology**.
- Tap **Network Switch**, tap a switch to enter the device details page, and then tap ··· **→ View Topology** in the upper-right corner.

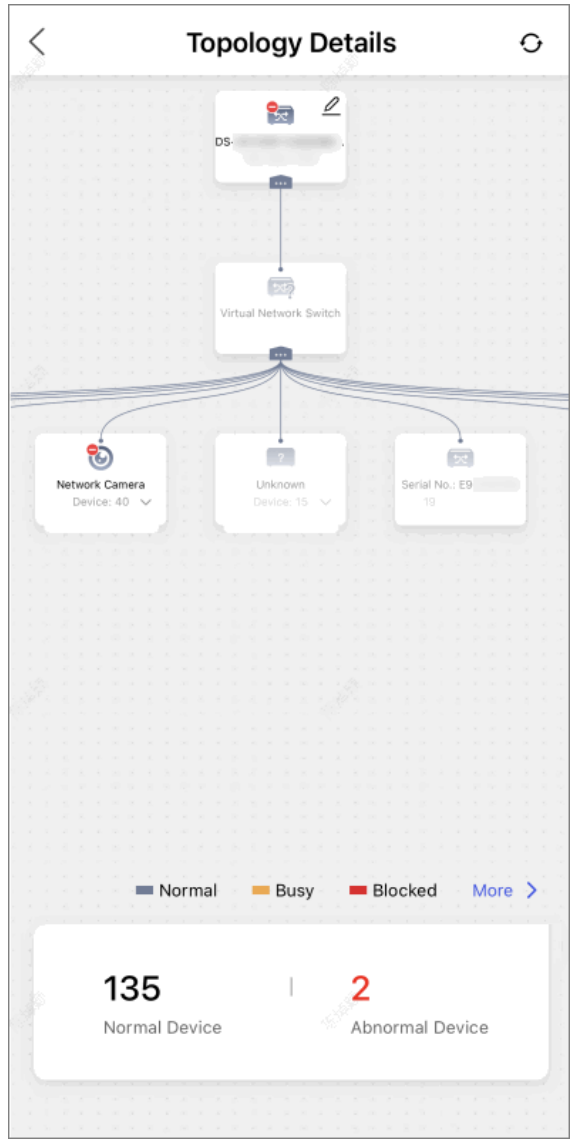


Figure 8-4 Topology Details

For detailed operations and descriptions about topology, refer to ***Network Topology*** .

Chapter 9 Notification Center

The Notification Center module shows all the history business notifications (including device management invitations, site sharing notifications, and device installation work order notifications) and notifications of device/channel exceptions, which help you take reactions in time for the smooth running of the devices. The module also keeps you informed about the system messages (such as the latest version of the system, newly added features, and successful company authentication) and the latest deals and offers (such as complimentary service packages).

Note

- All types of notifications received in the Notification Center can be sent as push notifications on your mobile device if you have push notifications enabled for the Mobile Client. Tap on a push notification to go straight to the corresponding details page.
- The total number of unread notifications is displayed as a red badge on the top right corner of the Mobile Client icon.

9.1 Business Notifications

In the Business Notification module, you can receive the device management invitations from Hik-Connect users for device management on Hik-Partner Pro, notifications concerning site sharing with the Maintenance Service Partner, and device installation work order notifications.

In the upper-right corner of the page, tap ✉ → **Business Notification** to enter the Business Notification page.

Device Management Invitations

Besides receiving the device management invitation from Hik-Connect users through an email, you can also receive it in the Business Notification on Hik-Partner Pro. After accepting the invitation, you will be able to manage the device on Hik-Partner Pro.
For details about accepting the invitation, refer to ***Accept a Device Management Invitation from Your Customer*** .

Site Sharing Notifications

Both the person who shares sites and the person who accepts site sharing (MSP/ISP) can view the notifications concerning site sharing.
For the person who shares sites, you can receive site sharing notifications involving the customers and/or the MSP/ISP. For example, when the MSP/ISP accepts or cancels the site sharing, when the customer cancels the site sharing authorization to you and/or the MSP, or when the customer modifies your and/or the MSP's device management permissions.
For MSPs, you can receive site sharing notifications involving the Installer and/or the customers. For example, when the Installer cancels the site sharing, when the Installer shares a site with you

and modifies your device management permissions, when the customer cancels the site sharing authorization to you and/or the Installer, or when the customer modifies your and/or the Installer's device management permissions.
For ISPs, you can receive site sharing notifications involving the ARC. For example, when the ARC cancels the site sharing.
For details about accepting site sharing, refer to ***Accept Site Sharing*** .

Device Installation Work Order Notifications

If an RMC from HikCentral ReGuard assigns a work order for device installation to you, a corresponding notification will be pushed to the Mobile Client. The notification shows the work order name, person who created it, and phone number. You can also tap the notification to handle the work order on the Mobile Client.

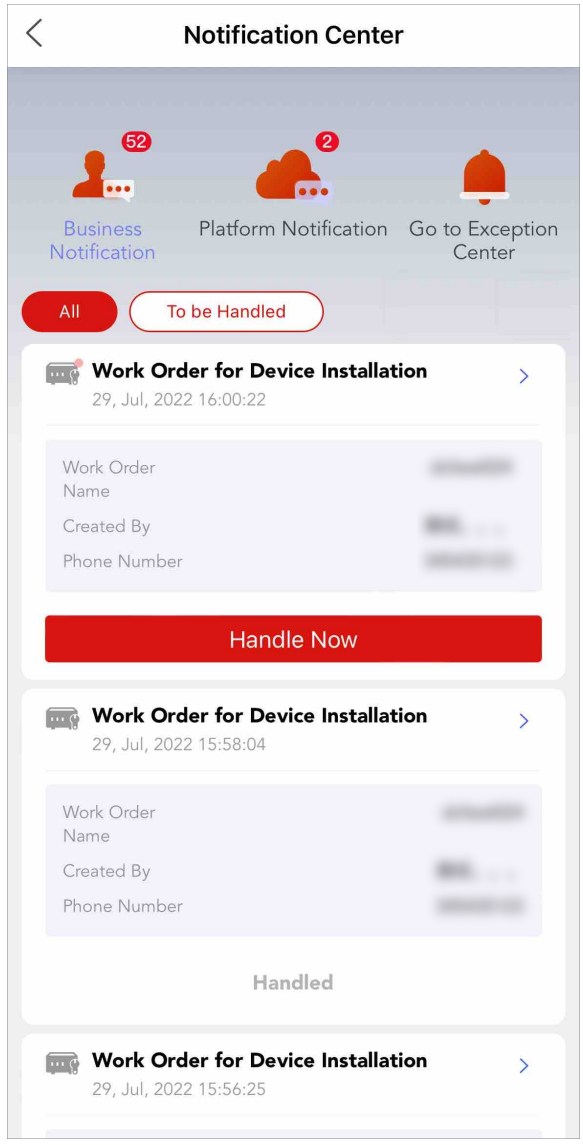


Figure 9-1 Work Order Notifications on Mobile Client

9.2 Exception Center

If you have enabled device exception detection, real-time notifications will be sent to the Mobile Client or email when device exception occurs. The Exception Center shows all the history notifications of device exceptions and channel exceptions.

Note

- This feature is available only when you have activated the Health Monitoring Service.
- 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 on the site which has been assigned to you.
- You need to set the exception rule first. For details, refer to ***Add Exception Rule*** .

You can enter the Exception Center page by the following ways:

- On the Home page, tap → **Exception Center** .
- On the Home page, tap **More → Maintenance → Health Monitoring → Exception Center** .
- On the Home page, tap **Health Monitoring → Exception Center** .
- Tap **Site → Health Monitoring → Exception Center** to enter the Exception Center page.

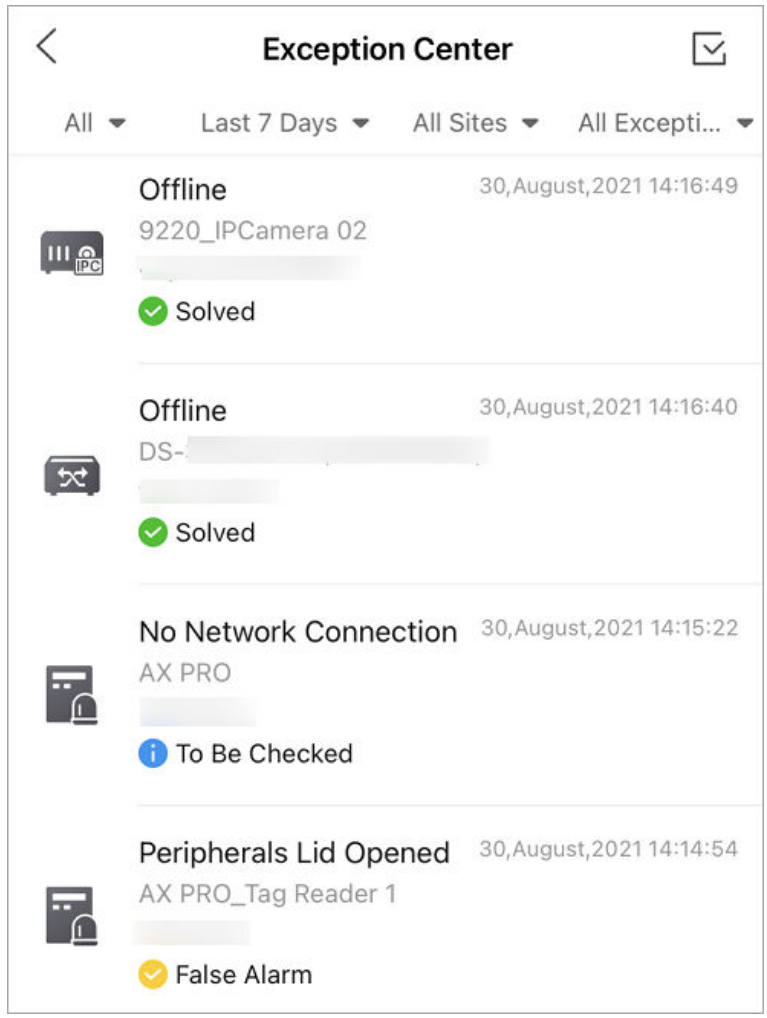


Figure 9-2 Exception Center

You can perform the following operations for Exception Center.

Filter the Exceptions

You can filter the exceptions according to your actual needs.

1. Set the handling result from all, unhandled, solved, to be checked, and false alarm.
2. Set the time period as Today, Last 7 days, Last 30 Days, Last 60 Days, or Last 90 Days, or customize a specific one. The exceptions received during the set time period will be displayed.
3. Select a source (including site, device, and channel) from the drop-down list to view the corresponding exceptions.
4. Select the exception types that you want to check. The exception types include device exception and channel exception.

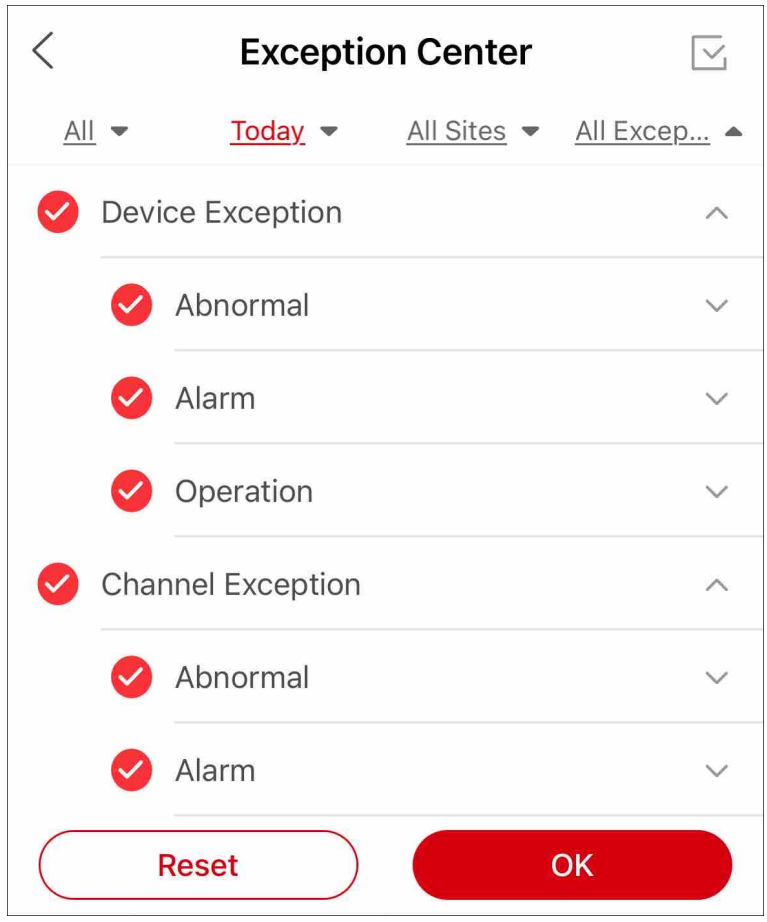


Figure 9-3 Exception Types

Handle an Exception

When you have solved an exception or you want to mark it for further examinations, you can select the handling result on Hik-Partner Pro. By handling the exceptions, you can better sort the exception list and avoid leaving some exceptions unattended. Your customer (the Site Owner) will also be informed of the handling result on Hik-Connect.
Follow the steps below to handle an exception.

1. Tap on the exception to show the Handle Exception page.

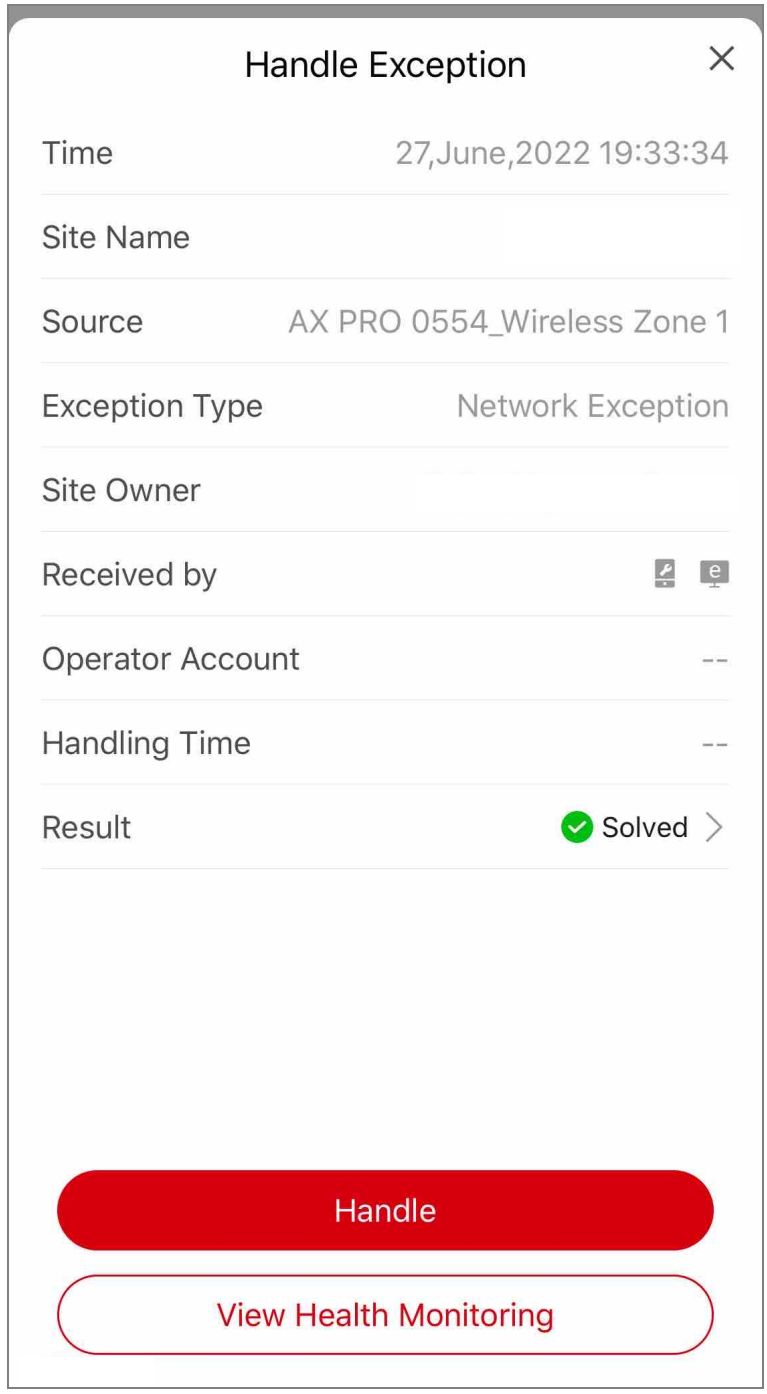


Figure 9-4 Handle Exception

2. Select a handling result in **Result**. You can select from **Solved**, **To Be Checked**, and **False Alarm**.
3. Tap **Handle** to save the changes.

Jump to Device Health Monitoring

On the Handle Exception page, you can tap **View Health Monitoring** to jump to the device's health monitoring page to troubleshoot the exceptions.

9.3 System Messages

The System Message tab of the Notification Center supports displaying system messages to keep you informed of any system-related information. You can view basic information of the messages in the list, including the message title, time when it was generated, the read/unread status, and the message content (in the form of texts or images).

In the upper-right corner of the page, tap ✉ → **System Message** to enter the System Message page.

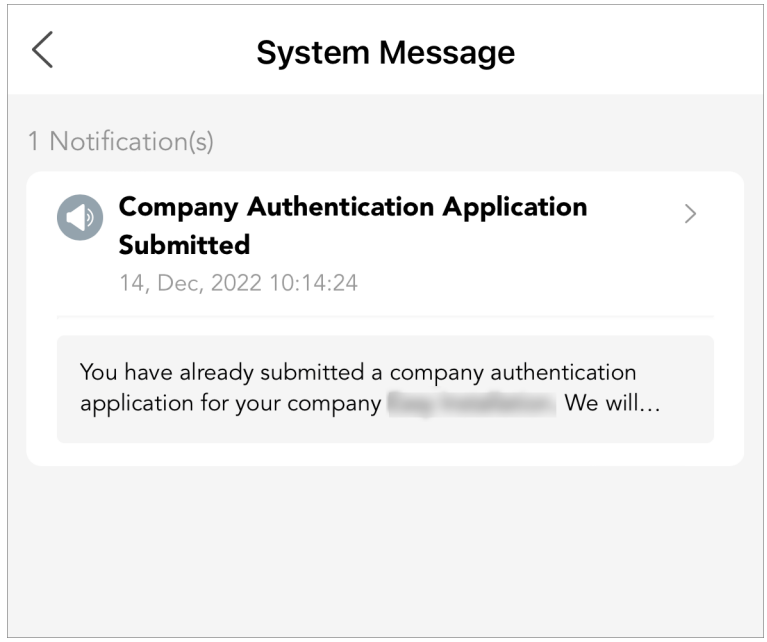


Figure 9-5 System Message Page

Feature and Version Updates

You can receive and view messages of system version updates and newly added features.

Complimentary Service Packages

You can receive and view messages notifying you of the complimentary value-added service packages issued to your account, which tell you the type of the service packages and the total quantity.

Company Authentication Application Related

You can receive and view messages related to company authentication applications, which include status change information such as application submitted, application approved, and application declined.

Note

- These are relevant for online applications only. If you are authenticating your account with an authentication code, status change information will not be displayed here.
- Only users who have the permission to manage company information can view messages of company authentication status change.

Case Related

You can receive and view messages related to cases, which include case updates such as case reply receiving, request to close the case, notification on upcoming auto-closing of case (7 days from closing-case request), and notification on completed auto-closing of case (14 days from closing-case request).

Points Balance Change

You can receive and view messages of changes to your reward points balance.

Company Merger Related

If you are the Installer Admin, you can receive and view messages related to company mergers that you have initiated, which include status change information such as merger failed, merger rejected, and merger completed. Besides, you can also receive invitation to merge with your company or reminders for initiating a merger if there are other companies with information similar to your company's detected.
For details about company merger, refer to .

9.4 Deals and Offers

You can receive notifications on the latest deals and offers available on the platform.

You can view the notifications concerning complimentary service packages and lottery draws (including the notifications of rejected receipts, obtained tickets, and lottery draw results). Tap on a notification to open the corresponding link of the deal/offer.

Chapter 10 Case

If you have any issues related to hardware, software, device password reset, etc., you can get professional help from our technical support via Case. On the Case page, you can submit cases to report your issues to us and follow up on the cases you submitted.

Note

- The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.
- This function is available only if your company is authenticated.
- All employee accounts of an authenticated company have the permission to use this feature.

Tap **Me → (at the top right) → Case** or tap **Home → More → Support → Case** to enter the Case page.

10.1 Submit Case

Enter different information for submitting Hardware Product Case, Software Product Case, Hik-Partner Pro Case, Device Password Reset Case and Dedicated Service Case.

Submit different types of cases as needed.

Note

- The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.
- Some installers can submit Dedicated Customer Service Case for focused troubleshooting from technical support.

10.1.1 Submit Hardware Product Case

You can submit hardware product cases for issues related to operations, configurations, or faults.

Steps

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

1. Tap **Me → (at the top right) → Case** or tap **Home → More → Support → Case** to enter the Case page.

   Enter the Case page.
2. Select **New Case → Hardware Products** .

3. Fill in the fields as required.

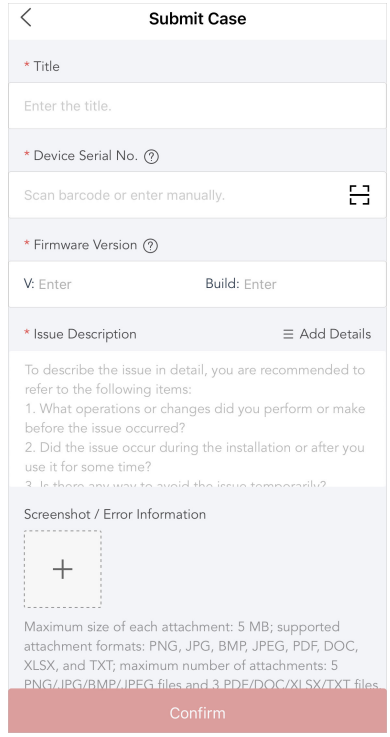


Figure 10-1 Hardware Case

Title

Enter the title of your case.

Note

The maximum length of the title is 100 characters.

Device Serial No.

Enter the device serial No. You can tap ⓘ to see where to find the serial No.

Firmware Version

Enter the version number and build number. You can tap ⓘ to see where to find the firmware version.

Issue Description

Describe your issue according to the suggestions in the blank.

Note

The length of issue description should vary from 20 to 2000 characters.

You can also tap **Add Details** to add issue details (software name, software version, network type, etc.) to your description as needed.

Screenshot / Error Information

Tap + to upload screenshots or error information.

Note

You can upload attachments in PNG, JPG, BMP, JPEG, PDF, DOC, XLSX, and TXT format.
No more than 5 PNG/JPG/BMP/JPEG files and 3 PDF/DOC/XLSX/TXT files are allowed.
The maximum size of each attachment is 5 MB.

Link for Accessing Files on Network Disk

For files larger than 5 MB, please upload them to a network disk.

Contact Information

This field is filled with your account information by default. You can edit it as needed.

4. Check the statement in the end.
5. Tap **Confirm** to submit the case.

10.1.2 Submit Software Product Case

You can submit software product cases for issues related to Hik-Connect and iVMS-4200.

Steps

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

1. Tap **Me → (at the top right) → Case** or tap **Home → More → Support → Case** to enter the Case page.

   Enter the Case page.
2. Select **New Case → Software Products** , and select **Hik-Connect/iVMS-4200** as the software name.
3. Fill in the fields as required.

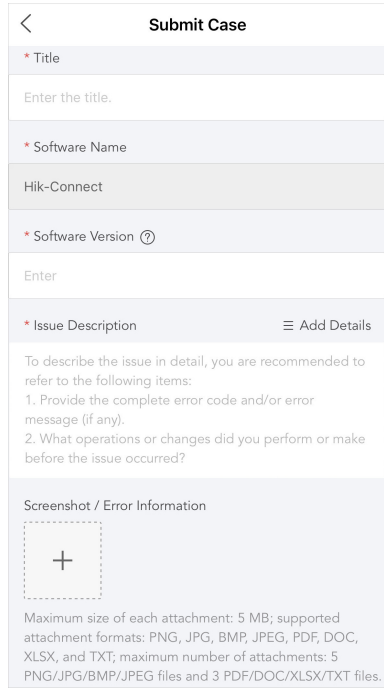


Figure 10-2 Software Case

Title

Enter the title of your case.

Note

The maximum length of the title is 100 characters.

Software Name

The software name is predefined and cannot be edited.

Software Version

Enter the software version. You can click ⓘ to see where to find the software version.

Issue Description

Describe your issue according to the suggestions in the blank.

Note

The length of issue description should vary from 20 to 2000 characters.

You can also tap **Add Details** to add issue details to your description as needed.

How did it occur?

The maximum length is 500 characters.

Phone/PC Operating System and Version

The maximum length is 72 characters.

Information About the Related Hikvision Devices

The maximum length is 500 characters.

Screenshot / Error Information

Tap + to upload screenshots or error information.

Note

You can upload attachments in PNG, JPG, BMP, JPEG, PDF, DOC, XLSX, and TXT format.
No more than 5 PNG/JPG/BMP/JPEG files and 3 PDF/DOC/XLSX/TXT files are allowed.
The maximum size of each attachment is 5 MB.

Link for Accessing Files on Network Disk

For files larger than 5 MB, please upload them to a network disk.

Contact Information

This field is filled with your account information by default. You can edit it as needed.

4. Check the statement in the end.
5. Tap **Confirm** to submit the case.

10.1.3 Submit Hik-Partner Pro Case

You can submit Hik-Partner Pro cases for 9 types of issues related to Hik-Partner Pro. The issues include account management, health monitoring, site management, account management, cloud storage, co-branding, code scanning and reward point market, solution and projects, and others. You can get professional help from our support team by submitting cases.

Steps

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

1. Tap **Me → (at the top right) → Case** or tap **Home → More → Support → Case** to enter the Case page.

   Enter the Case page.
2. Tap **New Case → Hik-Partner Pro** , and select an issue type from the 9 supported ones.

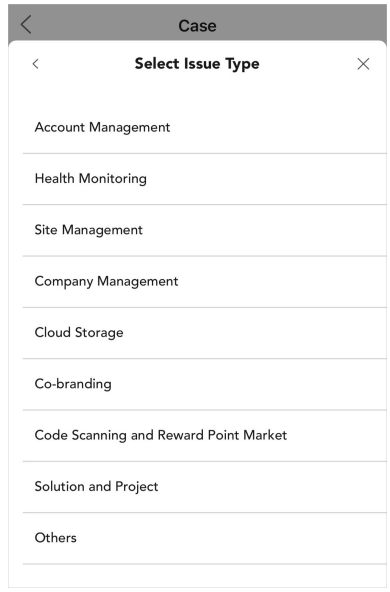


Figure 10-3 Issue Type

3. Fill in the fields as required.

Title

Enter the title of your case.

Note

The maximum length of the title is 100 characters.

Issue Description

Describe your issue according to the suggestions in the blank.

Note

The length of issue description should vary from 20 to 2000 characters.

Screenshot / Error Information

Tap + to upload screenshots or error information.

Note

You can upload attachments in PNG, JPG, BMP, JPEG, PDF, DOC, XLSX, and TXT format.
No more than 5 PNG/JPG/BMP/JPEG files and 3 PDF/DOC/XLSX/TXT files are allowed.
The maximum size of each attachment is 5 MB.

Link for Accessing Files on Network Disk

For files larger than 5 MB, please upload them to a network disk.

Authorization Code

This field is not available for the following issue type: Code Scanning and Reward Point Market, Solution and Project, and Others.

Other Contacts

Enter the email address of other contact.

Note

No more than 5 contacts can be added.

4. Tap **Confirm** to submit the case.

10.1.4 Submit Device Password Reset Case

You can submit device password reset cases, and after the support team replies, you can reset the password according to the apply.

Steps

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

1. Tap **Me → (at the top right) → Case** or tap **Home → More → Support → Case** to enter the Case page.
2. Select **New Case → Device Password Reset** .

   The instruction video is displayed by default. You can play it to get instructions about how to submit a device password reset case.

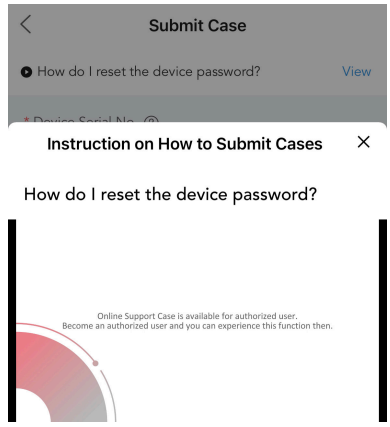


Figure 10-4 Instruction Video

3. Tap **Create Case Now** to start to create a case.
4. Fill in the fields as required.

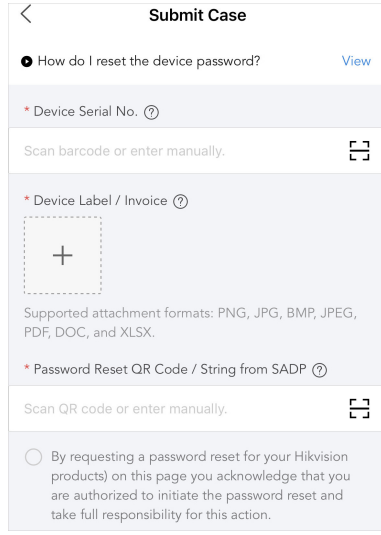


Figure 10-5 Device Password Reset Case

Device Serial No.

Enter the device serial No. You can tap ⓘ to see where to find the serial No.

Device Label / Invoice

Tap + to upload label pictures or invoices from the photo library, to take a photo, or to choose files.

Password Reset QR Code / String from SADP

Scan QR code or enter manually. You can tap ⓘ to see where to find the information.

5. Check the statement in the end.
6. Tap **Confirm** to submit the case.

10.1.5 Submit Dedicated Customer Service Case

You can report the issues found when using Hik-Partner Pro to the support team by submitting cases. The support team will respond to your case and provide support according to your case severity and language.

Steps

Note

- The function is only available for certain users in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.
- If you have more function-related requirements or improvement suggestions, please tell us via Feedback on the Me page.

1. Tap **Me → (at the top right) → Case** or tap **Home → More → Support → Case** to enter the Case page.

2. Tap **New Case** to enter the Submit Case page.
3. Enter a title for your case.
4. Select the language.

Note

The language options vary according to the country/region of your account.

5. Select the case severity.

Critical Business Down

Main functions which are critical to your business, such as logging in to the platform, creating sites, adding devices, receiving alarms, and handing over sites, are unavailable.

Business Impaired

Main functions work properly, but there are other function-related issues such as batch LAN configuration not working, probabilistic failure of remote configuration, and connection failure of some devices.

Functional Defects

There are some functional defects which do not affect your business or only affect your business slightly, such as wrong words on the page and high response latency.

Note

To get our rapid response when you have an urgent issue, select the case severity objectively.

6. Fill in the fields as required.

Issue Description

Describe your issue according to the suggestions in the blank.

Note

You're recommended to refer to the items listed on the page to describe the issue in detail. If the issue is difficult to describe with words, you can put links to related videos in the issue description and attach pictures below.

Screenshot / Error Information

Tap + to upload screenshots or error information.

Note

You can upload attachments in PNG, JPG, BMP, JPEG, PDF, DOC, XLSX, and TXT format.
No more than 5 PNG/JPG/BMP/JPEG files and 3 PDF/DOC/XLSX/TXT files are allowed.
The maximum size of each attachment is 5 MB.

Link for Accessing Files on Network Disk

For files larger than 5 MB, please upload them to a network disk.

Authorization Code

Set whether to provide the authorization code which is exclusive to the technical support staff for troubleshooting only. This field is not available for the following issue type: Code Scanning and Reward Point Market, Solution and Project, and Others.

Other Contacts

Enter the email address of other contact.

Note

No more than 5 contacts can be added.

7. Tap **Confirm** to submit the case.

Note

The case you submitted will be displayed in the My Case Records section. For more operations such as relying to the case and closing the case, refer to ***View and Handle Case Records*** .

10.2 View and Handle Case Records

You can view cases you submitted in the My Case Records section, view replies to a case, reply to a case, and close a case.

Tap **Me → (at the top right) → Case** or tap **Home → More → Support → Case** to enter the Case page.

Table 10-1 Available Operations on Case Page

Operation	Description
View All Submitted Cases	You can view cases you submitted in the My Case Records section, including the case ID, time the case was created, case title, casetype, and case status
View Case Details	Tap a case to enter the Case Details page to view the case creator, case description, replies from technical support, request from the technical support for closing the case, case status updates, and so on. **Note** If there is a new reply and the case status is changed, you will be notified by email or the Mobile Client. You can be redirected to details via the notifications.
Reply to Case	Tap a case to enter the Case Details page, tap **Reply** at the bottom, enter the reply content, and add attachments to reply to the current case.

Operation	Description
	Note For files larger than 5 MB, upload them to a network disk and provide the link for accessing the files.
Close Case	Tap a case to enter the Case Details page, and tap **Close Case** to close the case after your issue is solved. You can rate our services and give your comment when closing the case. **Note** The case will be closed automatically if you do not reply or do not close the case for 14 days.

Chapter 11 Return Material Authorization

Return material authorization (RMA) is an arrangement in which you can ship an item back for an exchange or repair due to a product defect or malfunction. The process is firstly Installers can initiate RMA applications, and contributors can repair the defected products after receiving applications. Finally the products will be returned after they are repaired and debugged.

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

11.1 Submit RMA Requests

You can register an RMA request for exchanging or repairing goods. After registration, you can check real-time status of the requests.

Note

The function is only available in certain countries and regions, and cross-country requests are not supported. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

Tap **Me → (at the top right) → RMA** or tap **Home → More → Support → RMA** to enter the Case page.

Add Product

Tap **Repair Request → +Add** to initiate a request, and enter the product serial No. or scan the product QR code to start the application.

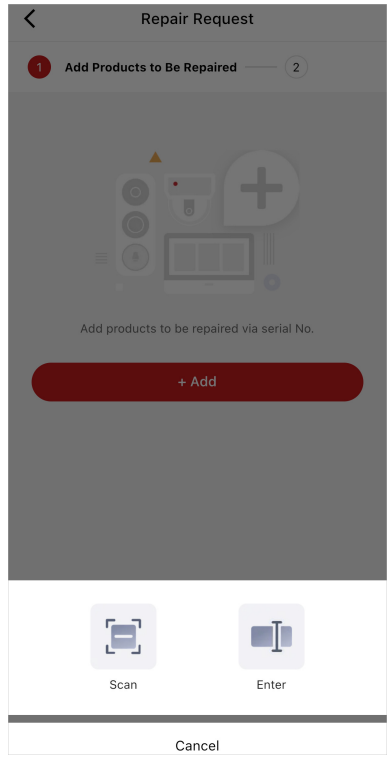


Figure 11-1 Add Product

- For countries and regions that support cross-contributor repair, if the contributor is identified according to the serial number, the contributor will be automatically selected. If not identified, you need to choose a contributor by yourself. After choosing a contributor, the contributor and product information will show up in the list. You can still tap to change distributors.
  By default, the repair location is the nearest location. You can also select among all locations of all contributors in the country.
- For countries and regions that do not support cross-contributor repair, the system will identify the contributor according to the serial code. The default choice is the nearest location of the contributor. If the contributor can not be identified according to the serial number, then the product can not be added.

If there are more devices to be repaired, tap **+Add** to add more devices, or you can tap **Confirm** to enter shipping information.

Note

It should be a Hikvision product sold in the current country or region.

Shipping Information

Complete the shipping information including fault description, shipping method (by shipping carrier or by myself), and remarks (optional).

Tap **Add a New Address** to add a new shipping address or select an existing address, then tap **Submit**, and the status of an RMA request will turn to Requested.
If you select by shipping carrier as the shipping method, you will also need to tap **Ship to Distributor** to enter shipping carrier and shipping order No.
If you select by myself, confirm that the product is shipped, and then the status of an RMA request will turn to Shipped to Distributor.

11.2 View and Handle RMA Requests

After an RMA application is submitted, you can view its status and perform further operations.

Note

The function is only available in certain countries and regions. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

Tap **Me → (at the top right) → RMA** or tap **Home → More → Support → RMA** to enter the Case page.

In the RMA list, each to-be-repaired product has an RMA number, and you can view its status and tap the application to view details.

Note

- When the status is Requested:
  - If you select by shipping carrier as the shipping method, you need to tap **Ship to Distributor** to enter shipping information (including shipping Carrier or shipping order No.).
  - If you select ship by myself as the shipping method, confirm that you have shipped the product.
  - You can tap **Cancel Request** to cancel the request.
- If the status is Repaired & Shipped, you can tap **Complete** to finish the request.

You can also tap **Filter** to filter requests by their status and time.

11.3 Find Repair Stations

You can view repair stations on the map. The available repair stations are displays according to their distances from your location, so you can choose which repair station you want to ship your products to.

Note

The function is only available in certain countries and regions, and cross-country requests are not supported. For details about whether your country or region supports the function, refer to the after-sales or local distributor.

Tap **Me → (at the top right) → RMA** or tap **Home → More → Support → RMA** to enter the Case page.

Tap **Repair Station Query**.

Your current location is displayed on the top of the page.

- On the map, your location and nearby repair stations are displayed.
- In the list, the available repair stations are displays according to their distances from your location. The information about repair stations includes station name, contributor name, station address, distance from you location to the station, and station phone number (Tap ☎ or tap **Make a Call** on the details page to make a phone call to the station staff for asking more information.).

Chapter 12 Value-Added Services

Hik-Partner Pro provides multiple value-added services for you to better serve your customers, including the health monitoring service, cloud attendance service, cloud storage service, people counting service, temperature screening service, alarm receiving center service, HikCentral Connect service, co-branding service, and employee account add-on.

Note

- Most of value-added services are only available in certain countries and regions. For more information, refer to the after sales or local distributor.
- All the value-added services are not supported by the solar camera.

12.1 View and Purchase Value-Added Services

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, cloud attendance service, people counting service, HikCentral Connect service, temperature screening service,co-branding 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 **Service Market** on the Home page or tap **Me → Service Market** to enter the Service Market page to view details of the value-added services or purchase services by service key (if your country or region supports).

12.2 View and Manage My Services

On the My Service page, you can conveniently view and manage all your services including the health monitoring service, cloud storage service, employee account add-on, and cloud attendance service. You can view information about the trial period, free package, services expiring soon, and numbers of used and remaining service packages, purchase services by service keys, and perform operations such as renewal and activation.

Note

This feature is not supported in regions only with support for free functions and is available only if you have the permission to purchase service packages.

Tap **Me** at the bottom right and tap **My Service** to enter the My Service page.

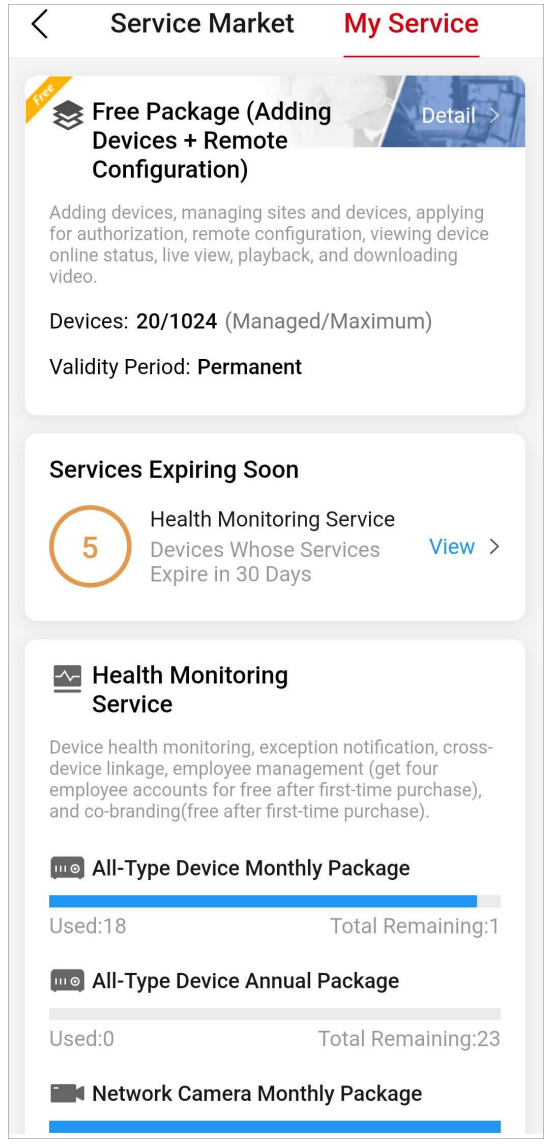


Figure 12-1 My Service Page

The service section introduces a service and shows the numbers of used and remaining service packages (or employee accounts as for employee account add-on). You can tap **Purchase by Service Key** to purchase the service by service key, tap **Buy Now** to send an email containing the Portal's URL for purchasing to your email address, and tap the section to go to the detail page for the service.

Note

- The page shows a service section only if you have purchased or are using the service.
- The Mobile Client does not support purchasing the services online. You can go to the Portal to purchase online, or purchase a service key from the local distributor offline first and then purchase the service by the service key via the Mobile Client.

The My Service page shows the following sections.

Trial Period Information

The page shows this section only when it is during the trial period.
This section presents the description and the end time of the trial period.

Free Package Information

This section presents the description of the free package, maximum number of manageable devices, and number of managed devices.
You can tap **Detail** in this section to view the differences between the free package and health monitoring package, and purchase health monitoring service packages by service keys.

Services Expiring Soon

The page shows this section only if there are services expiring soon.
You can tap **View** to go to the detail page for the service to renew it.

Health Monitoring Service

On the detail page for the health monitoring service, you can conveniently view the devices with services expiring in 30 days, devices with expired services, and devices with auto renewal, and perform operations as follows.

Table 12-1 Supported Operations on Details Page for Health Monitoring Service

Operation	Description
Filter Devices by Site	Tap **All Sites** and select a site to view the devices on the site and perform renewal / batch renewal, activation, etc.
Filter Devices by Service Status	Tap **All**, **Expire Soon**, **Expired**, or **Auto Renewal** to view devices with each service status.
Renew Service for Device	Tap to renew the service for one device.
Transfer Service	Tap to transfer the remaining service time to another device.
Enable/Disable Auto Renewal	Tap to enable/disable auto renewal for the device.

Operation	Description
Batch Renew for Devices	Tap **Batch Renew** at the bottom, select devices, and click **OK** to batch renew.
Activate Service	Tap **Activate Service**, select devices, select activation type, and click **OK**.

Cloud Storage Service

On the detail page for the cloud storage service, you can conveniently view the channels with services expiring in 30 days and channels with expired services, filter channels by service status, and renew the service for a specific channel.

Employee Account Add-On

On the detail page for the employee account add-on, you can conveniently view the added employees, and add, delete, enable, and disable employees.

Cloud Attendance Service

On the detail page for the cloud attendance service, you can conveniently view the cloud attendance systems expiring in 30 days and expired cloud attendance systems, and perform operations as follows.

Table 12-2 Operations Supported on Detail Page for Cloud Attendance Service

Operation	Description
Filter Cloud Attendance Systems by Site	Tap **All Sites** and select a site to view the cloud attendance systems on the site and renew systems.
Filter Cloud Attendance Systems by Service Status	Tap **All**, **Expire Soon**, **Expired**, or **Trial** to view systems with each service status.
Renew Cloud Attendance System	Tap to renew the system.

12.3 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-Partner Pro 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.

12.3.1 Set Cloud Storage for Hik-ProConnect Box

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

Steps

Note

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

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

   Note

   For details, see ***Add Device by Scanning QR Code*** and ***Add Device by Entering Serial No.*** .

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

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

   Note

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

   You enter the Select Device to Link page, on which the available devices are displayed.
4. Tap a device to enter the Select Channel to Enable Cloud Storage page.
5. Turn on the switch(es) to add channel(s) to the Hik-ProConnect box.
6. Tap **Next** to enter the Device Information page.
7. Set the device information, such as device IP address, user name, and password.

   Note

   The IP addresses of the devices and the Hik-ProConnect box should be on the same LAN.
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-Partner Pro 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 including 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.

12.3.2 Set Cloud Storage for NVR

You can enable and set up cloud storage for an NVR and its linked channels. When you complete the settings, the NVR will be able to upload event-related footage of its linked channels to the cloud.

Do I need a Hik-ProConnect box to enable cloud storage function for an NVR?

- If your NVR supports cloud storage, there is no need for a Hik-ProConnect box.
  This feature requires device capability. Refer to the *Hik-Partner Pro Compatibility List* for a complete list of supported models.
  See the next section for instructions.
- If your NVR does not support cloud storage, you can use a Hik-ProConnect box to help the linked channels of an NVR upload footage to the cloud.
  See details in ***Set Cloud Storage for Hik-ProConnect Box*** .

How to enable cloud storage for an NVR that supports cloud storage?

Select the NVR's site, and tap on the NVR to enter its settings page. Tap **Linked Channel** where you can set up cloud storage for each channel.

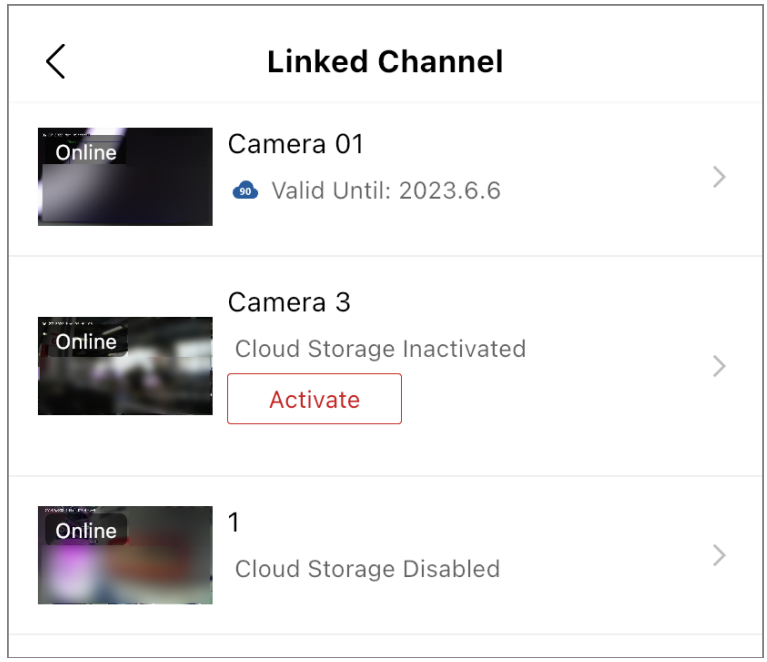


Figure 12-2 Linked Channel

When setting up the cloud storage, you need to read and follow the recommendations for the resolution and bit rate of the channels at the top of the page.

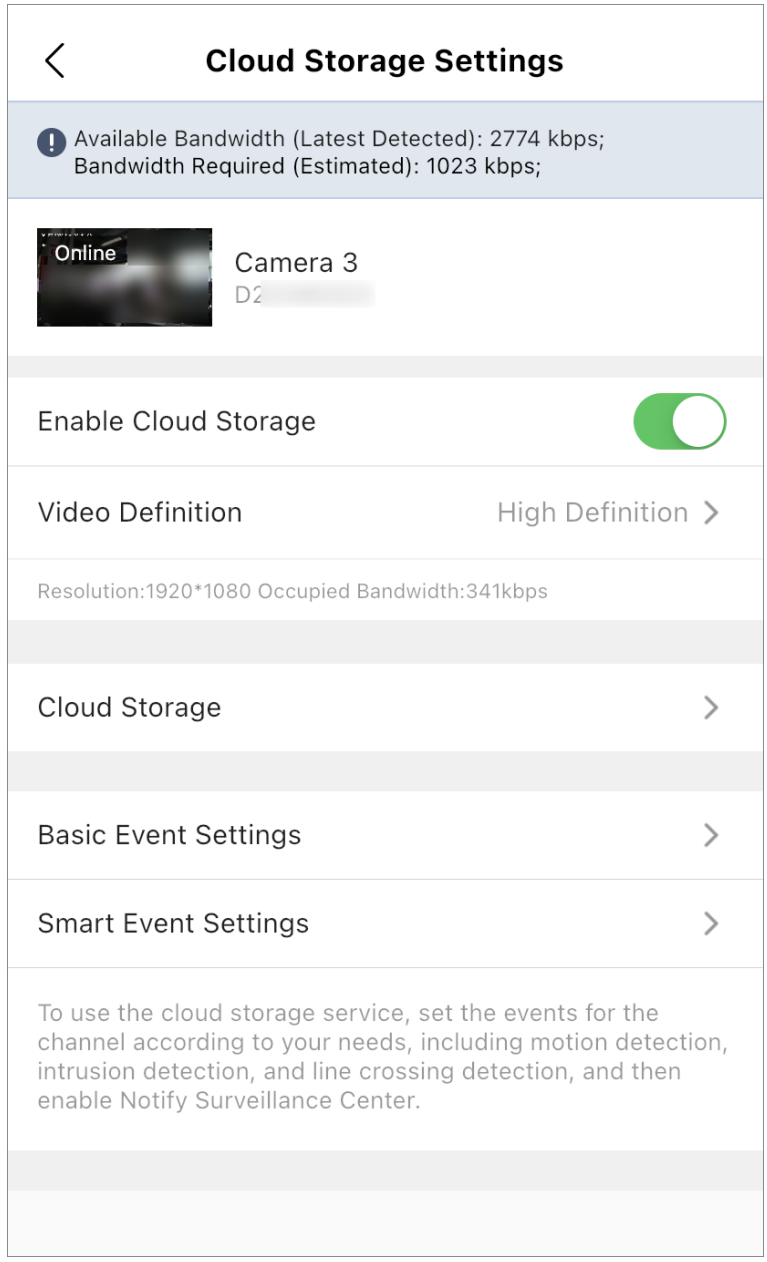


Figure 12-3 Cloud Storage Settings

The steps are similar to those of setting up cloud storage for a Hik-ProConnect box. You can refer to ***Set Cloud Storage for Hik-ProConnect Box*** for descriptions of the parameters such as **Video Definition**, **Cloud Storage**, and **Motion Detection**.

Note

- If Smart H.264+ / H.265+ encoding is enabled for the channel with cloud storage enabled, the quality of the footage on cloud will be affected. The platform will notify you to switch to disable Smart H.264+ / H.265+ encoding.
- If stream encryption is not enabled for an encoding device linked to an NVR that supports cloud storage, you cannot enable cloud storage for the channels of the encoding device.

12.3.3 Set Cloud Storage for DVR

When you complete adding a DVR that supports cloud storage 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 channels of the DVR that supports cloud storage, and activating cloud storage service for the channels. When you complete all these settings, the DVR that supports cloud storage will be able to upload event-related video footage from its linked channels to the cloud.

Steps

Note

- If your DVR does not support cloud storage, you can use a Hik-ProConnect box to help the linked channels of the DVR upload footage to the cloud.
- If you skip the cloud storage settings when completing adding the DVR that supports cloud storage, 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 DVR that supports cloud storage to the platform by Hik-Connect P2P.

   Note

   For details, see ***Add Device by Scanning QR Code*** and ***Add Device by Entering Serial No.*** .

   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 DVR that supports cloud storage 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-Partner Pro 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.

12.3.4 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.

12.3.5 Activate or Renew Service for a Channel

On the cloud storage service page for a site, you can view the service status of channels of the cloud storage device(s) added to the site. If cloud storage service is not activated for a certain channel, you need to activate the service before using the feature. If the service activated for a channel is about to expire or has already expired, you can renew the service for the channel.

Before You Start

Make sure you have added cloud storage device(s) to the site. For details, refer to ***Add Device by Scanning QR Code*** and ***Add Device by Entering Serial No.*** .

Steps

Note

For a device which does not support the Hik-Connect service, you need to add it to Hik-Partner Pro via the proxy of a Hik-ProConnect box first, and then activate the cloud storage service for channels of the device. See ***Add Devices Without Support for the Hik-Connect Service*** for details about how to add this type of devices.

1. Tap the **Site** tab at the bottom to enter the Site page.
2. Tap a site to enter the site details page.
3. Tap the **Cloud Storage** tab.

4. Tap **Enable Cloud Storage Service** and select an online device from the list to enter the page of its linked channels.

Note

If there is only one cloud storage device added to the site, you will enter the page of its linked channels directly after tapping **Enable Cloud Storage Device**.

5. Select the method for activating or renewing cloud storage service for a channel.
   - To activate the service for a channel, tap **Activate** and choose from **Activate by Service Key** and **Service Package**.
   - To renew the service for a channel, tap the channel to enter its cloud storage settings page, tap **Cloud Storage → Renew** , and choose from **Renew by Service Key** and **Service Package**.
6. Activate or renew the cloud storage service for the channel.
   - For activating/renewing with service package(s), select a package type and set the quantity of the service package(s) to be used for the channel.
   - For activating/renewing by service key, enter the 16-character service key.

Note

You can consult the distributor to get the service key.

7. Tap **Activate** or **Renew** to finish activating or renewing the service respectively.

Note

If a cloud storage device has at least one channel with cloud storage service activated, it will be displayed on the cloud storage service page under **Devices with Cloud Storage Service Activated**. Tap the device to view the service status of its linked channel(s). If needed, you can also tap to activate the service for a channel, or tap to renew the service for a channel.

12.4 Co-Branding

If you enable the co-branding service, your customers (i.e., the end user) will be able to view your company information, such as company logo, address, and phone number, on the Hik-Connect Mobile Client. This can help to promote awareness of your company brand, products, and services.

Note

- You can get the co-branding service for free after purchasing the annual type of health monitoring packages (including All Device Annual Package and Network Camera Annual Package) for the first time.
- In some countries/regions, you can also get the co-branding service for free for one year after authenticating your account and adding 3 devices via P2P. See details in ***Authenticate Your Account*** and ***Add Device by Entering Serial No.*** . After finishing the tasks, you can get the co-branding service for free in the following entrances:
  - Go to **Me → Service Market → Co-Branding** .
  - Go to **Me → Company Management → Co-Branding** .

- A window with notification about getting the co-branding service for free will pop up when your co-branding service expires in 2 months.
- You can redeem points for co-branding services in the Rewards Store. After that, the co-branding service will be available or its validity period will be extended if it is already available. See details in ***Rewards Store*** .
- In some countries/regions, you can either purchase co-branding service packages online or activate them by entering service keys purchased from local distributors offline on the Portal. Refer to *User Manual of Hik-Partner Pro Portal*.
- You can choose to or not to upload your company logo. If no company logo is uploaded, your company name, instead of your company logo, will be displayed on the Hik-Connect Mobile Client.

Tap **Me → Company Management → Co-Branding** to enter the Co-Branding page. Switch **Co-Branding** to on and the Logo area will be activated. Tap > to select a photo from your photo album as your company logo. After you edit the logo, the latest logo will be updated to the Company Information page.

Note

- To ensure the co-branding service works on the Hik-Connect Mobile Client, please inform your customers to update the Hik-Connect Mobile Client to the required version (V 4.15.0 or later if the company logo is uploaded and V 4.26.0 or later if the company logo is not uploaded). You can send the QR code or download link shown in the banner on the Home page to them for downloading the Hik-Connect Mobile Client.
- If all the devices of your customer are managed by the same installation company, the installation company's logo will be displayed on the login page and About page of your customer's Hik-Connect Mobile Client.
- If your customer's devices are managed by different installation companies, your customer can go to the device details page on the Hik-Connect Mobile Client to view the companies' logo and details.

Chapter 13 Products

The Products module supports viewing information of hot products or a certain type of products. You can search for or filter the products, download the related documents, and share the product information with others. The module also supports comparing the parameters/specifications of products to learn about their similarities and differences.

Note

The Products module is not supported in some countries/regions.

13.1 View and Search Products

You can search for products and view detailed product information, including the product picture, description, parameters, and related documents.

You can view a list of hot products on the home page under the tab **Products**, or view the products by product category in the Products module. You can search for a specific product by product name or model, or filter the products by brand, product category, type, series, and the relevant parameters. For a specific type of products, you can switch between gallery view and list view for different product display modes.

Tap on a product to view detailed information about the product, including the product picture, description, parameters, and related documents. On the product details page, you can also leave comments for the product, add it to Favorites, give it a thumbs up, download the related documents, or share the product information with others.

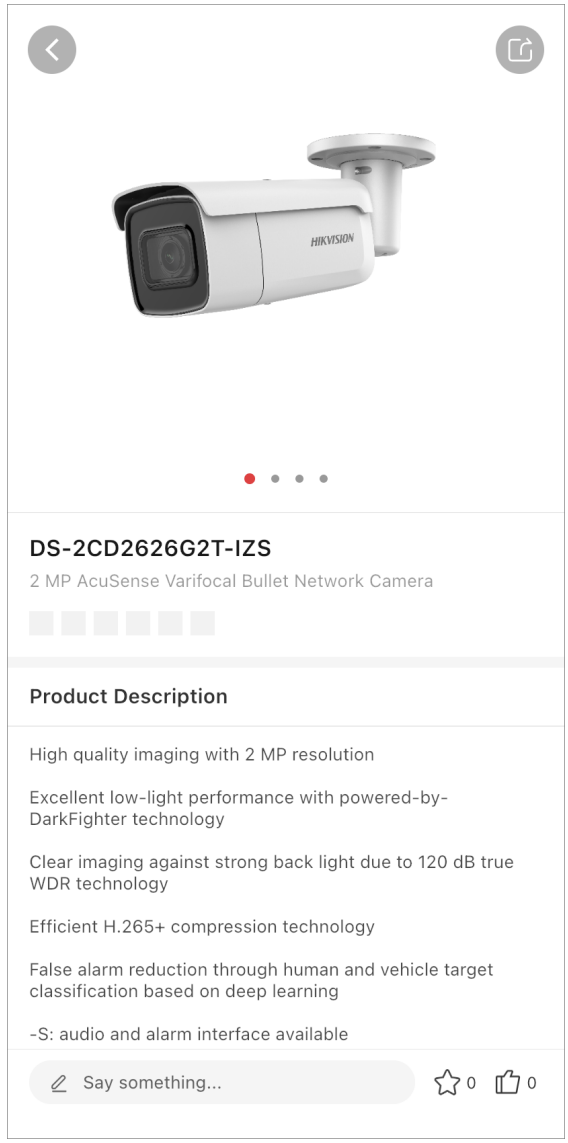


Figure 13-1 Product Details Page

Note

You can find the products you have added to Favorites later in **Me → My Favorites → Products** , and the comments you have left for the products in **Me → My Comments → Products** .

13.2 Compare Products

You can compare the parameters/specifications of products to learn about their similarities and differences.

On the product display page, you can add a product to the comparison list by tapping **+VS** next to it. You can check the comparison list by tapping VS on the top right with the total number of added products displayed on top.

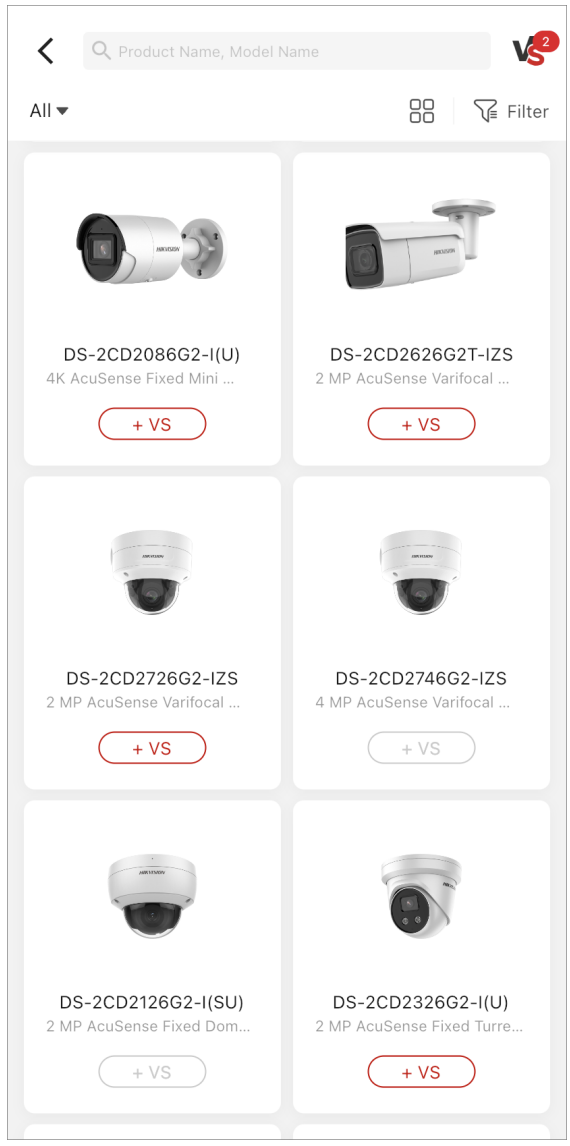


Figure 13-2 Select Products to Compare

To start comparing products, select at least two but no more than four products from the comparison list and tap **Start VS**. On the comparison result page, fields that are different are highlighted with a background color. You can switch on **Hide Same** on the top left to hide parts that are the same and focus only on the differences.

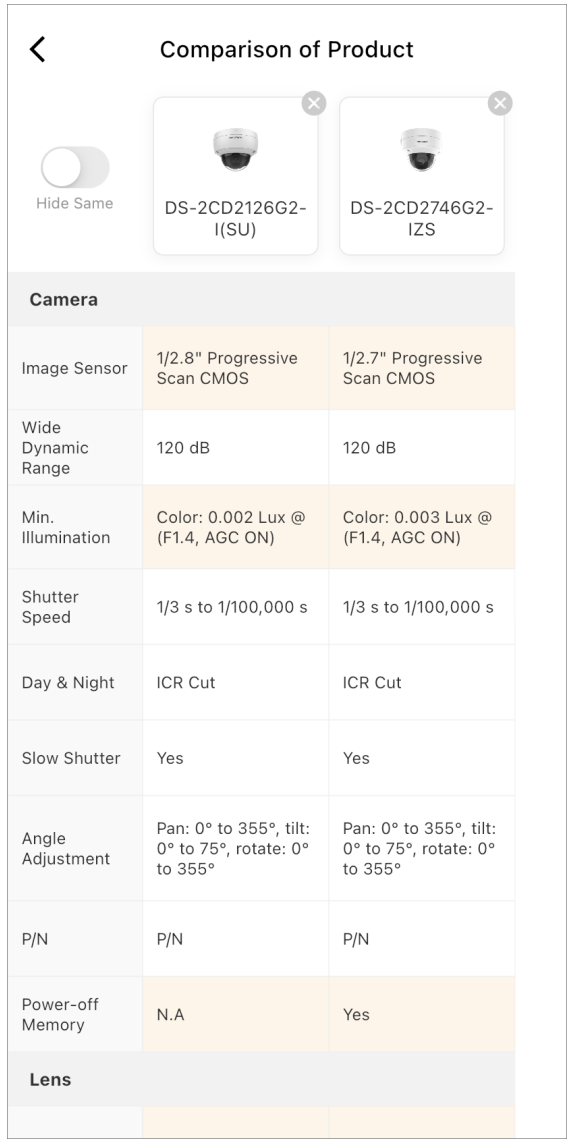


Figure 13-3 Product Comparison

Chapter 14 Partner Program

As a reseller, you can apply for partner programs on Hik-Partner Pro with the contract agreements signed both offline and online. You can also view your program history and the certificates that you get after your application is approved and the contract agreement is signed.

Note

- This function is not supported by some accounts or in some countries/regions.
- The contract agreements of partner programs are signed by three parties (the reseller, distributor, and Hikvision). Distributors can also manage and sign their program agreements on Hik-Partner Pro. For details, refer to ***Manage My Agreements*** .

Refer to the following sections to learn more.

- ***Submit Program Application***
- ***View Your Certificates***
- ***View Program History***

Submit Program Application

Go to **Me → Partner Program** , and tap a program in the **Program Application** section for application.
Select your signing status in the pop-up window according to whether you have signed the agreement with Hikvision offline or not.

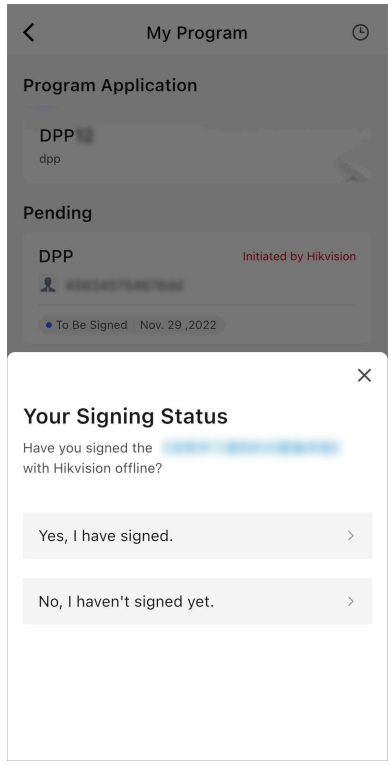


Figure 14-1 Select Signing Status

After you select your signing status, you will enter the details page to view the details and introduction about the partner program you are applying for. Tap **Next** to continue your application.

If you have signed the contract agreement with Hikvision offline, you should upload the contract agreement that you have signed when you submit the application.

If you haven't signed offline, you should select the level you want to apply for.

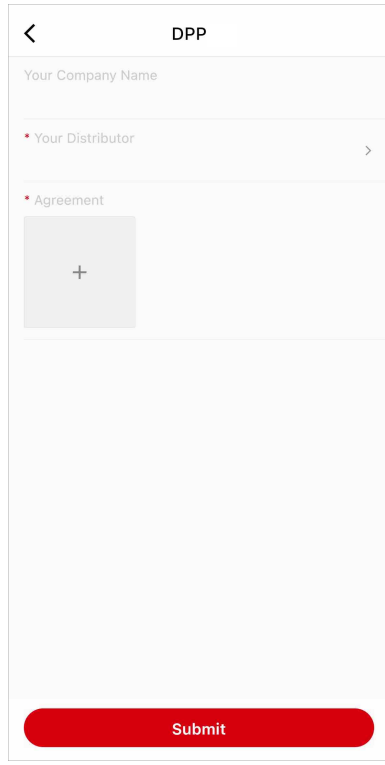


Figure 14-2 Application Page (Contract Agreement Already Signed Offline)

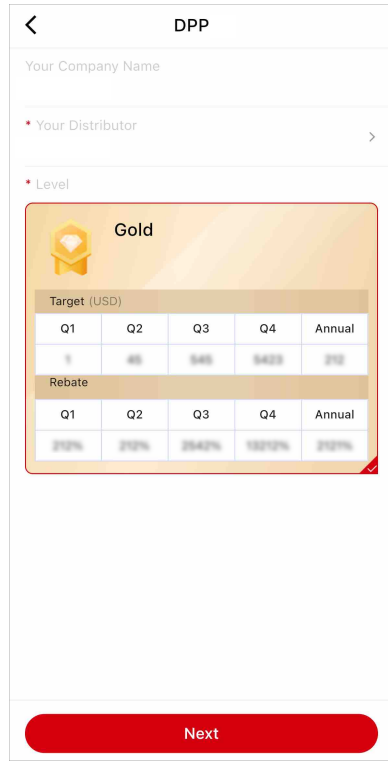


Figure 14-3 Application Page (Contract Agreement Not Signed)

Tap **Submit**/**Next** after you select your distributor and upload your signed agreement / select your level.

If you have uploaded your signed agreement during application, the application process is completed after you tap **Submit**. Otherwise, you may enter one of the following processes:

- If the level you select does not require you to communicate with Hikvision to confirm the targets offline, you will enter the details page of the contract agreement, and you should check **I agree with and accept this agreement** and tap **Next**.
- If the level you select requires you to communicate with Hikvision to confirm the targets offline, and after you communicate with the Hikvision sales representative offline, choose one of the followings:
  - Sign your contract agreement with Hikvision offline, and submit the application again online by yourself (you need to upload your signed contract agreement).
  - The Hikvision sales representative will initiate the signing process online for you and you need to sign the contract agreement online.

View Your Certificates

After your program application is approved and the contract agreement with Hikvision is signed, the program certificate will be issued to you. You can view the details of all your certificates in My Certificate.

Go to **Me → Partner Program** , you can swipe left and right to view the certificates in the My Certificate section, or tap **More** to enter the My Certificate page for more details and to perform more operations.

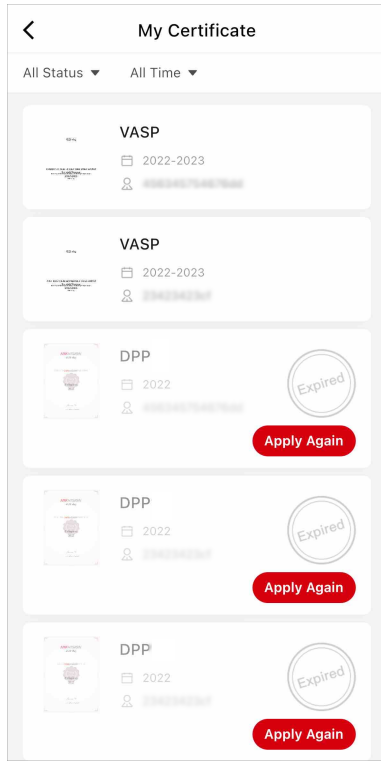


Figure 14-4 My Certificate

On the certificate list, you can view the program certificate name, certificate thumbnail, level, term of validity, distributor, and status (expired or not).
Tap **All Status** and/or **All Time** to filter the certificates.
Tap **Apply Again** to apply for the partner program of which your certificate has expired.
Tap a certificate in the list to enter the Certificate Details page. You can download the contract agreement you signed on this page.

View Program History

After you submit your program application or if there are programs initiated by Hikvision for you, you can view all these programs in Program History.
Go to **Me → Partner Program →** .

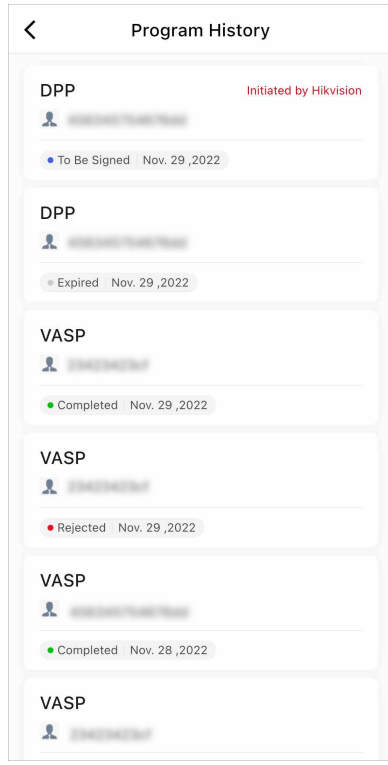


Figure 14-5 Program History

You can view the program name, application status (pending signing, completed, expired, and rejected), application time, and the distributor on the list. For program initiated by Hikvision, a red **Initiated by Hikvision** is displayed beside the name.

Tap an application record to enter the details page of the program application. You can view the application status, program name, distributor name, level, and contract agreement.

For the program application of which the status is **Pending Signing**, tap **Sign** on the bottom of the details page to sign the agreement online.

Chapter 15 Rewards Store

Hik-Partner Pro provides a reward point system to reward your trust and support. By completing specific tasks (e.g., check-in), you can get the reward points redeemable for lots of gifts (e.g., certain value-added services) in the Rewards Store.

Note

- The reward point system is only supported in some countries/regions.
- For some countries/regions, the reward points are available only when you have your company authenticated. For details about company authentication, see ***Authenticate Your Account*** .

Three ways to enter the Rewards Store page:

- Tap **Home → More → Rewards → Rewards Store** to enter the Rewards Store.
- Tap **Home → My Points** to enter the Rewards Store.
- Tap **Me → Available Company Points** to enter the Rewards Store.

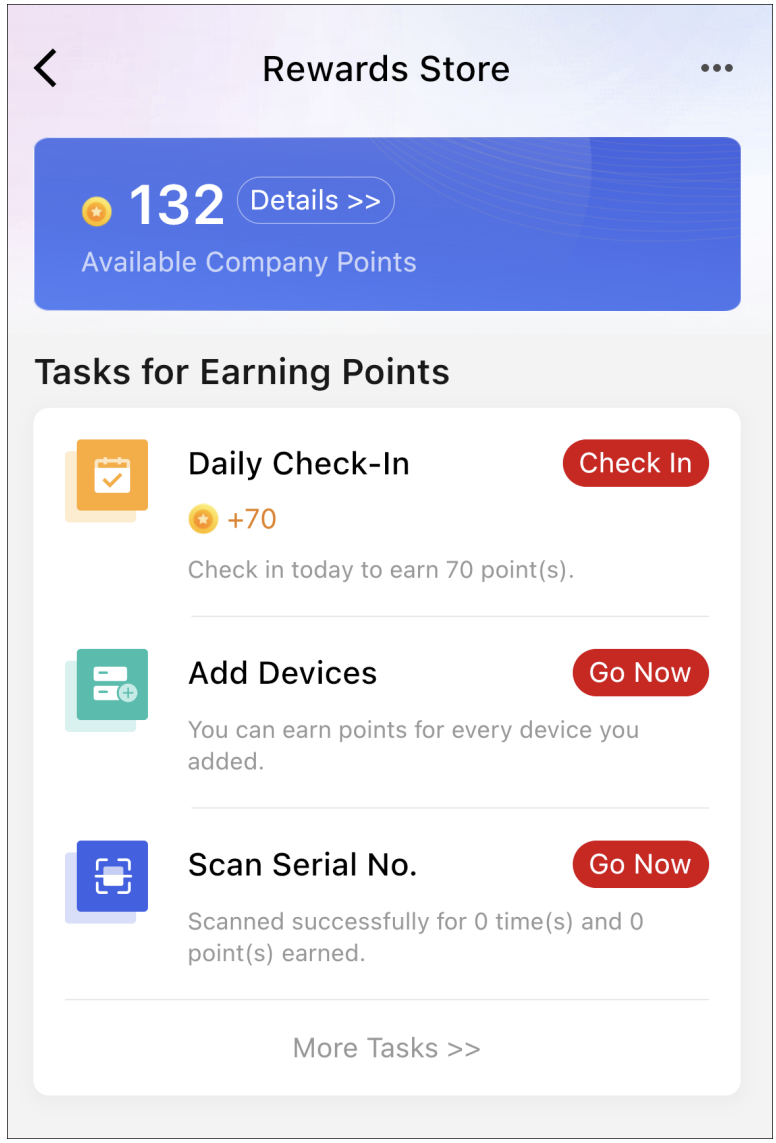


Figure 15-1 Rewards Store

For the Installer Admin and Installers, the information displayed on the My Points page varies. The Installer Admin can view more information and perform more operations. See the table below for details.

Table 15-1 Available Information/Operations for the Installer Admin / Installers

Information/Operation	Installer Admin	Installer
Available Company Points	√ View company total points.	√ View personal total points.
Points History	√	√

Information/Operation	Installer Admin	Installer
	View and filter points earned by each staff member.	View and filter points earned by the Installer.
Point Rules	√	√
Check-In Records	√ Records of all people in the company are available.	√ Only the Installer's own records are available.
Tier Information	√	√
Add Device to Earn More Points	√	√
View the Task List and Do Tasks **Note** The task types include inviting friends (by sharing the OR code, invitation code, or invitation link), answering questions, browsing/liking news and how-to articles, inviting staff members, scanning SN codes, and adding devices.	√	√ Installers can perform some of the tasks available for Installer Admin.
Redeem Points for Gifts	√	×
View My Gifts	√	×
Scan History	√	√
Lucky Draw	√ Only supported in some countries/regions.	×

Note

After user upgrading, if your original account and Hik-ePartner account are merged to one OneHikID account, the points in the two accounts will add up.

Chapter 16 Quotation Tool

The quotation tool allows you to calculate the total price of products for your customers. You can add products for quotations first, including Hikvision products and your own products, then you can create quotations with the added products. The generated quotations can be shared with your customers in the format of PDF or XLSX.

16.1 Add Products for Quotation

You can add products for quotations, including Hikvision products and your own products. For the added products, you can view their details, edit their prices, etc.

Steps

1. Enter the New Quotation page.
   - Tap **Home → More → Tools → Quotation Tool → New Quotation** .
   - Tap **Products**, tap any type of products to enter the product list, and tap ··· **Quote List** .

   Note

   For the first time you enter the New Quotation page, you need to select the currency.
2. Tap + in the upper-right corner of the page.
3. Select **Hikvision Products** or **My Products** and add products as needed.

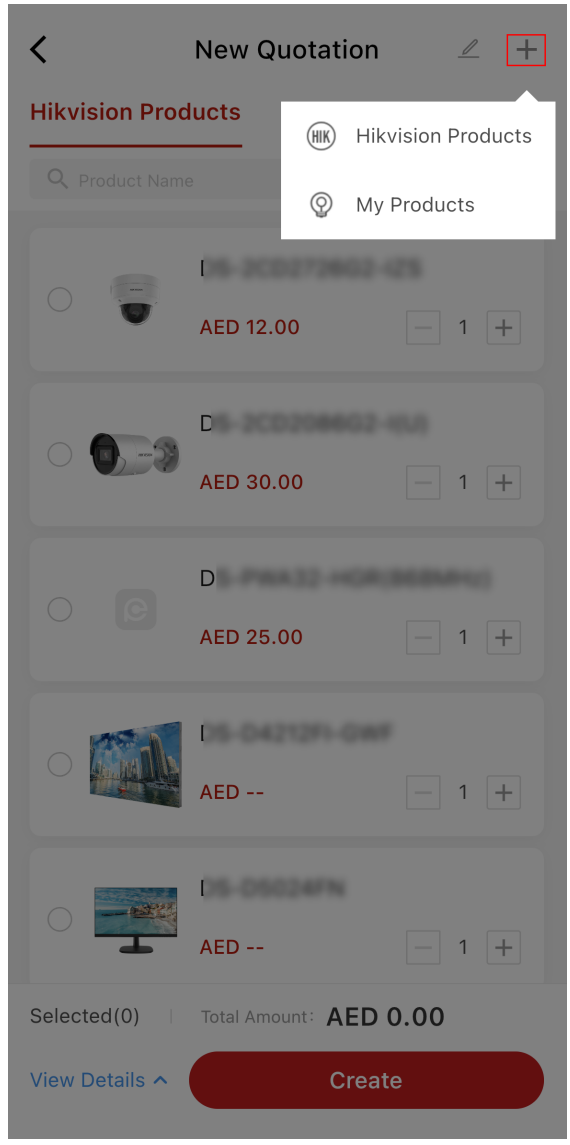


Figure 16-1 Add Products for Quotation

- Select **Hikvision Products**. On the desired product, tap ＋ → **+ Quote** to add it to the list on the New Quotation page.

  Note

  Tap ··· and you can view the total number of Hikvision products that have been added to the quote list.

- Select **My Products**. Enter the product information, including mode, description, and unit price, and tap **Confirm** to add it to the list on the New Quotation page.

4. **Optional:** Tap ··· → **Quote List** to go back to the New Quotation page and perform further operations.

Search for Products	Enter keyword(s) of product name in the search box to search for target products.
View Product Details	Tap a product to view its details, including the product description, product parameters, and related documents.
Edit My Products	Select one or multiple products and tap → **Edit Price** .
Delete Products	Select one or multiple products and tap → **Delete** .
Create Quotations	See details in ***Create Quotation*** .

16.2 Create Quotation

You can create quotations with the added products. Also, more information can be attached to the quotations, including the company information, customer information, numbers and prices of the added products, discount, and VAT.

Before You Start

Make sure you have added products for quotations. See details in ***Add Products for Quotation*** .

Steps

1. Enter the New Quotation page.
   - Tap **Home → More → Tools → Quotation Tool → New Quotation** .
   - Tap **Products**, tap any type of products to enter the product list, and tap ··· → **Quote List** .
2. Under the Hikvision Products tab and My Products tab, select one or multiple products and specify the number of each product.

   The number of selected items and the total amount of money are displayed at the lower bottom.

   Note

   - Make sure the products you select have their prices.
   - You can tap **View Details** to expand the details of the selected products.
3. Tap **Create** to enter the New Quotation page.

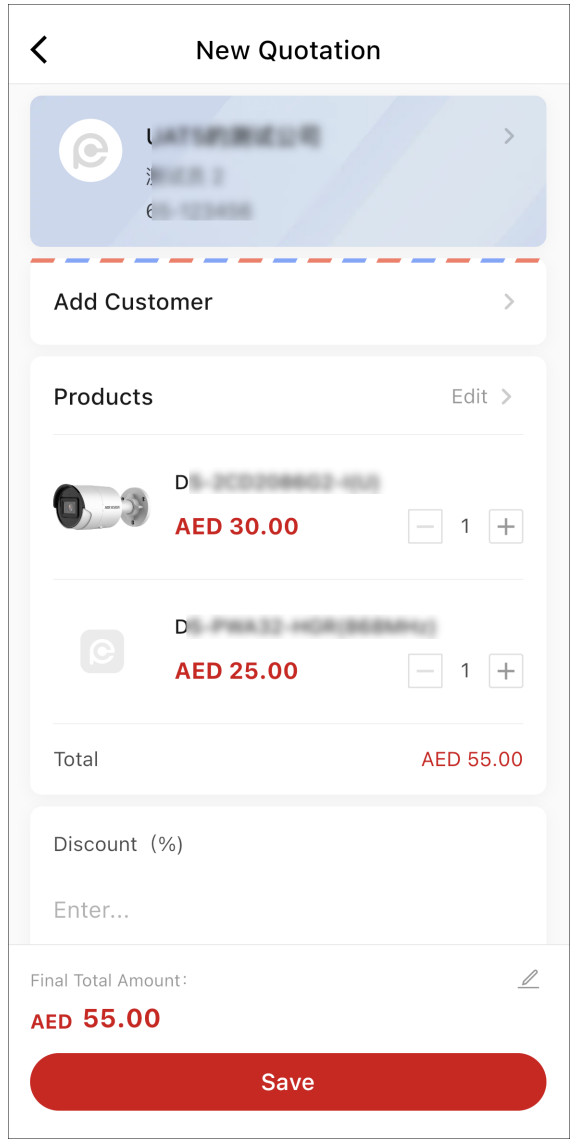


Figure 16-2 Create Quotation

4. **Optional:** Tap the information card at the top to edit the quotation currency, company details, contact person details, and bank details, and then tap **Save**.
5. Tap **Add Customer** to add the customer information and tap **Save**.
6. **Optional:** Edit the products (number and price) to be added to the quotation.
7. **Optional:** Enter the discount, VAT, and notes.
8. **Optional:** Edit the final total amount.
9. Tap **Save**.

Note

You can tap **Edit**/**Share** to edit/share it.

10. **Optional:** Go back to My Quotation page and perform further operations.

Search for Quotations	Enter keyword(s) of customer name in the search box to search for target quotations.
Filter Quotations	Tap to filter quotations by time period.
Edit a Quotation	Tap to edit a quotation.
Copy a Quotation	Tap to add a quotation based on the existing one.
Share a Quotation	Tap and select the file type to share it.

