Hik-Partner Pro Portal

User Manual

Legal Information

About this Manual

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

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

Trademarks

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

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

Disclaimer

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

YOU ACKNOWLEDGE THAT THE NATURE OF 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

Symbol Conventions

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

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

Contents

Chapter 1 Introduction

Hik-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 resolve 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.

Read the following sections to learn more about Hik-Partner Pro.

- ***Clients***
- ***Relationship Among Hik-Partner Pro, Hik-Connect, HikCentral Connect, and HikCentral ReGuard***

Clients

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 service providers logging in to 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.
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 users, manage and configure the devices, submit 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 for site information management permission, etc.
Hik-Connect Portal	Portal for customers to manage their employees' access level and attendance 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.

Client	Description
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.
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.

Relationship Among Hik-Partner Pro, Hik-Connect, HikCentral Connect, and HikCentral ReGuard

As the following diagram shows, Hik-Partner Pro provides certain value-added services related with Hik-Connect, HikCentral Connect, and HikCentral ReGuard. You can activate these value-added services to benefit yourselves or your customers (i.e., customers who use Hik-Connect, HikCentral Connect, and HikCentral ReGuard). For more information about the value-added services and how they relate to Hik-Connect,HikCentral Connect, and HikCentral ReGuard, see ***Value-Added Services*** and its sections.

Note

The availability of the value-added services is determined by your country/region. Some value-added services are not supported in every country/region.

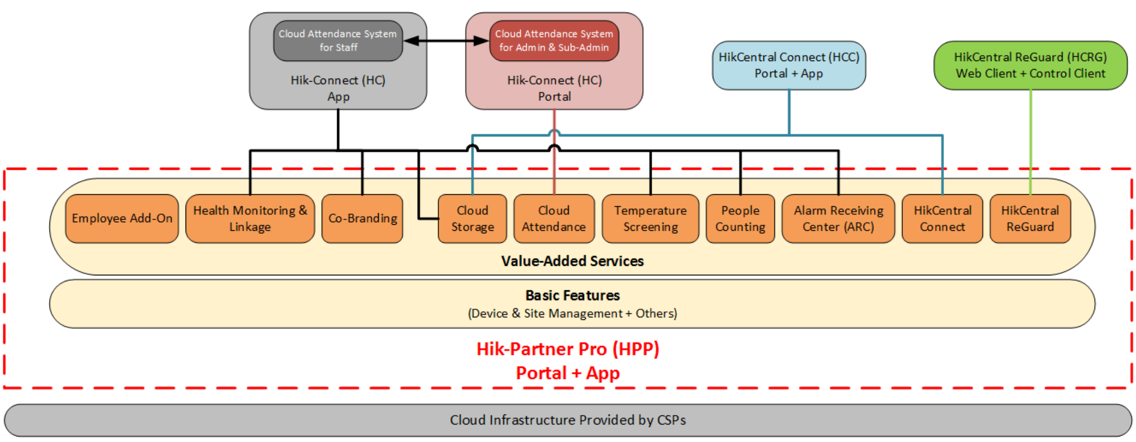


Figure 1-1 Relationship Diagram

1.1 Target Audience

This manual provides the service providers (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 Portal 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, project registration, product selection, Hikvision product order management, solution search, 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.

Note

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. For details, refer to ***Add Your Company to the ARC List*** .

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 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 recommended system for running the Portal.

Operating System

Microsoft Windows® 7/8.1/10 (32-bit and 64-bit).

CPU

Intel® Core™ i5-4460 CPU @3.20GHz 3.20GHz and above.

RAM

8 GB and above (4 GB at least).

Graphics Card

NVIDIA® GeForce GT 730

Web Browser

Versions of Firefox (32-bit and 64-bit), Chrome (32-bit and 64-bit), and Edge (32-bit and 64-bit) released in the latest half year.

1.4 Function Availability for Different Countries/Regions

Hik-Partner Pro offers both free functions and value-added functions that cost certain fees. You can purchase certain services in the Service Market of Hik-Partner Pro 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 some 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 functions only available in certain countries and regions.

Note

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

Service	Function(s) Only Available in Certain Countries and Regions
Health Monitoring Service	Only linkage rule. **Note** Linkage rule is unavailable in the United States and Canada.
Cloud Storage 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.
Purchase Employee Account Add-On	All functions contained in the service.
HCC Services	All functions contained in the services.
HikCentral ReGuard Service	All functions contained in the services.

1.4.2 Regions Only with Support for Free Functions

The following two tables shows the free functions and the countries and regions only with support for the free functions.

Table 1-2 Free Functions

Module	Function(s)
Account Management	• ***Register an Installer Admin Account*** • ***Manage Company Information*** • ***Set Account 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 Detected Online Device*** ◦ ***Add Device by Entering Serial No.*** ◦ ***Add Devices by IP Address or Domain Name*** ◦ ***Batch Add Devices*** • ***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 ◦ ***Control AX PRO and AX HYBIRD PRO*** ◦ ***Configure AX PRO and AX HYBIRD PRO*** ◦ ***Batch Configure AX PRO*** ◦ ***Batch Arm/Disarm AX PRO and AX HYBRID PRO*** • ***Remote Configuration*** • ***Reset Device Password*** • ***Unbind a Device from Its Current Account***
Video	• ***View Live Video*** • ***Play Back Video Footage***
Log	***Search Operation Log***
Tool	***Tools***
Solution	View and Search for Solutions, and Add to Favorites
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 • Receive and View Notices • Register for and Participate in Events
Project	• ***Create a Project*** • ***View Project History***
Order & Promotion	• ***View and Search for Products*** • ***Compare Products***

Module	Function(s)
	• ***Create an Order*** • ***View My Orders***
Incentive	• ***Rewards Store*** • ***Partner Program*** • ***Compensation***

Support	• Tools
	• Tutorial Center
	• Chatbot
	• Case
	  ◦ ***Submit Case***
	  ◦ ***View and Handle Case Records***
	• Feedback
	• Serial Number Inquiry
	Note
	This function is only available for accounts of authenticated channel partners.
	• Contact Us
	• RMA (Return Materials Authorization)
	  ◦ ***Submit RMA Request***
	  ◦ ***View RMA Request***
	Note
	This function is only available for accounts of authenticated channel partners.

Rebate	• ***The Process of Earning Rebates*** • ***The Way to Calculate Rebate Amount*** • ***View Rebate Details*** • ***View Bill of Sale***

Table 1-3 Countries and Regions Only With Support for Free Functions

Continent	Country/Region
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,

Continent	Country/Region
	Mozambique, Namibia, Niger, Nigeria, Rwanda, Senegal, Seychelles, Sierra Leone, Somalia, Tanzania, Togo, Uganda, Zambia, Zimbabwe
Asia	Japan, Taiwan (China)

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 permissions 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.

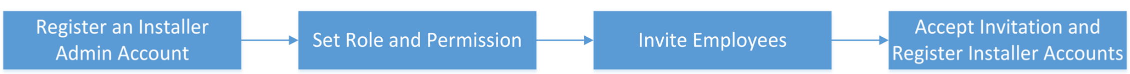


Figure 2-1 Flow Chart of Account Management

- **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*** .

  Note

  After you register Installer Admin account, you need to complete your company information after logging in to the account. For details, see ***Manage Company Information*** .
- **Set Role and Permission:** Before adding an employee to the system, you can create different roles with different permissions for accessing system resources. 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. For details, refer to ***Accept Invitation and Register Installer Account*** .

2.1 Register an Installer Admin Account

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

Steps

Note

You can click **Try Free Demo** on the login page to see what Hik-Partner Pro can do for you, without registering any account. The data displayed in the demo is for demonstration only, and you cannot perform any operations.

1. In the address bar of the web browser, enter ***https://www.hik-partner.com*** .

   Note

   For Russia, you can enter ***https://www.hik-partnerru.com*** in the address bar of the web browser.

   The Login page of Hik-Partner Pro will show.
2. On the Login page, click **Register** to register an account.

   Note

   If your account has been registered, you can click **Login** to log in to Hik-Partner Pro. For details about login, refer to ***Login*** .
3. 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*** .
4. Select whether you are to register by email or by phone number.

   Note

   In some countries/regions, only the registration by email is supported.
5. 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) Click **Register**.

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

6. Click **Authenticate Now** or **Later** to enter either of the following processes.
   - Click **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 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. Click **Confirm** to submit the application and enter Hik-Partner Pro.
   - Click **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. Click **Confirm** to enter Hik-Partner Pro.

Note

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

2.2 Manage Company Information

After registering an Installer Admin account, you can manage and edit your company information.

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.
- You can link your Installer Admin account to a distributor via the Hik-Partner Pro Mobile Client to get support and help from the distributor. For details, see *Hik-Partner Pro Mobile Client User Manual*.
- 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 click **Switch Company** on the top right of the page to switch to another company for using. For details, refer to ***Become a Hik-Partner Pro User After Product Upgrade*** .

1. Go to **Company → Company Information** or **My Hik-Partner → Company Management → Company Information** .

   Note

   If your company is an authenticated channel partner, the partner level will be displayed one the company logo.
2. Enter the name of your company.
3. Enter other information of your company, such as the address, GPS information, postal code, phone number, email, and user type.

   Note

   The country or region cannot be changed once you save the company information after registration.
4. Edit the VAT number of your company, which will be used for qualification verification.
5. **Optional:** If you want to upload the company logo, click **+** to upload the picture of your company logo, or click **Edit** to re-upload a picture to update the logo.

Note

- The picture should be in JPG, JPEG, or PNG format.
- Recommended picture size: Height = 200 px, 200 px ≤ Width ≤ 600 px.
- You are not allowed to enable the Co-Branding function if you have not set the company logo. For details about Co-Branding, see ***Co-Branding*** .

6. **Optional:** Enter the website of your company.
7. **Optional:** Enter or edit the description information, which will be displayed on Hik-Connect Mobile Client.
8. Click **Save** to save the configurations.

Note

You can check the percentage of completed information after saving.

2.3 Authenticate 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 the selected country or region when registering your account.

By Entering Authentication Code

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

1. Go to **My Hik-Partner → Company Management → Company Information** , and click **Authenticate Now**.
2. (Optional) If you have no authentication code, click **Get Authentication Code**, send the application email with the predefined content template, including your email address (the one which is used when registering your Installer Admin account) and company information, such as company ID, company name, and phone number, to Hikvision or the distributor, and apply for one authentication code.

   Note

   - You can click to edit the information in the template. The edited contents will be updated in the company information.
   - 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. After you get the authentication code, enter the authentication code on the account authentication page and click **OK** to authenticate your account.

-
-
-

By Submitting Online Application

For this way, you need to 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 **My Hik-Partner → Company Management → Company Information** page, and click **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. Click + to upload a picture (e.g., business license and business card) as evidence.
4. Enter 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).
5. Click **Authenticate Now**.
   The application information will be sent.

   Note

   After your application is approved, you will be notified via push notification and email.

2.4 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.

2.4.1 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 **Company Management → Company Information** .

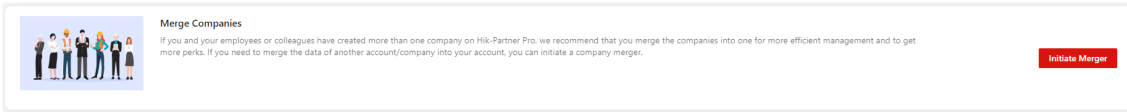


Figure 2-2 Entry on the Company Information Page

- 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.

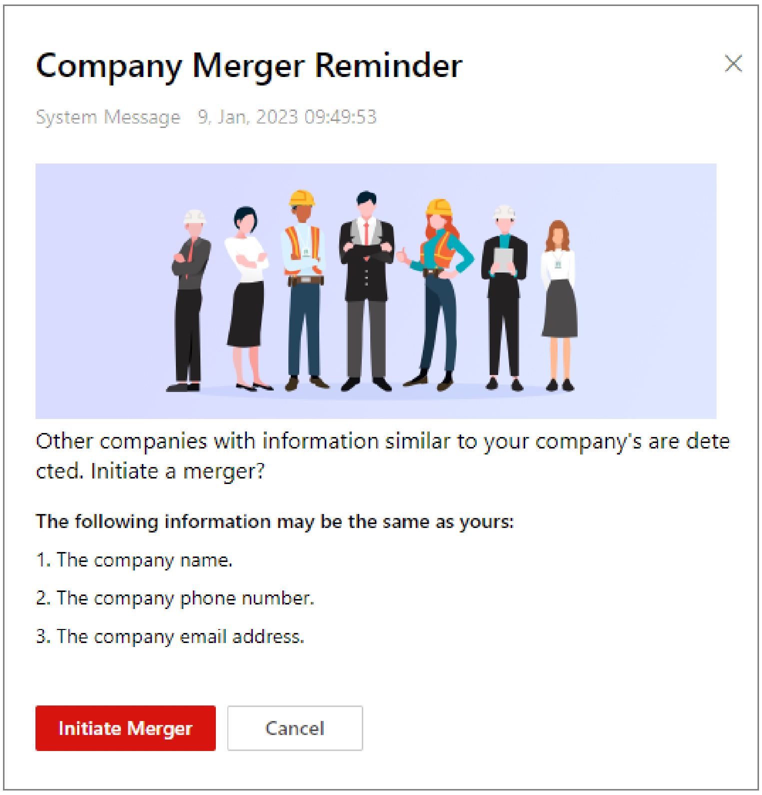


Figure 2-3 Entry in System Messages of Notification Center (Company Merger Reminder)

2. Click **Initiate Merger** to enter the Merge Companies page.

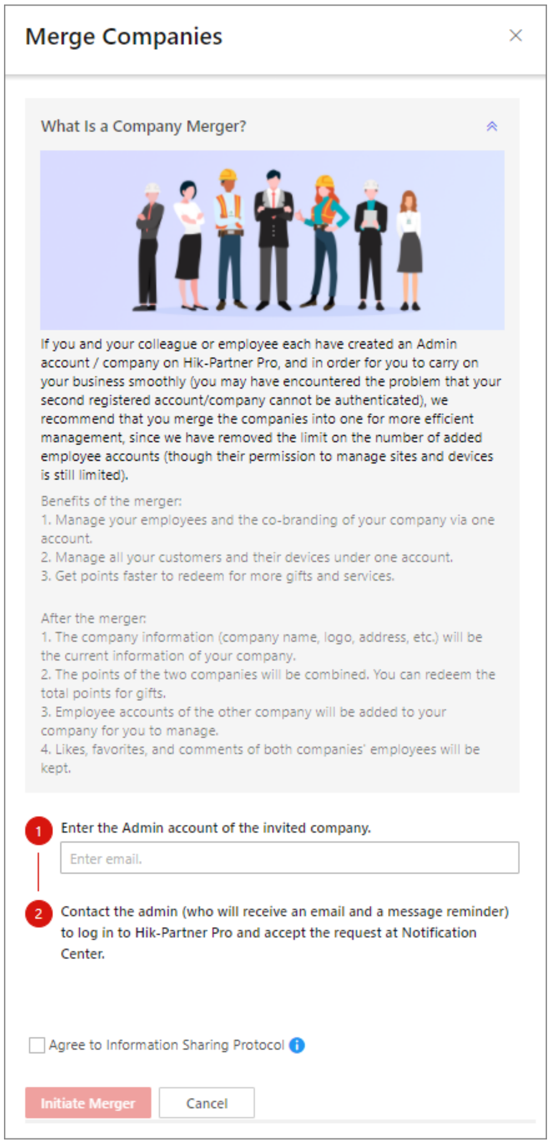


Figure 2-4 Merge Companies

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. Click **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**.

2.4.2 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 click the company merger notification to view the details.

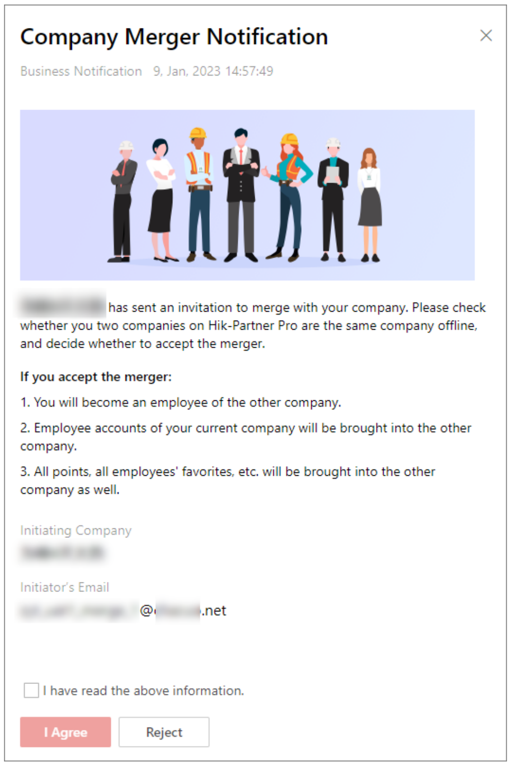


Figure 2-5 Company Merger Notification (Invitation)

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 click **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, click **Reject**.

2.5 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 or 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. Click **Company → Role and Permission** or **My Hik-Partner → Company Management → Role and Permission** to display all the roles.
2. Add a role.
   1) Click **Add Role** to open the Add Role panel.
   2) 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 Employee and Role and Permission page, adding and deleting accounts and roles. Employee and 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.

3) **Optional:** Enter remarks of the role in the **Description** field.
4) Click **OK**.

3. **Optional:** Check added roles and click **Delete** to delete the selected role(s).

Note

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

2.6 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 or 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. Open the Add Employee pane.
   - Click **Company → Employee → Add Employee** or **My Hik-Partner → Company Management → Employee → Add Employee** .
   - On the Home page, click **Company → Role and Permission** or **My Hik-Partner → Company Management → Role and Permission** , and then click **Add Employee** in the Operation column.
2. Enter the email of the to-be-invited employee.
3. Select a role for the employee.

   Note

   You can also create a new role. For details, refer to ***Manage Role and Permission*** .

   The permissions of the role will be displayed.
4. Click **Add**.

   The invited employee will receive an email delivering a link in the entered email box. The employee needs to click 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.

5. **Optional:** Perform the following operations after adding employees.

Enable/ Disable Employee

Click / in the Operation column to enable or disable the employee account.

Note

- Once disabled, the employee cannot log in to the platform 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 ***Purchase Employee Account Add-On*** .

To remove the account limits, you can 1) click in the Operation column or 2) hover your mouse cursor over in the Status column and click **Remove Limit**.

Delete Employees

Check one or more employees and click **Delete** to delete the selected employee(s) if needed.

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

Click an employee to open the Employee Details pane to view the employee's contact number, email address, role permissions, and so on.

Edit Role Assigned to Employee	Click an employee to open the Employee Details pane and click in the Role field to enter the Edit Role pane. Then you can click **Add** 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	Click an employee to open the Employee Details pane or click the information in the Managed column to view the list of all sites managed by the employee. You can click a site to view the site details. **Note** The above operation is supported only when the employee has site(s) to be managed.

2.7 Accept Invitation and Register Installer Account

The Installer Admin, and Installer whose role contains permission of **Manage Account and Role** can invite other employees to register Installer accounts. The employees can accept the invitation and register Installer accounts to manage sites and devices.

Before You Start

Installer Admin and Installer whose role contains permission of **Manage Account and Role** should first invite the employee first. For details, refer to ***Invite Employee*** .

Steps

1. After inviting the employee, the employee will receive an email from Hik-Partner Pro.
2. Click the button or the link in the email.
3. Click **Register** to open the Create Account page.

   Note

   If you have already registered a OneHikID account using your email address, you can log in with the account to join the company directly.
4. Set the type, name, verification code (for verifying the email address), 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.

5. Check **By clicking Register, I agree to Hikvision OneHikID's Privacy Policy.**
6. Click **Register**.

Result

You can log into Hik-Partner Pro with this account and perform other operations such as site management and configuration.

2.8 Set Account Information

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

Click the name at the upper-right corner and select **Account Settings** or click **My Hik-Partner → Account Information → My Profile** .

Set Basic Information

Set the basic information of the current account, including the name of the Installer, email address, phone number, etc.

Note

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

Click to set the profile of the current account.

Note

You can view your HIK ID on this page, but you cannot edit it.

Manage My QR Code

Hover over 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 click **Add Your Company Logo to the QR Code** to upload your company logo.
Click to download the QR code.

Change Password

Click to 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.

Change Account's Bound Email

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

1. In the Basic Information page of the account settings, click .

   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.

2. Enter a new email address in the **New Email** field.
3. Click **Verify**.
   In the new email address, you will receive an email with a verification code.
4. Enter the received verification code in the **Verification Code** field.
5. Enter the password of the current account.
6. Click **Save**.

Delete Installer Admin Account

For Installer Admin, if the account is no longer used, you can delete it in the Basic Information page of the account settings.

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. In the Basic Information page of the account settings, click **Delete Installer Admin Account**.
2. Enter the password of your Installer Admin account, and click **Next**.
3. Click **Delete Installer Admin Account** to confirm deleting.

2.9 View Employee Efficiency Statistics

You can view the efficiency statistics of all employees, including the latest active time, added sites, added devices, handed-over sites, handed-over devices, and handled device exceptions. You can also perform operations such as exporting the efficiency statistics.

Note

This is supported only if you have permissions to manage the employees.

You can enter the Employee Efficiency Statistics page via the following methods:

- Go to **Company → Employee Efficiency Statistics** or **My Hik-Partner → Company Management → Employee Efficiency Statistics** .
- Click **View All** in the Employee Efficiency Overview section.

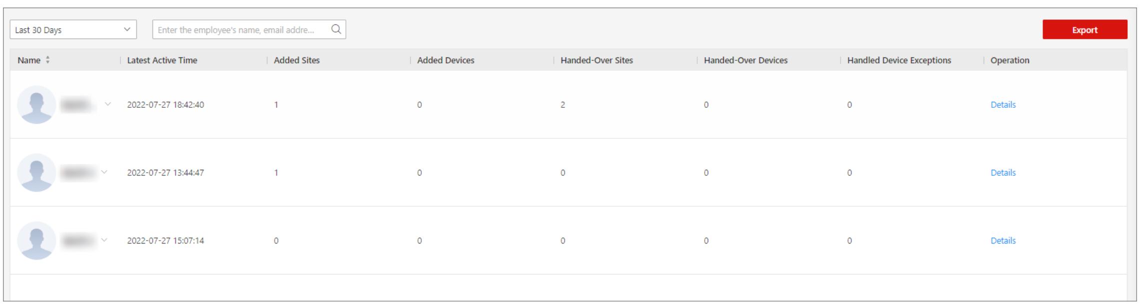


Figure 2-6 Employee Efficiency Statistics Page

You can perform the following operations if needed.

Table 2-1 Supported Operations

Operation	Description
View Operation Logs of an Employee **Note** This is not supported when your company is an authenticated channel partner.	Click **Details** in the Operation column to switch to the Operation Log page to view the operation logs of the corresponding employee.
Filter Statistics	Click ⌄ to filter the efficiency statistics by time period (i.e., today, yesterday, this week, last 7 days, last 30 days, or custom time period).

Operation	Description
Search for Statistics	Enter the employee's name, email address, or phone number in the search box to search for statistics.
Export Statistics	Click **Export** to export statistics in XLSX or CSV format.

2.10 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 **My Hik-Partner → Company Management → Agreement Management** to view your agreements.

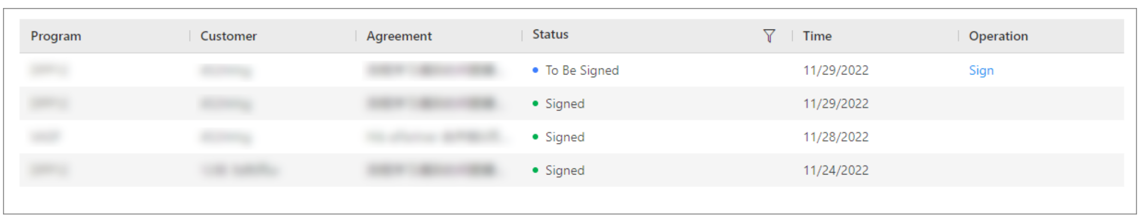


Figure 2-7 Agreement Management

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.

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

Click to filter the agreements by the signing status.

2.11 Manage My Shipping Address

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

Note

The function is only supported in certain countries and regions.

Go to **My Hik-Partner → Company Management → My Address** .

You can view and manage all your added shipping addresses if any, or you can add new shipping addresses if you haven't added any shipping address. Perform the following operations if needed.

Table 2-2 Supported Operations

Operation	Description
Add New Shipping Address	Click **New Address**, fill in all required information (contact person, country/state, address, postal code, etc.), check **Set this address as default** if you are to set it as the default shipping address, and click **Save**.
Edit Shipping Address	Click to edit the corresponding shipping address.
Delete Shipping Address	Click to delete the corresponding shipping address.
Set Default Shipping Address	Click **Set as Default** to set the corresponding shipping address as default.

2.12 View My Partner Network

You can view and export the basic information about your partners.

Note

This function is only available to some users in some countries/regions. For details, please contact Hikvision.

Go to **My Hik-Partner → Company Management → My Partner Network** to enter the My Partner Network page.

You will be able to view the partner No., partner name, partner type, partner level, VAT No., address, website, etc.

You can also click **Export** to export the information.

2.13 View Dashboard

You can have an overview of the status of all your projects and orders, and view the number of your DPPs/distributors.

Note

This function is only available to some users in some countries/regions. For details, please contact Hikvision.

Go to **My Hik-Partner → Dashboard** to enter the Dashboard page.

You can view the number of your DPPs/distributors. Click › to switch to My Partner Network to view details about your DPPs/distributors. Refer to ***View My Partner Network*** .

You can view the status of your projects, including draft, waiting for supporter, processing, approved, more information required, ineligible, closed won, closed lost, and closed canceled. Click **View Details** to switch to Project History for more details and operations. Refer to ***Project*** .

You can view the status of your orders, including in review, undelivered, fully delivered, and back order. Click **View Details** to switch to My Order for more details and operations. Refer to ***View My Orders*** .

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 an Installer Admin Account*** or ***Accept Invitation and Register Installer Account*** for details about registration.

Steps

1. In the address bar of the web browser, enter ***https://www.hik-partner.com*** .

   Note

   For Russia, you can enter ***https://www.hik-partnerru.com*** in the address bar of the web browser.

   The login page of Hik-Partner Pro will show.
2. Select a country or region where the account locates and a language from the drop-down lists at the top of the page.
3. Click **Log In by OneHikID (Hik-ePartner) Account / Log In by OneHikID Account** or **Hik-ProConnect** on the login page.

   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 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) Click **Forgot Password** to enter the resetting password page.
   2) Click **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) Click **OK**.

By default, you will be required to log in by the new password.

6. Click **Sign In** or **Login**.

Note

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 click **Switch Company** on the Company Information 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.

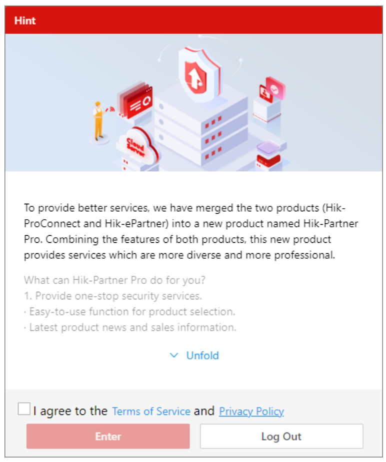


Figure 4-1 Product Upgrade

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 click **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 Click 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 click **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 click **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 click **Switch Company** on the Company Information page to switch to another company.

Chapter 5 Hik-Partner Pro Portal Overview

Hik-Partner Pro Portal is a B/S portal of Hik-Partner Pro platform. The service providers (e.g., installation company) can register an Installer Admin account on Hik-Partner Pro, and then the Installer Admin can invite employees to register Installer accounts. Each company has only one Installer Admin but can have multiple Installers.

After registration, the Installer Admin and Installers can log into the Hik-Partner Pro via the web browser and the Home page of the Hik-Partner Pro Portal will show.

5.1 Main Modules

The Hik-Partner Pro Portal is divided into several main modules. You can access these modules via tabs at the top.

Note

The available main modules for authenticated channel partners are different from that for users who are not the authenticated channel partners.

Table 5-1 Main Modules of Hik-Partner Pro Portal

Module	Description
Home	The layouts of Home page for authenticated channel partners are different from that for users who are not the authenticated channel partners. **Home Page (Except for Authenticated Channel Partners)** On the Home page, you can check the number of added sites or devices, view the wizard about how to add and manage devices, view the number of abnormal devices and total devices, check the number of not handled and to be followed up exceptions, check the efficiency statistics of all employees, view some banners showing the key features, functions, and important information, have an overview of your services, manage services, set more value-added services for devices, and view video tutorials and documents to learn more about the platform and the proper ways of using the platform. If you have any issues or suggestions generated when using Hik-Partner Pro, you can report them via Case or Feedback. You can also use some online tools to improve your work efficiency and quickly access some pages such as the site adding page, device adding page, and health monitoring page. Refer to ***Home Page*** for details.

Module	Description
	Home Page (For Authenticated Channel Partners) On the Home page, you can view the banners showing the key features, functions, and important information of Hik-Partner Pro, check the number of added sites and devices, have an overview and get the introductions of the projects, value-added services, order & promotion, or explore modules, and quickly access some pages such as the site adding page, device adding page, and products page. Refer to ***Home Page*** for details. **Note** If the region/country where you locate supports the lottery draw and the Hik-Partner Pro team has initiated a lottery, you will see an entry on the banner for uploading a sales receipt to get a ticket and participate in the lottery.
Site & Device	The module provides entries for main functions including the dashboard overview, the management and batch configuration of devices / customer sites / HikCentral Connect systems, health monitoring, and purchasing/managing services. Refer to ***Site & Device Module*** for details. **Note** • The dashboard overview is only available to authenticated channel partners who have the permission to access the Site & Device module. • The Site & Device module is not available to all authenticated channel partners.
Solution	The module provides all-around solutions for varied needs from Hik-Partner Pro users. These solutions are designed to provide comprehensive and end-to-end capabilities for diverse service providers, which can empower them to explore new business opportunities, optimize operations, and get a winning edge in the competition. You can perform the following operations in the Solution module. • View solutions listed for a variety of verticals. • Filter solutions of a vertical by tags of its sub verticals. • Display solutions in groups by different types, namely solutions by industry, by scenario, and by function. • Search for solutions keyword. • Sort the solutions in ascending/descending order by release date and/or number of views.

Module	Description
	• Add a solution to Favorites and view only those added to Favorites by checking My Favorites. • View the solution description and BOQ (Bill Of Quotation), and download the related documents. • Like solutions and share solutions you interested by sending the links to other persons. **Note** This function is only available to some users in some countries/regions. For details, please contact Hikvision.
Explore	The module collects the latest product information, marketing materials, and activity notifications of Hikvision. Service providers can easily keep up with the trend here, without having to find the latest feeds on other websites, and forward the interested materials to their customers. **Feeds** You can get and quickly share the latest information about Hikvision products and case studies with your customers. The product feeds are categorized by product type for easy search. **Event** You can view the upcoming and past events, such as training, seminar, exhibition, roadshow, lucky draws, lotteries, and promotions, initiated by the Hik-Partner Pro team and participate in the upcoming events. **Note** The lottery is only available to some users in some countries/regions. If you want to participate in a lottery, you can upload the sales receipt to get a ticket and wait for the draw. **How To** If you have troubles with product installation or software setup, you can view both documents and videos in How To for guiding you through solving all kinds of problems you encounter when using Hikvision products and services. The how-to documents and videos are categorized by product type for easy search. **Video** You can view product videos, case study videos, and how-to videos for getting the information you want when using Hikvision products

Module	Description
	and services. The product videos and how-to videos are categorized by product type for easy search. **Notice** You can view notices announced by the Hik-Partner Pro team to know some important information about the product, such as updates in the current version. The Notice window will automatically pop up once you logged in to the Hik-Partner Pro Portal. If you check **Do Not Show Again** before closing the window, it will not pop up for your next time login. **Note** • For Feeds and How To, you can like or comment them, and add them to the Favorites. You can also go to **My Hik-Partner → Account Information → My Comments / My Favorites** to view your historical comments or favorites. • This function is only available in certain countries/regions. For details, please contact Hikvision.
Project	This module provides the support (e.g., trainings, consultations, and learning materials) and pricing for users who have new projects to help them better complete their projects. For how to register a project, refer to ***Project*** . **Note** This function is only available to some users in some countries/regions. For details, please contact Hikvision.
Order & Promotion	This module supports viewing the information about hot products or a certain type of products. You can search for or filter the products, download the related documents, share the product information with others, compare parameters/specifications of products to learn about their similarities and differences, and submit orders to purchase products. For details, refer to ***Order & Promotion*** . **Note** This function is only available to some authenticated channel partners. For details, please contact Hikvision.
Incentive	**Rewards Store**

Module	Description
	It is a reward point system to reward your trust and support. You can complete specific tasks to get the reward points redeemable for lots of gifts. For details, refer to ***Rewards Store*** . **Note** This function is only available in certain countries/regions. For some countries/regions, the function is available only when you have your company authenticated. **Compensation** For distributors who keep a supply of products from Hikvision at a fixed price in advance, but later sell products at a lower price due to getting project support, you may apply for compensation online. After a compensation application is approved, the compensation amount may be issued to your e-wallet, or you may be compensated by credit notes against receivables or free items. **Note** This function is only available to some authenticated channel partners in some regions/countries. **Partner Program** Resellers can apply for partner programs on Hik-Partner Pro with the contract agreements signed both offline and online. Resellers can also view their program history and the certificates that they get after their application is approved and the contract agreement is signed. **Note** This function is only available to some users in some regions/ countries.
Support	This module is available to you in many helpful formats. Wherever you are, whenever you need it, we have resources ready. Whether you are installing hardware or have questions about our services, our online support, documentation, and knowledgeable representatives are only a mouse-click away. **Tools** You can use some online tools to improve your work efficiency. **Tutorial Center**

<table>
<tr><th>Module</th><th>Description</th></tr>
<tr><td></td><td>You can view video tutorials and documents in the Tutorial Center to learn more product information and the proper ways to use our products.
Chatbot
If you have any question about Hik-Partner Pro, you can try finding the answer here.
Case
If you have any issues when using Hik-Partner Pro, you can get professional services from our technical support via Case. For details, refer to Case .
Feedback
If you encounter any problems while using the product or if you have any functional needs or suggestions, please feel free to contact us via Feedback.
After opening the feedback window, you can select a type for your feedback and then enter your suggestions in the pop-up window and attach a picture if necessary. Enter an email address. After we receive your feedback, we will send an email to this address if we get a conclusion. Click Submit to submit your feedback to us.
Contact Us
You can get the contacts (i.e., address, phone, and email) of our headquarter and the local office, and the email address of your sales representative.
RMA (Return Material Authorization) / Serial Number Inquiry
The RMA is an arrangement in which you can ship an item back for an exchange or repair due to a product defect or malfunction. For the detailed process, refer to Return Materials Authorization .
After you submit RMA requests, you can search for requests by the device serial No. to view the request status.
Note
This function is only available to some users in some countries/ regions. For details, please contact Hikvision.</td></tr>
<tr><td>My Hik-Partner</td><td>This module deals with all the management and administration aspects of a single installation company.
Company Management</td></tr>
</table>

Module	Description
	Company Information View and manage the company information. See ***Manage Company Information*** for details. **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 of **Manage Account and Role** can also invite other employees to be Installers by registering Installer accounts. See ***Invite Employee*** for details. **Employee Efficiency Statistics** Shows the efficiency statistics of all employees, including the latest active time, added sites, added devices, handed-over sites, handed-over devices, and handled device exceptions. See ***View Employee Efficiency Statistics*** for details. **Manage My Agreements** Distributors can manage and sign contract agreements of partner programs with resellers and Hikvision on Hik-Partner Pro. **Note** This function is only available to some users in some regions/ countries. **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. See ***Manage Role and Permission*** for details. **Operation Log** View the operation logs of your accounts and sites in the current company. See ***Search Operation Log*** for details. **Note** This function is not available to authenticated channel partners. **Co-Branding**

Module	Description
	Enable to display the company logo on the Hik-Connect Mobile Client for brand promotion to the end users. For details about how to get the co-branding service for free and enable the service, refer to ***Co-Branding*** . **My Address** Manage your shipping addresses for receiving items (e.g., gifts, repaired devices). See ***Manage My Shipping Address*** for details. **Note** This function is only available in certain countries/regions. For details, please contact Hikvision. **Verify Gifts** Distributors verify the gifts redeemed offline and export the records. **Note** This function is only available in certain countries/regions. For some countries/regions, the function is available only when you have your company authenticated. **My Partner Network** You can view and export basic information about your partner. For details, refer to ***View My Partner Network*** . **Note** This function is only available to some authenticated channel partners in some countries/regions. For details, please contact Hikvision. **Account Information** **My Profile** Edit your account information, including profile photo, name, email address, password, and phone number. Refer to ***Set Account Information*** for details. **My Favorites / My Comments** View your historical comments to news and how-to articles, and view the news, how-to articles, and solutions that are added to your Favorites. **Dashboard**

Module	Description
	Have an overview of the status of all your projects and orders, and view the number of your DPPs/distributors. For details, refer to ***View Dashboard*** . **Note** This function is only available to some users in some countries/ regions. For details, please contact Hikvision. **Order** View your order details, invoices, balances of your e-wallet, financial reports, stock lists, price lists, and so on. For details, refer to ***View My Orders*** . **Note** This function is only available to authenticated channel partners. For details, please contact Hikvision. **Rebate** For authenticated channel partners to view the rebates they earn from successfully promoting services of Hik-Partner Pro to their customers. See ***Rebate*** for details. **Note** This function is only available to some authenticated channel partners in some countries/regions. For details, please contact Hikvision.

5.1.1 Home Page

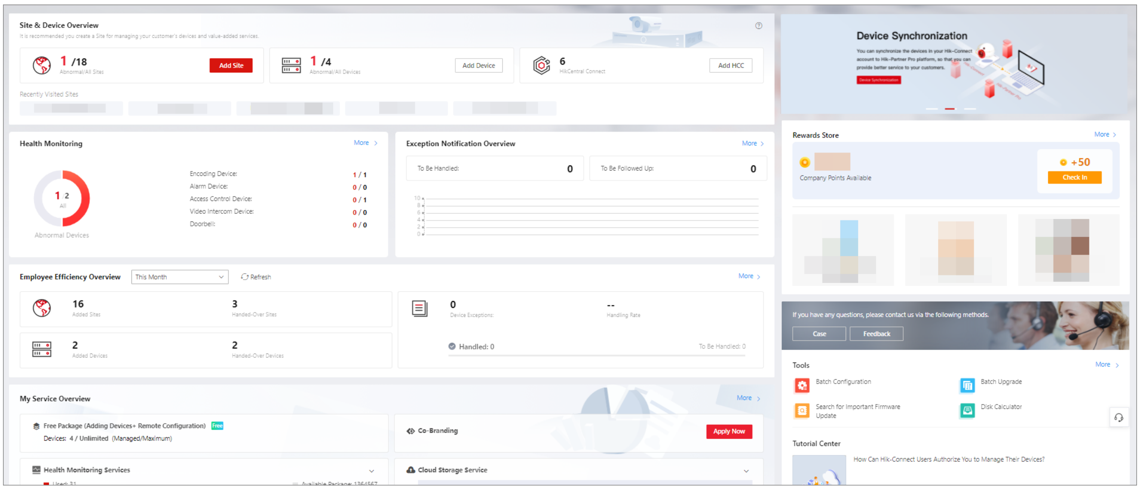


Figure 5-1 Home Page (Except for Authenticated Channel Partners)

Table 5-2 Home Page Description (Except for Authenticated Channel Partners)

Name	Introduction
Site, Device, and HikCentral Connect Overview	You can view the total number of sites/devices, the number of abnormal sites/devices, and the total number of HikCentral Connect systems managed by you. Click **Add Site** to add a new site. For details, refer to ***Add New Site*** . Click **Add Device** to add a device. You can also click ? in the top right corner of the Site & Device Overview pane to open the wizard about adding devices, handing over devices to customers, and remote configuration, and click **Add Device Now** to start adding a device. For details, refer to ***Add Device*** . Click **Add HikCentral Connect** to add a HikCentral Connect system. For details, refer to ***Create HCC Systems*** . The recently visited sites will be displayed on the Site & Device Overview pane and you can click a site name to enter the site details page.

Name	Introduction
	Note • If there are no sites, devices, and HikCentral Connect systems added, the wizard will automatically be displayed on this pane. • A prompt will appear at the top of this pane to show the number of notifications to be handled, and you can click **Handle Now** to enter the Notification Center module to handle these notifications. • The HikCentral Connect service is only available in certain countries or regions.
Health Monitoring Overview	You can view the number of abnormal devices and total devices, including devices overall and each device type respectively. **Note** You can click **More** to enter the Health Status page to check the details about device status. For detailed instructions about Health Status, refer to ***View Status of Devices in All Sites*** and ***View Status of Devices in a Specific Site*** .
Exception Notification Overview	You can view the number of not handled and to be followed up exceptions and numbers of top 5 types of the not handled exceptions. You can click a number on a chart to enter the Exception Center page and the exceptions will be filtered correspondingly. For example, if you click the number on the Not Handled chart, the exceptions will be filtered by the status of Not Handled on the Exception Center page. **Note** • To receive exception notifications, you need to configure the recipient when setting the exception rule. For details, refer to ***Add Exception Rule*** . • The number of exceptions you view here may not be the same as that in Exception Center. You can click **More** to enter the Exception Center page to check the received exceptions. For detailed instructions about Exception Center, refer to ***Exception Center*** .
Employee Efficiency Overview	You can view the efficiency statistics of all employees, including the numbers of added sites and handed-over sites, the numbers of added devices and handed-over devices, the number of device exceptions, the exception handing rate, and the numbers of handled and to be handled exceptions.

<table>
<tr><th>Name</th><th>Introduction</th></tr>
<tr><td></td><td>
You can also filter statistics data by this month, this week, and today, or click Refresh to display the latest statistics data.
If you want to view more data, click More to enter the Employee Efficiency Statistics page. For details, refer to <u>View Employee Efficiency Statistics</u> .
Note
This is only supported only if you have permissions to manage the employees.
</td></tr>
<tr><td>My Service Overview</td><td>
You can have an overview of your services and manage the services.
Free Package (Adding Devices + Remote Configuration)

Display number of managed devices and devices that can be added.
Display the entrances for adding devices and synchronizing devices from Hik-Connect.

Co-Branding
Display the company logo when co-branding is enabled and the entrance for enabling the co-branding.
Health Monitoring Service

Display the numbers of used and available service packages and the entrance for activating the service.
Display the number of devices with expiring or expired service and the entrance for details, if there are devices with the service expiring within 30 days.
Display the numbers of device exception notifications and scheduled reports if there are devices using the health monitoring service.
Displaying the entrance for renewing/expanding.
Display the entrance for getting the free health monitoring packages (if any).
Display the entrances for enabling the device exception notifications and configuring the scheduled reports.

Cloud Storage Service
</td></tr>
</table>

<table>
<tr><th>Name</th><th>Introduction</th></tr>
<tr><td></td><td>

Display numbers of used and available service packages.
Display the number of devices with expiring or expired service and the entrance for details, if there are devices with the service expiring within 30 days.
Display the entrances for renewing/expanding and activating the service.

Employee Account Add-On

Display used and available employee accounts.
Display the expiry time when the service is expiring within 30 days and displaying the entrance for renewing the service
Display the entrances for inviting employees and managing employees.

Cloud Attendance Service

Display numbers of used and available service packages.
Display numbers of expiring and expired cloud attendance systems and the entrance for details.
Display the entrance for adding cloud attendance systems.

Alarm Receiving Center (ARC) Service

Display the status of your application for joining as ARC if your company has applied, and displaying the entrance for applying if your company has not applied or the application failed.
Display the number of companies added to the local ARC list and the name of last joined company.
Display the numbers of managed devices.
Display the entrance for viewing the local ARC list and searching for ARCs.
Display the entrance for configuring the ARC service.

Note
This section will be displayed only if your country/region supports the ARC service, and your company type is ARC or there are companies added to the local ARC list.
Note

This feature is supported only if you have the permission to manage service packages and orders.
Only the services for which you have available service packages will be displayed on My Service Overview.

</td></tr>
</table>

Name	Introduction
More Value-Added Services	You can set related service (such as temperature screening and people counting) for devices after adding them to sites. Click **Set** in the upper right corner, and select a site in the list to enter the site details page.
Help	View online documents including the Device Compatibility List, User Manual, Datasheet, and What's New.
Banner	There are some banners, showing the key features, functions, and important information of Hik-Partner Pro. **Note** If the region/country where you locate supports the lottery draw and the Hik-Partner Pro team has initiated a lottery, you will see an entry on the banner for uploading a sales receipt to get a ticket and participate in the lottery.
Rewards Store	You can view the total available points, check in to earn points, and view available gifts for redeeming. Click **More** to enter the Rewards Store page and perform more operations. For details, refer to ***Rewards Store*** .
Case/Feedback	The Case is a center for you to report any issues generated when using Hik-Partner Pro. Our technical support will receive your issues and help you resolve them as soon as possible. The Feedback is a center for submitting your own suggestions or suggestions from your customers.
Tools	You can use some online tools to improve your work efficiency. Click **More** to view all the provided tools.
Tutorial Center / How To	Under the **Tutorial Center** tab, you can view three latest video tutorials to learn more about Hik-Partner Pro and the proper ways of using the platform. Under the **How To** tab, you can view three latest how-to documents or videos for guiding you through solving all kinds of problems you encounter when using Hikvision products and services. Click **More** to view all video tutorials and how-to documents/videos on the corresponding pages.

Name	Introduction
	Note The **How To** tab will not be displayed if there is no related information.
Event/Feeds	Under the **Event** tab, you can view three latest upcoming and past events, such as training, seminar, exhibition, roadshow, lucky draws, lotteries, and promotions, initiated by the Hik-Partner Pro team. Under the **Feeds** tab, you can view three items of latest information about Hikvision products and case studies. Click **More** to view all events and feeds on the corresponding pages. **Note** These two tab will not be displayed if there is no related information.

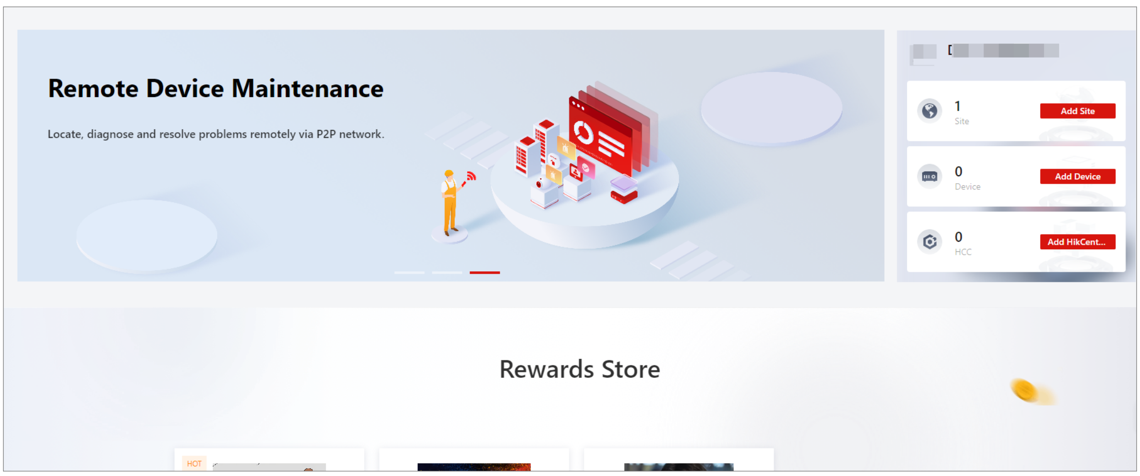


Figure 5-2 Home Page (for Authenticated Channel Partners)

Table 5-3 Home Page Description (for Authenticated Channel Partners)

Name	Introduction
Banner	There are some banners, showing the key features, functions, and important information of Hik-Partner Pro. **Note** If the region/country where you locate supports the lottery draw and the Hik-Partner Pro team has initiated a lottery, you will see an entry

Name	Introduction
	on the banner for uploading a sales receipt to get a ticket and participate in the lottery.
Company, Site, Device, and HikCentral Connect Overview	You can view your company logo and name, the partner level, the total number of sites, devices, and HikCentral Connect systems managed by you. Click **Add Site** to add a new site. For details, refer to ***Add New Site*** . Click **Add Device** to add a device. For details, refer to ***Add Device*** . Click **Add HikCentral Connect** to add a HikCentral Connect system. For details, refer to ***Create HCC Systems*** . **Note** • The HikCentral Connect service is only available in certain countries or regions. • If the Site & Device module tab is not displayed in the top navigation menu, the entrances for adding sites / devices / HikCentral Connect systems will also not be displayed.
Project Overview	Click **Project Registration** to view the features about the Project module. You can click **Register a New Projects** to go to the Project page and create a project. For details, refer to ***Create a Project*** **Note** This function is only available to some authenticated channel partners in some countries/regions. For details, please contact Hikvision.
Rewards Store Overview	You can view the available gifts for redeeming, and redeem your reward points for gifts. Click **More** to enter the Rewards Store page and perform more operations. For details, refer to ***Rewards Store*** .
Trending Products Overview	You can click / view the information about the hot products. Click **More** to enter the Order & Promotion module and perform more operations, such as submitting an order, comparing products, and so on. For details, refer to ***Order & Promotion*** . **Note** This function is only available to some authenticated channel partners. For details, please contact Hikvision.

Name	Introduction
Explore Overview	You can view the hot news and how-to articles to keep up yourself with the trend. Click **More** to enter the news or how-to details page.
Solution Overview	You can switch to view some basic information about hot solutions. Click **More** to enter the Solution page to search for and view more solutions. **Note** This function is only available to some authenticated channel partners in some countries/regions. For details, please contact Hikvision.

5.1.2 Site & Device Module

The Site & Device module is divided into several sections. You can access these sections via the navigation pane on the left.

Note

- The Site & Device module is not available to all authenticated channel partners.
- You can click to pin or unpin the navigation pane on the left of the page.

Table 5-4 Site & Device Module

Name	Introduction
Dashboard	The dashboard overview is only available to authenticated channel partners who have the permission to access the Site & Device module. You can check the total number of sites / devices / HikCentral Connect systems, view the wizard about how to add and manage devices, view the number of abnormal devices and total devices, check the number of not handled and to be followed up exceptions, check the efficiency statistics of all employees, have an overview of your services, manage services, set more value-added services for devices, and view online documents to learn more about the platform and the proper ways of using the platform. The layout of the dashboard for authenticated channel partners is similar to that of the Home page for users who are not authenticated channel partners. For details, refer to ***Table 5-2*** .
Site & HCC	**Customer Site**

Name	Introduction
	A site represents a physical location where devices are installed and through which the Installer Admin/Installer can manage the devices. **Site Map** If sites are configured with the GPS information, they can be displayed on the map for viewing the site details, such as the site name, site owner, site location, and number of online/offline/abnormal devices. **HikCentral Connect** A system created by installers via the Hik-Partner Pro Portal for providing a Video Security as a Service (VSaaS) solution for enterprise users. For details, refer to the user manuals of HikCentral Connect. **Note** HikCentral Connect is only available in the certain countries or regions.
Install & Configure	• Batch configure online encoding devices on the same LAN with the Portal via custom templates. See ***Batch Configure Devices on LAN*** for details. • Remotely batch configure AX PRO devices via custom templates. See ***Batch Configure AX PRO*** . • Batch arm/disarm AX PRO devices on different sites. See ***Batch Arm/Disarm AX PRO and AX HYBRID PRO*** . • Batch upgrade devices including security control panels, encoding devices, etc., on the same LAN. See ***Batch Upgrade Devices on LAN*** .
Health Monitoring	**Health Status** The Installer can view the devices overall, normal, and abnormal status, locate the abnormal devices, and perform troubleshooting quickly. **Exception Center** After setting the exception rules, when an exception occurs on the device, the device will push a notification to the Portal and you can view all the received notifications of exception in the Exception Center. **Scheduled Report** The platform can send the health check reports of encoding devices and AX PRO devices to target recipients regularly.

Name	Introduction
	Maintenance Quotation You can create quotation for providing the device maintenance service for your customers. Thus, you can standardize the service process, improve customer satisfaction, and expand your business.
Service	• **Service Market:** Hik-Partner Pro provides value-added services and you can purchase these service packages or renew them. You can also view details of the free package. • **My Service:** View all services you purchased and the details, such as free package and cloud storage service package. • **Order:** View the order list and order details.
Add Device	An entrance for quickly accessing the Add Device page. For details about adding devices, refer to ***Add Device*** .
Reset Device Password	An entrance for quickly resetting the password of a device. For details about resetting devices' passwords, refer to ***Reset Device Password*** .

5.2 Other Modules

Global Search

Click in the top right corner of the Portal to open a search pane. Select **All**, **Sites**, **Device**, **Feeds**, or **How To** and enter the corresponding keyword to search for sites, devices, feeds, or how-to documents/videos.

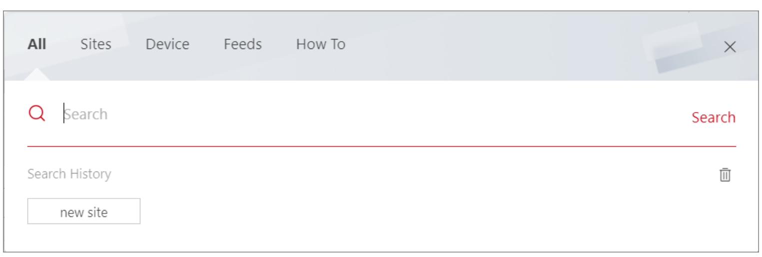


Figure 5-3 Global Search Pane

The search results will be listed in a new page. You can view the site information (including the site owner, phone number of the site owner, site address, site type, and site manager), the device information (including device name, device type, device serial No., online status, and health monitoring status), and the short descriptions of feeds or how to. You can also click a result item to enter the corresponding details page.
The search history will be displayed on the search pane, and you can click a historical keyword to search again or clear the search history.

Get Co-Branding for Free

Click on the top right of the Portal to get the co-branding for free. See ***Co-Branding*** for details.

Note

The display of the icon on the top right is not supported in all countries/regions.

Check In to Earn Point

For the first time login in a day, you can click **Check In** on the top of the Portal to check in and the reward points will be credited to your account.
And then you can view your total points on the Home page (except for authenticated channel partners), on the Dashboard page in the Site & Device module (for authenticated channel partners), or on the Rewards Store page and perform more operations, such as completing tasks to earn points, viewing point history, and redeeming points for gifts. For details, refer to ***Rewards Store*** .

Switch Company

Click in the top right corner of the Portal to switch companies for login if you have upgraded and become a Hik-Partner Pro user and your account still exists in more than one company.

Notification Center

Shows all the history business notifications (including device management invitations, site sharing notifications, and notifications about device installation work orders), notifications of device/ channel exceptions, new features of the system messages, and the latest deals and offers. For more details about the notification center, refer to ***Notification Center*** .

Help

Click in the top right corner of the Portal to show a drop-down list.

User Manual

Provides an entrance for viewing the user manual of the Hik-Partner Pro Portal online.

Wizard

View a wizard that guides you through the process of configurations and operations.

Click **Next** or **Previous** to go through the introductions in the wizard. You can click the image on the right to view the large image and check the details on the image if necessary.

Click **Skip** to close the wizard.

Questionnaire

Provides an entrance for joining the survey to help us provide a better experience and service for you.

Note

This icon is displayed only when a survey has been initiated.

Chatbot

Provides an entrance for asking questions and getting answers.

After-Sales Authorization Code

Provides an entrance for you to view the after-sales authorization code of your company. 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 (name, type, etc.), manage sites, remotely devices (AX PRO, etc.), perform health monitoring, etc.

You can click **Extend** to extend the validity period for the current authorization code or click **Invalidate Authorization Code** to invalidate the code right away.

Note

One company can only have one valid after-sales authorization code. If the code is invalidated or your company has no authorization code, you can choose to generate one.

Profile Photo and Account Name

In the upper-right corner of the Portal, click the account name or profile photo to open the drop-down list.

Account Settings and Upgrade Account

Provides an entrance for editing the basic information of the account or deleting the Installer Admin account if it is no longer used. For details, refer to ***Set Account Information*** .

When you logged in by the Hik-ProConnect account, you can select **Upgrade Account** in the drop-down list and click **Register** or click **Login** to register an OneHikID account or log in by an existing OneHikID account.

Subscribe to Newsletters

Provides an entrance for subscribing to newsletters. You can also unsubscribe here at any time. After the unsubscription, you will not receive any newsletter emails (such as new product introduction, service introduction, and questionnaires) from us.

Link with Hik-Connect Account

Provides an entrance for linking your Hik-Partner Pro or OneHikID account with multiple Hik-Connect account, so the devices managed in the Hik-Connect account can be synchronized to Hik-Partner Pro account or OneHikID account automatically. For details, refer to ***Synchronize Devices with Hik-Connect Account*** .

My QR Code

Provides an entrance for downloading your QR code, so your customers can scan via the Hik-Connect Mobile Client to add you as the service provider and authorize you to manage devices.

You can also go to **My Hik-Partner → Account Information → My Profile** page to view your QR code.

Note

This feature is only supported by accounts with the Manage Assigned Sites permission.

Verify Gifts

Provides an entrance for distributors to verify the gifts redeemed offline and export the records.

About

View the version of the current system, and read the agreements, including terms of service, privacy policy, and open source license. You can also scan the QR code with your mobile phone to download the Hik-Partner Pro Mobile Client.

Switch Company

Provides an entrance for switching companies for 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.

Log Out

Log out of the current account and return to the login page.

Floating Tool Bar

Shopping Cart

Provides an entrance for entering your shopping cart to view the added products. For details, refer to ***Create an Order*** .

Note

This function is only available to authenticated channel partners. For details, please contact Hikvision.

Order Upload

Provides an entrance for quickly submitting orders by uploading information (material code, quantity, etc.) of products with a predefined template. For details, refer to ***Create an Order*** .

Note

This function is only available to authenticated channel partners. For details, please contact Hikvision.

VS **Product Compare**

Provides an entrance for comparing multiple products with their same specifications hidden, so you can quickly choose products as needed. For details, refer to ***Compare Products*** .

Note

This function is only available to some users in some countries/regions. For details, please contact Hikvision.

Chatbot/Feedback

Provides entrances for asking questions and getting answers, submitting your own suggestions or suggestions from your customers.

Questionnaire

Provides an entrance for joining the survey to help us provide a better experience and service for you.

Note

This icon is displayed only when a survey has been initiated.

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".

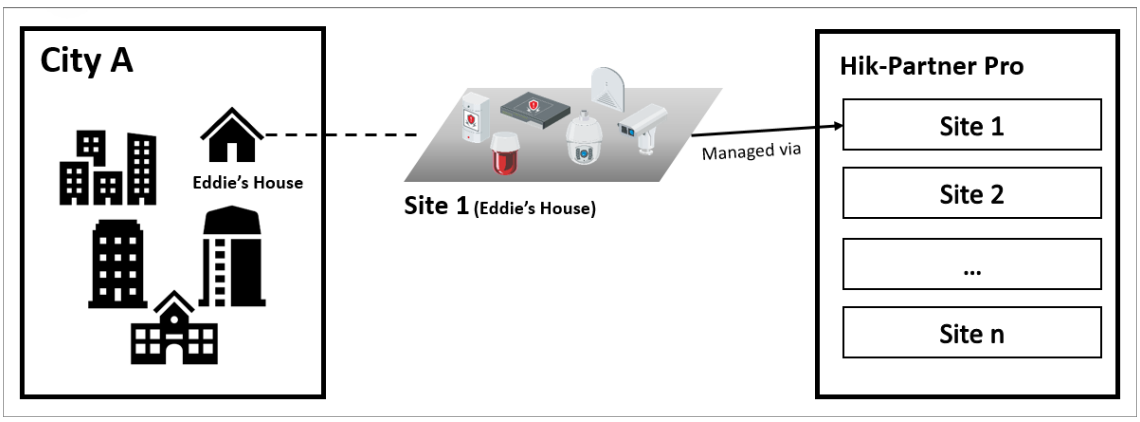


Figure 6-1 Manage Devices via "Site"

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.

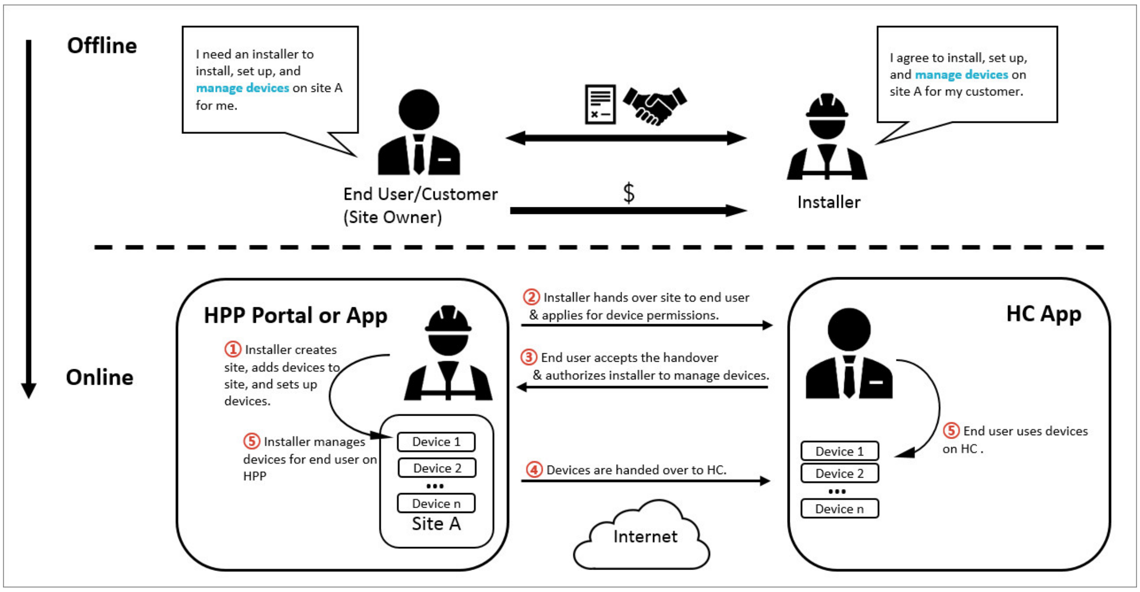


Figure 6-2 Scenario and Process

6.1 Site Page Overview

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

Enter the Site page.

- Move your cursor to the **Site & Device** tab. Select **Customer Site** to enter the Site page.
- Click on the number of sites or click **Add Site** on the Home page to enter the Site page.

Click the search box on the top right of the Customer Site page and click **Site with Offline Device** to display sites with offline devices.

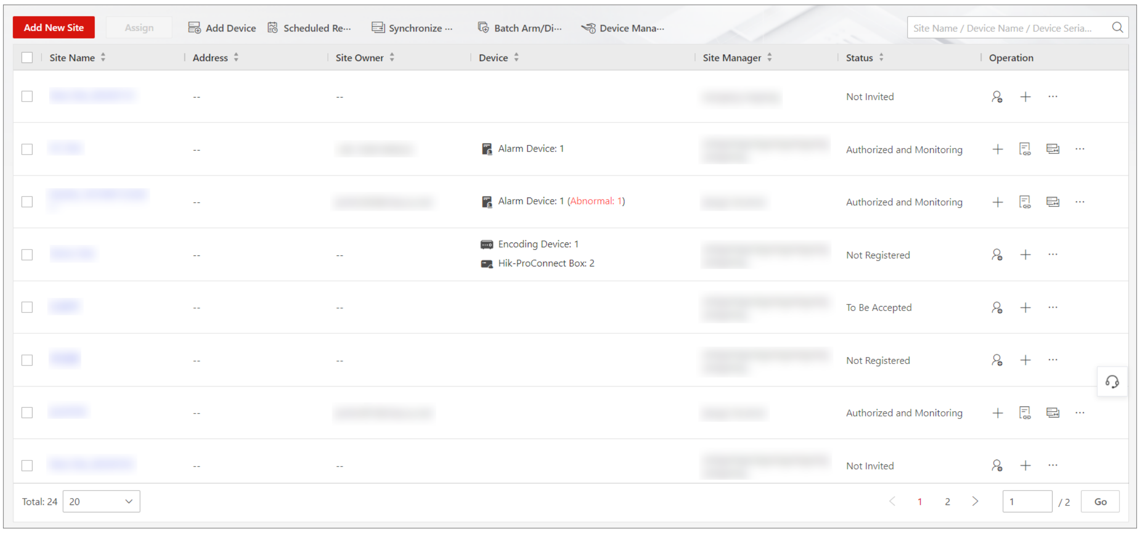


Figure 6-3 Site Page

There are different status for the sites in site list.

Not Handed Over

The site is newly added, and you have not handed over site to the customer.

Not Registered

The handover has been sent to customer who has not registered a Hik-Connect account.

To Be Accepted

The handover has been sent but not be accepted by customer who has registered a Hik-Connect account.

Handed Over, Not Authorized

The site is handed over to the customer, but the site is not authorized to the Installer.

Authorized and Monitoring

The Installer gets the authorization of the site from the customer.

Note

According to site status, the Installer Admin and Installers with related permissions 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	Authorized and Monitoring
Search Site	√	√	√	√
Assign Site	√	√	√	√

Supported Operations	Not Handed Over	To Be Accepted Not Registered	Handed Over, Not Authorized	Authorized and Monitoring
Hand Over Site	√	√	×	×
Manage Device	√	√	×	√
Edit Site	√	√	×	√
Delete Site	√	√	√	√
Apply for Authorization	×	×	√	×
Share Site	×	×	×	√

Note

- See ***Add Device*** for details about how to add devices to the site.
- See ***Synchronize Devices with Hik-Connect Account*** for details about how to synchronize devices with Hik-Connect account.

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.

Before You Start

Make sure you have the permission of adding a new site.

Steps

1. Enter the Site page.
   - Move your cursor to the **Site & Device** tab. Select **Customer Site** to enter the Site page.
   - Click on the number of sites or click **Add Site** on the Home page to enter the Site page.
2. Click **Add New Site → New Site** .

   Note

   If an existing site of end user is not authorized to any installation company, you can select **Existing Site** to add the existing site. For more details, refer to ***Add Existing Site*** .
3. Set the site name, time zone, scene, site address, city, and state/province/region.

Note

- When setting the site address, you can click on the map to locate a place, or you can enter keywords in the search box to locate a place on the map.
- 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.

4. **Optional:** Check **Sync Time & Time Zone to Device** to synchronize the time and time zone of the site to the devices added to the site.
5. **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.

6. Click **OK** to add a new site to the list.
7. **Optional:** According to the site's status and authorization, perform one of the following operations.

Note

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

Search Site	Enter keywords in search filed, and click to display the search results in the list.
View Site Details	Click the site name to view the site details, including managed devices, site information, and so on.
Edit Site	On the right side of the Site Details page, click to edit the site name, site address, city, state/province/region, remarks, and whether to check **Sync Time & Time Zone to Device** or not. **Note** When editing the site address, you can find and click the place on the map, or you can enter keywords in the search box to locate the place on the map.
Delete Site	Hover the cursor over ··· on Operation column and click 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**, click on Operation column on Site page or click **Hand Over** on Site Details page to hand over the site to an end user. **Note** For more details, refer to ***Hand Over Site*** .
Manage Device	For the site in the status of **Not Handed Over**, **Not Registered**, **To Be Accepted**, or **Authorized and Monitoring**, you can click the corresponding icon on Operation column or enter Site Details page to manage the devices, such as adding device to the site, upgrading device, deleting devices, applying for live view or configuration permission, adding linkage rule, adding exception rule, etc. For more details, refer to ***Device Management*** . **Note** If a security control panel is armed, it cannot be deleted unless being disarmed first.
Export Site Information	Click **Export** to export all sites and device information under the account.

6.3 Add Existing Site

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

Steps

1. Enter the Site page.
    - Move your cursor to the **Site & Device** tab. Select **Customer Site** to enter the Site page.
    - Click on the number of sites or click **Add Site** on the Home page to enter the Site page.
2. Click **Add New Site** and select **Existing Site**.

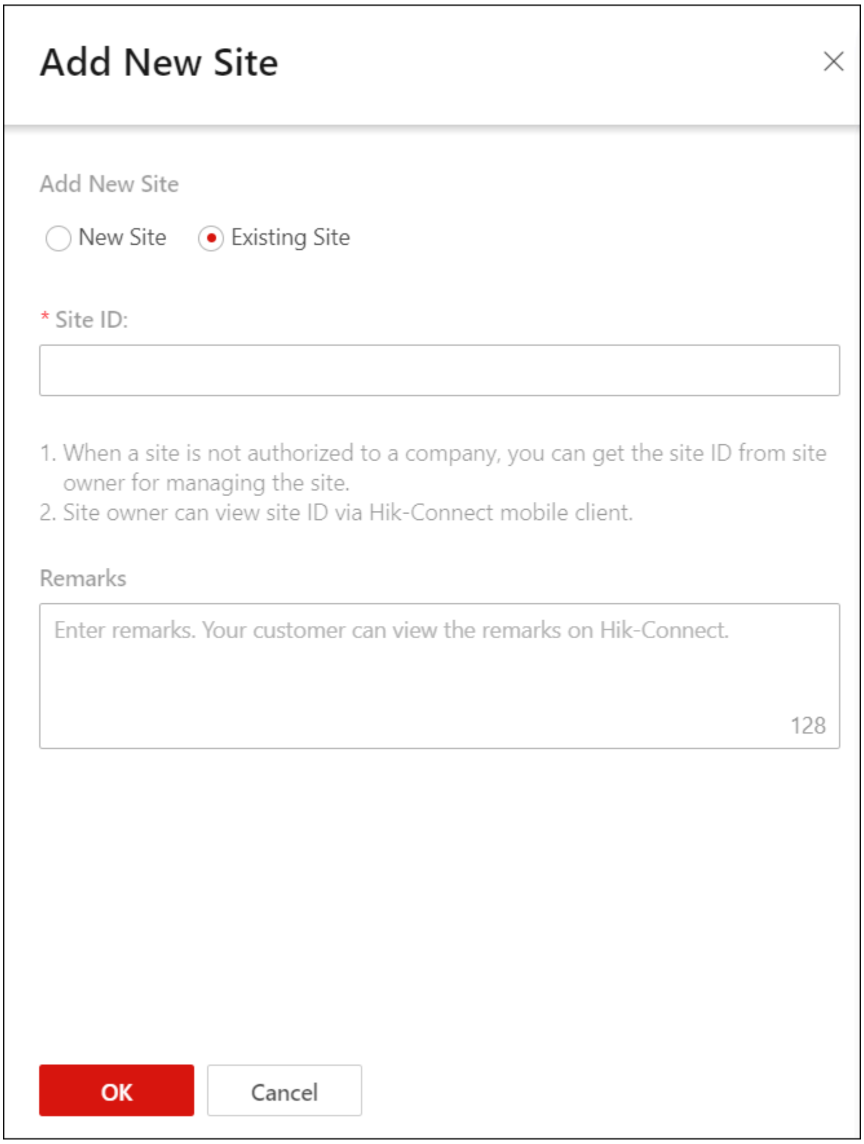


Figure 6-4 Add Existing Site

3. Enter the site ID provided.

Note

- You can get the site ID form the site owner, who can view the site ID via Hik-Connect Mobile Client.
- Please inform your end users to download or update the Hik-Connect Mobile Client (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.

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. Click **OK**.

   The site will be added in the site list and the site owner will receive an application. After the site owner approves the application, the site will be authorized 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 the Manage All Sites permission.

Steps

1. Enter the Site page.
   - Move your cursor to the **Site & Device** tab. Select **Customer Site** to enter the Site page.
   - Click on the number of sites or click **Add Site** on the Home page to enter the Site page.
2. Select one or multiple sites for assignment.
3. Click **Assign**.
4. Select one or multiple Installers as the site manager(s) of the selected site(s).

Note

No more than 100 site managers can be assigned to each site.

5. Click **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 assigning sites.

Steps

1. Move your cursor to the **Site & Device** tab.
2. Select **Customer Site** to enter the Site page.
3. Select a site to be handed over.
   - Select a site and click in the Operation column.

- Click the site name to enter the Site Details page and click **Hand Over Now**.

You will enter the Hand Over Site page.

4. **Optional:** Check **Allow Me to Disable Hik-Connect Mobile Client Remote Use**.

Note

- If checked, after you hand 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 clicking or setting the **Hik-Connect Mobile Client Remote Use** switch to off. You can also delete the devices from the your customer's Hik-Connect account without her/his authorization.

5. **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 configuration permissions for devices on the current site which your customer cannot edit.
6. Select **Email** or **Phone Number** as handover mode.
7. Enter the site owner's email address or phone number.
8. **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, or playback when handing over the site.
- If the following permissions are selected, when the customer 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.

9. **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 Hikvsion has been added to the site and activated, the check-box will appear on the Hand Over Site page.
- If the 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.

10. **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***

11. 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.
12. Click **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 the 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 customer will become the site owner.

    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 to them.

    - If there are maintenance requirements for the devices added in the Hik-Connect Mobile Client, but not added and managed in the site, after the customer accepts the handover and becomes the site owner, he/she can authorize the permissions about these devices to the Installer.
13. **Optional:** Before your customer accepts the handover, click **Hand Over Again** 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 the 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.

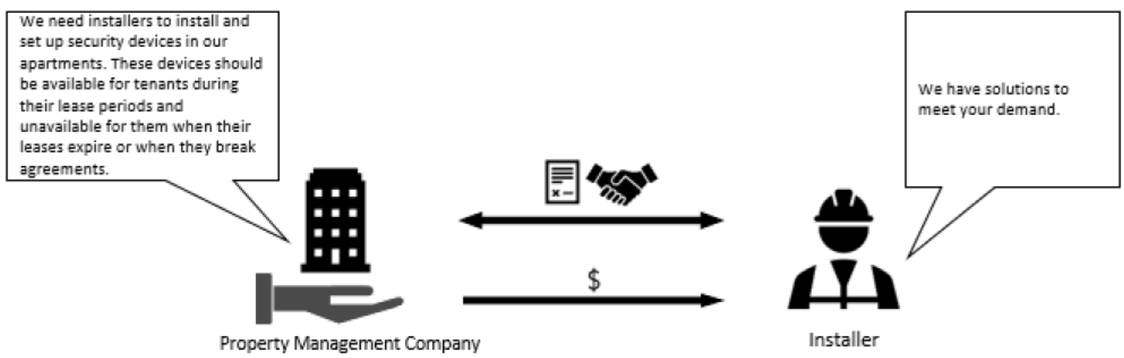


Figure 6-5 Agreement Reached Between the Property Management Company and Installer

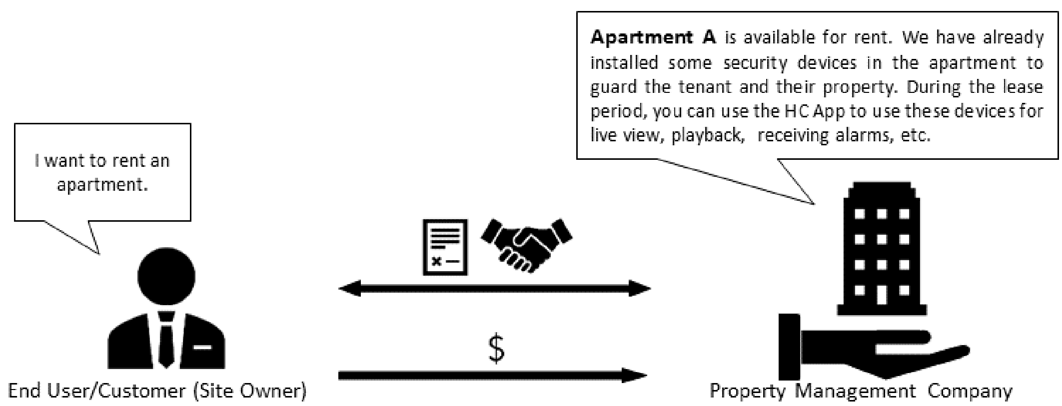


Figure 6-6 Agreement Reached Between the Tenant and Property Management Company

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 is shown below:

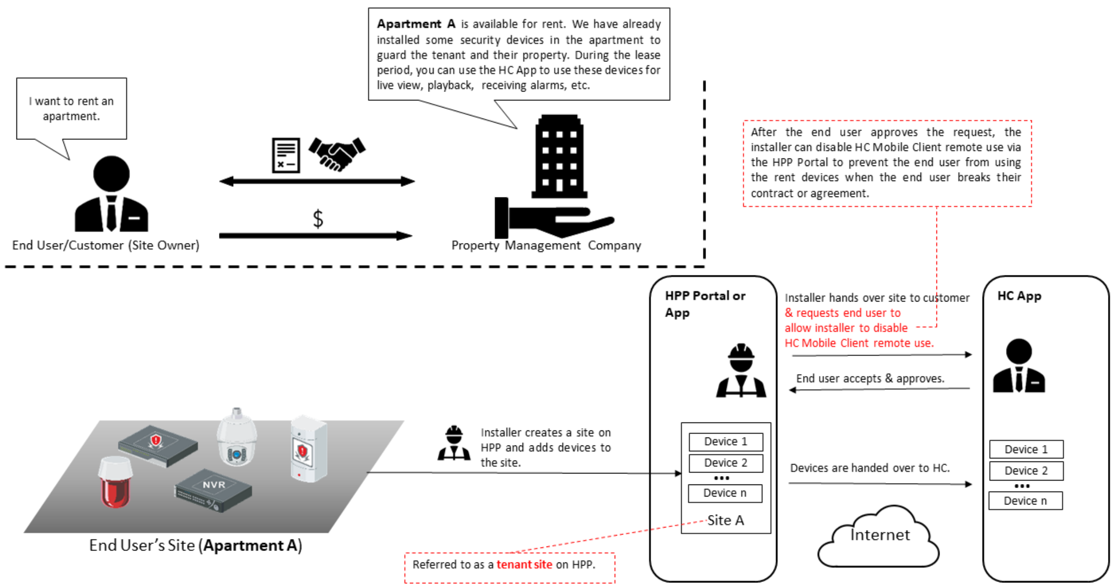


Figure 6-7 Hand Over Devices to the Tenant

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 PRO*** 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, 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. Move your cursor to the **Site & Device** tab.
2. Select **Customer Site** to enter the Site page.
3. Select a Site.
4. Enter Apply for Authorization page.
   - Select a Site and click on Operation column.
   - Click the Site name to enter Site Details page and click **Apply for Authorization**.
5. Enter the remarks and click **OK** to send the application.

   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 (V 4.15.0 or later). You can send the QR code 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.

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

Apply for Device Permission	Click the Site name to enter Site Details page and apply for permissions.
Discard Authorization	On the Site list page, click ··· → to discard authorization or 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 a Hik-Connect User

You can accept a device management invitation from your customer (i.e., a Hik-Connect user) to manage a device already 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 the device on Hik-Partner Pro. Compared with synchronizing the device in Hik-Connect with the device in Hik-Partner Pro, which requires your customer to share their Hik-Connect account name and password with you, this way is more privacy-friendly and easier to be accepted.

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

- ***Overall Process***
- ***Introduction About the Device Management Invitation on Hik-Partner Pro***
- ***The Email of Device Management Invitation***
- ***The Notification of Device Management Invitation***
- ***How Can Your Customer Invite You to Manage Their Device via Hik-Connect***

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 **Notification Center → 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.

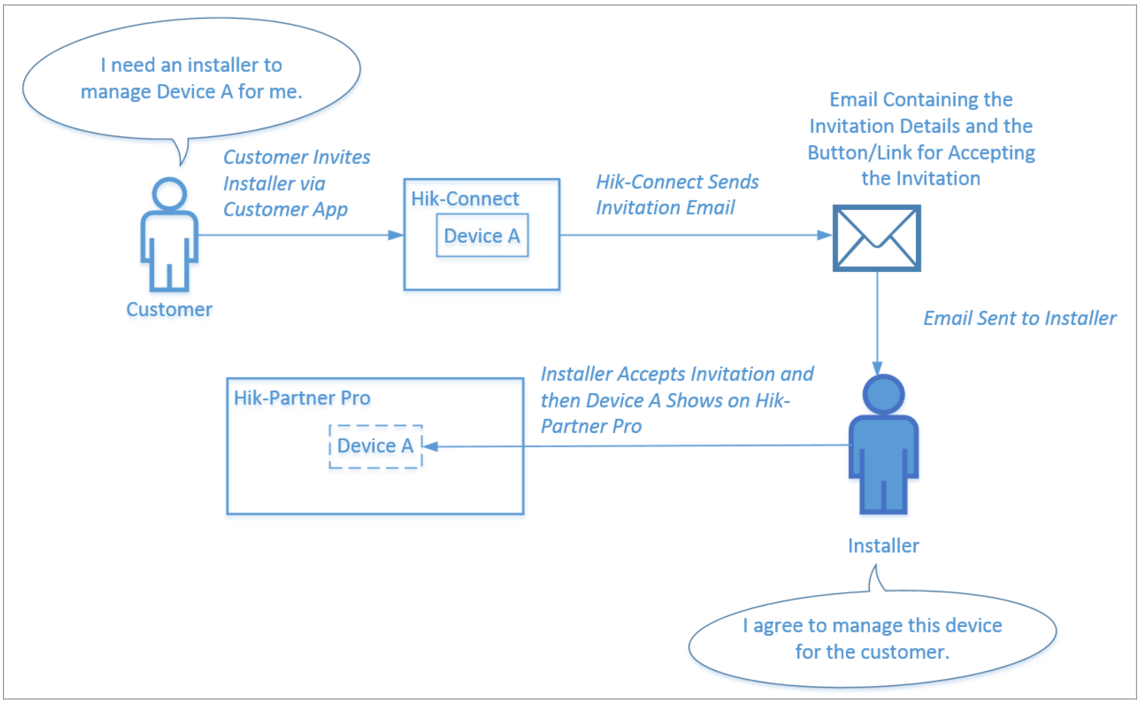


Figure 6-8 Overall Process Diagram

Introduction About the Device Management Invitation on Hik-Partner Pro

You can go to the site list page, and then click **Device Management Invitation from Customer** to open the window shown below. This shows 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 Service Provider who manages their device.

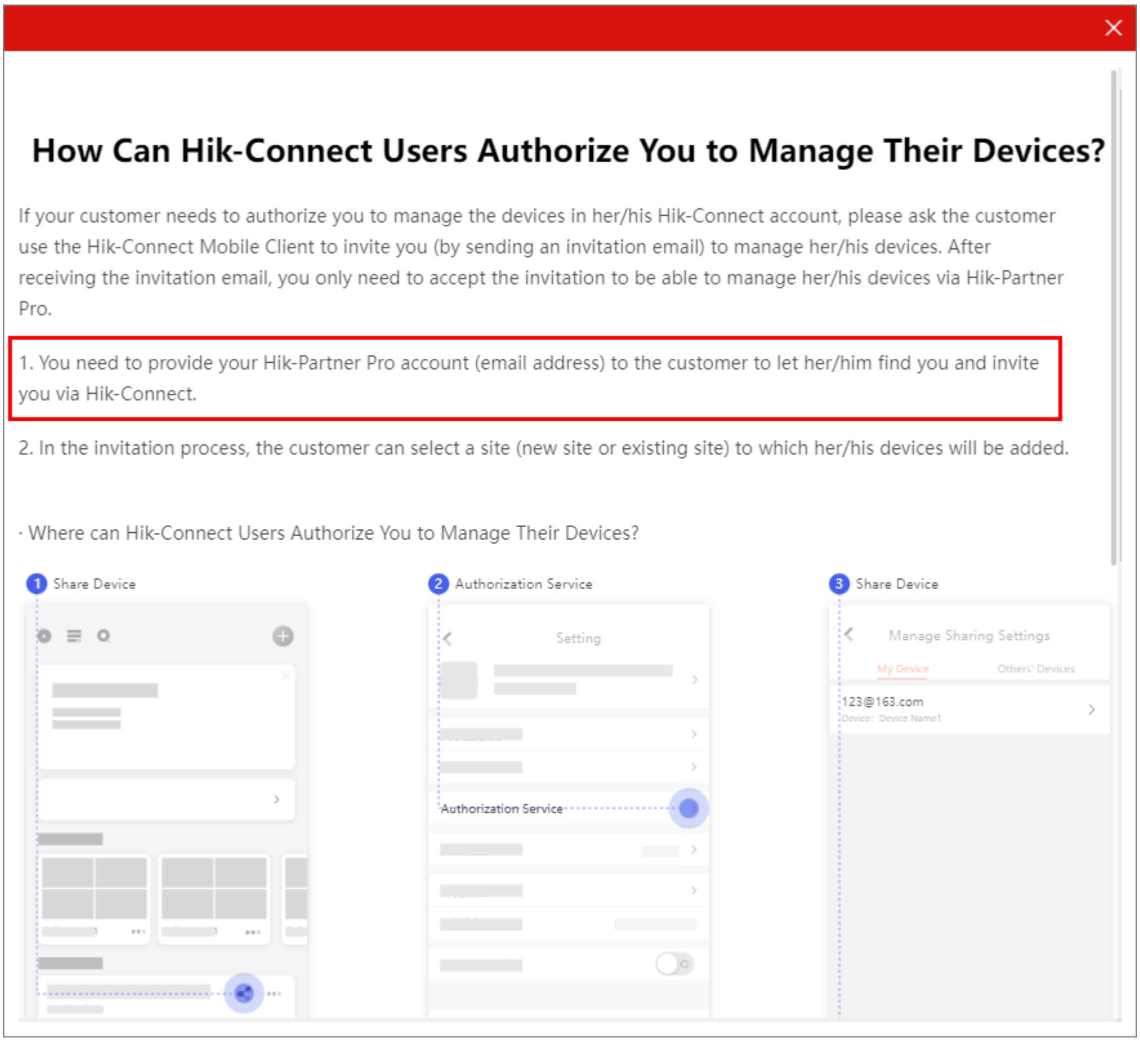


Figure 6-9 The Pop-Up Window

The Email of Device Management Invitation

The email shows the invitation details including device name, device serial No., 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., and the Hik-Connect user account. 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.

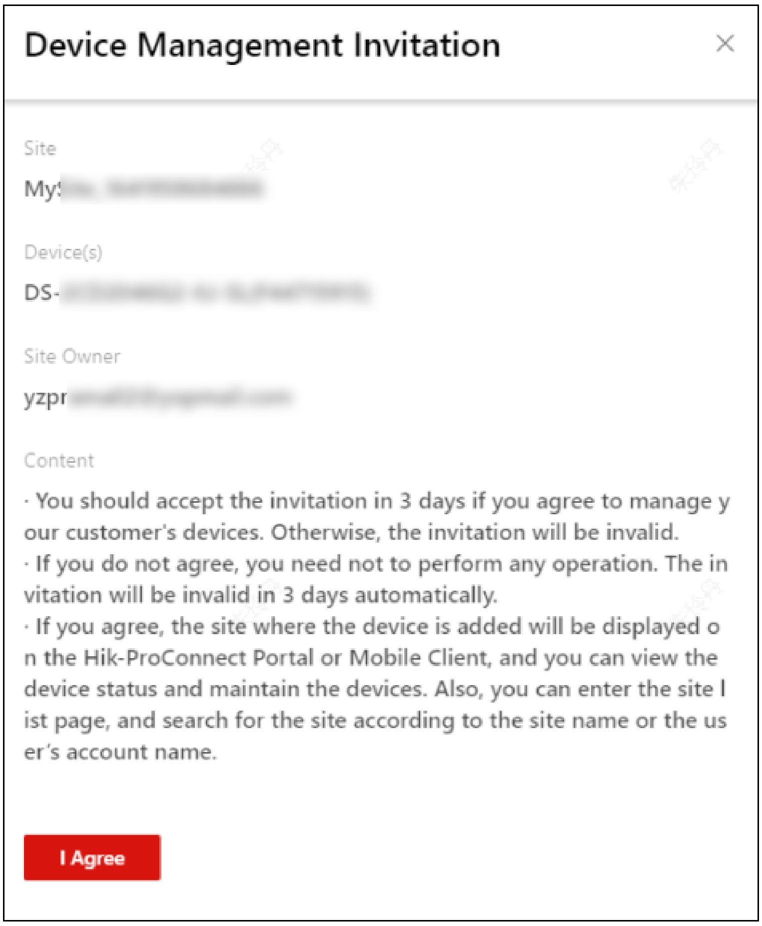


Figure 6-10 Notification Example

How Can Your Customer Invite You to Manage Their Device via Hik-Connect

Refer to the following steps for details about how can your customer invite you to manage their device via the Hik-Connect Mobile Client.

1. In the device list, tap of the device and the Share Device page will pop up. Or select **Me → Manage Sharing Settings → Share Device** to show the Share Device page.

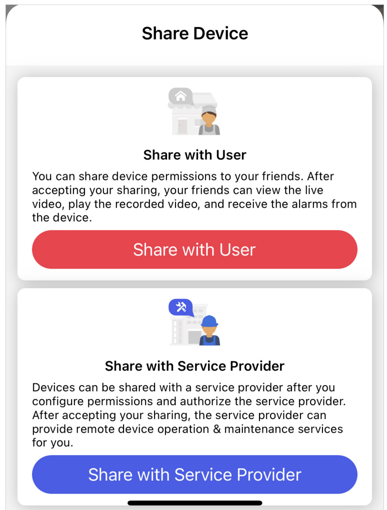


Figure 6-11 Share Device

Note

If this page doesn't show, it means the device cannot be managed by a Service Provider and can only be shared with another Hik-Connect user.
Possible reasons: the device is shared from others; the device is already managed by a Service Provider; the device is not enabled with the Hik-Connect service; or the Hik-Partner Pro service (Service Provider service) is not available in your customer's country or region.

2. Tap **Share with Service Provider**.
3. Tap **New Service Provider** and enter the Service Provider's account to share device permissions with a new Service Provider; or select an existing Service Provider.

Note

After entering the new Service Provider's account, if the account has been linked with two or more companies, you should select a company to share device permissions with.

4. Select the Site where the device will be added and the device permissions to be granted to the Service Provider.

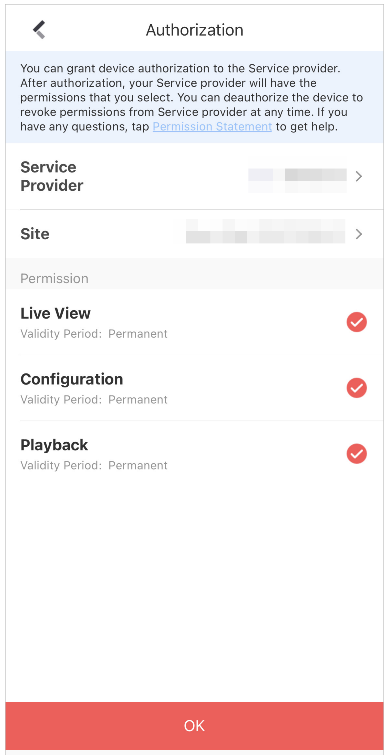


Figure 6-12 Authorization

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 MSP'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.

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 *Share a Site Before Handover* .

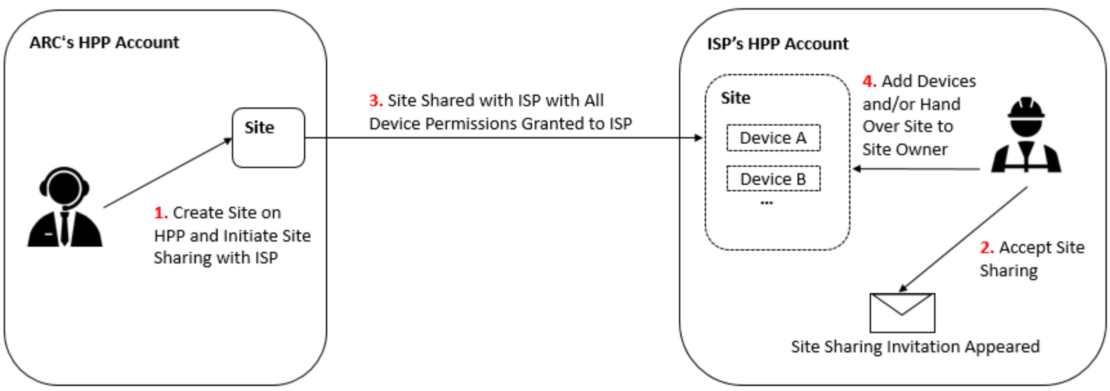


Figure 6-13 Overall Process

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* .

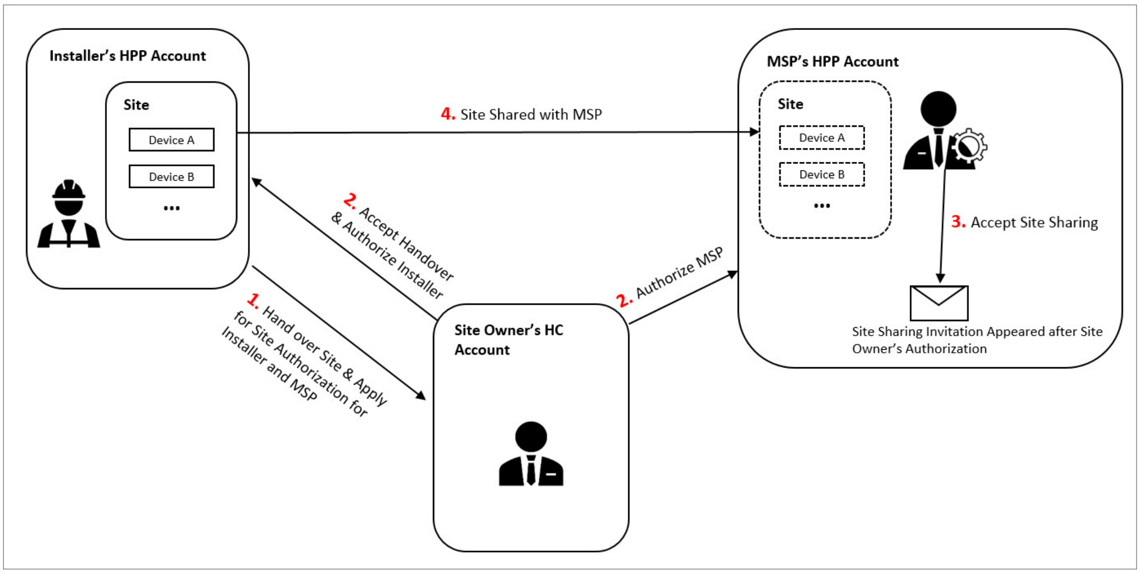


Figure 6-14 Overall Process

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*** .

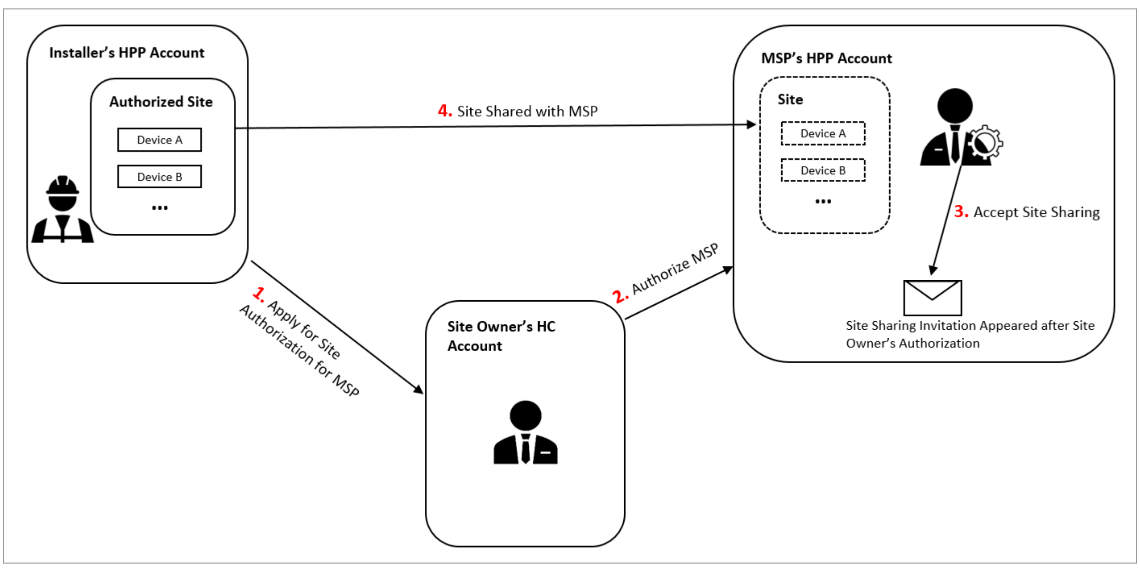


Figure 6-15 Overall Process

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 Before Handover

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.

Before You Start

- Make sure site sharing is supported in both your and the ISP's countries/regions and by both accounts.
- Make sure the site status is **Not Handed Over** and you have the permission to manage all sites or assigned sites.
- The ISP's account should have the Manage All Sites or Manage Assigned Sites permission and should not be an account of your company.
- Your account and the ISP's account need to be in the same country/region.

Steps

1. Move your cursor to the **Site & Device** tab.
2. Select **Customer Site** to enter the site page.
3. Go to the Site Sharing page.
   - On the site list, select ··· → .
   - Click a site to go to the site details page, click **Site Sharing** on the top left of the page.

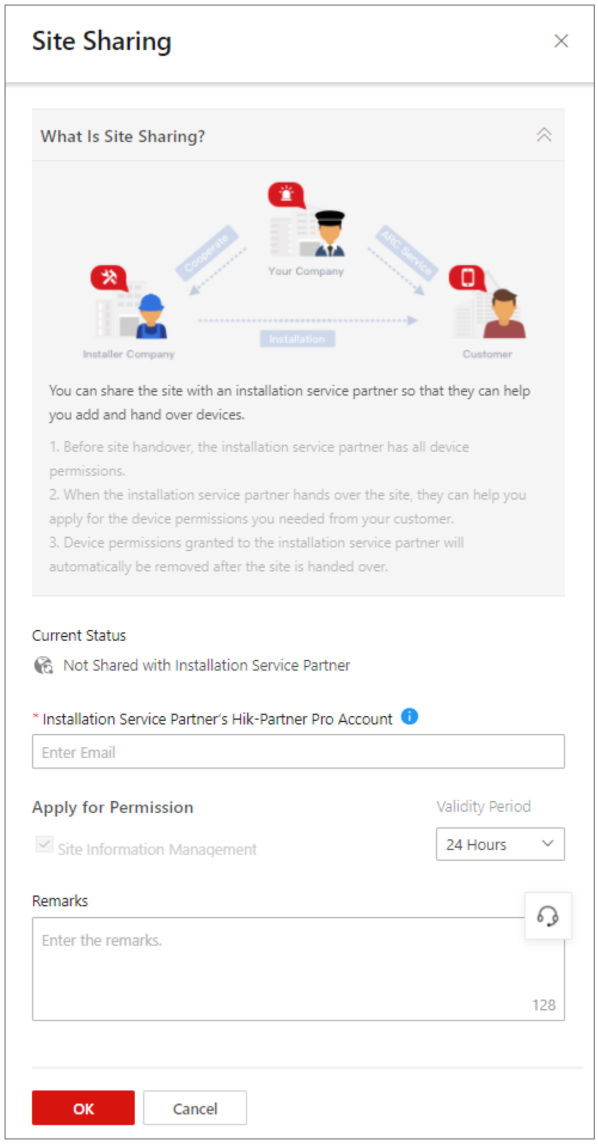


Figure 6-16 Site Sharing (with ISP)

4. Enter the ISP's Hik-Partner Pro account.

Note

Make sure the account you enter has permission to Manage All Sites or Manage Assigned Sites, otherwise it will not be able to manage the site.

5. Select the validity period of the permission granted to the ISP.

Note

- When the set validity period ends, the site sharing will be automatically canceled.
- Before the set validity period ends, the ISP has all permissions for devices on the shared site if the site sharing is not canceled and the site is not handed over.

6. **Optional:** Enter the remarks.
7. Click **OK**.

Note

- The site sharing will be canceled automatically and all device permissions will be removed from the ISP's account if the set permission validity period ends, or the site is handed over to the customer, or the site is deleted.
- You will receive notifications in Notification Center if the ISP accepts/rejects/cancels the sharing.

8. **Optional:** Perform the operation(s) below if needed.

View Site Sharing	You can enter the Site Sharing page of the site you just shared to view the sharing status (to be accepted, shared, rejected, etc.), the ISP's account, and the validity period.
Cancel Site Sharing	After the ISP accepts/rejects the site sharing, you can cancel site sharing.
Share Again	After the ISP rejects the site sharing or if the site sharing is to be accepted, you can go to the site sharing page, and edit the ISP's account and/or the validity period to share the site again.

6.9.2 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, check **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. Click **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.

6.9.3 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 Monitoring** 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. Move your cursor to the **Site & Device** tab.
2. Select **Customer Site** to enter the Site page.
3. Select a site for site sharing.
4. Enter the Site Sharing page.
   - Move the cursor to ··· in the Operation column and click .
   - Click the site name to enter the site details page and click **Site Sharing**.
5. 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.
6. 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.

7. Enter the remarks, such as the reason for site sharing.
8. Click **OK**.
9. **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 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.

6.9.4 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. In the upper-right corner of the page, click to enter the Notification Center.
2. Click the **Business Notification** tab.
3. Click **I Agree** to accept the site sharing.

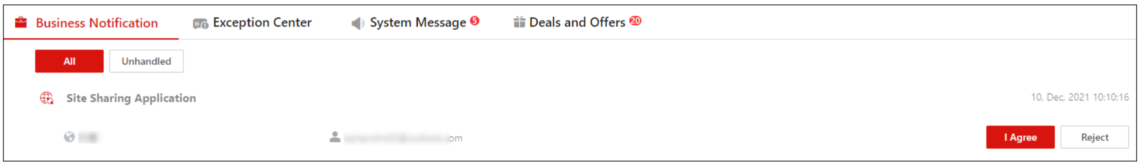


Figure 6-17 Site Sharing Application

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.

6.9.5 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.

6.10 View Sites on the Map

If you have configured GPS information for the sites, you can view them on the map.

Move your cursor to the **Site & Device** tab. Select **Site Map** to enter the Site Map page.

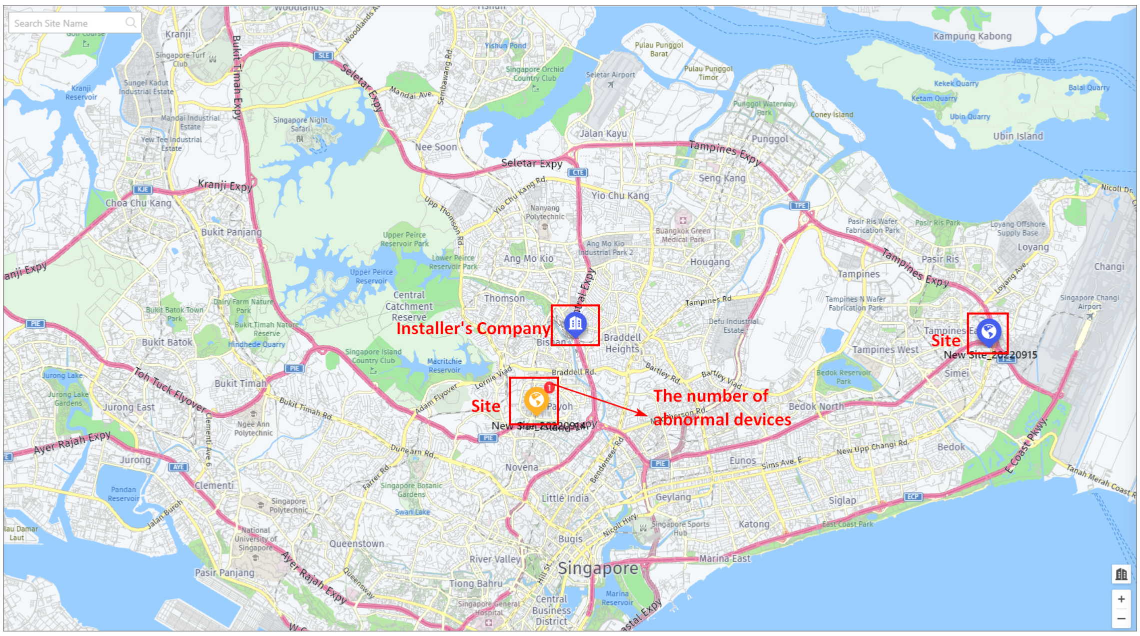


Figure 6-18 Site Map

Note

- Installer's company is in the center of the map by default.
- : There are device(s) that have been activated the health monitoring service in this site.
- : There is no device that has been activated the health monitoring service in this site.

You can perform the followings on this page.

- You can view companies and sites whose GPS information have been configured on the map. For details about configuring GPS information for companies and sites, refer to ***Add New Site*** and ***Manage Company Information*** .
- You can click a site to view its information, including site name, site owner, site location, the number of online/offline/abnormal devices, etc. Also, you can click **Site Details** to enter site details page to view more information about the site. You can click **Health Monitoring Details** to enter the health status page and view the health status of all the devices added to this site.

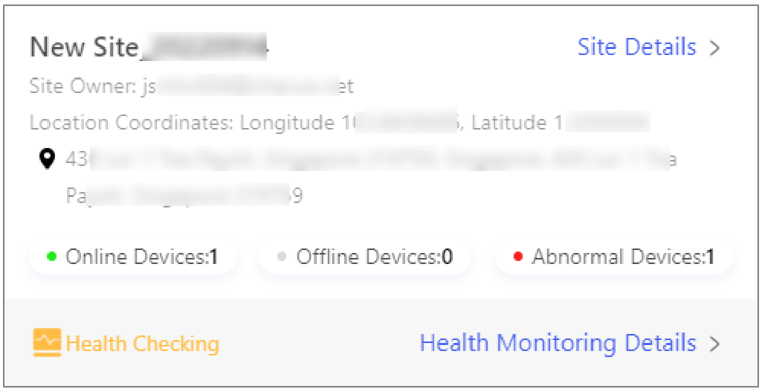


Figure 6-19 Site Information

- You can drag the map as needed. You can scroll the mouse or click + / − in the down-right corner to zoom in/out the map. Also, you can click to view the company's location on the map.
- You can enter keyword(s) in the search box in the upper-left corner to search for the site name.

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, doorbell. After adding them to the system, you can manage them and configure settings, including remotely configuring device parameters, configuring exception rule, linkage rule, people counting, temperature screening, etc.

Note

Some functions may not be available in specific countries and regions.

7.1 Batch Configure Devices on LAN

You can batch configure online devices on the same Local Area Network (LAN) with the PC on which the Hik-Partner Pro Portal 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 effort compared with configuring devices one by one.

Note

- For entering the device batch configuration page for the first time, a video tutorial about how to batch configure devices on LAN will pop up and automatically play in the down-left corner.
- The 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 PC on which the Hik-Partner Pro Portal runs.

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

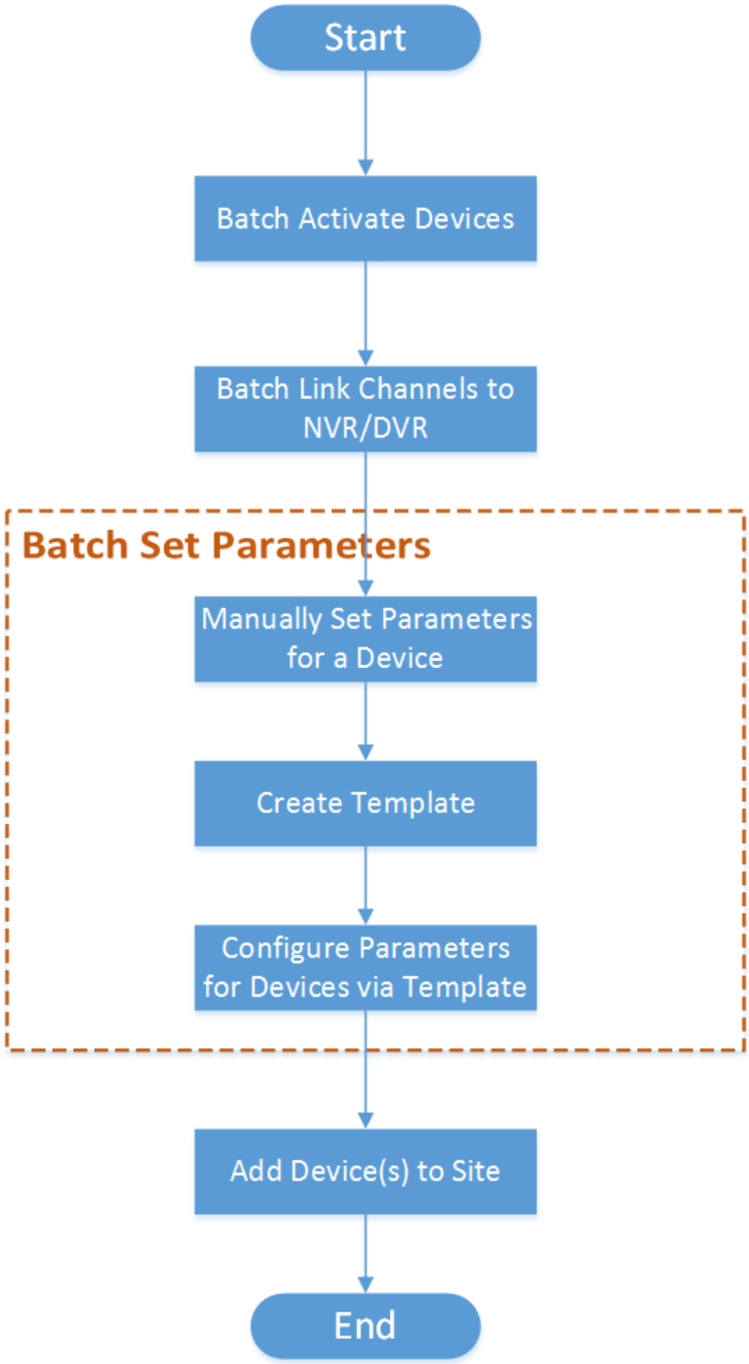


Figure 7-1 Flow Chart

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 PC on which the Hik-Partner Pro Portal 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 or DVR, link channels to NVR or 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 Template for Setting Parameters*** for details.
	Create Template	Created a template based on the manually configured device. See ***Create Template 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 via Template*** for details.
Add Device(s) to Site	N/A	If required, add the activated and configured device(s) to a Site. See ***Add Detected Online Device*** for details.

7.1.1 Batch Activate Devices and Assign IP Addresses for Them

The Portal can detect available devices connected to the same network with the Portal, and then 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. Click **Install & Config → On-Site Config** to enter the batch device configuration page.

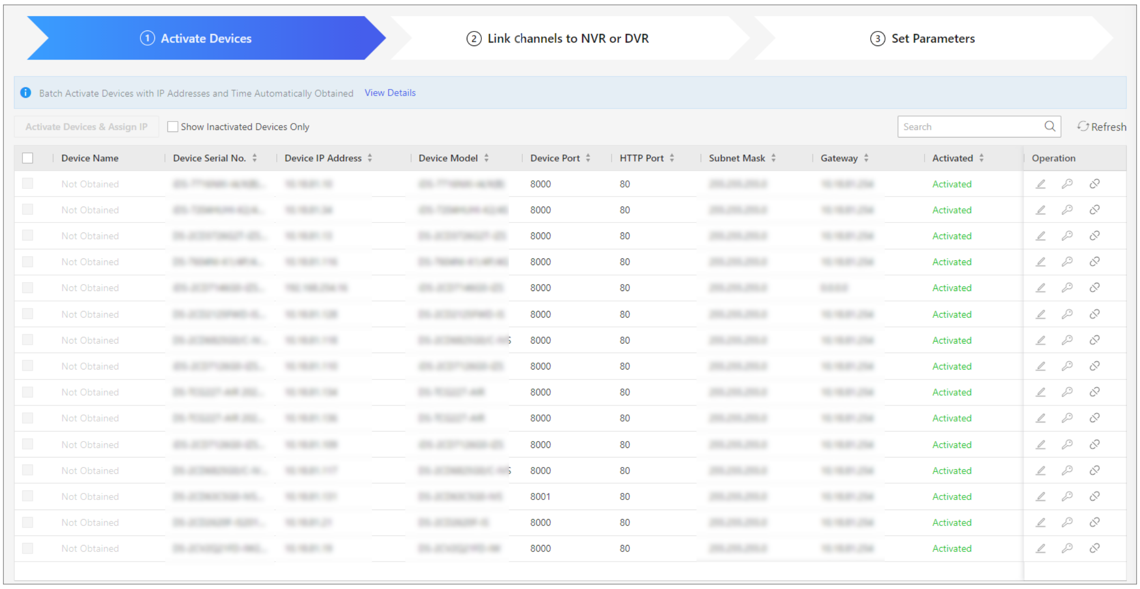


Figure 7-2 Batch Device Configuration

2. Select the detected online devices to be activated.
3. Click **Activate Devices & Assign IP** to open the Activate Devices & Assign IP window.
4. Enter the device admin password and confirm the password.
5. Click **Activate Devices & Assign IP**.

Note

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

The devices are activated, and the device IP address are assigned by the Portal.

The time of the computer will be synchronized to the activated devices.

6. **Optional:** After the devices are activated, you can perform the following operations.

Operation	Description
Edit Device Network Parameters	Click to edit the device network parameters, including IP address, device port, HTTP port, subnet mask, gateway, device admin password and then click **OK**.
Reset Device Admin Password	Click to reset the admin password of the device.
Unbind Device	Click and then enter the device password and verification code to unbind the device from its current account. After unbound, the device can be added to another account.

What to do next

After activating the devices, you should batch add channels to NVR or 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 camera to the NVR and 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. See ***Batch Activate Devices and Assign IP Addresses for Them*** for details.

Steps

Note

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

1. On the Link Channel page, select an NVR or DVR on the left.

   Note

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

2. Click **Next**.

   Channels that have been linked will be displayed in the middle.

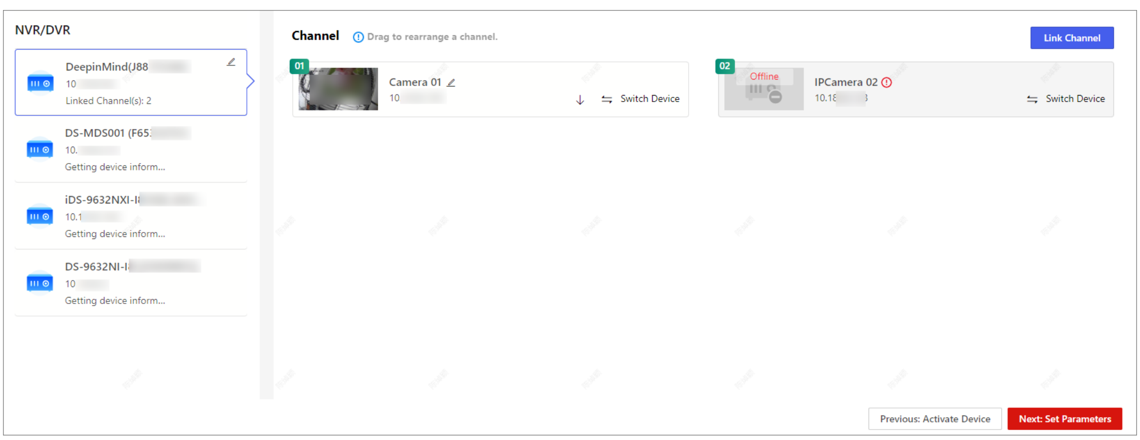


Figure 7-3 Channels on the Same LAN

Note

If a linked channel is offline, ⓘ will be displayed beside the channel name. Hover the cursor on the icon to view the reason for being offline. You can click **Set Parameters** to change channel parameters to try again.

3. Click **Link Channel** to open the Link Channel panel.
4. **Optional:** Select a device and click ⇅ to log in to the device and get device information.
5. Click **+** to link the device.
6. **Optional:** Perform the following operations.

Edit NVR/DVR/Channel Name	Click ✎ to edit the NVR/DVR/channel name.
Sort Channels	Click ↑ or ↓ to sort the channels.
Replace Device	Click **Replace Device** to unlink this channel and link a new device.
Unlink Device	Click 🗑 to unlink channel.

What to do next
Click **Next** to batch set parameters for devices. See ***Batch Set Parameters for Devices via Template*** for details.

7.1.3 Create Template for Setting Parameters

Before batch configuring parameters for devices, you should create a template. After creating a template, you can batch apply it to 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. Click a device name or **Set Parameters** to enter the remote configuration page.
2. On the remote configuration page, set parameters for the device.
3. Click **Save as Template** on the top right.
4. Set a template name and check the parameters you want to save in the template.
5. Click **Save** to save the parameters as a template.
6. **Optional:** Add a new template based on device with configured parameters.
   1) Click **Manage Template → +** .
   2) Enter template name.
   3) Select device type.
   4) In the template content field, select a device.
   5) Click **Save**.

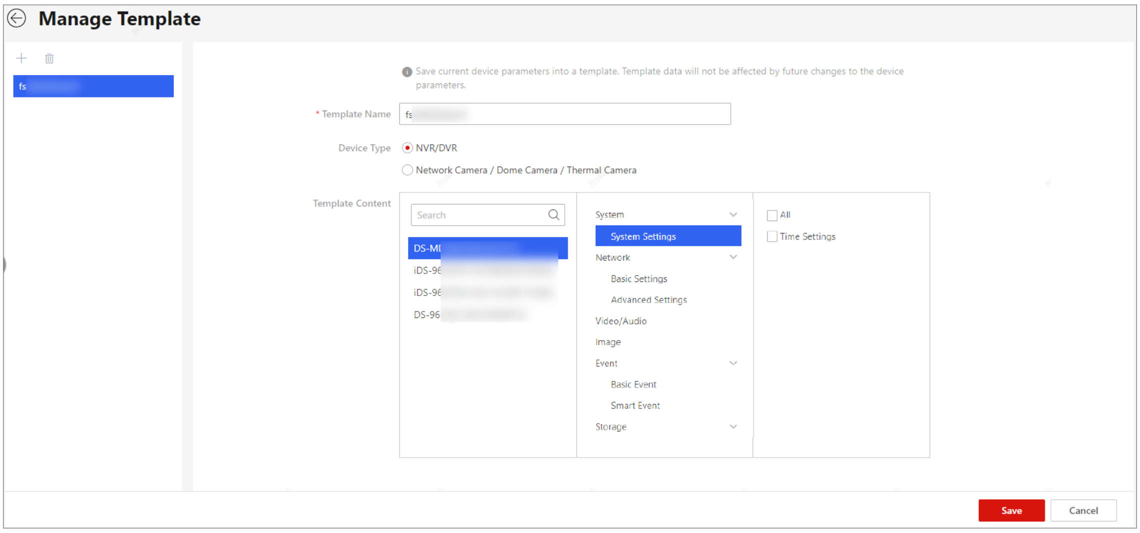


Figure 7-4 Add Template

7. **Optional:** Click 🗑 to delete a template.

7.1.4 Batch Set Parameters for Devices via Template

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 Template for Setting Parameters*** for details.

Steps

1. Check device(s) and click **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.

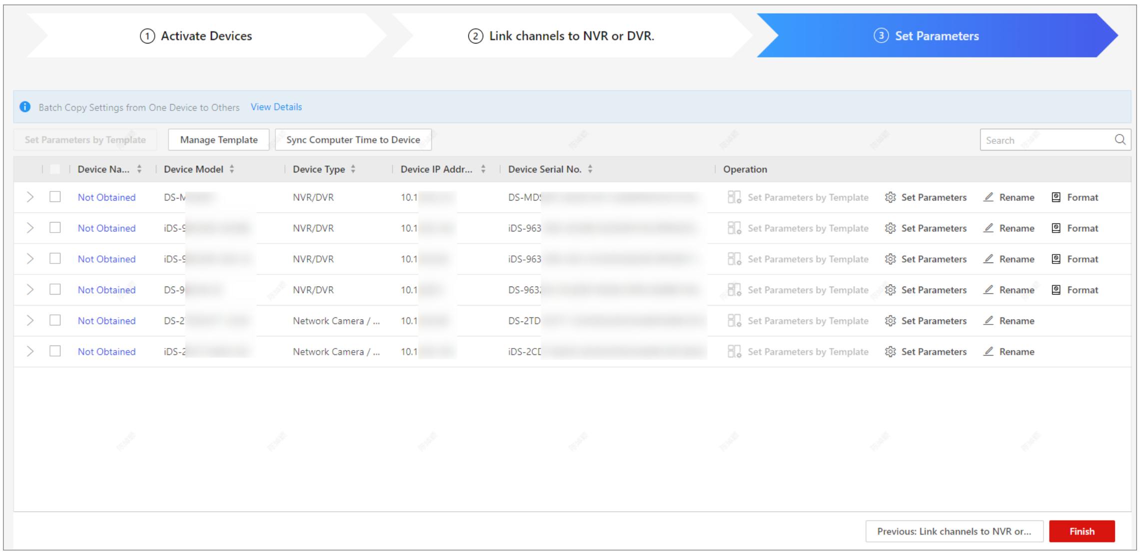


Figure 7-5 Set Parameters

3. Click **Apply Parameters** to apply the configured parameters to devices.

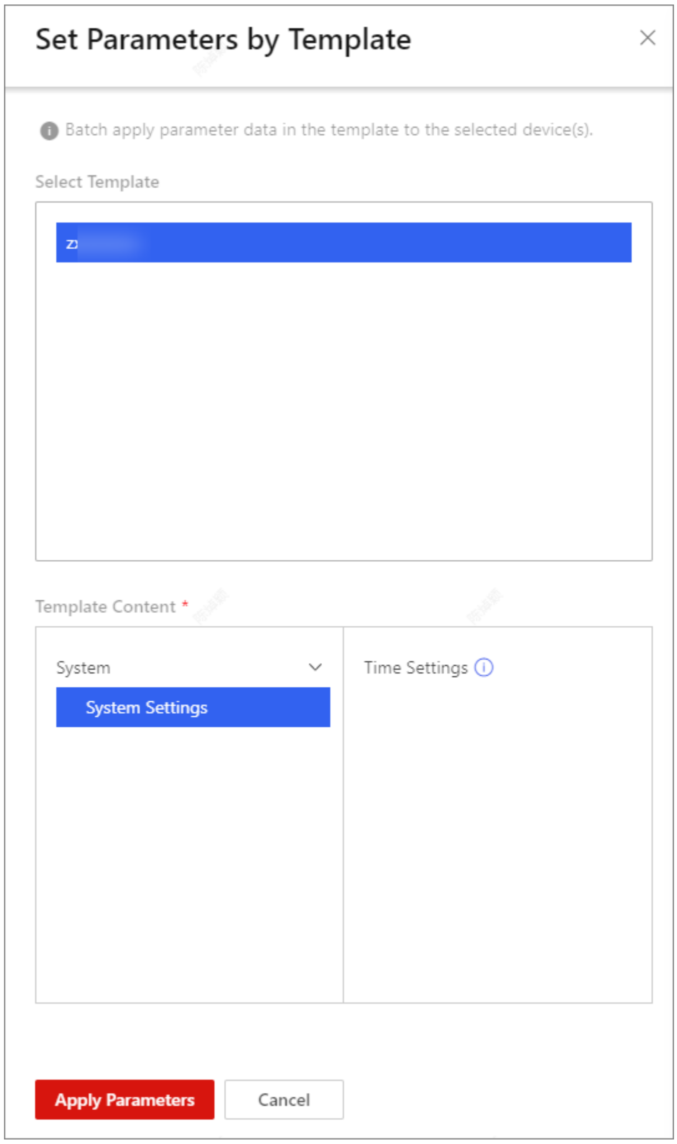


Figure 7-6 Set Parameters by Template

The application process and application results will be displayed.

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

Add Device to Site	Add devices to Sites. See ***Add Device*** for details.
Manage Template	Click **Manage Template** to add new template or delete template. See ***Create Template for Setting Parameters*** for details.
Edit NVR or Channel Name	Click **Rename** to edit name(s) of NVR or channels of NVR.
Synchronize Computer Time to Device	Check device(s) and click **Synchronize Time to Device**. And then check devices and click **OK**.

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 communication (between Hik-Partner Pro and devices) and full access to features based on the Hik-Connect service, such as device handover and exception notification; the latter provides faster data communication but no access to the features based on 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 Detected Online Device*** • ***Add Device by Entering Serial No.*** • ***Synchronize Devices with Hik-Connect Account*** • ***Add Devices Without Support for the Hik-Connect Service*** **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 get full access to the features based on the Hik-Connect service.
Device IP Address/Domain Name	• ***Add Devices by IP Address or Domain Name*** • ***Batch Add Devices***

7.2.1 Add Device(s) after Batch Configuring Them

After batch configuring devices, you can add the device(s) to the existing site or a new site.

Select one of the following ways to enter the Add Device page.

- After batch configuring device(s), click **Add Device** in the prompt box.

  Note

  For details about batch configuring devices, refer to ***Batch Configure Devices on LAN***
- On the Home page, click **Add Device**.
- On the navigation pane, click **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your region).
  - Click **Add Device** on the top of the site list.
  - Click + in the Operation column of the site list.
  - Click the site name to enter the site details page, and then go to **Device → Add Device** .

Select **Scan for Devices on LAN**, **Enter Serial No.**, **Enter IP Address / Domain**, **Batch Import**, or **Synchronize devices from the Hik-Connect** as the adding method.

Select the device(s) to be added, and perform one of the following two ways to add the device(s) to the site.

- Select **Existing Site** and then click the site in the drop-down list.
- Select **New Site** and edit the following parameters to create a new site.

Site Name

The name of the site, which can describe the site location, function, etc.

Time Zone

Select the time zone in the drop-down list according to the location the site belongs to.

Scene

Select the scene of the site in the drop-down list according to the usage scene, such as house, department, villa, and store.

Site Address

Enter the site address, such as street and number, apartment suite, unit, building, floor, etc.

City

Enter the city of the site.

State/Province/Region

Enter the state, province or region of the site.

Sync Time & Time Zone to Device

After checked, the time and time zone will be synchronized to the device from the site.

Click **Next** and perform the operations according to the prompts on the page. For more details, refer to ***Add Device*** .

7.2.2 Add Detected Online Device

The Portal can detect available devices connected to the same network with the Portal, which makes the devices' information about themselves (e.g., IP address) recognized by the Portal. Based on the information, you can add the devices quickly.

Note

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- You can add up to 15 detected online devices simultaneously.

On the navigation pane, click **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your region).

On the Add Device page, click **Scan for Devices on LAN**.

Note

For details about how to enter Add Device page, refer to ***Add Device(s) after Batch Configuring Them*** .

The device(s) connected to the same LAN with the Portal will be displayed on the device list. You can view information including device serial No., device IP address, activation status (activated or not), Hik-Connect status (connected to Hik-Connect service or not), etc.

Check the online device(s) to be added and click **Next**. Perform part or all of the following 4 steps based on the status of the selected devices before you can add them.

Table 7-3 Step Description

Step	Description
Activate Device	If there are device(s) not activated, activate them. See ***Activate Device*** for details. **Note** If a device is activated, the platform will automatically assign a fixed IP address for it.
Enter Device Password	Enter admin password of the device. See ***Enter Device Password*** for details.
Automatically Connect to Hik-Connect Service	Connect device(s) to the Hik-Connect service. See ***Connect to Hik-Connect Service*** for details.
Set Device Verification Code	If a device is connected to the Hik-Connect service successfully, the platform will automatically get device verification code from device. If not, you need to set verification code for it. See ***Set Device Verification Code*** for details.

Note

- 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.

After adding devices to the Portal, you can perform the following operations if required.

Table 7-4 Available Operations after Adding Devices

Operation	Description
Edit Device	Click the device name to edit it. Or move the cursor to the device and then click to edit device name.
Configure Linkage Rule	Click to configure linkage rule for the device. **Note** For details, see ***Add Custom Linkage Rule*** .
Activate Health Monitoring Service	Click **Activate Service** on the adding result page. Or hover the cursor onto on the device card on the site details page, and then click **Activate Service**. **Note** • For details about how to activate the health monitoring service, see ***Activate the Health Monitoring Service for Devices*** . • For details about Health Monitoring service, see ***Health Monitoring Service*** .
Delete Device	Click → to delete the device. **Note** • Deleting device (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.
Upgrade Device Firmware	When device adding completes, the platform will start detecting whether the device firmware version is compatible. Some functions (including health monitoring, linkage rule, and remote

Operation	Description
	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. 1. Select **Upgrade to Compatible Version** on the **Upgrade or Not** column, and click **Add and Upgrade**. 2. Enter device user name and password to add and upgrade the device.
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. Click **Set Device Type** and select a device type from the drop-down list. You can edit it again after the selection.
Unbind Device from Its Current Account	If the adding result page shows that a device fails to be added and has been added to another account, you can click to unbind it. When the device is unbound, you can add it to your account. For details about unbinding device, see ***Unbind a Device from Its Current Account*** .

Activate Device

If there are inactivated device(s) in the selected devices, create a device admin password for all the inactivated device(s) on the pop-up window to activated them.

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.

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.
If multiple devices share the same password, enable **Batch Enter admin Password** to enter the password for all the devices in a batch. If any devices' passwords are incorrect, a notification will prompt showing these device(s) for you to enter the correct password(s).

Note

Before entering admin password, you should make sure that no repeated device IP address exists, or one of the devices with the same IP address will fail to be added. You can click in the Operation column, and then edit the device IP address.

Connect to Hik-Connect Service

After entering device admin passwords, the platform will automatically start connecting the device(s) to the Hik-Connect service. Devices that are failed to be connected to the Hik-Connect service cannot be added.

Note

Make sure that no repeated device IP address exists and that the IP addresses of the to-be-connected devices are in the same network segment with the PC running Hik-Partner Pro, or connection exception will occur. You can click in the Operation column, and then edit the device IP address.

Set Device Verification Code

- If a device is connected to the Hik-Connect service successfully, the platform will automatically get device verification code from device. If the platform failed to get the verification codes from any devices, you need to manually enter their verification codes.
  If multiple devices share the same verification code, enable **Batch Enter Verification Code** and enter the verification code for all of them.
- If device(s) failed to be connected to the Hik-Connect service, you need to set a shared device verification code for multiple devices, or set verification codes for each device. After you complete device verification settings, the device(s) will be connected the Hik-Connect service.

Note

For EZVIZ devices, admin password is not required, and device verification code is required.

7.2.3 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.
- Make sure the device has been activated and connected to Hik-Connect service.

Steps

1. On the navigation pane, click **Customer Site → Site** (or **Customer Site** if HikCentral Connect is not available in your region).

2. Open the Add Device page.

Note

For details, refer to ***Add Device(s) after Batch Configuring Them*** .

3. Select **Enter Serial No.** as the adding mode.
4. Enter the device serial number and device verification code.

Note

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

5. Click **Next**.

Note

Hik-Partner Pro will start detecting whether the device firmware version is compatible with the Hik-Partner Pro. Some functions (including health monitoring, linkage, and remote configuration) cannot be used if the device is not compatible with the Hik-Partner Pro. Firmware version detection will not happen if a site is authorized. For devices incompatible with the Hik-Partner Pro, you need to upgrade them.

   1) Select **Upgrade to Compatible Version** on the **Upgrade or Not** column, and click **Add and Upgrade**.
   2) Enter device user name and password to add and upgrade the device.
6. Check the device(s) to be added.
7. Click **Add**.

Note

- After you add an AX PRO device to Hik-Partner Pro, you will be able to log into the AX PRO device 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.

8. **Optional:** Perform the following operations after adding device(s).

Edit Device Name	Click the device name to edit it. Or move the cursor to the device and then click to edit it.
Delete Device	Click ··· → . **Note** • Deleting device (except devices added by IP/domain) is not supported if the Site is authorized to you. • 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.
Upgrade Device	Refer to ***Upgrade Device*** .
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. Click **Set Device Type** and select a device type from the drop-down list. You can edit it again after the selection.
View DDNS Status	Click and hover the cursor on . See ***Configure DDNS for Devices*** for details about configuring device DDNS.
Activate Health Monitoring Service	Click **Activate Service** on the adding result page. Or hover the cursor onto on the device card on the site details page, and then click **Activate Service**. **Note** • For details about how to activate the health monitoring service, see ***Activate the Health Monitoring Service for Devices*** . • For details about health monitoring service, see ***Health Monitoring Service*** .
Configure Cloud Storage	For the Hik-ProConnect box, DVR that supports cloud storage, and NVR that supports cloud storage, you can click **Cloud Storage Service** to configure Cloud Storage settings. See ***Set Cloud Storage for Hik-ProConnect Box*** , ***Set Cloud Storage for DVR*** , and ***How to enable cloud storage for an NVR that supports cloud storage?*** for details.

7.2.4 Add Devices 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, Hik-Partner Pro will generate a QR code containing the device information. After completing device setup, you can share the QR code to your customer. And then your customer can scan the QR code via the Hik-Connect Mobile Client to add the device to her/his Hik-Connect account.

Before You Start

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

Steps

Note

- Devices added in this mode do NOT support the device handover process. If you need to hand over a device to your customer after completing the device setup work, please add it in one of following two methods: ***Add Detected Online Device*** or ***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. On the navigation pane, click **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your region).
2. Open the Add Device page.

   Note

   For details, refer to ***Add Device(s) after Batch Configuring Them*** .
3. Select **Enter IP Address / Domain** as the adding mode.
4. Enter the device's name, IP address/domain name, port number, 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.
5. Click **Add**.

   A QR code containing the device information will be generated and displayed in the device card on the site details page.

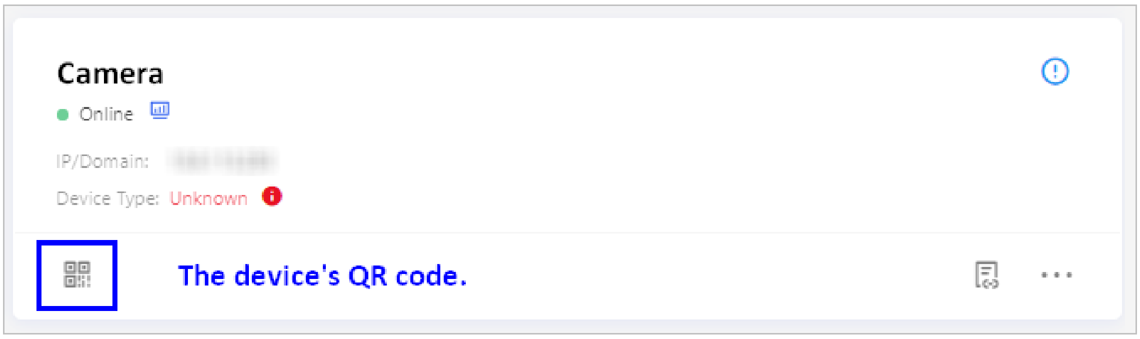


Figure 7-7 The QR Code of the Added Device

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

Encrypt Device QR Code

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

a. Click to display the QR code.
b. Create a password to encrypt the QR code, and then click **Save**.

View and Edit Device Information

Click the device's IP address or domain name to view the device basic information. If the device's information changed, or a network exception occurs, you can edit its information accordingly.

Select a device, and click • • • → to edit the device's name, IP address/domain name, port number, user name, and password.

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. Click **Set Device Type** and select a device type from the drop-down list. You can edit it again after the selection.

Activate Health Monitoring Service

Hover the cursor onto on the device card on the site details page, and then click **Activate Service**.

Note

- For details about how to activate the health monitoring service, see ***Activate the Health Monitoring Service for Devices*** .
- For details about the health monitoring service, see ***Health Monitoring Service*** .

Delete Device

Click • • • → .

Note

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

7.2.5 Batch Add Devices

You can batch add multiple devices to the client by entering the device parameters in a predefined template.

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

- The devices added in this mode cannot be handed over to your customer. If you need to hand over a device to your customer after completing the device setup work, please add it by Hik-Connect (P2P). For details, see ***Add Detected Online Device*** or ***Add Device by Entering Serial No.*** .
- Only encoding devices mapped in WAN support this function.

1. On the navigation pane, click **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your region).
2. Open the Add Device page.

   Note

   For details, refer to ***Add Device(s) after Batch Configuring Them*** .
3. Select **Batch Import** as the adding mode.
4. Click **Download Template** to save the predefined template (CSV file) in your PC.
5. Open the downloaded template file and enter the required information of the devices to be added in the corresponding column.
6. Click **Upload Template** to upload the edited template to Hik-Partner Pro.
7. **Optional:** Perform the following operations after adding the devices.

Encrypt Device QR Code	A QR code will be generated and displayed in the device information area. If an end user did not add the device to his/her Hik-Connect account, he/she can add it to the Hik-Connect account by scanning this QR code using Hik-Connect. a. Click to display the QR code. b. Enter a password to encrypt the QR code, and then click **Save**.
Activate Health Monitoring Service	Hover the cursor onto on the device card on the site details page, and then click **Activate Service**.

Note

- For details about how to activate the health monitoring service, see ***Activate the Health Monitoring Service for Devices*** .
- For details about Health Monitoring service, see ***Health Monitoring Service*** .

View and Edit Device Information	Click the device's IP address or domain name to view the device basic information. If the device's information changed, or a network exception occurs, you can edit its information accordingly. Select a device, and click ••• → ✎ to edit the device's name, IP address/ domain name, port number, user name, and password.
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. Click **Set Device Type** and select a device type from the drop-down list. You can edit it again after the selection.
Delete Device	Click ••• → 🗑 . **Note** • Deleting device (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.

Note

- It is highly recommended to encrypt the device QR code for security reasons.
- 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.
- 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 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.

7.2.6 Synchronize Devices with Hik-Connect Account

You can synchronize devices in your Hik-Connect account with devices in the Hik-Partner Pro account. After synchronization, the devices are still managed in your Hik-Connect account and you can continue to use Hik-Connect service.

In the following two cases, you need to synchronize devices in the Hik-Connect account with devices in the Hik-Partner Pro account.

- **Case 1**: Before using Hik-Partner Pro, you managed the devices for the customer by the Hik-Connect Mobile Client after the customer shares her/his devices to your Hik-Connect account.
- **Case 2**: Before using Hik-Partner Pro, you already have a Hik-Connect account and have added device(s) to it.

Under the above two circumstances, you can synchronize these devices (including the ones the customers shared to you, or the ones added in your Hik-Connect account) with the Hik-Partner Pro account for quick and convenient devices adding and better device management and maintenance.

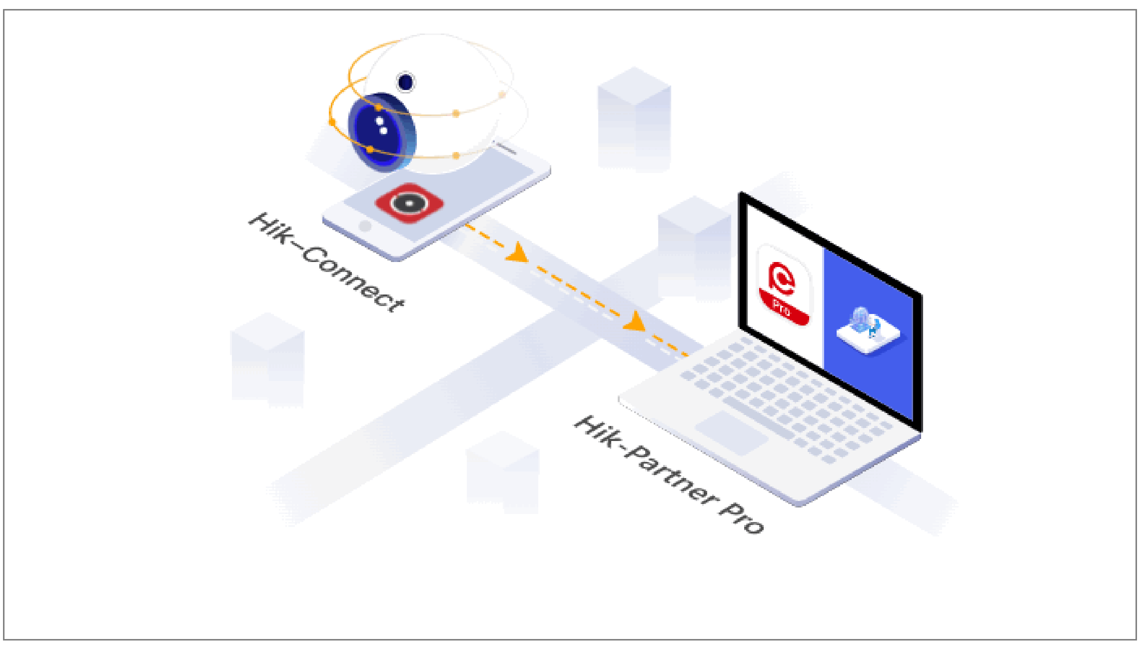


Figure 7-9 Synchronize Devices With Hik-Connect Account

There are three entries.

- On the Customer Site page, click **Synchronize Devices from Hik-Connect** on the top of the site list.
- On the Add Device page, click **Synchronize Devices from Hik-Connect**.
- Click the user name in the upper-right corner, click **Link with Hik-Connect Account** in the drop-down menu, and click **Link with Account**.

Log into Hik-Connect

First, you need to log into **Hik-Connect** by entering your account or by scanning QR code.
(Optional): Check **Get Your Account and Device Information** to allow Hik-Partner Pro to get these information.
Check **Authorize Automatic Device Synchronization from Your Account to the Current Hik-Partner Pro Account** to authorize automatic device synchronization. After authorization, devices newly added to Hik-Connect will be automatically synchronized to Hik-Partner Pro.

Select Device for Synchronization

Secondly, you need to select the devices for synchronization.
After login, the devices added to your Hik-Connect account, as well as the ones others shared to you, will be displayed in the device list.
You can filter the devices by selecting **Show All Devices**, **Show My Devices Only** (the devices added to your Hik-Connect account), or **Show Others' Devices Only** (the devices shared to your Hik-Connect account from the customer) in the drop-down list.
Select the devices you want to synchronize with Hik-Partner Pro account, and click **Next**.

Configure Site for My Devices

Thirdly, you need to set the site information in Hik-Partner Pro for your devices to be synchronized.
For the devices added in your Hik-Connect account (displayed in My Devices list), you can add them to different sites or to the same site according to your actual needs.

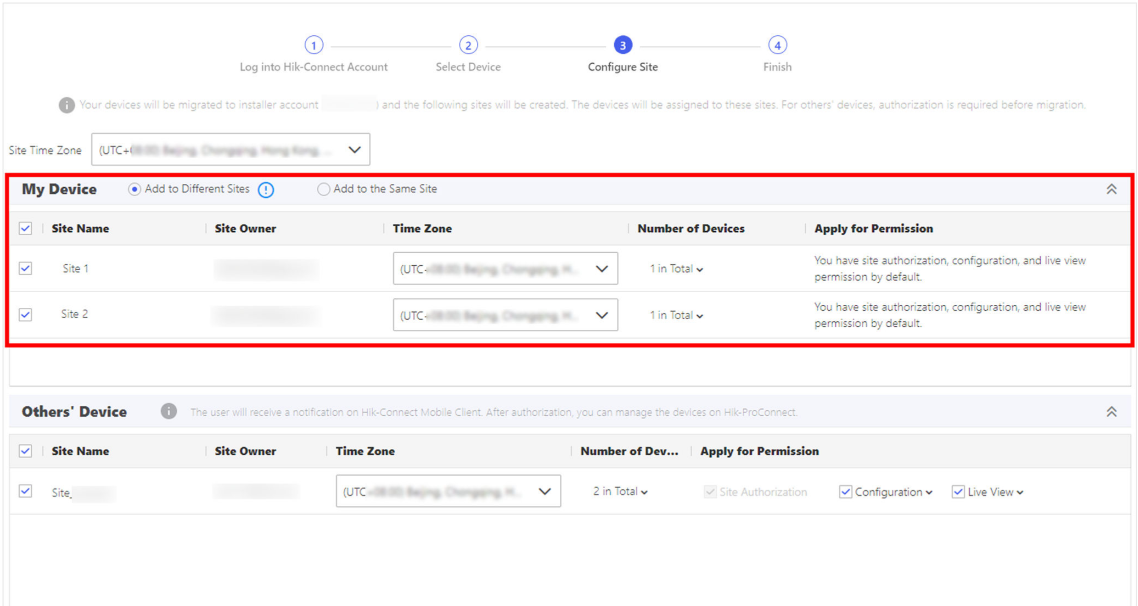


Figure 7-10 Configure Site for My Devices

Add to Different Sites

If your devices are shared to different customers, select this option and you can add them to different sites.

For the devices which have been shared to the customers, the system will automatically create sites by the user names of the customers, and then add the devices to these sites. If there already exists a site the site owner of which is the customer, the information of this site (site name and time zone) will be displayed and the corresponding devices will be added to this site automatically.

For the devices which are not shared to anyone, the system will automatically create a site named after your Hik-Connect account user name, and then assign them to this site.

You can hover over the site name and click to edit the site name.

Add to the Same Site

You can also add these devices to the same site. The system will automatically create a site named after your Hik-Connect account user name, and then add all these selected devices to this site.

You can hover over the site name and click to edit the site name.

By default, after synchronization, you will have site authorization permission of the automatically created site(s), and configuration as well as live view permission of the devices in My Devices list.

Configure Site and Permissions for Others' Devices

Fourthly, you need to set the site information in Hik-Partner Pro and set the device permission for the devices shared to you.

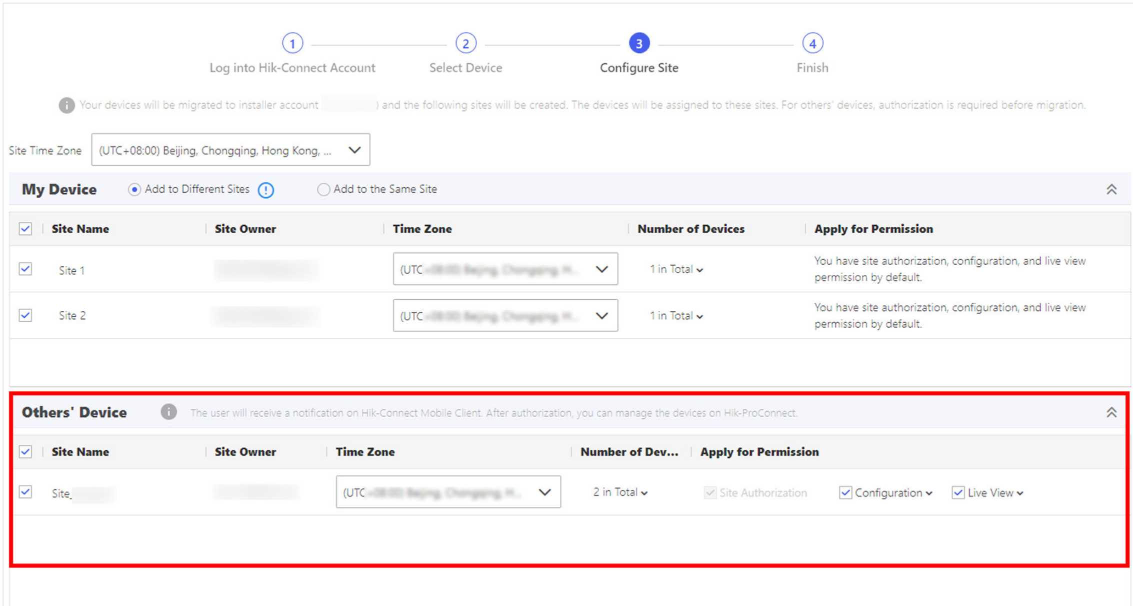


Figure 7-11 Configure Site and Permissions for Others' Devices

For the devices shared to you by others, usually customers, (displayed in Others' Devices list), they will be added to different sites. The system will automatically create sites named after the user names of the customers, and then add all these selected devices to this site. If there already exists a site the site Owner of which is the customer, the information of this site (site name and time zone) will be displayed and the corresponding devices will be added to this site automatically.

You can hover over the site name and click ✎ to edit the site name.

In the **Apply for Permission** list, you need to select the permissions that you want to apply from the customers for the devices. By default, you will have site authorization permission of the automatically created site(s). After synchronization, the customers will receive a notification on Hik-Connect Mobile Client. After authorization by the customers, you can manage the devices on Hik-Partner Pro.

Set Time Zone

Fifthly, you can set the time zone of the devices if needed.

You can set the time zone for each device, or you can select a time zone in the **Set Time Zone** drop-down list at the upper-left corner to set a time zone for the devices in a batch.

Start Synchronization

Finally, start device synchronization.

After setting the sites and device permissions, select the devices in the My Devices and Others' Devices list, and click **Synchronize** to start synchronization.

For devices shared from the customers in Others' Devices list, the system will send a request to the customers. After the customers approving the authorization request, the devices will be synchronized successfully.

Click **Continue** to select other devices for synchronization, or click **Finish and View** to view the devices synchronized after creating sites in the site list.

7.2.7 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, exception rule, and remote configuration) 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 Entering Serial No.*** or ***Add Detected Online Device*** .

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 device, in addition to the above-mentioned features, linkage rule is not supported as well.

---

1. On the navigation pane, click **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your region).
2. Click the name of a site with Hik-ProConnect boxes added.

   You enter the site details page.
3. Click a Hik-ProConnect box to show its details panel, and then select **Proxied Device → Add To-Be-Proxied Device** to enter the following page.

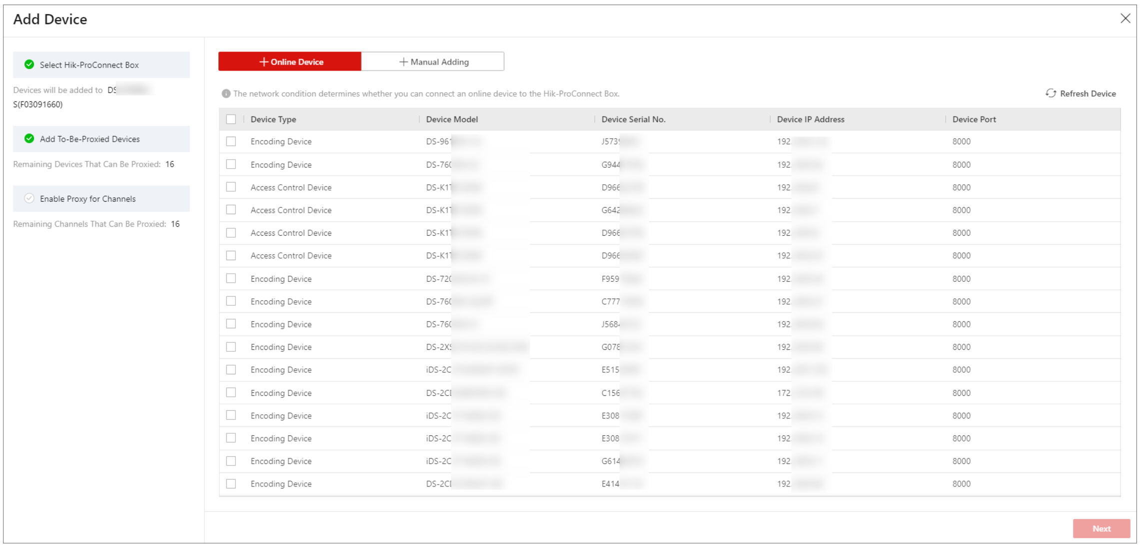


Figure 7-12 Add To-Be-Proxied Devices

4. Add devices in one of the following two ways.

Table 7-5 Add Devices

Way	Description
Online Device	Add devices on the same LAN with the Portal. a. Select devices, and then click **Next**. b. Select all devices, and then click **Batch Verification** to set a user name and a password shared by all devices. Or enter the device user name and password for each device. c. Click **Next**.
Manual Adding	Add a device manually. a. Click **Add Device**. In the Manual Adding window, select the target Site, and then enter the device IP address and device port No. b. Click **OK** and the device will be displayed in the device list. c. Click **Enter user name and password.** in the User Name/ Password column to enter the device user name and password.

Way	Description
	Note You can also add multiple devices first, and then click **Batch Verification** to set a user name and a password shared by all these devices. d. Click **Next**.

The adding result page shows.

5. If adding failures exist, you can view the failure reasons on the adding result page and do corresponding operations (e.g., entering password again if the failure is caused by incorrect password).
6. Click **Next**.
7. If there are encoding devices, enable proxy for channels of encoding devices before you can view live video and video footage of these channels.
   1) Click **Enable Proxy** in the Operation column.
   2) Select channels and then click **OK**.
8. Click **Complete**.
9. **Optional:** View the proxy information on the device details page of the Hik-ProConnect box.

7.3 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 to needs to have been authorized to you.
  - The device needs to be added by Hik-Connect (P2P). 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 need to configure these related configurations again also.

1. Go to **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your country or region).
2. Click the name of an authorized Site to enter its details page.
3. Click **Move Device** to open the Move Device pane.

4. Click **Select Device to Move**, select device(s), and click **Next**.

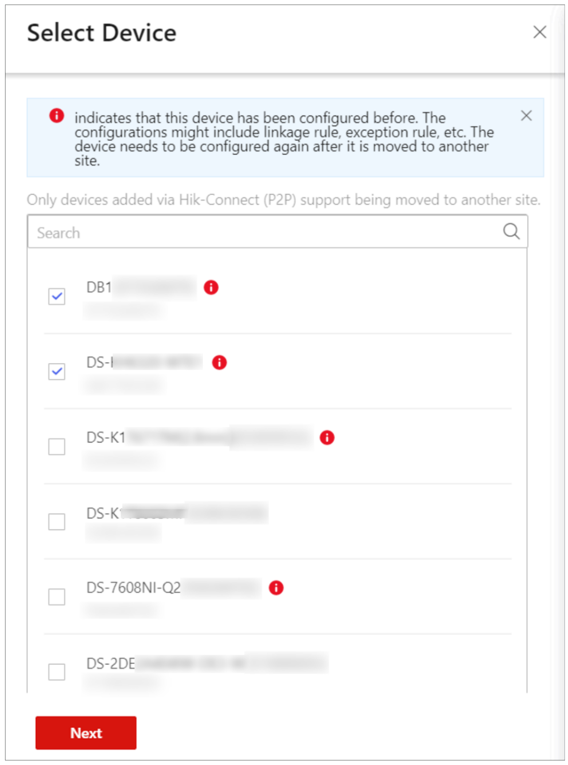


Figure 7-13 Select Device

5. Select a Site.

Note

- **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.

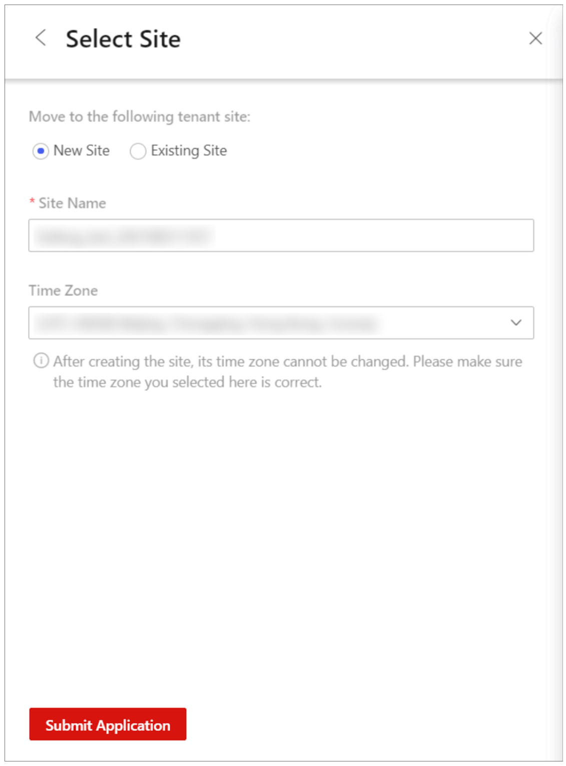


Figure 7-14 Select Site

6. Click **Submit Application**.

Note

The application will expire if not handled within 7 days.

7. **Optional:** On the Move Device pane, click **View Device Movement Record** to enter the Device Movement Record page, and perform the following operation(s) if needed.

Apply Again	Click **Apply Again** to send an application for device movement again if the former one has been rejected or expired.
View Details	Click an application record to enter its details page to see the details.
Move More	Click an approved or sent application, and then click **Move More** to move more devices.

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, and if you need to view the live view/recorded videos of devices added to the Site or configure the devices added to the Site, you can apply for the permission accordingly from the end user.

Steps

1. Click the name of a Site to enter the site details page.
2. On the **Device** tab, click **Apply for Permission → Apply for Configuration Permission/Apply for Live View Permission/Apply for Playback Permission** .
3. Check device(s) you want to apply for permission, and click **Apply**.
4. In the **Validity Period** drop-down list, select a validity period for the permission.

   Note

   You can select **Permanent**, **1 Hour**, **2 Hours**, **4 Hours**, or **8 Hours** as the validity period.
5. **Optional:** Enter the remarks for the permission.
6. Click **Apply** to apply for the permission from end user.

   If the end user approves your application, you will get corresponding permission(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 handed over to you.

Steps

1. Click a site in the site list to enter the site details page.
2. Click a device to show the device details page.
3. In the Permission section, select a permission, and click → **OK** 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 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.

7.5.1 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.

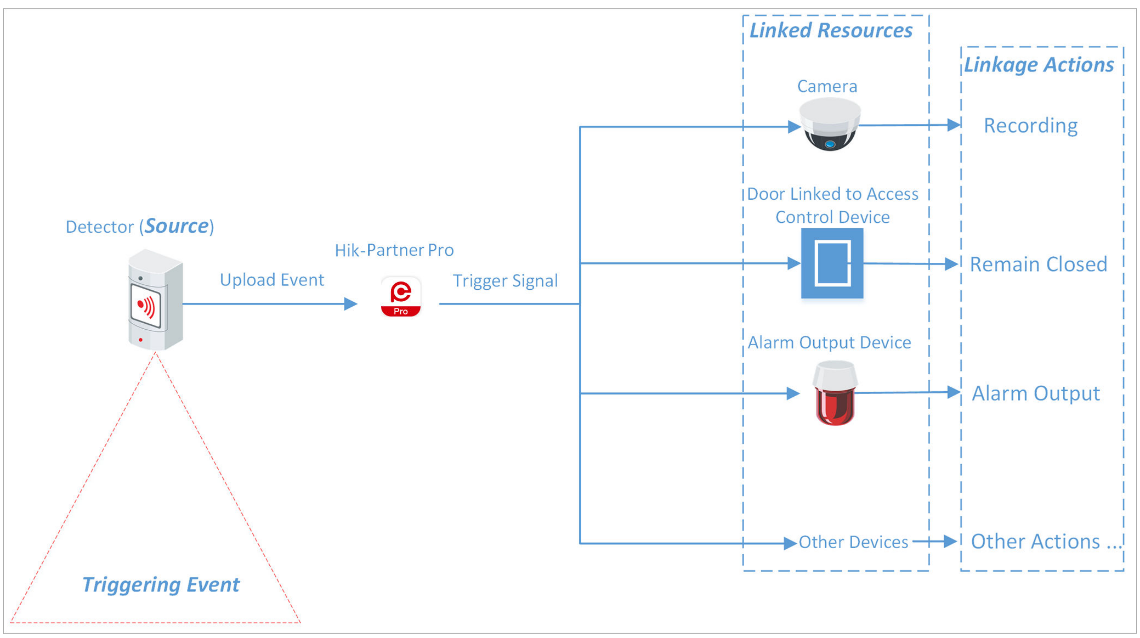


Figure 7-15 Linkage

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 resource.
- 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.
- If the Source or Linked Resource is an AX security control panel, when EN50131 Compliant mode is enabled on the device, make sure that you have done authentication by entering the device password, otherwise the configuration of linkage rule will fail.
- 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. On the navigation pane, click **Customer Site** to enter the site list page.
2. Open the Add Linkage Rule panel.
   - Select a site and click ··· → in the Operation column.
   - Click the name of a site to enter the site details page, and then click **Linkage Rule → Add Linkage Rule** .
   - Click the name of a site to enter the site details page, and then select a device and click .
3. Set the required information.

   Linkage Rule Name

   Create a linkage rule name.

   Trigger

   Define the trigger for the linkage action.

Select Source

Select a resource as the Source.

Set Triggering Event

Select an event as the triggering event.

Note

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

Table 7-6 Available Triggering Events for Different Resource Types

Resource	Triggering Event
Camera	• Motion Detection • Face Detection • Intrusion • Line Crossing Detection
Access Control Device	• 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 • 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 Triggering Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm.
Doorbell	• Calling • PIR Detection

Linkage

Click **Add** to select Linkage Action(s) and Linked Resource(s).

Note

- After selecting a Linkage Action, the resource(s) available to be set as Linked Resource(s) will appear.
- Up to 128 Linkage Actions or 10 Linked Resources can be selected.

Linkage Action

Select linkage action(s).

Table 7-7 Linkage Action Description

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

Linked Resource	Linkage Action	Description
		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. **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.

Linked Resource	Linkage Action	Description
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.

Linked Resource

Select resource(s) as the trigger source of the Linkage Action.

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.

Note

After selecting Linkage Action(s) and Linked Resource(s), you can check the check-box(es) and then click **Delete** to delete the selected Linked Action(s) and Linkage Resource(s).

Linkage Schedule

Define the scheduled time during which the linkage is activated.

All Days

The external 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.

4. Click **OK**.

   The linkage rule will appear on the Linkage Rule list.

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

Edit Linkage Rule	Click ··· → to edit the linkage rule.
Delete Linkage Rule	Click ··· → to delete the linkage rule.
Disable Linkage Rule	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 of Portal 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 table below) of linkage rule.

Before You Start

Make sure you have the permission for the configuration of the devices. If not, you need to apply for the permissions first. For details about applying for permission, see ***Apply for Device Permission*** .

Table 7-8 Template Description

Template	Description
Intrusion	The Intrusion Template: Used for improving security level by triggering the linkage actions including capture, recording, and alarm output, when the intrusion event (people, vehicles, or other objects enter a pre-defined area) occurs.
Forced Entry Alarm	The Forced Entry Alarm Template: Used for improving security level by triggering the linkage actions including capture, recording, remaining door closed, alarm output, and calling preset when a door is opened abnormally.
Back to Home/Office	The Back to Home/Office Template: Used for lowering the security level and enabling privacy protection by triggering the linkage actions including disarming and enabling privacy mask, when you are back to home or office.
Away	The Away Template: Used for improving security level and canceling privacy protection by triggering the linkage actions including arming and disabling privacy mask when you leave your home or office.
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. On the navigation pane, click **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your country or region).
2. Open the Add Linkage Rule panel.

- Click the name of a site to enter the site details page and select the **Linkage Rule** tab, and then click **Forced Entry Alarm** template in the Linkage Template area.
- Click ··· → in the Operation column, and then select the **Forced Entry Alarm** template from the left side of the Add Linkage Rule panel.
- Click the name of a site to enter the site details page, click **Add Linkage Rule** and then select the **Forced Entry Alarm** template from the left side of the Add Linkage Rule panel.

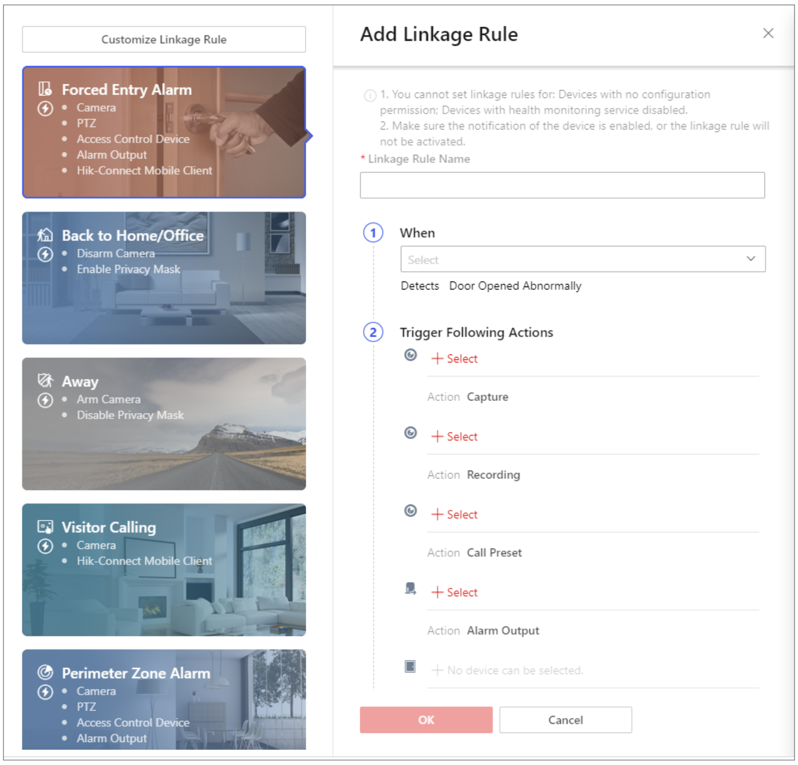


Figure 7-16 Add Linkage Rule by Template

3. 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

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

Note

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

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.

4. Click **OK**.

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

5. **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, 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.

7.5.2 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. For applying 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 a notification. 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. On the navigation pane, click **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your country or region).
2. Click the name of a site to enter the site details page, and then click **Exception**.

   The exception rules of all the devices added in this site are displayed by default.
3. **Optional:** Click **Unfold Channels** to display all the channels of the device.

   Example

   For security control panels, all the zones and alarm outputs are displayed.
4. Set the types of exceptions which can trigger the notification.

   1) Move the cursor to the **Exception** field of the device or channel and click .

Figure 7-17 Edit Exception

   2) Check the exception type(s) that you want to set exception rules for.

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.
- For network switch, you can set exception rules for the following: PoE Port Power Off, SFP Port Disconnected, RJ45 Port Disconnected, Port Blocked, Port Busy, and PoE Power Exceeds Limit.

3) Click **OK**.

5. Set where the notifications will be sent.
   1) Move the cursor to the **Received by** field and click .
   2) Check the receiving mode(s) according to actual needs.

Portal

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

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

Note

For checking the received notification in Portal, refer to ***Exception Center*** .

Hik-Partner Pro App

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

Email

When an exception is detected, the device will push an 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) Click **OK**.

6. Set who will receive the notification.
   1) Move the cursor to the **Recipient** field and click .
   2) 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 checked by default and you cannot edit it.
- If you select **Hik-Connect App (Site Owner)** in the previous step, your customer will receive the exception notifications.

3) Click **OK**.

7. Set when the recipient can receive the notification.
   1) Move the cursor to the **Schedule** field and click .
   2) Select the schedule.

   All Day

   The recipient can always receive the notification from Monday to Sunday, 7 days × 24 hours.

   Custom

   Customize the days and time period on the selected days according to the actual needs.

   3) Click **OK**.
8. **Optional:** Set or edit the exception rules of the devices in the site in a batch.
   1) Click **Batch Edit**.
   2) Check the devices or channels you want to set the exception rules.
   3) Click in the bottom to set/edit the exception types, receiving mode, recipient, and notification time.

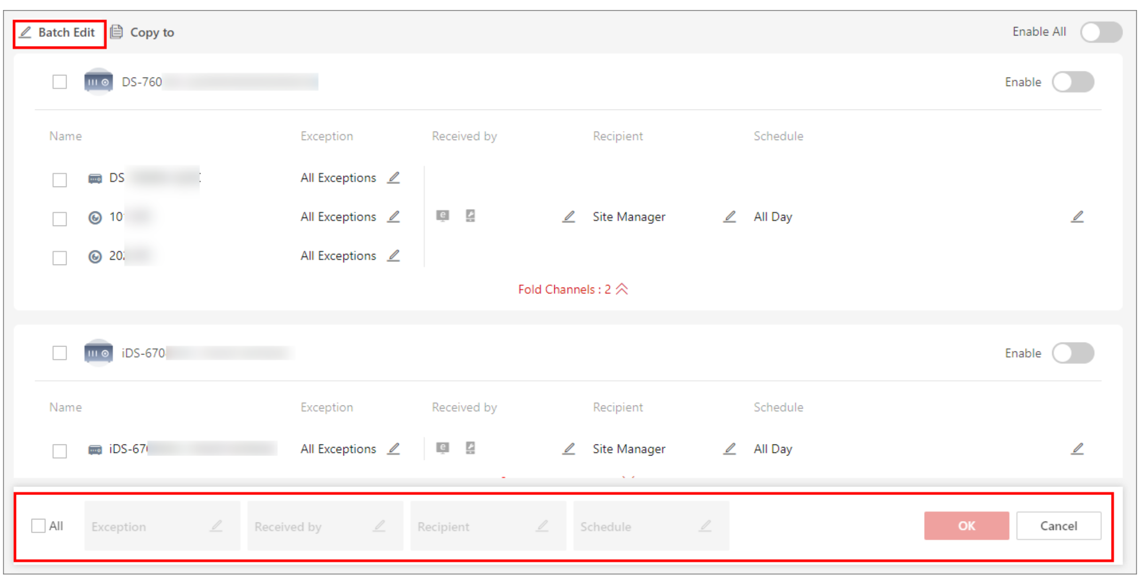


Figure 7-18 Batch Set/Edit Exception Rules

   4) Click **OK** to save the settings.
9. **Optional:** After setting one rule, you can copy the rule settings to other devices or channels for quick settings.
   1) Click **Copy to**.

2) In the **Copy Exception Settings from** field, select device(s) or channel(s) as the sources.
3) In the **To** field, select the target resources of the same type as the selected sources.
4) Click **Copy** to copy the rule settings of the sources to the target resources and back to the exception rule list. Or you can click **Copy and Continue** to copy the rule settings and continue to copy other settings.

10. After setting the exception rule, you need to set the **Enable** switch in the upper-right corner of the rule to on to enable the device's exception rule, or set the **Enable All** switch to on to enable the all the devices' exception rules in the site.

    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.

7.5.3 Enable Device to Send Notifications

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

Steps

Note

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

1. On the navigation pane, click **Site & HCC → Customer Site** (or **Customer Site** if HikCentral Connect is not available in your country or region).
2. Click a site in the site list to enter the site details page.
3. Select the **Device** tab.
4. Click ··· → 🔔 to open the Notification Settings window.

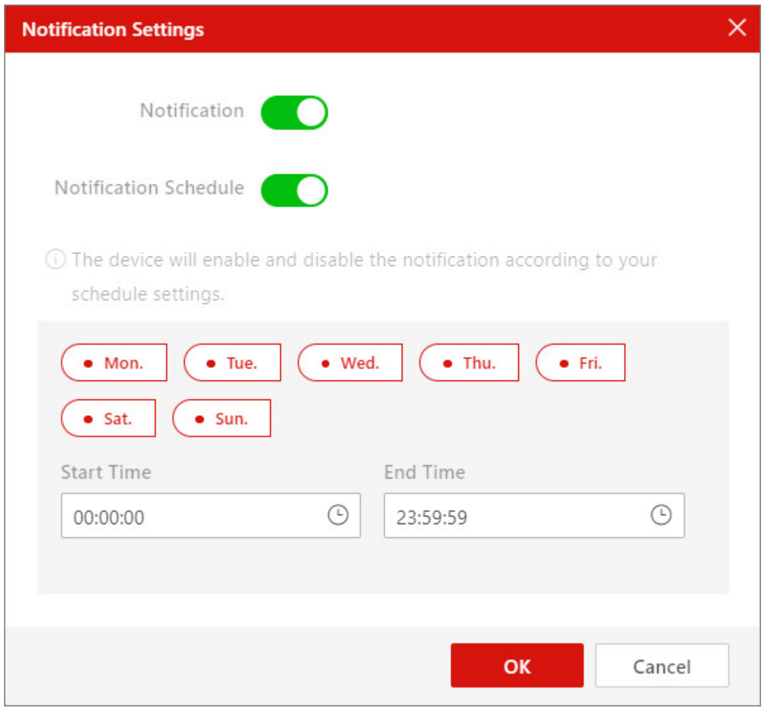


Figure 7-19 Notification Settings

5. Set the parameters.

   Notification

   Make sure the functionality is enabled.

   Notification Schedule

   After enabling the Notification functionality, set a time schedule for uploading the events detected by the Source to the Hik-Partner Pro system and the Hik-Connect Mobile Client.

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

6. Click **OK**.

Note

- Please notify the end user after handing over the site to her/him 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.

7.6 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 the 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*** .

On the navigation pane, click **Site** to enter Site page.

Select the device and click ••• → **Reset Device admin Password** . There are two methods to reset 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.

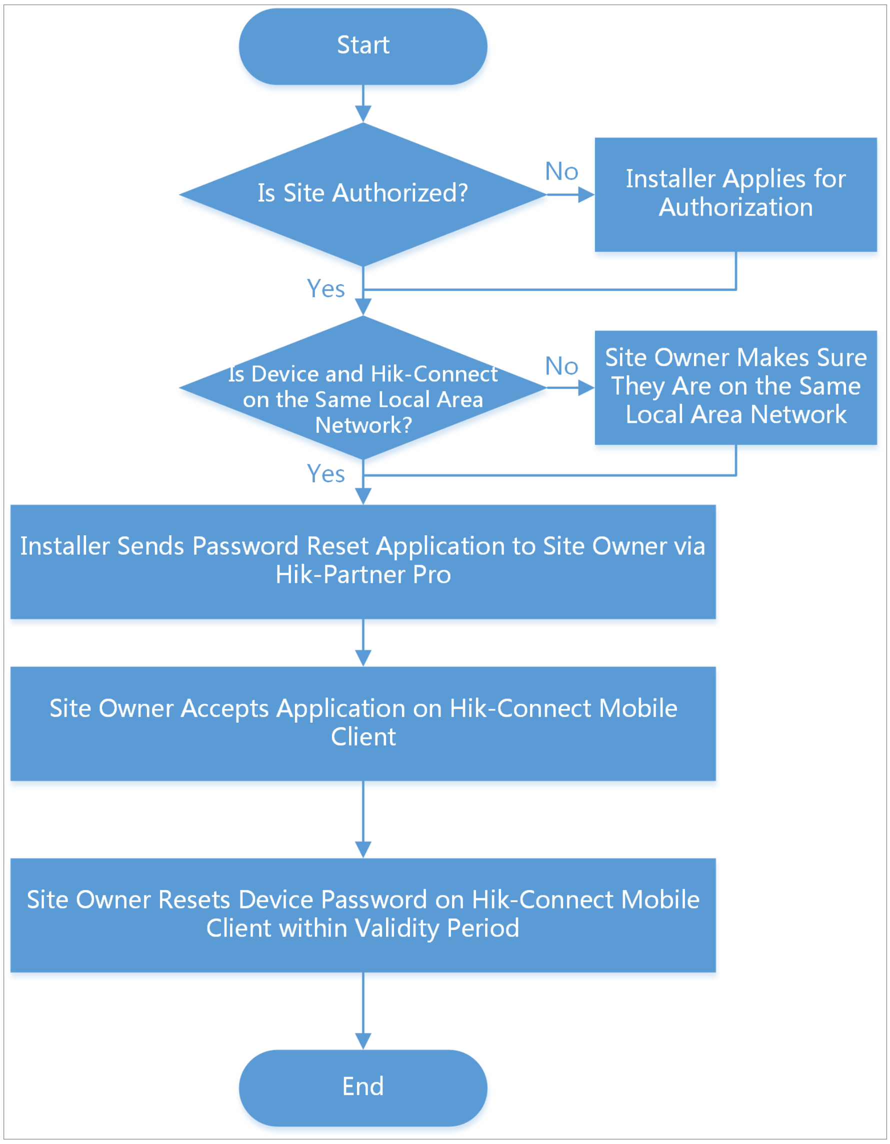


Figure 7-20 Flow Chart of Resetting Device Password Offsite

- **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.

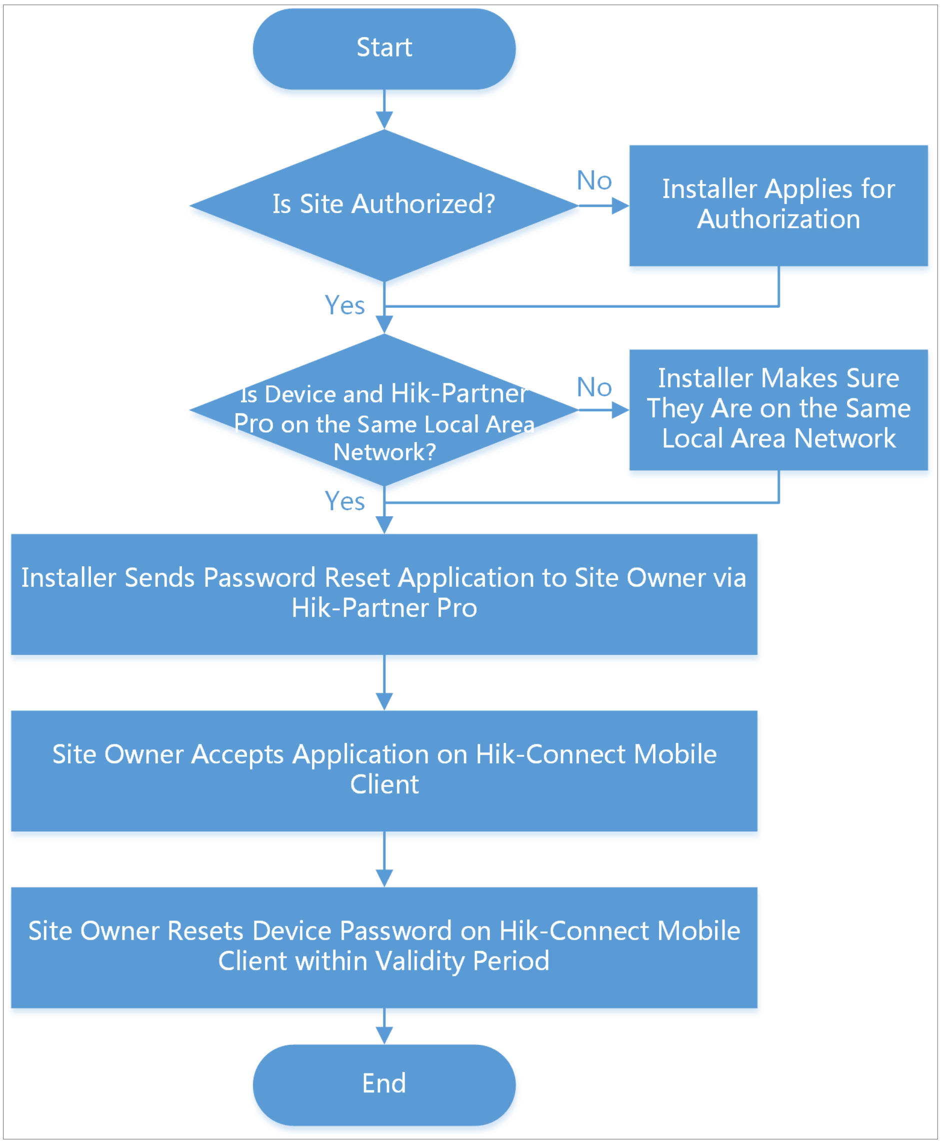


Figure 7-21 Flow Chart of Resetting Device Password Onsite

7.7 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 supports 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. Enter the site list page.
2. Click a site to enter the site details page.

   The devices added in the current site are displayed.
3. Find the device in the device list, and click **Remote Log Collection**; or click the device to enter its details page, and click **Remote Log Collection**.

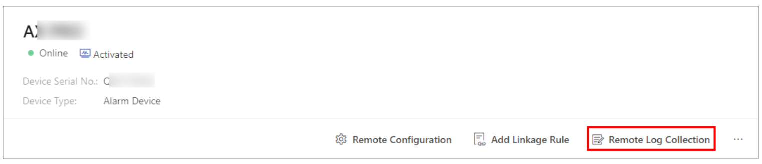


Figure 7-22 First Entry to Remote Log Collection

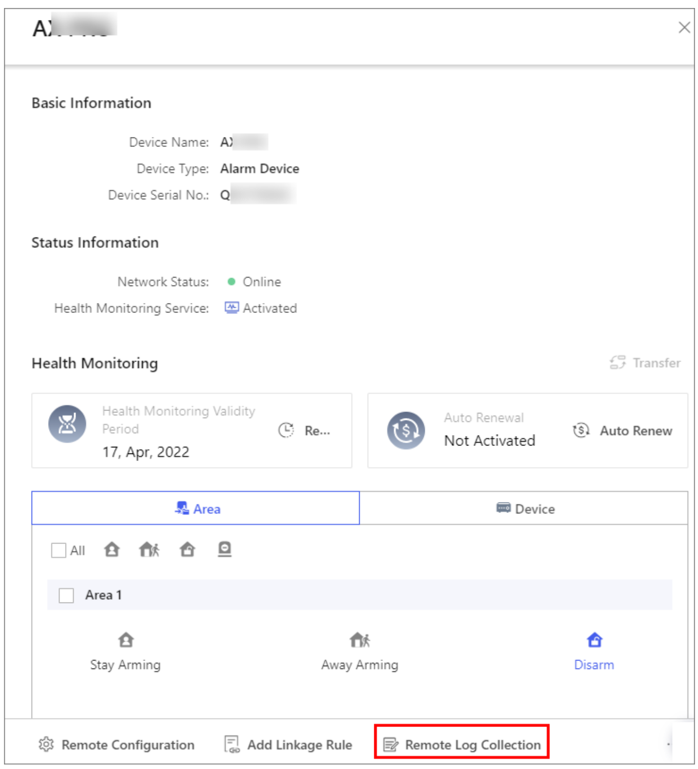


Figure 7-23 Second Entry to Remote Log Collection

The Remote Log Collection window pops up.

4. Click **Authorize**.
5. Select the validity period from the drop-down list.

Note

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

6. Click **Enable** to enable the function.

   The Remote Log Collection icon turns from to .
7. **Optional:** Disable the function.
   1) Click **Remote Log Collection**.
   2) Click **Deauthorize** in the pop-up window.

7.8 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"), including batch arming/disarming and batch device configuration by template.
- 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 enabling ARC service, running health monitoring, setting rules for linkage or exception reporting, and configuring parameters remotely. For details, refer to ***Enable ARC Service for Devices*** , ***Health Monitoring*** , ***Linkage Rule and Exception Rule*** , and ***Remote Configuration*** respectively.

7.8.1 Control AX PRO and AX HYBIRD PRO

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

Click **Site & HCC → Customer Site** or **Customer Site** to enter the site list page, and then click the name of a site to enter site details page.

Click the AX PRO or AX HYBIRD PRO device to open the operation panel. You can perform the following operations.

Function	Operation
Stay Arm an Area	Select the **Area** tab, and then click **Stay Arming** to stay arm the area.
Away Arm an Area	Select the **Area** tab and then click **Away Arming**.
Disarm an Area	Select the **Area** tab and then click **Disarm**.
Stay Arm Multiple Areas	Select the **Area** tab. Select areas and click .

Function	Operation
Away Arm Multiple Areas	Select the **Area** tab. Select areas and click .
Disarm Multiple Areas	Select the **Area** tab. Select areas and click .
Clear Alarms of Multiple Areas	Select the **Area** tab. Select areas and click . **Note** This function is not supported by the AX HYBIRD PRO device.
Filter Peripheral Device by Area	Select the **Device** tab. Click and select an area to only display the peripheral devices linked to the selected area, or select **All** to display all peripheral devices linked to all the areas. **Note** The AX HYBIRD PRO device only supports adding keyfobs as the peripheral device.
Bypass Zone	Select the **Device** tab. 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.

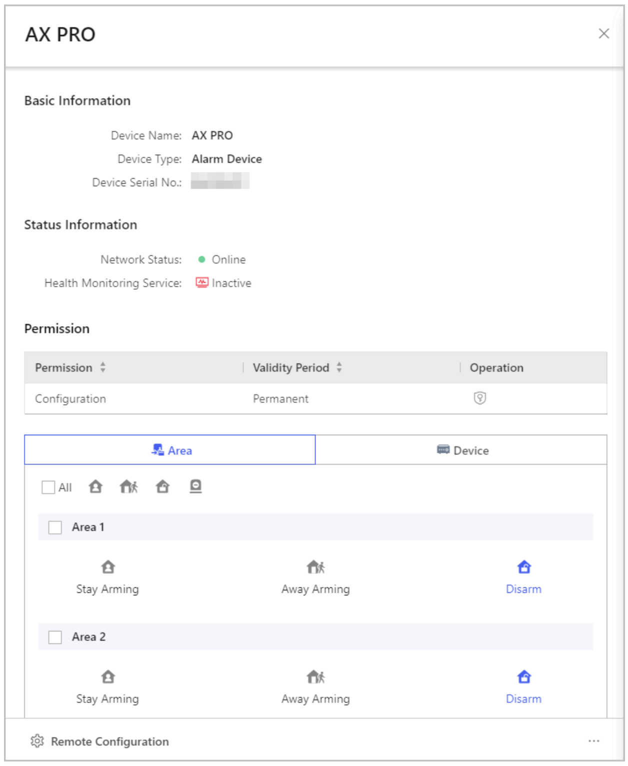


Figure 7-24 Operation Panel of AX PRO

7.8.2 Configure AX PRO and AX HYBIRD PRO

You can remotely configure AX PRO and AX HYBIRD PRO device parameters, apply for PIN (required for upgrading firmware), and switch the language of the device.

Click **Site & HCC → Customer Site** or **Customer Site** to enter the site list page, and then click the name of a site to enter site details page.

Remotely Configure AX PRO / AX HYBIRD PRO

You can click **Remote Configuration** to enter the web page of the device to configure its parameters.

Note

For details about remote configuration, see the user manual of the device.

Apply for a PIN

You can click ••• → **Apply for a PIN** to get a PIN code for verification.

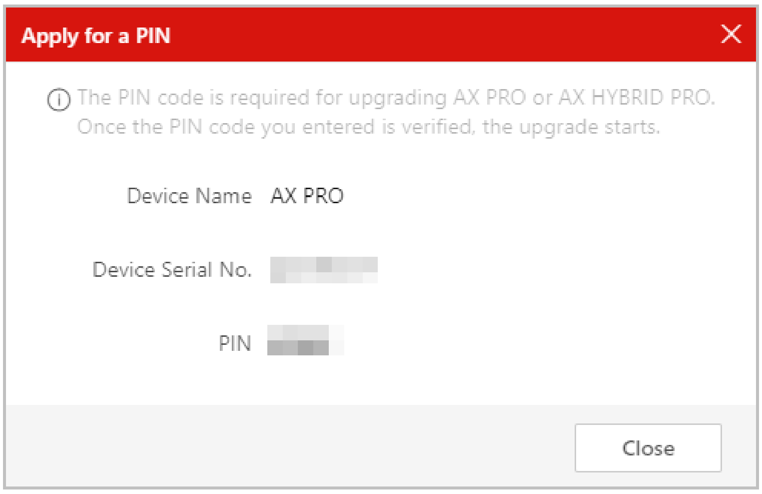


Figure 7-25 Apply for a PIN

Switch Language

You can click ● ● ● → ⇆ **Language** and set the device language. After you click **OK**, a pop-up window will ask you if you need to reset the names of the device and its areas. Click **Reset** to switch the device language and switch the names to the default names in the switched language; click **Cancel** to switch the device language only.

Note

A PIN code is required for switching language.

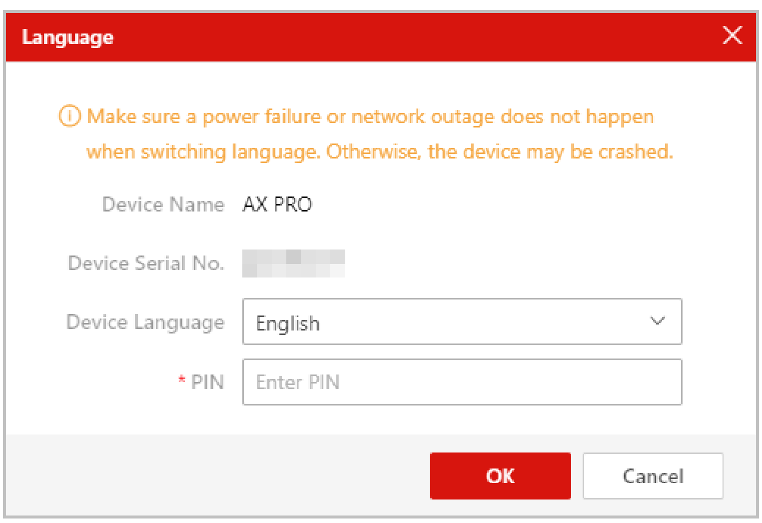


Figure 7-26 Language Window

7.8.3 Batch Configure AX PRO

You can batch configure parameters for the added AX PRO devices by creating templates. You can also batch upgrade the firmware of multiple AX PRO devices.

Note

- Only AX PRO devices (Version 1.1.0 and later) and AX HYBRID PRO devices are supported.
- The function is only supported in certain countries and regions.

Create a Template

You can create a template for batch configuring parameters of AX PRO devices.

1. Go to **Install & Config → Remote Batch Config → Manage Template** to enter Manage Template page.
2. Add a template.
   - Click **Add Template** for adding a template for the first time.
   - If not, click + .
3. Edit the template by configuring parameters as needed, and these configured parameters can be batch applied to AX PRO devices later. See the following for the detailed parameters explanations.

Arming Schedule

Enable auto Arm

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

Enable 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 the area will not be armed or disarmed on the weekend.

Holiday Exception

Enable the function and set the holiday schedule. The area will not be armed or disarmed on the holiday.

Note

You can set up to 12 holiday groups.

Panel Alarm Duration

The time duration of the panel alarm.

Alarm Receiving Center

Protocol Type

Select **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, ***ADM-CID**, **CSV-IP**, **FSK Module**, **RDC Module** and **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 Name** as the address type, and enter the IP address or domain name of the alarm receiver server accordingly.

Port No. (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 from.

Impulse Counting Time

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

Attempts

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

Polling Rate

Enable the function and set the interval between 2 live polling.

Event Types Notification (Alarm Receiving Center)

Select which alarm receiving center to receive event notifications and the corresponding event types, including alarms and tampers, life safety alarms, maintenance and faults, zone alarm/lid opened, 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.

FTP Settings

Address Type

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

Port No.

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.

Batch Configure AX PRO by Template

You can batch configure parameters for AX PRO devices by the predefined template.

Steps

1. Go to **Install & Config → Remote Batch Config** .
2. Select multiple AX PRO devices to be configured.
3. Click **Set Parameters by Template**.
   A window of Set Parameters by Template pops up on the right side.
4. Select a template from the list.

Note

- If you have not added a template, you should click **Manage Template** to enter Manage Template page and add a template for AX PRO devices. For details, refer to ***Create a Template*** .
- You can view the general template content on the lower side.

5. **Optional:** Click **Details** to view the details of the template.
6. Click **Apply** to start applying parameters to the devices.

What to do next

View the applying results. If applying failed, you can view the failure reasons.

Batch Upgrade AX PRO

You can batch upgrade the firmware of multiple AX PRO devices to ensure the proper functioning of these devices. If the firmware version of an AX PRO device is too old, some features might be unavailable.

Steps

1. Go to **Install & Config → Remote Batch Config** to enter the page shown below.

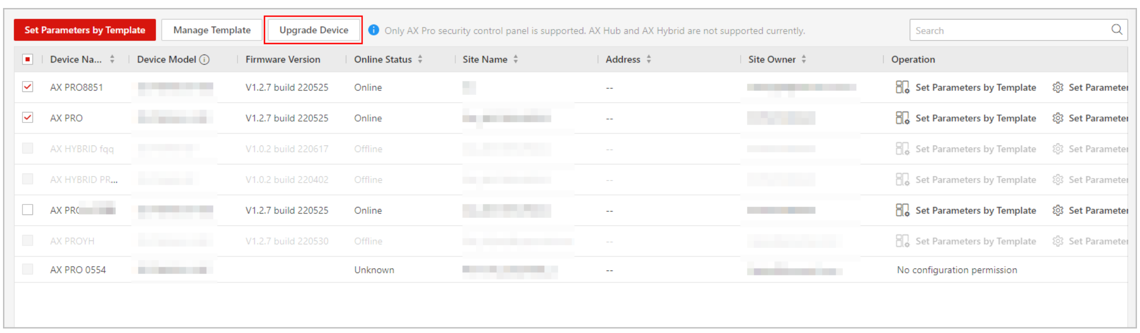


Figure 7-27 Remote Batch Configuration

2. Select AX PRO devices and then click **Upgrade**.

   The **Upgrade Device** window will pop up.
3. Click **Apply for a PIN** to get one.

   The PIN code will be automatically entered.
4. Click **Update**.

7.8.4 Batch Arm/Disarm AX PRO and AX HYBRID PRO

You can batch arm or disarm multiple AX PRO / AX HYBRID PRO devices on multiple sites by grouping the devices. For example, assume that your customer needs to have her office building cleaned in the period from 7:00 a.m. to 8:00 a.m. everyday, you can add all the AX PRO / AX

HYBRID PRO devices in the building to a group and then disarm the group in the period everyday to avoid the nuisance of false alarms triggered by the cleaning.

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 available in some countries/regions.

1. Go to **Install & Config → Batch Arm/Disarm** .

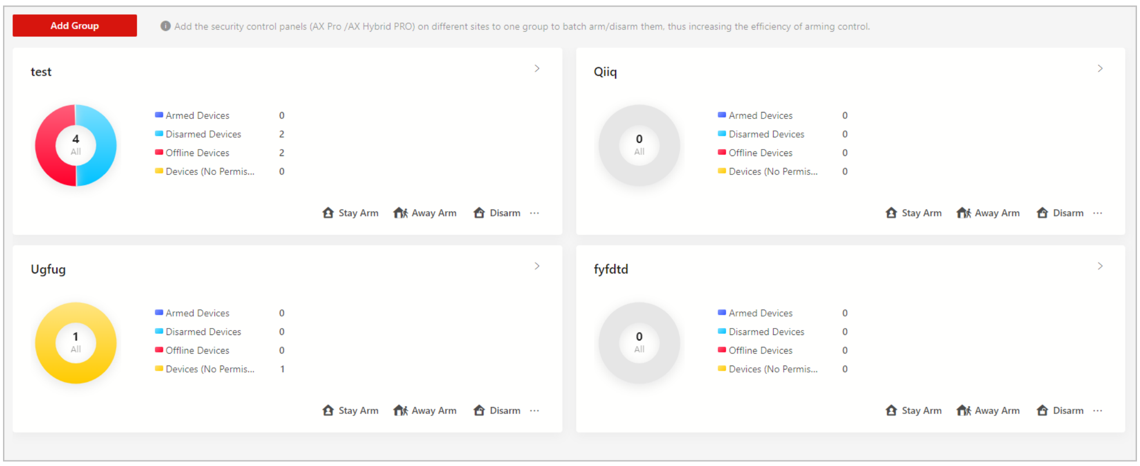


Figure 7-28 Batch Arm/Disarm Page

2. Click **Add Group**.
3. Create a name for the group.
4. Add devices to the group.
   1) Click **Add** and select the devices in different Sites.

   Note

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

   2) Click **OK**.
   3) **Optional:** Select devices and click **Delete** to remove them from the group.
5. Click **OK**.

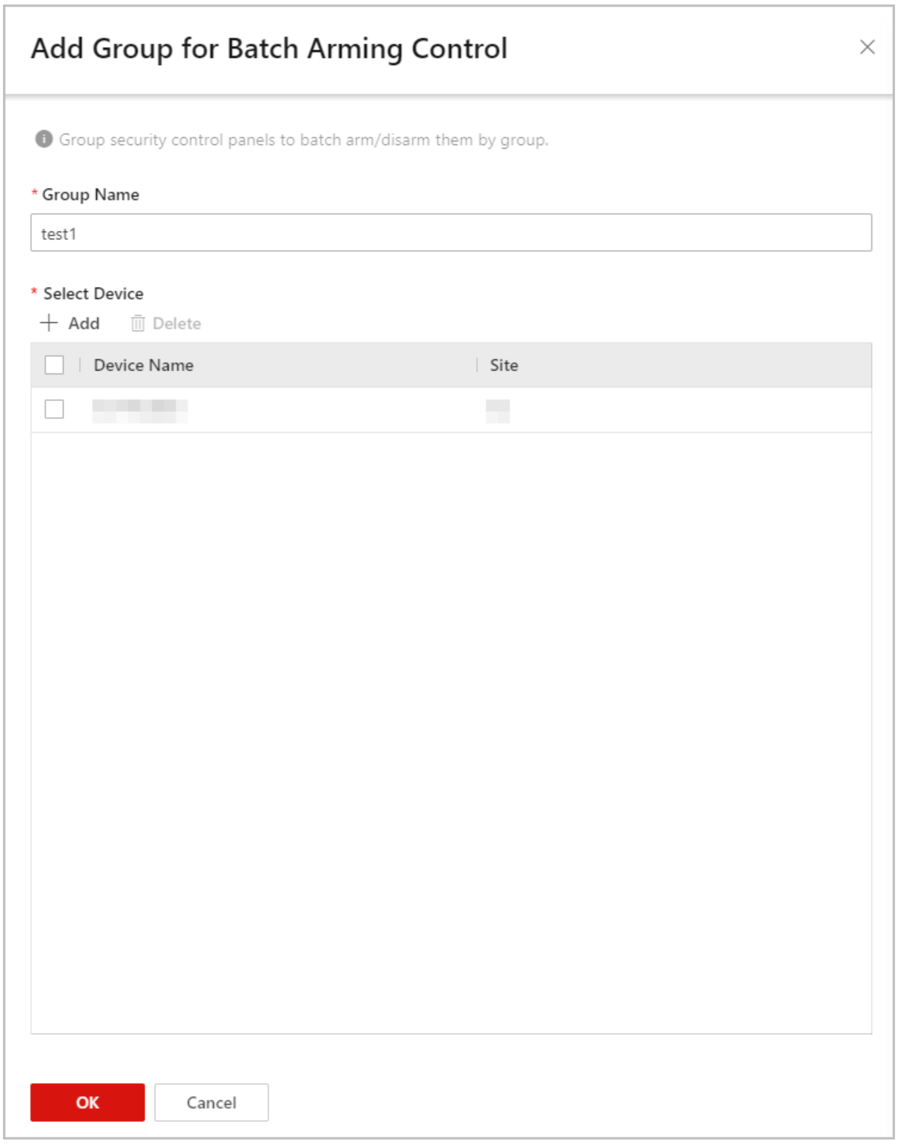


Figure 7-29 Add Group for Batch Arming Control

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

View Group Details	Click on the group to view its details, including devices in the group and their arming/disarming status.
Arm/ Disarm Group	Click **Stay Arm** or **Away Arm** to arm all devices in the group. Or click **Disarm** to disarm the group.

Note

- If you leave the page after starting arming/disarming, you can click in the upper-right corner to go back. When the arming/disarming process is completed, a notice of result will pop up. Click **Details** to check full result.
- You will also be notified on the Mobile Client when the arming/disarming process is completed.

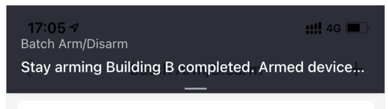


Figure 7-30 Notice on the Mobile Client

Check Last Result
Click **Last Arming Control Record** to check the last arming/disarming results. If there are devices that failed to be armed/disarmed, you can check the failure reasons and arm/disarm the failed ones again.

Edit Group
Click → **Edit** to edit group name or edit devices in the group.

Delete Group
Click → **Delete** to delete the group.

7.9 View Video

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

7.9.1 View Live Video

By viewing live view of managed cameras, you can check whether the camera is installed and located properly by capturing pictures, recording, PTZ control, etc.

Click **Encoding Device** on the top of the Site Detail page to show all the encoding devices of the site. Select an encoding device and click to start live view. The live view will work for up to five minutes. When the live view ends, you can still start a new live view. Hover the cursor on the live view window and click icons on the tool bar to start recording, conduct digital zoom and PTZ control, capture a picture, switch image quality, and turn on/off audio. Double-click the live view image to enter the full-screen mode, and double-click the image again to exit full-screen mode.

Note

- Up to 16 live view windows are supported.
- 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 to them.
- Make sure the device is online, otherwise the function cannot be used.

7.9.2 Play Back Video Footage

Video playback shows what happens when emergencies occur. If an end user approves your application for device playback permission, you will be able to play back the recorded video footage stored on the device.

Note

- Make sure your account has the permission for playback. Otherwise, you cannot enter the playback page. See ***Apply for Device Permission*** for details about applying device permission.
- This function needs to be supported by device.
- Make sure you have configured recording schedule for the device and there is video footage stored in the device.

On the Device tab page, select a device and click to enter the playback page. You can select a date and time on the calendar to view the playback during a certain time range.

You can select channels from the drop-down list on the top right. Drag the time bar at the bottom to jump to different video footage. Hover the cursor on the time bar and zoom in the time bar to select a more accurate time. Hover the cursor on a playback window and click icons on the tool bar to capture a picture, clip video footage, perform digital zoom, download video footage, and turn on the audio.

For devices (including the added online devices) added by Hik-Connect Service without configuring DDNS, the playback will work for up to five minutes; for devices added by IP/Domain Name, and devices (including the added online devices) added by Hik-Connect Service with DDNS configured, the playback duration is not limited.

Note

Up to four playback windows are supported.

7.10 Other Management

You can perform more operations for device management, including upgrading device firmware, unbinding device from its current account, configuring DDNS for devices added by Hik-Connect service, and remotely configure parameters for devices such as encoding devices and security control devices.

7.10.1 Upgrade Device

On the device list page, will appear beside the name of a device if it is upgradable. You can upgrade the device to make it compatible with the Hik-Partner Pro.

Steps

Note

- The function is supported by devices such as security control panels (including AX PRO), doorbells, and certain models of network cameras, Hik-ProConnect boxes, and DVRs/NVRs that support cloud storage.
- The system supports upgrading encoding device, some access control devices and video intercom devices connected to the same LAN with the PC where the platform runs.
- You can also upgrade devices in the Health Monitoring module. For details, see ***Health Monitoring*** .
- You can also upgrade devices when you add them. See ***Add Detected Online Device*** and ***Add Device by Entering Serial No.*** for details.

1. Click a site name to enter the site details page.
2. Hover over , click **Upgrade Device** and then select upgradable device(s).
3. Click **Upgrade**.
4. **Optional:** If there are devices which have enabled EN50131 Compliant mode, enter the device passwords and click **OK**.

   Note

   - Once started, the upgrade cannot be stopped. Make sure a power failure or network disconnection does not happen during the upgrade.
   - You can enable EN50131 Compliant mode on device configuration page via the Web Client. See device user manual for details.
   - For the device failed to be upgraded, you can click to download the upgrade firmware package, and then upgrade the device on the remote configuration page of device or via other upgrade tools.

   A window will pop up showing the upgrade progress. If there are devices failed to be upgraded, the causes will be displayed on the window.

7.10.2 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. Click **Install & Config → On-Site Batch Upgrade** .

Note

A video tutorial about how to use search tool for important firmware update on Hik-Partner Pro Portal will pop up in the lower-right corner of the page.

2. Select device(s) that need to be upgraded.
3. Click **Upgrade Online** or **Upgrade by Local File** to upgrade the selected device(s).

7.10.3 Unbind a Device from Its Current Account

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

Note

- For details about adding detected online device, see ***Add Detected Online Device*** .
- If you checked **Allow Me to Disable Hik-Connect Mobile Client Remote Use** when handing over a Site to your customer, you cannot unbind the devices added to this Site. For details about Site handover, see ***Hand Over Site*** .

On the adding result page, click in the Operation column, and then enter the device password and click **OK** to unbind it from its current account. When the device is unbound, you can click in the Operation column to add the device 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.

7.10.4 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. On the navigation pane, click **Site** to enter Site page.
2. Select a device, and click → to open the DDNS Settings window.
3. Switch **Enable DDNS** on to show the DDNS parameters.

Note

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

4. 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

   You enter the service port and HTTP port manually.
5. Enter the device's domain name.
6. 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.

7. Click **OK**.

7.10.5 Remote Configuration

You can perform device remote configuration if you need.

Note

Only site manager can perform the following operations and configurations of a site. See ***Assign Site to Installer*** for details about assigning site.

On the navigation pane, click **Site** to enter Site page. Click a site's name to enter the site's page. And then click **Device** tab to show the site's devices.

Click ⚙ to open the remote configuration page of the device and set the device's parameters.

Note

- Only doorbells, encoding devices, indoor stations, and security control panels support remote configuration.
- Make sure the device is online, otherwise the function cannot be used.
- For doorbells, you don't need to enter the device user name and password before accessing the remote configuration page.

- For encoding devices, if you have already entered the device's user name and password when adding it, you do not need to enter these information before remote configuration. For NVR and DVR, operations including rebooting, HDD formatting, and network settings are supported.
- For security control devices:
  - If the security control device is in the same LAN with the Portal, you need to enter the user name and password before accessing the remote configuration page.
  - If the AX Hub device and AX Hybrid device are not in the same LAN and EN50131 Compliant mode is enabled, you need to enter the devices' admin passwords for verification first. After that, you can enter their remote configuration page after entering password of setter account.
- For encoding devices and security control devices, if the device is not in the same local area network with the Portal, some operations in the remote configuration (such as device account management, enabling Hik-Connect, and restoring device, etc.) are not available.
- See device user manual for details about remote configuration.
- If you have changed device parameters by other software or client (such as device page, Hik-Partner Pro Mobile Client, iVMS-4200, , HikCentral Professional, etc.), and the parameters on the Portal's remote configuration page are not updated to the latest, you can click **Clear Cache** in the drop-down list on the top right of the remote configuration page to update the device parameters.

Chapter 8 Health Monitoring

The Health Status module provides 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 of importance 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.

Note

- A video tutorial on how to check device health status will pop up in the lower-right corner of the page when you enter the Health Status module.
- 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.
- 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*** .

8.1 View Status of Devices in All Sites

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

Click **Health Monitoring → Health Status** on the Navigation panel to enter the Health Monitoring page, and then select **All Sites** from the site list.

You can view the total number of devices and the number of abnormal devices of each device type.

Refer to the following table to get to the device description and operations.

Table 8-1 Links of Different Device Types

Encoding Device	Refer to ***Encoding Device*** .
Access Control Device	Refer to ***Access Control Device*** .
Alarm Device	Refer to ***Alarm Device*** .
Video Intercom Device	Refer to ***Video Intercom Device*** .
Doorbell	Refer to ***Doorbell*** .
Hik-ProConnect Box	Refer to ***Hik-ProConnect Box*** .
Network Switch	Refer to ***Network Switch*** .

Encoding Device

You can view the status including network status, the number of offline linked cameras, storage status, HDD usage, last inspected time, overwritten recording status, etc.

Note

For analog camera, you can view the status if video loss occurs.

Offline Cameras

The number on the left of the slash represents the number of offline/total cameras linked to the device.

Offline Duration

The 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)". You can click**Offline Duration** to sort devices by offline duration.

You can perform the following operations.

Operation	Description
View Device Name and Version	Hover the cursor over the device name to view its device type and device version.
Remotely Configure Device	Click ⚙ in the Operation column to remotely configure the device parameters. For details, see the device user manual.
Inspect All Encoding Devices	Click **Refresh** to inspect all the encoding devices in all sites.
Inspect Selected Encoding Device	Click ⇄ in the Operation column to inspect the selected encoding device manually.
Display Abnormal Devices	Check **Display Abnormal Devices Only** to display the abnormal devices only.
Display Authorized Devices	Check **Display Authorized Devices Only** to display the devices of which configuration permission has been authorized to you.
View Camera Status	Click › to show the cameras linked to the device, and then you can view the online/offline status of each camera.
View HDD Information of DVR	Click › to show the HDD information of the DVR, including self-inspection evaluation result, overall evaluation result, running status,

Operation	Description
	running time, HDD temperature, and S.M.A.R.T information.
View Site Owner and Site Manager Information	Move the cursor to in the Site column to view the information of the Site Owner and Site Manager, such as name and phone number.
Live View	Click in the Operation column and then select camera(s) to view live video(s). **Note** • If you have no permission to view the live video, you can apply for the live view permission from the end user. For details, see ***Apply for Device Permission*** . • If a selected camera has enabled stream encryption, you should enter the device verification code before you can view its live video. • The device verification code is created when you connecting the device to the Hik-Connect service. For details, see ***Add Detected Online Device*** .
Playback	Click in the Operation column and then select camera(s) to playback video(s). **Note** • If you have no permission to view the video playback, you can apply for the playback permission from the end user. For details, see ***Apply for Device Permission*** . • If a selected camera has enabled stream encryption, you should enter the device verification code before you can view its video playback. • The device verification code is created when you connecting the device to the Hik-Connect service. For details, see ***Add Detected Online Device*** .

Operation	Description
Apply for Permission or Reconfigure Device	appearing beside the device name represents that you have no configuration permission for it, the IP address/domain set for the device is invalid, or DDNS is invalid. You can hover the cursor on the icon, and then apply for the permission from the end user, reconfigure its IP address/domain, or reconfigure DDNS respectively based on the prompts. **Note** • For details about applying for configuration permission, see ***Apply for Device Permission*** . • For details about configuring device IP address/domain, see ***Add Devices by IP Address or Domain Name*** . • For details about configuring DDNS, see ***Configure DDNS for Devices*** .
Search for Device	Enter the keywords in the search field and click to search for specific devices.
Auto Update	You can switch on **Auto Update** so that the latest device exceptions and status received by the Portal will be displayed in real time.

Access Control Device

You can view the status including network status, door number, last inspected time, etc.
You can perform the following operations.

Operation	Description
View Device Name and Version	Hover the cursor over the device name to view its device type and device version.
Inspect All Access Control Devices	Click **Refresh** to inspect all access control devices.
Inspect Selected Access Control Device	Click in the Operation column to inspect the selected access control device manually.
Display Abnormal Devices	Check **Display Abnormal Devices Only** to display the abnormal devices only.

Operation	Description
Display Authorized Devices	Check **Display Authorized Devices Only** to display the devices of which configuration permission has been authorized to you.
View Site Owner and Site Manager Information	Move the cursor to in the Site column to view the information of the Site Owner and Site Manager, such as name and phone number.
Apply for Permission or Reconfigure Device	appearing beside the device name represents that you have no configuration permission for it. You can apply for the permission from the end user. **Note** For details about applying for configuration permission, see ***Apply for Device Permission*** .
Search for Device	Enter the keywords in the search field and click to search for specific devices.
Auto Update	You can switch on **Auto Update** so that the latest device exceptions and status received by the Portal will be displayed in real time.

Alarm Device

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

Note

Displaying peripheral device's remaining power is not supported.

You can perform the following operations.

Operation	Description
View Device Name and Version	Hover the cursor over the device name to view its device type and device version.
Remotely Configure Device	Click in the Operation column to remotely configure the device parameters. For details, see the device user manual.

Operation	Description
	Note Remote configuration is not supported if the device is armed.
Inspect Access Control Device	Click to inspect access control devices.
Display Abnormal Devices	Check **Display Abnormal Devices Only** to display the abnormal devices only. After **Display Abnormal Devices Only** is checked, you can check different exceptions (offline, low battery, lid opened, etc.) to display abnormal devices with different exceptions accordingly.
Export Abnormal Devices	Click **Export Abnormal Devices** and the Export Abnormal Alarm Devices page will pop up on the right side. You can export the file to the local PC in Excel or CSV format.
Display Authorized Devices	Check **Display Authorized Devices Only** to display the devices whose configuration permission has been authorized to you.
Upgrade Device	If appears beside the device name, hover the cursor over the icon and then click **Upgrade** on the pop-up dialog to upgrade the device. For details, see ***Upgrade Device*** .
Authenticate or Apply for Permission	appearing beside the device name represents that EN50131 Compliant mode has been enabled on the device, or that you have no configuration permission for it. For the former situation, you should hover the cursor over the icon and then click **Authenticate** on the pop-up dialog for authentication before you can view the device status; For the latter situation, you can apply for the permission from the end user. **Note** For details about applying for configuration permission, see ***Apply for Device Permission*** .

Operation	Description
View Zone and Peripheral Device Status	Click > to view the status of the zones and peripheral devices linked to the security control panel.
View Detailed Exceptions	You can hover the cursor over a specific zone to view its detailed exceptions.
View Site Owner and Site Manager Information	Move the cursor to in the Site column to view the information of the site owner and site manager, such as name and phone number.
Search for Device	Enter the keywords in the search field and click to search for specific devices.
Auto Update	You can switch on **Auto Update** so that the latest device exceptions and status received by the Portal will be displayed in real time.

Video Intercom Device

You can view the status such as network status and last inspected time.
You can perform the following operations.

Operation	Description
View Device Name and Version	Hover the cursor over the device name to view its device type and device version.
Inspect All Video Intercom Devices	Click **Refresh** to inspect all video intercom devices.
Inspect Selected Video Intercom Device	Click in the Operation column to inspect the selected device manually.
Display Abnormal Devices	Check **Display Abnormal Devices Only** to display the abnormal devices only.
Display Authorized Devices	Check **Display Authorized Devices Only** to display the devices of which configuration permission has been authorized to you.
Apply for Permission or Reconfigure Device	appearing beside the device name represents that you have no configuration permission for it. You can apply for the permission from the end user.

Operation	Description
	Note For details about applying for configuration permission, see ***Apply for Device Permission*** .
Search for Device	Enter the keywords in the search field and click to search for specific devices.
Auto Update	You can switch on **Auto Update** so that the latest device exceptions and status received by the Portal will be displayed in real time.

Doorbell

You can view the information including device model, network status, SD card status, last checked time, etc.
You can perform the following operations.

Operation	Description
View Device Name and Version	Hover the cursor over the device name to view its device type and device version.
Inspect All Doorbells	Click **Refresh** to inspect all doorbells.
Inspect Selected Doorbell	Click in the Operation column to inspect the selected doorbell manually.
Display Abnormal Devices	Check **Display Abnormal Devices Only** to display the abnormal devices only.
Display Authorized Devices	Check **Display Authorized Devices Only** to display the devices whose configuration permission has been authorized to you only.
Remotely Configure Device	Click in the Operation column to remotely configure parameters of the device. For details, see the user manual of the device.
Live View	Click in the Operation column and then select camera(s) to view live video(s).

Operation	Description
	Note • If you have no permission to view the live video, you can apply for the live view permission from the end user. For details, see ***Apply for Device Permission*** . • If a selected camera has enabled stream encryption, you should enter the device verification code before you can view its live video. • The device verification code is created when you connecting the device to the Hik-Connect service. For details, see ***Add Detected Online Device*** .
Upgrade Device	If appears beside the device name, hover the cursor over the icon and then click **Upgrade** on the pop-up dialog to upgrade the device. For details, see ***Upgrade Device*** .
Apply for Permission	appearing beside the device name represents that you have no configuration permission for it. You can apply for the permission from the end user. **Note** For details about applying for configuration permission, see ***Apply for Device Permission*** .
Search for Device	Enter the keywords in the search field and click to search for specific devices.
Auto Update	You can switch on **Auto Update** so that the latest device exceptions and status received by the Portal will be displayed in real time.

Hik-ProConnect Box

View information including network status of the box, number of offline channels (cameras) added to the box, and the latest time when the device was inspected.
You can perform the following operations:

Operation	Description
View Device and Channel Information	Click to view the basic information (e.g., device serial number and device model) and the detailed list of online and offline channels.
Remotely Configure Device	Click in the Operation column to remotely configure parameters of the device. For details, see the user manual of the device.
Inspect Selected Device	Click in the Operation column to inspect the selected device manually.

Network Switch

View information including network status of the switch (online/offline), the number of online ports of the switch, and the latest time when the device was inspected.
You can also perform the following operations:

Operation	Description
Inspect Selected Device	Click in the Operation column to inspect the selected device manually.
Remotely Reboot Device	Click in the Operation column to reboot the network switch remotely.
View Typology	Click in the Operation column to view the topology of this switch. For details about topology, refer to ***Network Topology*** .
View Switch Details	Click to view the detailed information of the switch, including the memory usage, CPU usage, POE power, peak POE power, working duration, port status (alarm, normal, not connected). **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.

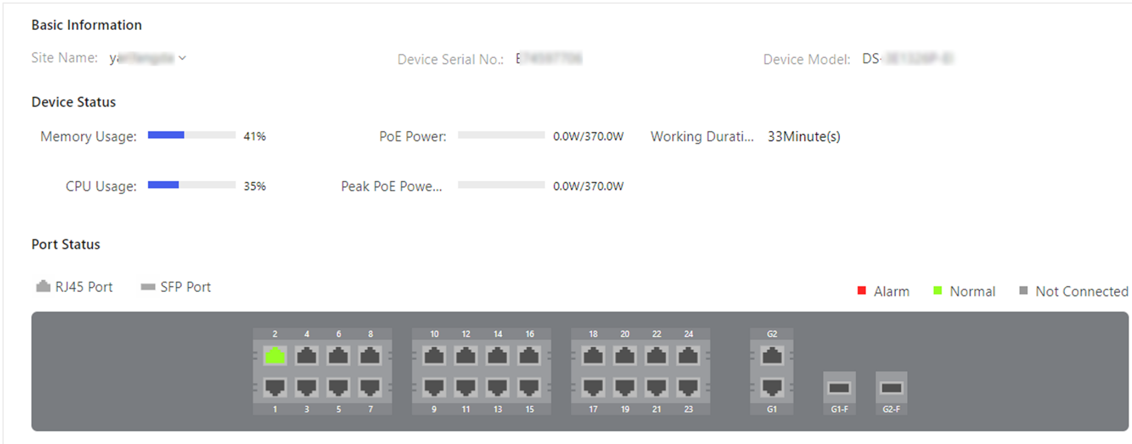


Figure 8-1 Switch Details

On the Switch Details page, You can perform the following operations:

Operation	Description
View Enlarged Port Picture	Hover the cursor onto the switch picture to view the enlarged picture of the ports.
Clear Alarm	For port with alarm(s), click ··· → **Clear Alarm** to clear the alarm(s) of this port.
Restart Port	For the abnormal port, click ··· → **Restart Port** to restart this port.
Extend Port Transmission Range	Click ··· → **Enable Extend Mode/Disable Extend Mode** to extend the transmission range of this port or not. **Note** When enabled, the transmission range of the port will be extended from 200 to 300 m. Meanwhile, its bandwidth will be limited within 10 Mbps.

8.2 View Status of Devices in a Specific Site

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

Steps

1. Click **Health Monitoring → Health Status** on the Navigation panel to enter the Health Status page.

2. Select a specific site from the site list.

   The status of the devices in the site will be displayed.

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

Filter Data	Check **Display Abnormal Devices Only** to display the abnormal device(s) only. Check **Display Authorized Devices Only** to display the device(s) of which configuration permission has been authorized to you only.
Auto Update	You can switch on Auto Update so that the latest device exceptions and status received by the Portal will be displayed in real time.
Upgrade Device Firmware	If there are device(s) available for upgrade, a number in red will be displayed on **Upgrade** showing the number of upgradable device(s). You can click **Upgrade**, select the upgradable device(s), and then click **Upgrade** to upgrade them. Select a device to view its basic information. If the device firmware is upgradable, you can click **Upgrade** in the Firmware Version field to upgrade it. **Note** For details, see ***Upgrade Device*** .
Diagnose Devices of the Site	Click **Health Check** to open the Health Check window, and click **Check Now** to diagnose the devices of the site. When the checking completed, you can view the status of each device in the site. For AX PRO security control panel, NVR, and DVR, you can click **View Report** to export the diagnostics report as a PDF file to the local PC.
View Site Owner Information	Click **Site Owner** to view the Site Owner information, including name, email address, and phone number.
View Site Manager Information	Click **Site Manager** to view the Site Manager information, including name, email address and phone number. Up to 100 site managers can be displayed.
Inspect Devices in the Sites	Click **Refresh** to inspect all the devices in the site.
Remote Configuration	Select a device and then click **Remote Configuration** to remotely configure the parameters of the device.

Note

- The device should be online, or remote configuration will be unavailable.
- For details, see the user manual of the device.

Inspect a Single Device	Select a device and then click to inspect it.
Search for Device	Enter the keywords in the search field and click to search for specific devices.
Reconfigure IP/ Domain of Encoding Device	Move the cursor to , and then click **Edit IP/Domain** to reconfigure the device's IP/domain. For details about configuring IP/Domain, see ***Add Devices by IP Address or Domain Name*** .
Reconfigure DDNS	Move the cursor to , and then click **Configure DDNS** to reconfigure the device's DDNS. For details about configuring DDNS, see ***Configure DDNS for Devices*** .
View Encoding Device Details	You can view the network status, storage status, HDD usage, and overwritten recording status, etc. You also click the encoding device to view its details, including basic information such as device type and serial No., and the network status of each camera linked to it. You can click and select linked cameras, and then click to view live videos. If the encoding device is a DVR, you can also view its HDD information, including self-inspection evaluation result, overall evaluation result, running status, running time, HDD temperature, and S.M.A.R.T information. For analog camera, you can view if video loss occurs.

Note

- If you have no permission to view the live video, you can apply for the live view permission from the end user. For details, see ***Apply for Device Permission*** .
- If a camera has enabled stream encryption, you should enter its device verification code in the pop-up window before you can view its live video.
- The device verification code is created when you connecting the camera to the Hik-Connect service. For details, see ***Add Detected Online Device*** .

View Access Control Device Details	Click an access control device to view its details, including basic information such as device type and serial No., and the device status including network status and the number of its linked doors.
View Security Control Panel Details	Click a security control panel to view its details, including the basic information of the security control panel, and status of the zones, the linked peripheral devices, and the linked cameras. The following list shows the description of each status icon. • : Sufficient battery power. • : Insufficient battery power. • : Normal strength of the communication signals between the peripheral device and the security control panel. • : Weak strength of the communication signals between the peripheral device and the security control panel. • : Alarm triggered. • : Device tampered. • : Zone bypassed. • : Trigger exception.
View Video Intercom Device Details	Click a video intercom device to view its basic information and its network status.
View Doorbell Details	Click 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 also click a linked camera to view the live video.
View Hik-ProConnect Box Details	Click 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	The network switches are displayed by card. Click a switch to view its information, including the device model, device type, device serial No., the time of last inspection, network status, memory usage, CPU usage, PoE Power, peak PoE power in latest 70 days, working duration, port status (alarm, normal, not connected). **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. Hover the cursor onto the picture of switch to view the enlarged picture of the switch.

Click **Topology** at the top of the page to view the topology of this switch. For details about topology, refer to ***Network Topology*** .

Click in the Operation column to inspect the device manually.

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

For the abnormal port, click → **Restart Port** to restart this port.

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

Note

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

8.3 Send Report 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.

Steps

1. Enter the Scheduled Report page.
   - Go to **Health Monitoring → Scheduled Report** .
   - Click **Customer Site → 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. Enter the editing mode.
   - To configure the report sending schedule for a single site, click **Edit** on the right side of a site.
   - To configure the report sending schedule for multiple sites, click **Batch Configure** 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 to Daily, Weekly, Monthly, Quarterly, Semiannually, or Annually.

Recipient Email Address

Add and edit the email addresses of the recipients.

Note

- You can check **Site Owner's Email** to send a copy of the report to your customer.
- 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. Click **OK**.
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** in the upper-right corner.

   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 "...".
6. **Optional:** On the Search filled, enter the keywords and click to search for specific sites.
7. **Optional:** Click **Report Sample** to view a report sample.

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 the network links between devices and shows the link exceptions and abnormal devices, which helps you to locate 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 the 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 heath monitoring service for devices, see ***Activate the Health Monitoring Service for Devices*** .

You can enter the network topology page in the following ways:

- On the navigation pane, click **Site** to enter the Site page, and then click the name of a site to enter the site details page, and then click **View Topology**.

Note

If you have NOT enabled the Health Monitoring service for the network switch, you can enter the network topology page in this way only.

- On the navigation pane, click **Health Monitoring → Health Status** , select **All Sites** from the site list, and then select **Network Switch**, and then click in the Operation column in the network switch list.
- On the navigation pane, click **Health Monitoring → Health Status** , select a site from the site list to enter the site details page, and then click **Topology**.

Figure 8-2 Network Topology

The following table shows the descriptions of the available operations on network topology.

Table 8-2 Available Operations

Operation	Description
View Legend	You can click next to **More** to view the legends.

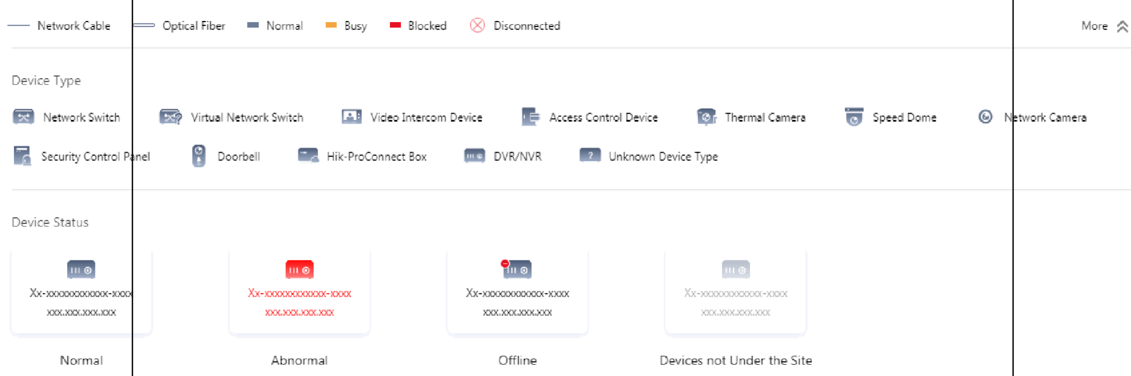
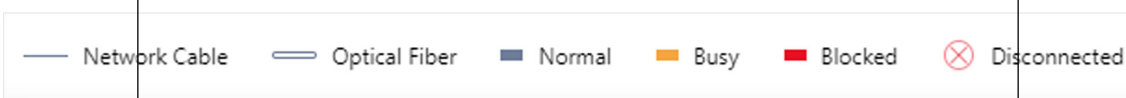
<table>
<tr><th>Operation</th><th>Description</th></tr>
<tr><td></td><td>

Figure 8-3 Legend</td></tr>
<tr><td>Edit Root Node</td><td>When multiple network switches are added to a site, the platform will randomly select one of them as the root node by default for the network topology. If the randomly-selected network switch is not the real root node, you can hover the cursor over the current root node, and then click to select a network switch as the root node.

Figure 8-4 Edit Root Node</td></tr>
<tr><td>Refresh Topology</td><td>Click Refresh to refresh the topology structure.
Note
The device status will not be refreshed.</td></tr>
<tr><td>Display in Cards</td><td>If you want to view more device status information of all the devices connected to the network switch(es), click Display in Cards to display device information in cards.</td></tr>
</table>

Operation	Description
Move Network Topology	Drag the network topology to move it.
Zoom In/Out	You can click + / – in the upper left corner to zoom in/out the topology.
Adjust Topology Size	You can click in the upper left corner to fit the topology size into the display window. You can click in the upper left corner to display the topology in full-screen mode.
Display Thumbnail	If you have zoomed in the topology to a large scale, you can click to show the thumbnail which shows the current cursor location on the topology.
Search Devices in Topology	You can enter the keyword of a device to search for it on the topology. Once the device is found, the topology will pan and zoom automatically to display the found device.
View Link Information	You can view link information based on the legends shown in the figure below.  **Figure 8-5 Link Information Legend**
View Link Details	You can hover the cursor over a specific link to view its details, such as the upstream, downstream, port name, and port status.
Apply for Configuration Permission	If you don't have the permission to configure a device, a prompt will pop up asking you to apply for the permission first. You can click **Apply for Permission** to apply for it. **Note** If you don't have the permission, the position of the device in the network topology might be incorrect.
View Network Switch Details and Control It	You can click a network switch on the topology to view the information about the network switch, including basic information, device status, and port status. You can also perform operations such as rebooting the network switch and restarting the port. For details, see ***Network Switch*** and ***View Status of Devices in a Specific Site*** .

Operation	Description
	Note You cannot view details of a virtual network switch.
View Another Device's Details and Configure It	If an online device is connected to the network switch and added to the same site with the network switch, its device icon and device serial number will be displayed. And you can click the device to view its information including the basic information (e.g., device model) and device status (e.g., network status). You can also click to configure device parameters. **Note** • If an unknown device (e.g., a PC) is connected to the network switch, it will be displayed as  . And you cannot view its information. • If an online device is connected to the network switch but is NOT added to the same site with the network switch, its serial number displayed will be a randomly-generated virtual serial number. And you cannot view its information.

8.5 Create a Maintenance Quotation

You can create a quotation for providing the device maintenance service for your customer. Thus, you can standardize the service process, improve customer satisfaction, and expand your business.

Before You Start

Make sure your company is authenticated. See ***Authenticate Account*** for details.

Steps

1. Go to **Health Monitoring → Maintenance Quotation** .
2. Click **Create Quotation**.
3. Set the quotation information.

   Quotation Details

   Enter a name for the quotation, and if needed, edit the quotation No. which is generated automatically.

   Customer Information

   Set the customer information including the name, email, phone number, and address. Enter the information manually, or click **Get from Site** and then select a site from the drop-down list to automatically synchronize the customer (site owner) information.

Item

Click **Add Item** to set the quotation items. Add default items (remote maintenance, health check report, on-site maintenance (annual), on-site maintenance (additional), etc.) or custom items. After adding the items, set the device model, unit price, and quantity. The quotation tool will automatically add up the prices of all set items to calculate the total price.

Set Discount

If needed, enable **Set Discount** and enter the discount percentage to give your customer a discount.

Set VAT Rate

If needed, enable **Set VAT Rate** and enter the VAT rate to include the value-added tax.

Service Provider Information

The service provider information, including the name, email, phone number, address, and company logo, is automatically set according to your company information. Edit the information (except for the company logo) if needed.

4. **Optional:** Click **Preview/Export** to see how the quotation will be presented and to export it as a PDF file.
5. Click **Save**.

Note

You can create no more than 10 quotations if co-branding is enabled; otherwise, you can only create 3 quotations.

6. **Optional:** Perform the following operations after creating the quotation.

Edit a Quotation	On the quotation list, click **Edit** to edit a quotation.
Delete a Quotation	On the quotation list, click ··· → **Delete** .
Preview/Export a Quotation	On the quotation list, click **Preview/Export**.

Chapter 9 Search Operation Log

All operations information (including operator, operating time, site, operation target and result, etc.) of the employees (referring to Installer Admin and Installers) will be recorded so that you can search the operation log(s) of any employee to make sure what makes the sites wrong.

Note

This feature is not available to authenticated channel partner.

Click **My Hik-Partner → Company Management → Operation Log** to display the employee list and all the operation logs. You can search logs by employee, site, and time.

Note

- Logs of all accounts are available for accounts with the permission for managing account and role. For accounts without permission for managing account and role, they can only view their own logs.
- Logs of all sites are available for accounts with the permission for managing all sites. For accounts without permission for managing all sites, they can only view the logs of assigned site.

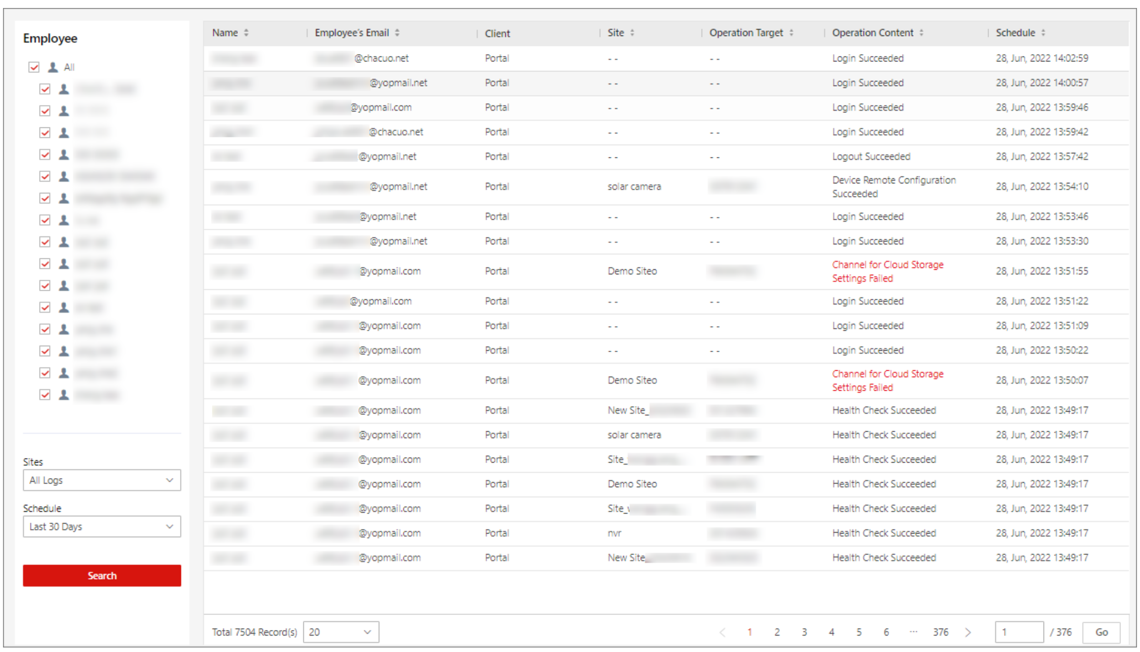


Figure 9-1 Search Operation Logs

Chapter 10 Notification Center

The Notification Center module shows all the history business notifications (including device management invitations, site sharing notifications, and notifications about device installation work orders) 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).

10.1 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, and notifications concerning device installation work order.

Go to the **Notification Center** page. Click **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 a Hik-Connect User*** .

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*** .

Notifications about Work Order for Device Installation

If an RMC from HikCentral ReGuard assigns a work order for device installation to you, the message will be displayed in **Notification Center → Business Notification** .
The message shows the work order name, person who created it, and phone number. You can handle the work order on the Mobile Client.

10.2 Exception Center

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

Note

- For Installer Admin, you can view all the exceptions of the devices in all the added sites. For Installers, you can view the exceptions of the devices in the site which has been assigned to you.
- Device exception messages can be preserved for up to 90 days.
- You need to set the exception rule first. For details, refer to ***Add Exception Rule*** .

Go to the **Notification Center** page. Click **Exception Center** to enter the Exception Center page.

Filter the Exceptions

You can filter the exceptions according to your actual needs.

1. Select a site in the site list to view the exceptions of the devices in this site. You can also select a device or a channel to view the exceptions occurred on the device or channel.
2. Set the time period. The exceptions received during this time period will be displayed.
3. Set the handling result from **All Status**, **Not Handled**, **Solved**, **False Alarm**, and **To Be Checked**.
4. Select the exception types that you want to check. The exception types include alarm, exception, and operation.

You can switch on **Auto-Update** so that the latest exceptions received by the Portal will be displayed in the table in real time.

Note

The auto-update will be invalid when viewing history records (including records after page 1 and records received before today).

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. Click **Handle** in the Operation column to show the Handle Exception pop-up window.

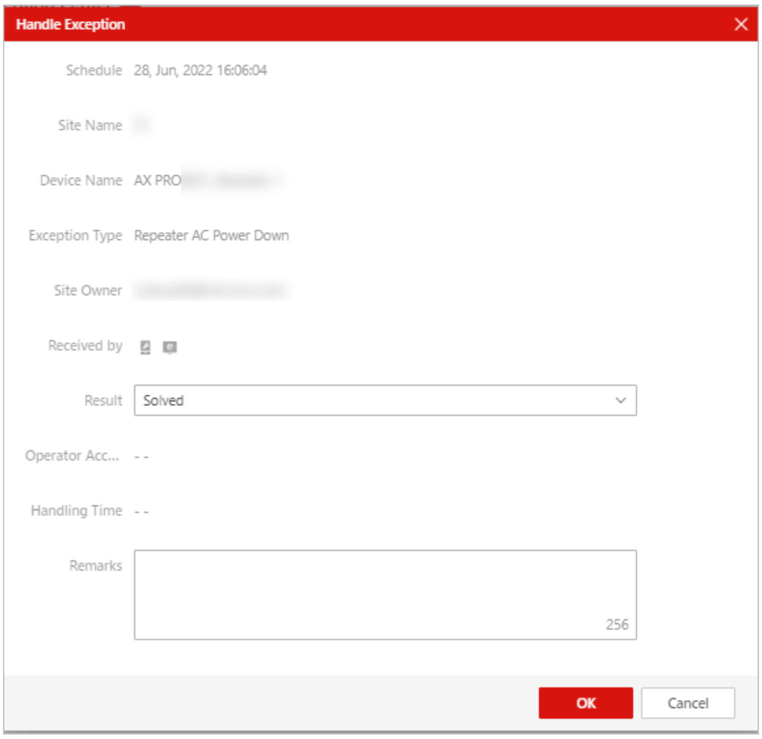


Figure 10-1 Handle Exception

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

Batch Handle Exceptions

If the handling results of several devices are the same, you can select multiple exception items and click **Batch Handle** to batch handle them.

Jump to Device Health Monitoring

Click in the Operation column to jump to the device's health monitoring page to troubleshoot the exceptions.

Export Exception Records

After filtering the exceptions, click **Export** and select the format of the file to export these exception records to your local PC.

Note

Currently, the supported formats of the exported file include CSV, Excel, and PDF.

Open in New Window

Click **Open in New Window** in the upper-right corner to open a new window of the browser to view the Exception Center. With this function, you can view the Exception Center and other pages at the same time.

10.3 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).

On the top right of the page, click 🔔 to go to the Notification Center. Click **System Message** to enter the System Message page.

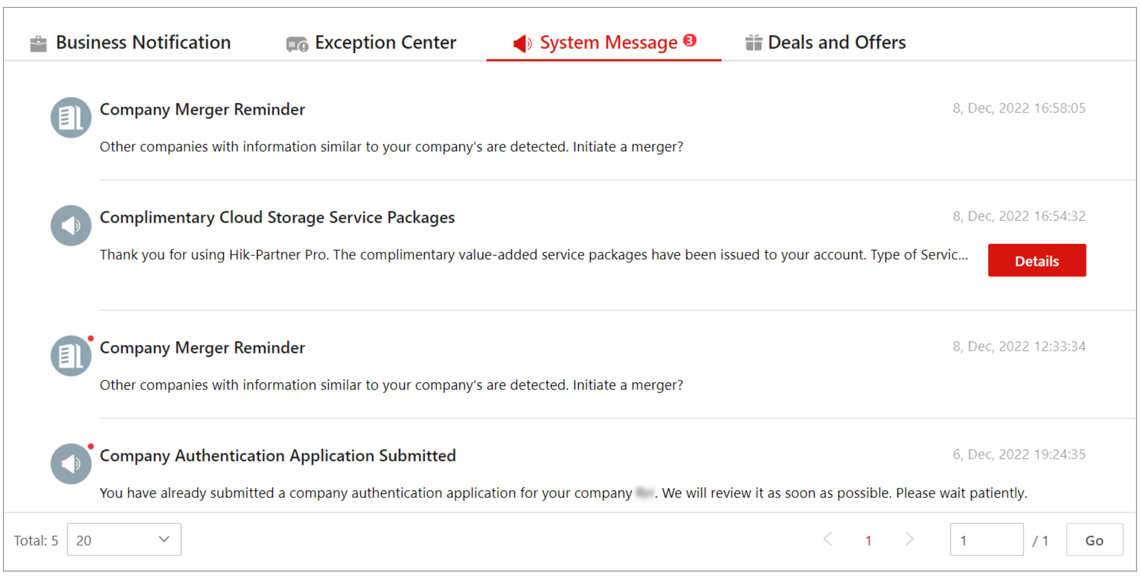


Figure 10-2 System Message Page

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 ***Company Merger*** .

10.4 Deals and Offers

The Notification Center supports displaying notifications of the latest deals and offers.

Go to the **Notification Center** page. Click **Deals and Offers** to enter the Deals and Offers page.

You can view the notifications concerning complimentary service packages and lottery draws (including the notifications of rejected receipts, obtained tickets, and lottery draw results).

You can view basic information of the notifications in the notification list, including the notification type, title, time when it was generated, the read/unread status, and the notification content (in the form of texts or images). You can also jump to corresponding pages from the notifications.

Chapter 11 Project

After you register your projects on Hik-Partner Pro, you can not only receive special pricing on essential components, but also receive technical support for your projects.

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 Create a Project

Projects can be created by distributors or system integrators/installers. A project contains project information, information about who creates the project, end user information, support information, product information, and project document.

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. Click **Project** on the top of the page after login.
2. Click **New Project**.
3. Fill in the blanks.
   - If you are a distributor, enter project information, system integrator / installer information, end user information, support information, and product selection. Then upload the project document if there is any.
   - If you are a system integrator / installer, enter project information, distributor information, end user information, support type, support information, and product selection. Then upload the project document if there is any.

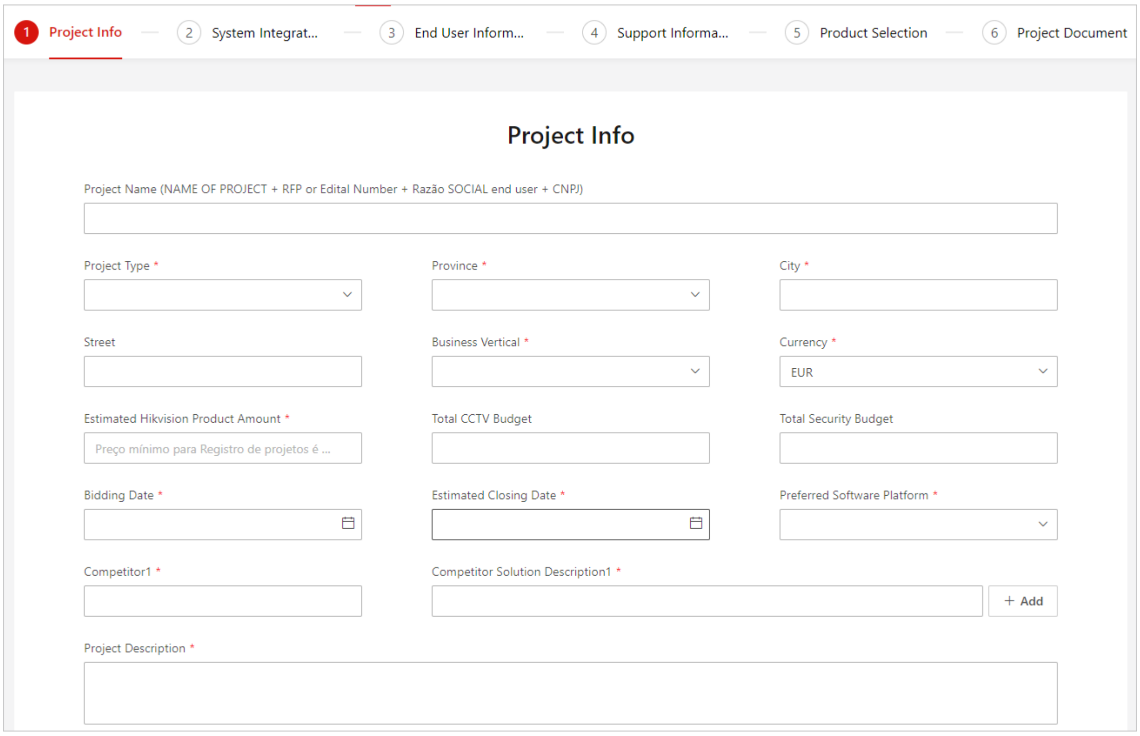


Figure 11-1 Add Project

Note

- For product selection, click **Add** → , select products and click **Confirm**.
- When you select products, you can click to compare products. For details about comparing products, refer to ***Compare Products*** .

4. Click **Save & Submit**.

   The project will be displayed on the Project History page, and the **Status** will be **Waiting for supporter**.

What to do next

For further operations, refer to ***View Project History*** .

11.2 Compare Products

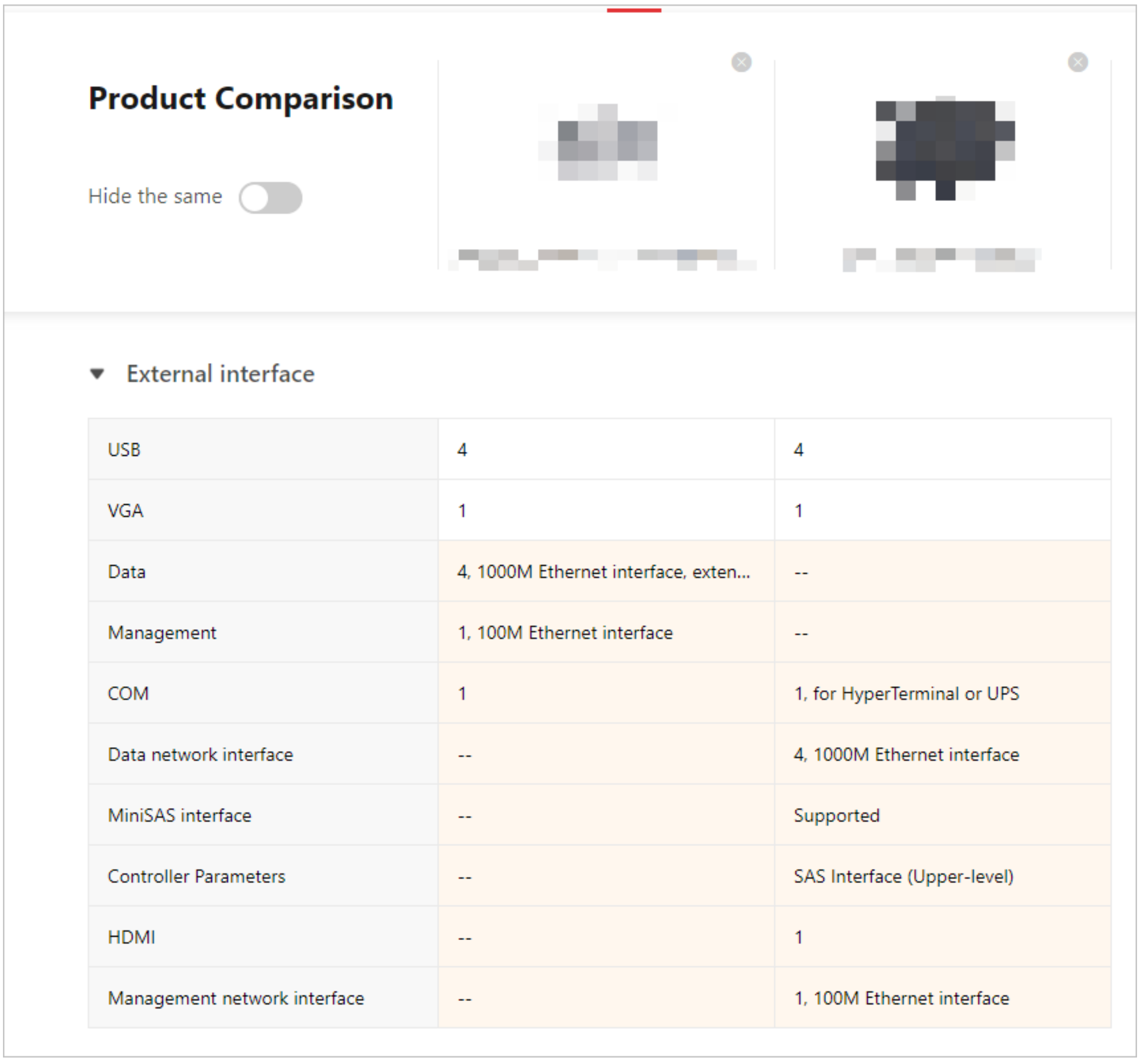
When you select products, you can add multiple products and compare them with their same specifications hidden. In this way, different specifications will be directly displayed and you can choose products as needed.

Note

Only products of the same category and subcategory can be compared.

Click **Project → New Project** , and in the Product Selection part, click to start compare products. You can also click at the right bottom, and add products to compare them.

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



USB	4	4
VGA	1	1
Data	4, 1000M Ethernet interface, exten...	--
Management	1, 100M Ethernet interface	--
COM	1	1, for HyperTerminal or UPS
Data network interface	--	4, 1000M Ethernet interface
MiniSAS interface	--	Supported
Controller Parameters	--	SAS Interface (Upper-level)
HDMI	--	1
Management network interface	--	1, 100M Ethernet interface

Figure 11-2 Compare Products

11.3 View Project History

You can view all projects on the Project History page. You can check the information 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.

Click **Project** on the top of the page after login.

For Distributors

There are three tabs **All**, **Project Supported by Hikvision**, and **Project Supported by Me**.

All

All projects will be displayed under this tab. FW means the project is forwarded to you. S means the project is shared to you. For shared projects, you can only check the information but not quote.

Project Supported by Hikvision

It includes projects submitted by you and projects shared to you.

Project Supported by Me

It includes projects forwarded to you. You can click **Go to Quote**, enter distributor prices, and click **Save&Send Quote to Customer** to generate a quote and send it to the customer.

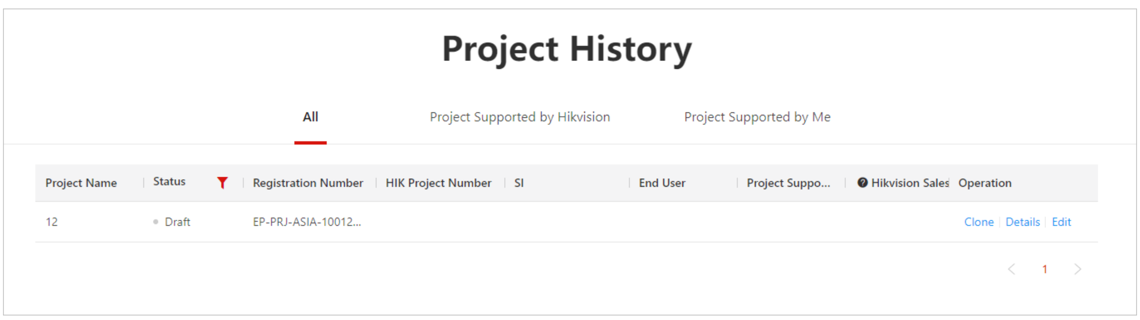


Figure 11-3 Project History for Distributors

For System Integrators / Installers

You can view all projects that you created. In the Operation column, you can click **Quote** and click the document in the Download column of the pop-up window to check the quote list.

Further Operations

Operations	Description
Filter Projects by Status	Click in the Status column to filter projects by their status. Here are some project status types.

Operations	Description
	• Draft: The project is only saved but not submitted. • Waiting for supporter: The project is submitted but not yet processed. • Processing: The project is currently being processed by Hikvision. • Approved: It is only available in some countries and regions. It suggests that the project be approved. • More Info Required: Hikvision needs more information to decide whether to approve the project. • Ineligible: The project is rejected by Hikvision. You can check the comments for why the project is rejected.
Close Project	Click **Close Project** and select among **Close Won**, **Close Lost**, and **Closed Canceled**. • Closed Won: It means the project is closed won, and you can enter Closed Won Amount and upload Purchase Order Document to accept the quote and close the project. • Closed Lost: It means the quote of the project is rejected, and you can select reasons, enter comments and close the project. • Closed Canceled: It means the project is canceled and closed, and you can select reasons, enter comments and close the project.
Copy Project	Click **Copy** to copy the project.
Edit Project	If the status turns to More Info Required or the project is only saved but not submitted, you can click **Edit** to edit the project.
View Details	Click **Details** to view the project details.

Chapter 12 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

- This feature is only available for some countries and regions.
- This feature is available only if your company is authenticated.
- All employee accounts of an authenticated company have the permission to use this feature.

The methods to access Case are as follows:

- Click **Support → Case** .
- Click **Case** on the right side of the dashboard.

The Case page will be opened in a new tab page.

12.1 Submit Case

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

Submit different types of cases as needed.

Note

- Hardware Product Case, Software Product Case, and Hik-Partner Pro Case are only available to some countries and regions.
- For device password reset, please submit cases on the Hik-Partner Pro Mobile Client.
- Some installers can submit Dedicated Customer Service Case for focused troubleshooting from technical support.

12.1.1 Submit Hardware Product Case

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

Steps

1. Go to the Case page.

   Note

   For how to enter the Case page, refer to ***Case*** .
2. Select **Submit Case → Hardware Products** .
3. Fill in the fields as required.

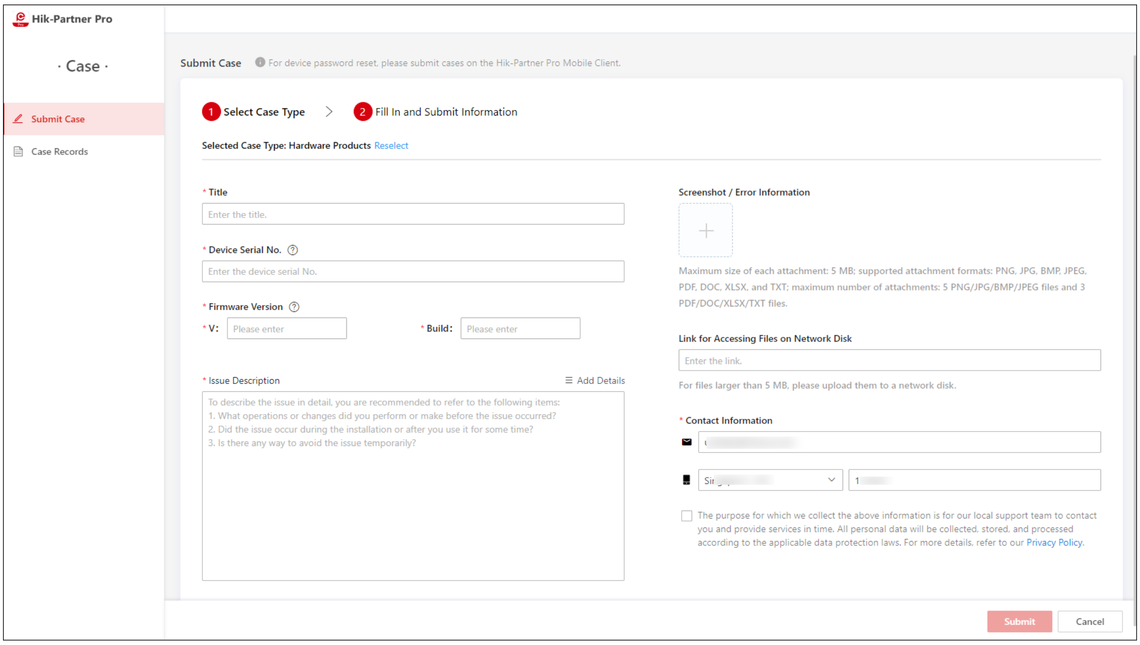


Figure 12-1 Submit Hardware Product Case

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 click ⓘ to see where to find the serial No.

Firmware Version

Enter the version number and build number. You can click ⓘ 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 click **Add Details** to add issue details (software name, software version, network type, etc.) to your description as needed.

Screenshot / Error Information

Click + 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. Click **Submit** to submit the case.

Note

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

12.1.2 Submit Software Product Case

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

Steps

1. Go to the Case page.

Note

For how to enter the Case page, refer to ***Case*** .

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

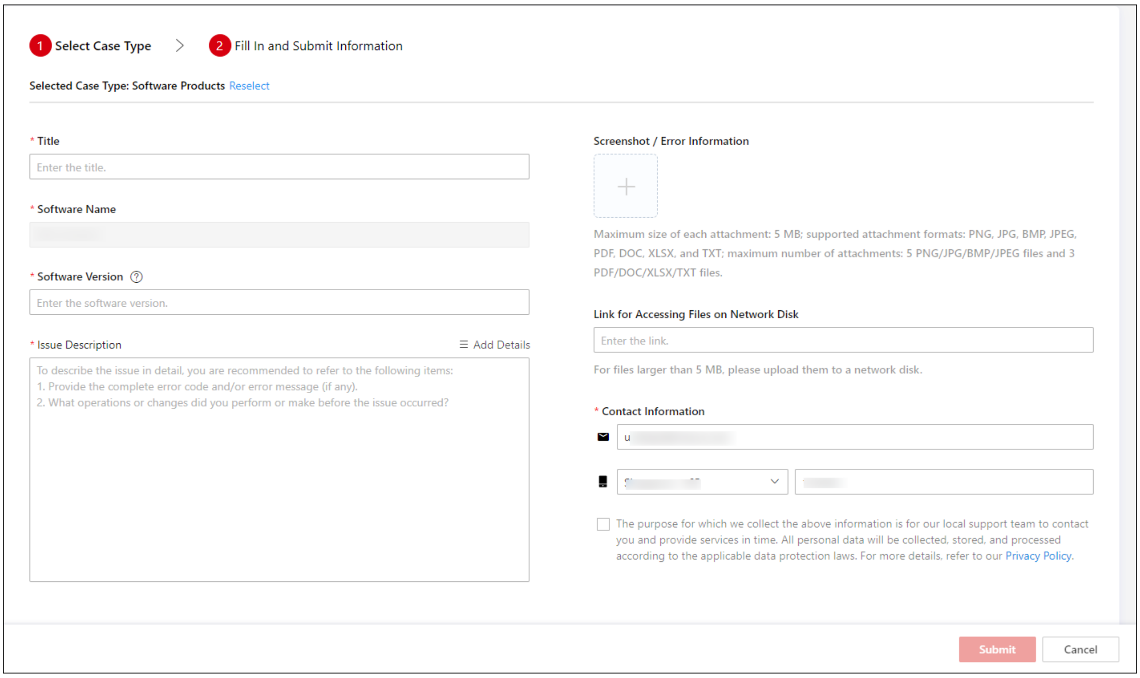


Figure 12-2 Submit Software Product Case

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 click **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

Click + 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. Click **Submit** to submit the case.

Note

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

12.1.3 Submit Hik-Partner Pro Case

You can submit Hik-Partner Pro cases for issues related to Hik-Partner Pro.

Steps

1. Go to the Case page.

Note

For how to enter the Case page, refer to ***Case*** .

2. Select **Submit Case → Hik-Partner Pro** , and select an issue type from the supported ones.
3. Fill in the fields as required.

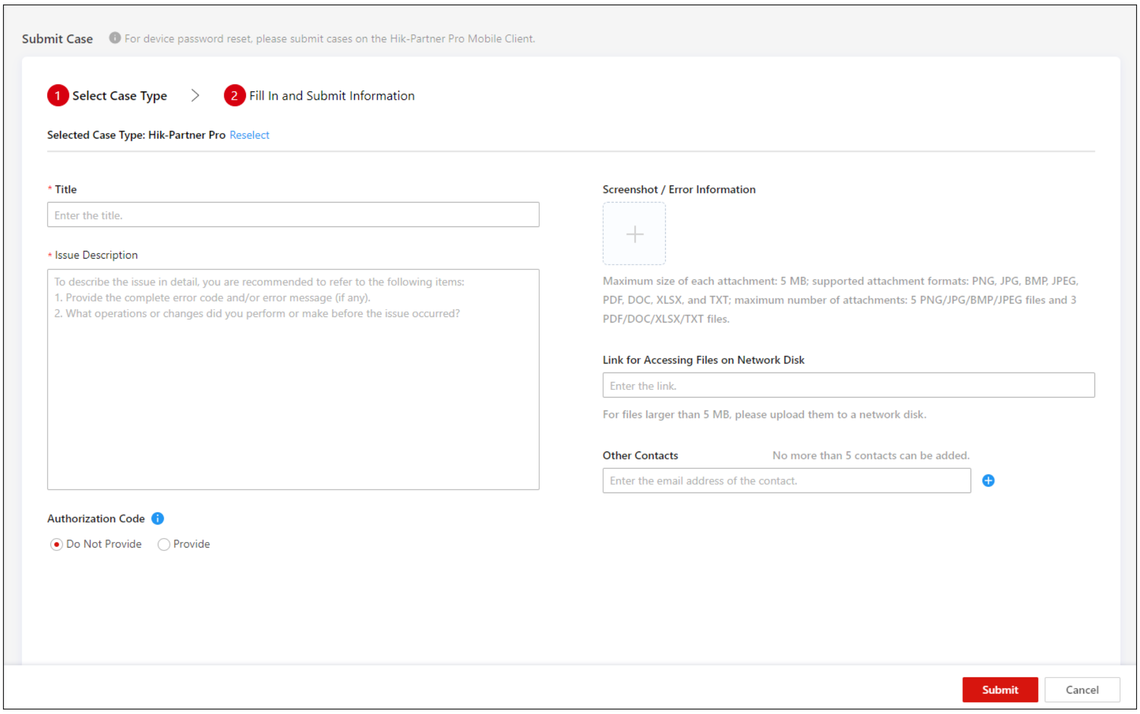


Figure 12-3 Submit Hik-Partner Pro Case

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.

Authorization Code

The after-sales authorization code is exclusive to Hikvision's technicians for troubleshooting only. You can give your authorization code to the technicians when it is necessary for them to log in to your account for troubleshooting.

Note

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

Screenshot / Error Information

Click + 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.

Other Contacts

Enter the email address of other contacts.

Note

No more than 5 contacts can be added.

4. Click **Submit** to submit the case.

Note

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

12.1.4 Submit Dedicated Customer Service Case

You can report the issues found when using Hik-Partner Pro to us by submitting dedicated customer service cases. We will respond to your case and provide support according to your case severity and language. Submitting dedicated customer service cases is only available for some installers, for focused troubleshooting from technical support.

Steps

Note

If you have more function-related requirements or improvement suggestions, you can give your feedback. For details, refer to ***Hik-Partner Pro Portal Overview*** .

1. Go to the Case page.

Note

For how to enter the Case page, refer to ***Case*** .

2. Click **Submit Case** on the left.

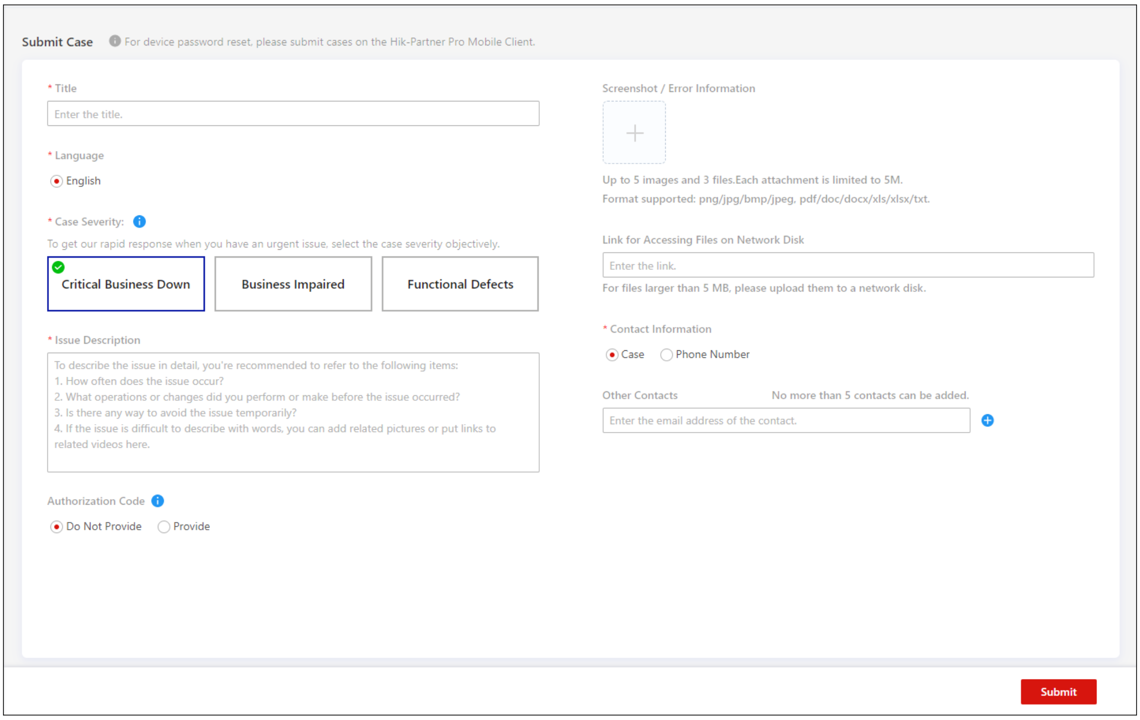


Figure 12-4 Submit Dedicated Customer Service Case

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. Enter the issue description.

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.

7. Set whether to provide the authorization code for the technical support staff for troubleshooting.

Note

For details about the authorization code, refer to ***Hik-Partner Pro Portal Overview*** .

8. **Optional:** Click + to upload screenshots or error information.

Note

You can upload attachments in PNG, JPG, BMP, JPEG, PDF, DOC, DOCX, XLS, 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.

9. **Optional:** Enter the link for accessing files on network disk.

Note

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

10. Select Case or Phone Number as Contact Information.

Note

If you select the latter, select the country/region code and enter the contact number.

11. **Optional:** Enter the email addresses of other contacts.

Note

No more than 5 contacts can be added.

12. Click **Submit**.

Note

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

12.2 View and Handle Case Records

You can view cases you submitted on the Case Records page, view replies to a case, reply to a case, and close a case.

Go to the Case page and click **Case Records** on the left.

Note

For how to enter the Case page, refer to ***Case*** .

Table 12-1 Available Operations on Case Records Page

Operation	Description
View All Submitted Cases	You can view cases you submitted on the Case Records page, including the case ID, time the case was created, case title, case type, and case status.
View Case Details	Click a case to enter the Case Details page to view the case creator, issue description, replies from technical support, request from the technical support for closing the case, case status updates, and so on. **Note** You will be notified via emails and push notifications on the Mobile Client if there are new replies or updates of case status.
Reply to Case	Click a case to enter the Case Details page. Click **Reply** on the bottom right corner, enter the reply content, and add attachments in the Reply section. Click **Confirm** to submit your reply to the current case.
Close Case	Click a case to enter the Case Details page, and click **Close Case** on the bottom right corner 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 within 14 days.

Chapter 13 Return Materials 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 distributors 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.

13.1 Submit RMA Request

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

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.

Steps

1. Go to **Support → RMA** .
2. Click **Add** to add products.
   - You can input the serial number of the products of interest, click **Add**, and enter fault description and reference. Click **Add Attachment** to add attachments if there are any.
   - You can click **Download Template**, enter information of multiple products, and click **Upload Serial List** to batch upload products.

   Note

   It should be a Hikvision product sold in the current country or region.
3. After all products are added, click **Next** to select shipping information.
4. Select shipping information.
   - For countries and regions that support cross-distributor repair, if the distributor is identified according to the serial number, the distributor will be automatically selected. If not identified, you need to click **Change Shipping Address** to choose a distributor by yourself. After choosing a distributor, the distributor and product information will show up in the list.

     By default, the selected repair station is the nearest one. You can also select among all stations of all distributors in the country.
   - For countries and regions that do not support cross-distributor repair, the system will identify the distributor according to the serial number. The default choice is the nearest location of the distributor. If the distributor can not be identified according to the serial number, then the product can not be added.
5. Check the information in the list, and click **Submit**.

Whether your application is submitted successfully or not is displayed.

6. You can perform the following operations.

Operation	Description
Download Document	Click RMA number to download document.
Back to Menu	Click **Back to Menu** to check details and track status.
Create More	Click **Create More** to add more applications.

13.2 View RMA Request

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

Go to **Support → RMA** , and the successfully submitted applications are displayed in the list. You can perform the operations as needed.

Operation	Description
Search for RMA Applications	You can search for an application by its Reference Number, RMA Number, Date, Application Number, and Serial Number.
Filter by Status	Click ▽ , and select among Saved, Unreceived, In Repair, Waiting For Customer Response, Ready for Shipment, and Completed.
View Details	Click **Detail** to view application details.
Download Document	Click **Download Document** to download the application file.

Chapter 14 Order & Promotion

The Order & Promotion module supports viewing information of regular products, hot products, and promotional products that are discounted or are put on clearance. You can search for and select products to place an order or submit your product order by uploading a predefined template.

Note

The module is only available to authenticated channel partners.

14.1 View and Search for Products

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

Under the B2B tab of the Order & Promotion module, you can view information of hot products and the products you have recently viewed. You can also view information of the regular products or promotional products (e.g., discount products, clearance products, etc.) by selecting the corresponding tabs under the navigation bar. You can filter the products by product category and search for specific products by product name or model.

Click a product to view its detailed information, including the product picture, description, stock availability, and other related parameters. If needed, you can add a product to Favorites by hovering over it and clicking .

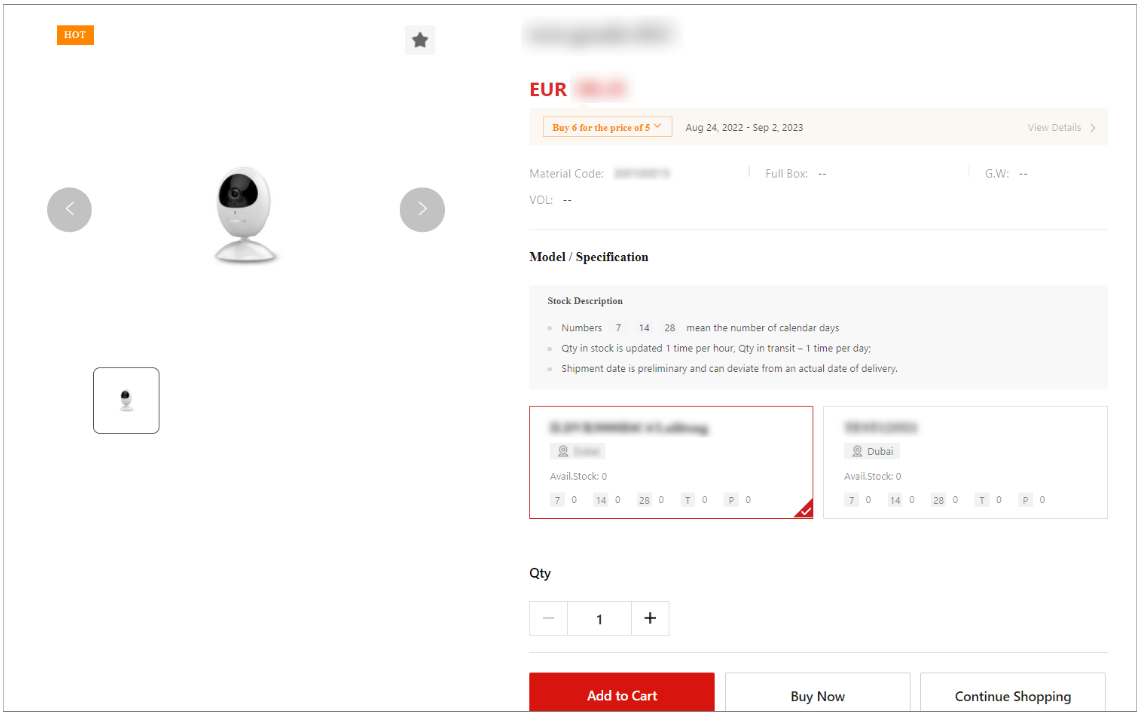


Figure 14-1 Product Information Details

Note

You can find the products you have added to Favorites later in **My Hik-Partner → Account Information → My Favorite → B2B Product** .

14.2 Create an Order

You can place an order by adding products to the shopping cart, selecting the products you need for checkout, and entering the required shipping information.

Steps

Note

Besides adding products to the shopping cart, you can also submit an order by uploading information (material code, quantity, etc.) of products with a predefined template via **Order Upload**.

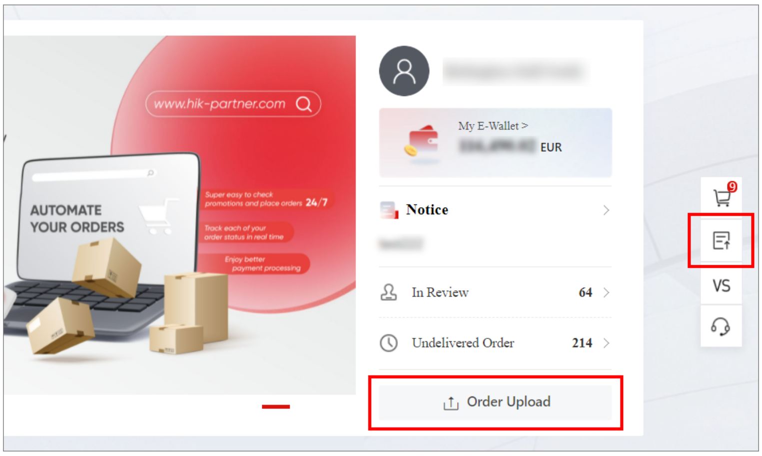


Figure 14-2 Ways for Accessing Order Upload

1. View or search for the products to be ordered.

   Note

   For details, refer to ***View and Search for Products*** .

2. Hover over a product of interest, set the quantity to be ordered, and click **Add to Cart**. Repeat this step to add multiple products to your shopping cart as needed.
3. Click on the right to go to your shopping cart.
4. Select the products to be ordered, adjust the quantity for each product if needed, and click **Next**.
5. On the Check Order Information page, enter your shipping/billing address, select a preferred shipping method, and confirm the order details (quantity to be ordered, total cost, etc.).

   Note

   - You can also set a preferred future date of delivery and upload a project register form if needed.
   - If you have entered a shipping/billing address before, check whether the address information displayed on the page is correct.

6. Click **Submit**.

   You can track the status of the submitted order via **My Hik-Partner → Order → My Order** . For details, refer to ***View My Orders*** .

14.3 View My Orders

After submitting an order, you can track the status of your order, perform operations such as canceling or reordering as needed, and view related information such as invoices and transaction records.

The following order related information can be accessed via **My Hik-Partner → Order** .

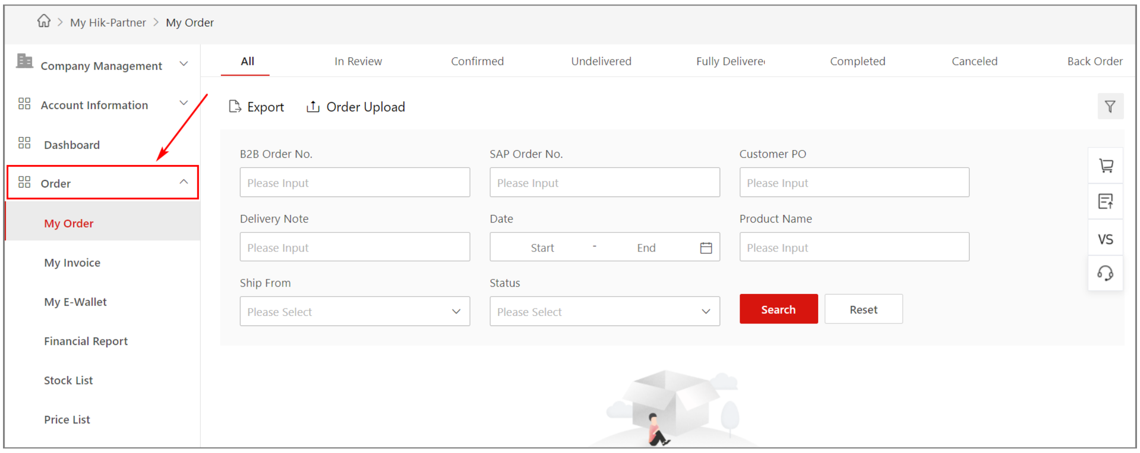


Figure 14-3 Order Related Information of Your Company

My Order Page

On the My Order page, you can view your orders by different status (e.g., In Review, Confirmed, Fully Delivered, Completed, etc.) and click an order to view the order details, including the products selected, total cost, and shipping related information.

Note

The My Order page can also be accessed via the In Review and Undelivered Order tabs displayed on the B2B page of the Order & Promotion module.

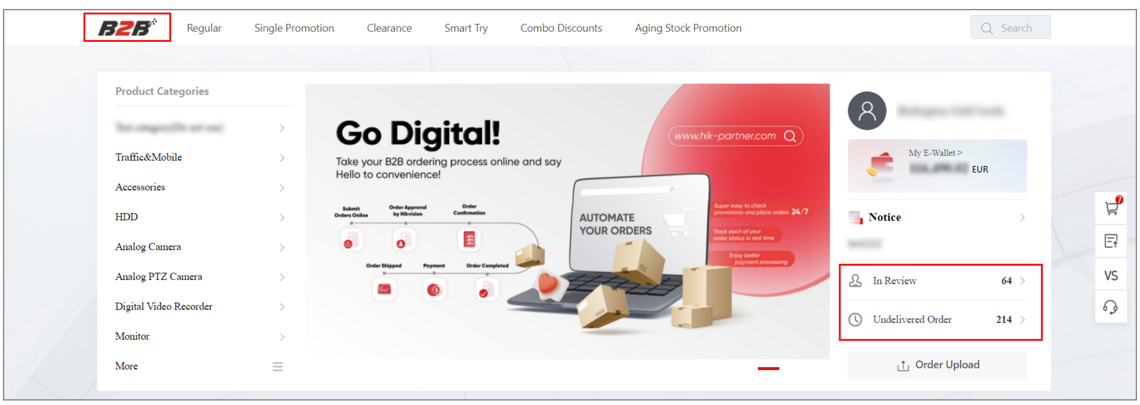


Figure 14-4 Another Way for Accessing the My Order Page

If needed, you can click **Export** to export the list of orders to your local PC, click **Order Upload** to submit an order using a predefined template, click next to an order No. to copy the order No., or click to reorder the same products of an order. To cancel ordering a product, click an order to enter the order details page, and click **Cancel** next to the product.

Note

The ordering of products that are fully delivered or the stock clearance / combo discount products are not allowed to be canceled.

My Invoice Page

On the My Invoice page, you can search for and view invoices of your past orders and export the list of invoices if needed.

My E-Wallet Page

On the My E-Wallet page, you can view your E-Wallet balance and transaction records, and search for specific records as needed.

Note

- If the type of a record is "Compensation", the number displayed is the amount you received when the corresponding compensation application is approved. For details about compensation, refer to ***Compensation*** .
- You can also click the E-Wallet balance displayed on the B2B page of the Order & Promotion module to access your E-Wallet.

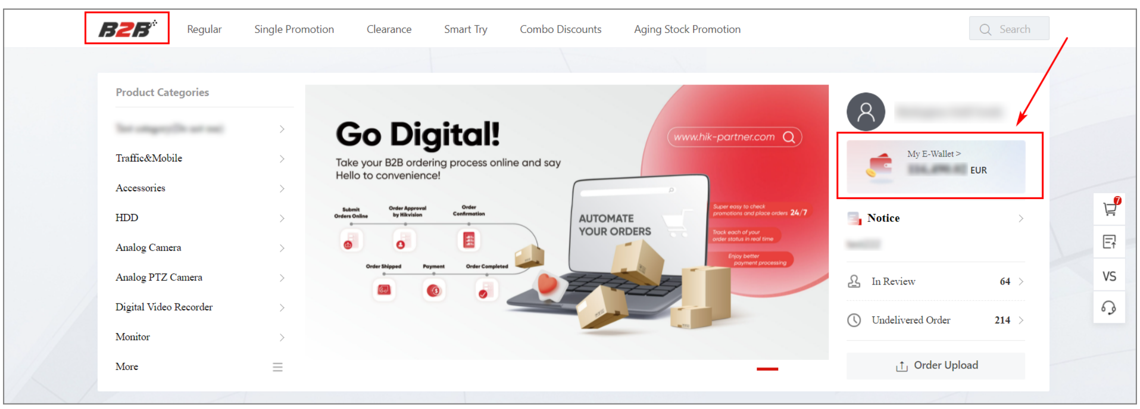


Figure 14-5 Another Way for Accessing the My E-Wallet Page

Financial Report Page

On the Financial Report page, you can view details of your credit status, account payable balance, and basic information of the invoices.

Stock List Page

On the Stock List page, you can view and search for stock related information of your products and export the full stock list or specific search results to the local PC as needed.

Price List Page

On the Price List page, you can view and search for price related information of all products and export the full price list or specific search results to the local PC as needed.

Chapter 15 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.
- Only the cloud storage service is supported by the solar camera.

15.1 Health Monitoring Service

Hik-Partner Pro offers a free package containing a series of basic features such as viewing device online status once you complete account registration. In some cases, for the capacity and functionality limitation of the free package, these basic features are insufficient for you to satisfy higher level needs of your customers (i.e., end users), such as their need for the maintenance of a large number of devices. Compared with the free package, the health monitoring package not only allows you to add more devices to Hik-Partner Pro, but also monitor the health status of your customers' devices and configure other value-added features. You can access the health monitoring service by purchasing health monitoring packages in the Service Market.

The following table shows the differences between the free package and the health monitoring package.

Note

For the countries and regions where the health monitoring service is currently free, the details of the health monitoring package might be different from the information displayed in the table below. Refer to the distributors or after-sales in these countries and regions for details.

Table 15-1 Differences Between Free Package and Health Monitoring Package

<table>
<tr><th>Functionality</th><th>Free Package</th><th>Health Monitoring Package</th></tr>
<tr><td>Adding Devices</td><td rowspan="5">• Supported
• Manageable Devices: 1024</td><td rowspan="5">• Supported
• Manageable Devices: More than 1024 based on the package you purchase.</td></tr>
<tr><td>Site & Device</td></tr>
<tr><td>Applying for Authorization</td></tr>
<tr><td>Viewing Device Online Status</td></tr>
<tr><td>Remote Configuration</td></tr>
</table>

Functionality	Free Package	Health Monitoring Package
Live View/Playback/ Downloading Video		
Device Firmware Remote Upgrade		
Health Monitoring	Not Supported	Supported
Exception Rule	Not Supported	Supported
Linkage Rule	Not Supported	Supported
Employee Management	Not Supported	Employees Accounts: 4 **Note** You can get 4 employee accounts for free only when purchasing the health monitoring service for the first time.
Role/Permission Management	Not Supported	Supported
Searching Operation Logs of Employees	Not Supported	Supported

15.1.1 Purchase Health Monitoring Service

You can purchase the health monitoring service packages online in the Service Market in Hik-Partner Pro or purchase a service key from the local distributor offline first, and then activate the health monitoring service packages by the service key in the Service Market.

Steps

Note

Purchasing the service by service key is only supported in some countries and regions. Contact the local distributor for details.

1. Go to the Service Market page.
2. In the Health Monitoring Package area, click **Online Purchase** to enter the Purchase Health Monitoring Package page.

Note

If your country or region supports service key and you have purchased a service key from the distributor, you can also click **Activate by Service Key** to purchase the service.

3. Select service packages and set the number of service packages that you want to purchase.

All-Type Device Monthly Package

An All-Type Device Monthly Package can be used to activate the service for a device of nearly any type. And the activated service lasts one month.

"All-Type 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-Type Device Monthly Package * 20

20 All-Type Device Monthly Packages sold as a batch. Set the number of batches to purchase.

All-Type Device Monthly Package * 100

100 All-Type Device Monthly Packages sold as a batch. Set the number of batches to purchase.

All-Type Device Annual Package

An All-Type 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-Type 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.

All-Type Device Annual Package * 20

20 All-Type Device Annual Packages sold as a batch. Set the number of batches to purchase.

All-Type Device Annual Package * 100

100 All-Type Device Annual Package sold as a batch. Set the number of batches to purchase.

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 Monthly Package * 20

20 Network Camera Monthly Packages sold as a batch. Set the number of batches to purchase.

Network Camera Monthly Package * 100

100 Network Camera Monthly Packages sold as a batch. Set the number of batches to purchase.

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.

Network Camera Annal Package * 20

20 Network Camera Annual Packages sold as a batch. Set the number of batches to purchase.

Network Camera Annual Package * 100

100 Network Camera Annual Packages sold as a batch. Set the number of batches to purchase.

4. Enter your VAT number.

Note

The VAT number entered here will be displayed in the payment receipt.

5. Select **Credit/Debit Cards** as the payment method.
6. Click **Checkout** to enter the payment page and finish the payment.
7. **Optional:** Go to **Service → Service Market → My Service → Health Monitoring Service** to view your health monitoring packages and manage them.

Note

For details, see ***Manage Your Health Monitoring Service*** .

15.1.2 Activate the Health Monitoring Service for Devices

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. For details, see ***Purchase Health Monitoring Service*** .

Steps

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

1. Enter the Activate Health Monitoring Service page in one of the following ways.
   - Choice 1: Click the **Site & Device** tab. Go to **Service → My Service → All Services** , and then click **Activate Health Monitoring Service**.
   - Choice 2: Click the **Site & Device** tab. Go to **Service → My Service → Health Monitoring Service** , and then click **Activate Health Monitoring Service**.
   - Choice 3: Go to the site details page, and then hover the cursor onto on the device card, and then click **Activate Service** on the pop-up dialog.
   - Choice 4: Go to the site details page, and then click a device to show the device details panel, and then hover the cursor onto on the panel and click **Activate Service**
   - Choice 5: Click **Activate Service** on the adding result page after adding detected online devices or adding a device by Hik-Connect (P2P). See ***Add Detected Online Device*** or ***Add Device by Entering Serial No.*** for details.

   The Activate Health Monitoring Service page will be displayed as one of the following two figures show.

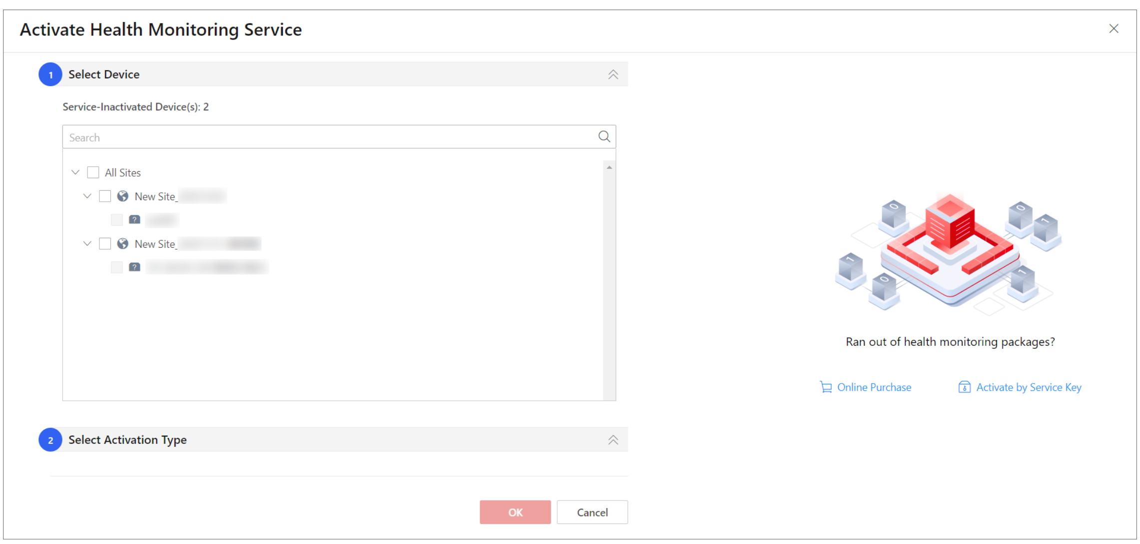


Figure 15-1 Select Devices to Activate Health Monitoring Service

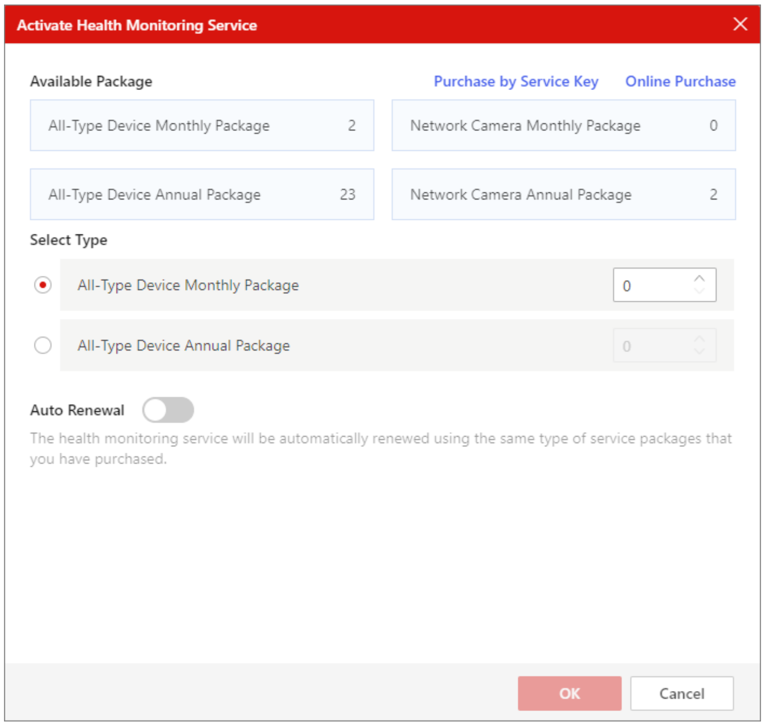


Figure 15-2 Activate Health Monitoring Service for One Selected Device

2. Select devices.

Note

Skip this step if you enter the Activate Health Monitoring Service page as ***Figure 15-2*** shows.

3. Select the activation type.

Note

- The number you set represents the number of months/years that the service lasts for each selected device.
- If service packages are insufficient, you can click **Online Purchase** or **Activate by Service Key** to purchase more. For details, see ***Purchase Health Monitoring Service*** .

Use All Device Package Only

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

Auto Renewal

When enabled, if the service for a device expires, the service will be automatically renewed using the same service package in previous activation. For example, assume that you activated a 1-month health monitoring service for a NVR using an All Device Monthly Package on 5/14/2021, the 1-month service will be automatically renewed using another All Device Monthly Package on 6/14/2021.

4. Click **OK**.

   After the health monitoring service is activated for devices, the notifications of all exceptions will be enabled by default.
5. **Optional:** Click **Site & Device → Customer Site** , and select a site to open to the site details page, and then perform the following operations if needed.

Renew the Service	Click a device with the service activated to show the device details panel, and click **Renew** to renew the service for the device.
Transfer the Service	Click a device with the service activated to show the device details panel, and click **Transfer** to open the Transfer Health Monitoring Service window, and then select a device to transfer the remaining service time from the current device to the selected device.
Enable Auto Renewing the Service	Click a device with the service activated to show the device details panel, and click **Auto Renewal** to Open the Auto Renew window, switch on **Auto Renewal**, and then select a type of service packages for auto renewal.
View Health Status of Devices	View health status of all devices on the device list, and view health status of a specific device on the device details panel. For details, refer to ***View Status of Devices in All Sites*** and ***View Status of Devices in a Specific Site*** .
Inspect Devices in the Sites	Click **Refresh** to inspect all the devices in the site.
Inspect a Single Device	Select a device and then click to inspect it.
Diagnose Devices of the Site	Click **Health Check** to open the Health Check window, and click **Check Now** to diagnose the devices of the site. When the checking completed, you can view the status of each device in the site. For AX PRO security control panel, NVR, and DVR, you can click **View Report** to export the diagnostics report as a PDF file to the local PC.
Filter Devices by Health Status	Click **Filter Devices** and filter devices by Normal Devices / Abnormal Devices / Devices Without Permission.

15.1.3 Manage Your Health Monitoring Service

In My Service, you can manage your health monitoring service. The available features for the management include viewing remaining service packages, service activation, service renewal, service transfer, service auto renewal, and so on.

Go to **Service → My Service → Health Monitoring Service** to enter the health monitoring service page (as the figure below shows).

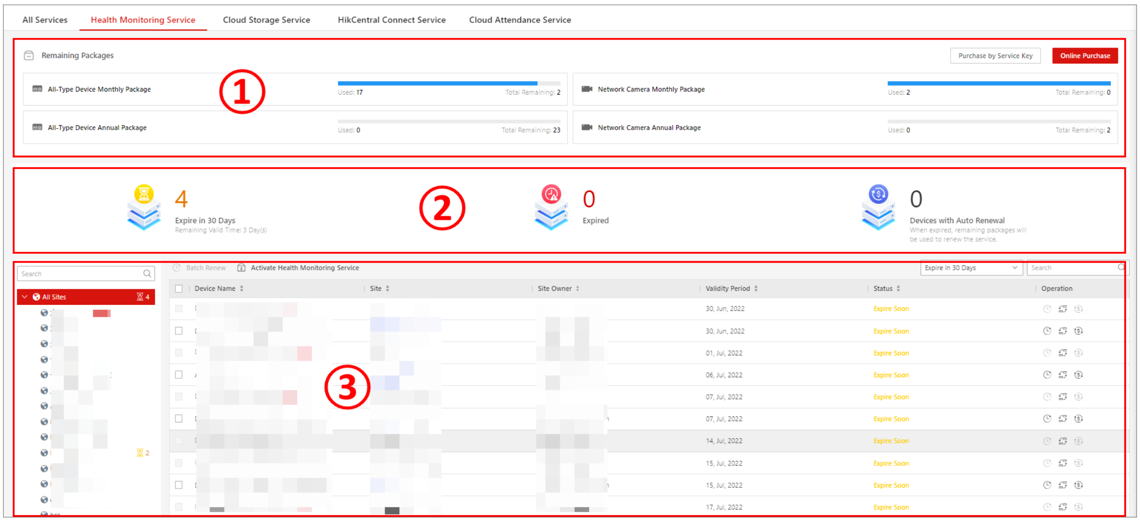


Figure 15-3 Manage Your Health Monitoring Service

On the page, the following features are available.

Table 15-2 Available Features

Area No.	Feature	Description
1	View Remaining Packages & Purchase More	View used number and remaining number of each type of heath monitoring packages. Click **Activate by Service Key** or **Online Purchase** to purchase more packages. For details, see ***Purchase Health Monitoring Service*** .
2	View Expiration and Auto Renewal Information	• **Expires in 30 Days**: The number of devices whose health monitoring services expire in 30 days. You can click **Expires in 30 Days** to view these devices in the device list below. • **Expired**: The number the devices whose health monitoring services have expired. You can click **Expired** to view these devices in the device list below. • **Devices with Auto Renewal**: The number of devices for which you have enabled service auto-renewal. You can click **Devices with Auto Renewal** to view these devices.
3	Filter Devices or Search by Keywords	Select a Site from the site list on the left, and then select a filter type (All, Expire in 30 Days, or Expired) from the drop-down list to filter devices. Or enter key words to search for matched devices.

Area No.	Feature	Description
3	Activate Service	Click **Activate Health Monitoring Service** to activate the heath monitoring service for specific devices. For details, see ***Activate the Health Monitoring Service for Devices*** .
3	Batch Renew Service for Devices	Select devices and then click **Batch Renew** to renew the service for the selected devices. The process of renewing the service is similar to that of activating the service. See ***Activate the Health Monitoring Service for Devices*** for details.
3	Renew Service for a Device	Click in the Operation column to renew service for a device. The process of renewing the service is similar to that of activating the service. See ***Activate the Health Monitoring Service for Devices*** for details.
3	Transfer Service	Click in the Operation column to transfer the remaining service time from the current device to another.
3	Enable Service Auto Renewal	Click in the Operation column to open the Auto Renew window, switch on **Auto Renewal**, and then select a type of service packages for auto renewing the health monitoring service.

15.2 Purchase Employee Account Add-On

Hik-Partner Pro offers only one Installer Admin account for your company to manage resources in the system. You can invite more employees to join Hik-Partner Pro to work collaboratively. By default, the status of employees are limited and some operations like managing sites are not available to them. However, the account limits can be removed by purchasing the employee account add-on. You can purchase the employee account add-on online in the Service Market in Hik-Partner Pro or purchase a service key from the local distributor offline first, and then activate the employee account add-on by the service key in the Service Market.

Steps

Note

Activating the service by service key is only supported in some countries and regions. Contact the local distributor for details.

1. Go to the Service Market page.

2. In the Employee Account Add-On area, click **Online Purchase** to enter the Purchase Employee Account Add-On page.

Note

If your country or region supports service key and you have purchased a service key from the distributor, you can also click **Activate by Service Key** to purchase the service.

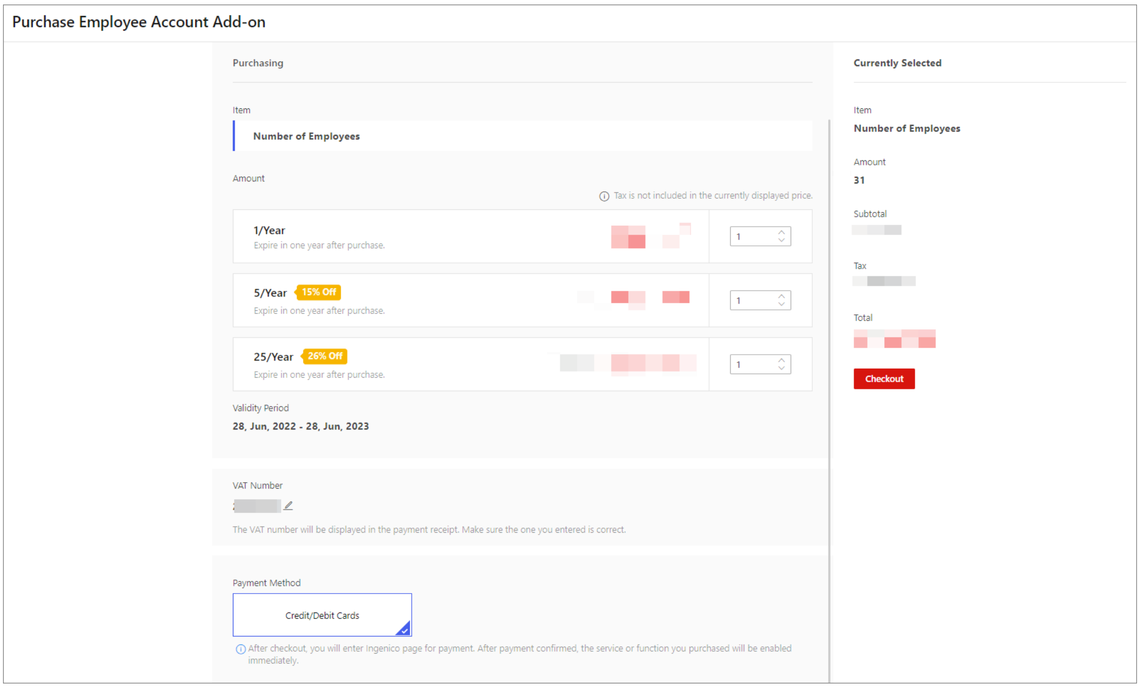


Figure 15-4 Purchase Employee Account Add-On

3. Select type(s) of add-on and set the number of employee accounts that you want to purchase.

Note

An **1/Year**, **5/Year**, or **25/Year** add-on can be used to invite 1, 5, or 25 employee accounts which will expire after one year.

4. Enter your VAT number.

Note

The VAT number entered here will be displayed in the payment receipt.

5. Select **Credit/Debit Cards** as the payment method.
6. Check your purchasing information and click **Checkout** to enter the payment page and finish the purchase.

15.3 Cloud Attendance Service

The cloud attendance service provides a cloud-based and all-in-one solution for access control and attendance management in various businesses. You can create cloud attendance systems for your customers, so that your customers, such as managers of small organizations or human resource director, can configure the system on the Hik-Connect portal (***http://www.hik-connect.com***) and use it to manage the attendance of the employees. Employees of your customers can check in or check out via the devices configured in the cloud attendance system. With the Hik-Connect Mobile Client V4.13.0 or later, the employees can control doors and check attendance records on their mobile phones.

Note

The cloud attendance service is only supported in some countries and regions currently. You might fail to find related functionality due to its unavailability in your country or region. If you need related functionality, please feel free to contact the local distributor or our branch office.

15.3.1 Flow Chart for Setting the Cloud Attendance Service

The flow chart below shows the recommended process for setting cloud attendance service.

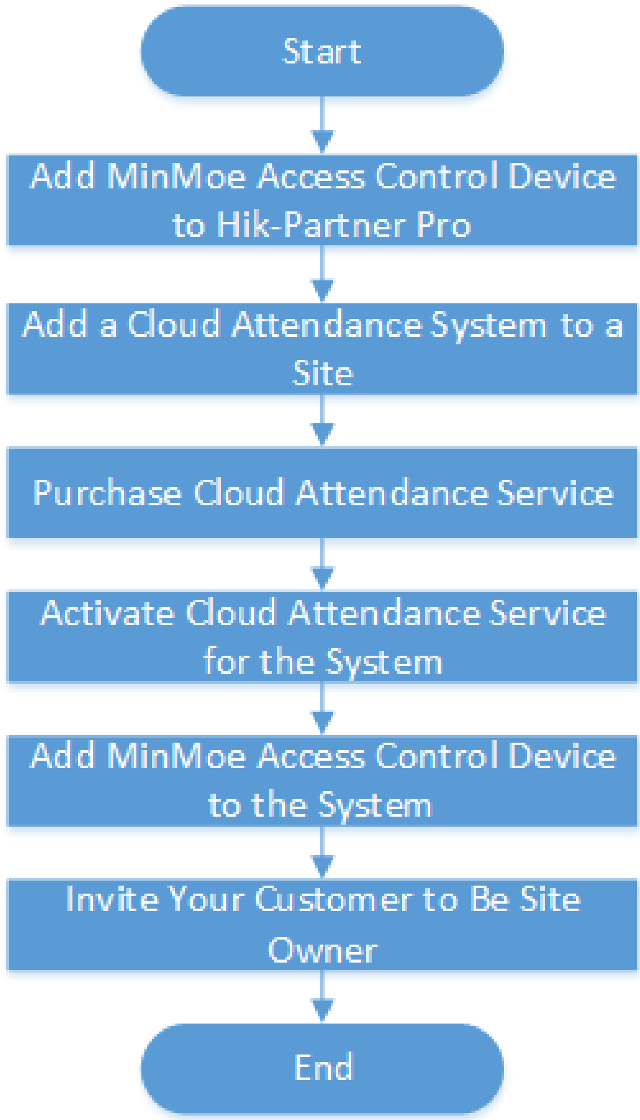


Figure 15-5 Flow Chart

The table below shows the description of each step and the link to corresponding section.

Table 15-3 Flow Chart Description

Step	Description
Add MinMoe Access Control Devices to Hik-Partner Pro	Add MinMoe access control devices to site(s) which are owned by the same customer. For details about adding devices to Hik-Partner Pro, see ***Add Device*** and its sections.
Add a Cloud Attendance System to a Site	Add a cloud attendance system to a specific site. The cloud attendance system is used for grouping and managing MinMoe

Step	Description
	access control devices. For details about adding the system, see ***Add Cloud Attendance System*** .
Purchase Cloud Attendance Service	See ***Purchase Cloud Attendance Service*** for details.
Activate Cloud Attendance Service	Activate the cloud attendance service for the system. For details, see ***Add Cloud Attendance System***
Add Cloud Attendance Devices to the System	Add MinMoe access control devices to the system. For details, see ***Add Cloud Attendance System*** .
Hand Over Site to Your Customer	After completing the required configurations, hand over the site to your customer and so they will be the site owner. For details, see ***Hand Over Site*** . **Note** When your customer accept the site handover and approving activating the cloud attendance service on the Hik-Connect Mobile Client (V 4.15.0 or later), they will be able to set access levels and attendance rules for their employees via the Hik-Connect Portal (***http://www.hik-connect.com***), and their employees will be able to use the Hik-Connect Mobile Client to check their attendance records.

15.3.2 Purchase Cloud Attendance Service

You can purchase the cloud attendance service packages online in the Service Market in Hik-Partner Pro or purchase a service key from the local distributor offline first, and then activate the cloud attendance service packages by the service key in the Service Market.

Steps

Note

Activating the service by service key is only supported in some countries and regions. Contact the local distributor for details.

1. In the left navigation, click **Service → Service Market** to enter the Service Market page.
2. In the Cloud Attendance area, click **Online Purchase** to enter the Purchase Cloud Attendance Package page.

Note

If your country or region supports service key and you have purchased a service key from the distributor, you can also click **Activate by Service Key** to purchase the service.

3. Select the service packages (purchase by month or by year), and set the number of service packages that you want to purchase.

   Cloud Attendance Package (Monthly)

   The service term is one month. The service term starts when you activate the service.

   12 * Cloud Attendance Package (Monthly)

   12 Cloud Attendance Packages sold as a batch.

Note

The price of the package changes when you purchase different numbers of packages.

4. Click to enter the VAT number, and click to confirm.

Note

The VAT number will be displayed in the payment receipt.

5. Select **Credit/Debit Cards** as the payment method.
6. Click **Checkout** to enter the payment page and finish the payment.
7. **Optional:** Go to **Service → Service Market → My Service → Cloud Attendance Service** to view your cloud attendance packages and manage them.

Note

For details, see ***Manage Your Cloud Attendance Service*** .

15.3.3 Add Cloud Attendance System

You can add a cloud attendance system for a site to set up the basic attendance management environment for the Site Owner.

Steps

1. Go to the Customer Site page.
2. Select the site where you want to add the cloud attendance system.
3. Select the **Cloud Attendance** tab.
4. Click **Add Cloud Attendance System**.
5. Create a name for the system.
6. Click **OK**.

Note

The service is inactivated.

7. Activate the cloud attendance service for the site.
   1) Click **Free Trial**.

2) Click **Confirm** in the pop-up window.

Note

You can view the trial capacity of the service (25 persons) and the expiry date.

8. **Optional:** If you need to expand and renew the service, click **Expand & Renew**.

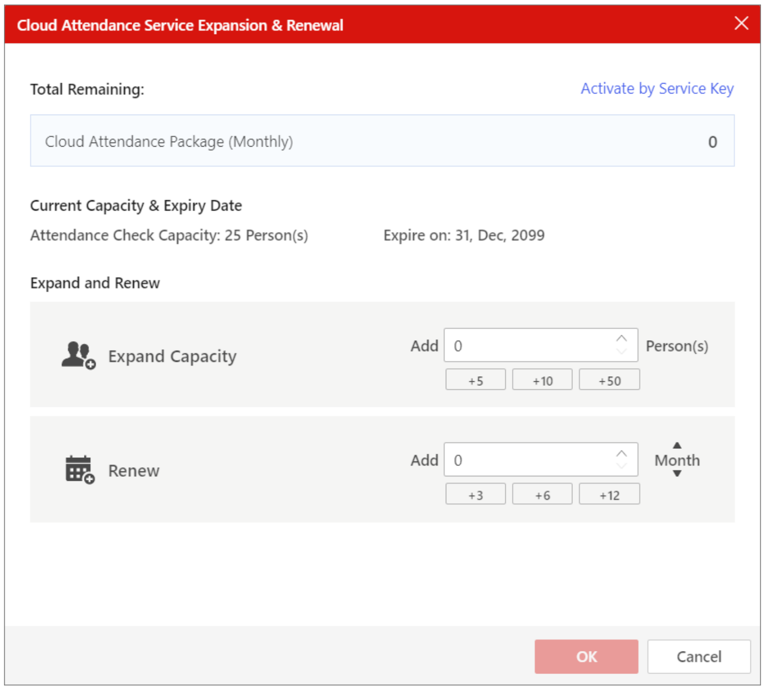


Figure 15-6 Cloud Attendance Service Expansion & Renewal

1) Set the number of person(s) to be added.
2) Set the month(s) to be renewed.

Note

You can view the number of cloud attendance service packages needed after the service is expanded and renewed.

3) **Optional:** If service packages are insufficient, you can click **Online Purchase** or **Activate by Service Key** in the upper-right corner to purchase more.

Note

For details, refer to ***Purchase Cloud Attendance Service*** .

4) Click **OK**.

9. Click **Add Device** or **Edit** to add access control devices to the cloud attendance system or edit the devices.
   - To add the devices in the current site to the system, click **Add**, select the devices, and click **OK**.
   - To add the devices in the other sites that belong to the same Site Owner, click **Add Other Sites' Devices**, select the devices, and click **OK**.

Note

Make sure to switch on **Cloud Attendance** for the devices.

What to do next

Hand over the site to the Site Owner and inform the Site Owner to accept the cloud attendance service permission application. See details in ***Hand Over Site*** .

15.3.4 Manage Your Cloud Attendance Service

In My Service, you can manage your cloud attendance service. The available features for the management include viewing remaining service packages, service activation, service renewal, and so on.

Go to **Service → My Service → Cloud Attendance Service** to enter the cloud attendance service page (as the figure below shows).

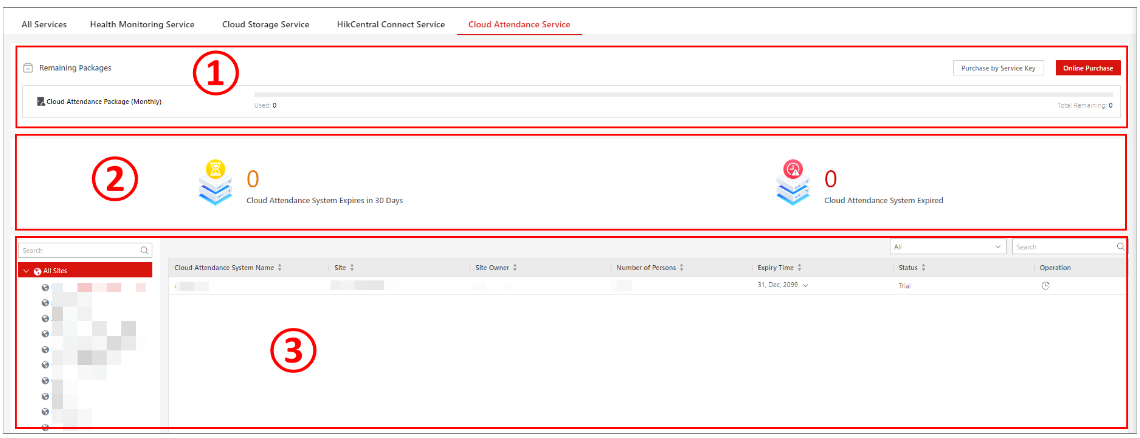


Figure 15-7 Manage Your Cloud Attendance Service

On the page, the following features are available.

Table 15-4 Available Features

Area No.	Feature	Description
1	View Remaining Packages & Purchase More	• View used number and remaining number of each type of cloud attendance packages. • Click **Activate by Service Key** or **Online Purchase** to purchase more packages. For details, see ***Purchase Cloud Attendance Service*** .
2	View Expiration Information	• **Cloud Attendance System Expires in 30 Days**: The number of cloud attendance systems that expire in 30 days.

Area No.	Feature	Description
		You can click **Cloud Attendance System Expires in 30 Days** to view these cloud attendance systems in the list below. • **Cloud Attendance System Expired**: The number of cloud attendance systems that expired. You can click **Cloud Attendance System Expired** to view these cloud attendance systems in the list below.
3	Filter Cloud Attendance Systems or Search by Keywords	• Select a Site from the site list on the left, and then select a filter type (All, Expire in 30 Days, Expired, or Trial) from the drop-down list to filter cloud attendance systems. • Enter keywords (of cloud attendance system name, site name, or site owner name) to search for the matched cloud attendance systems.
4	Renew Service	Click in the Operation column to renew the service. See ***Add Cloud Attendance System*** for details.

15.4 Cloud Storage Service

Hik-Partner Pro offers cloud storage solution for the event-related video footage, which refers to the video footage recorded when a pre-defined event is detected by the channel of an encoding device.

After you add a cloud storage device to the platform and complete cloud storage settings, the device will function as the transmission medium by uploading the event-related video footage from its linked channels to the cloud. The uploaded video footage will be retained for 7 days, 30 days, 90 days, 180 days, or 365 days on the cloud, basing on the types of the cloud storage service packages purchased from the service market.

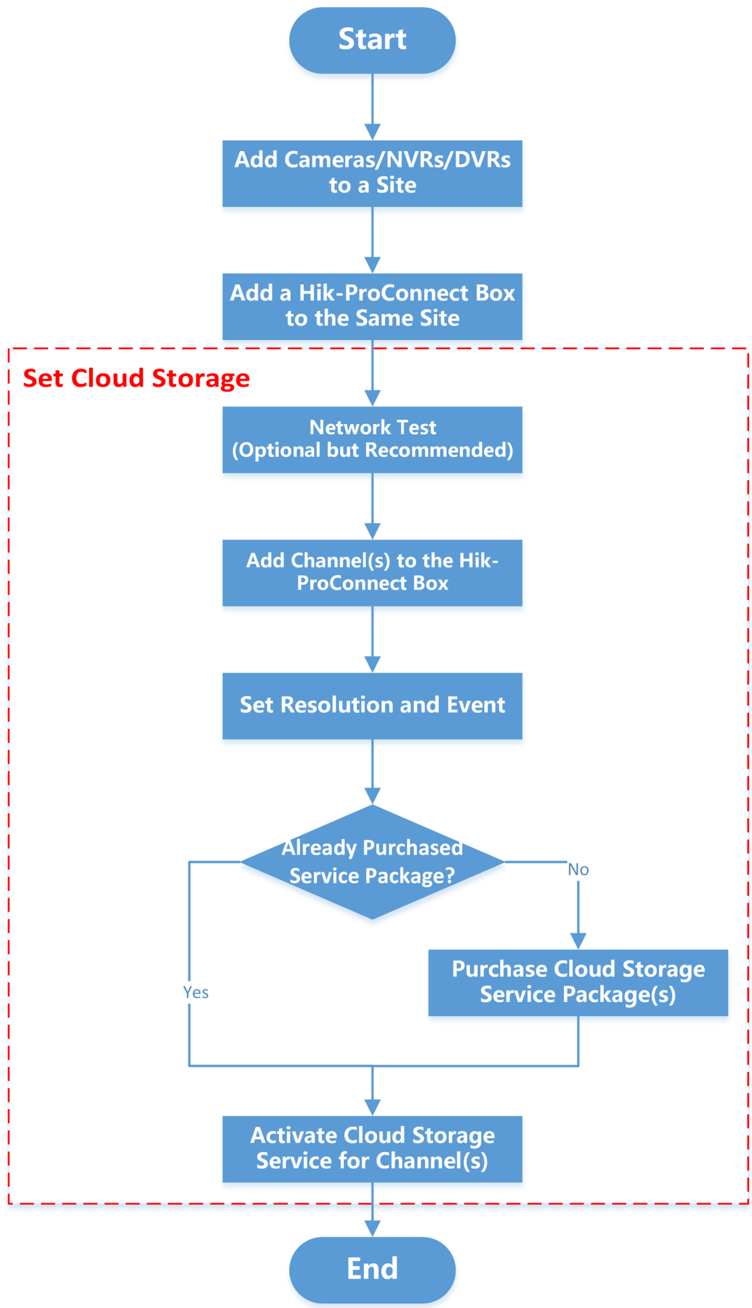
15.4.1 Flow Chart for Setting Cloud Storage Service

The flow charts below shows the recommended procedures for using cloud storage service by Hik-ProConnect box, DVR that supports cloud storage, NVR that supports cloud storage, and solar camera.

Note

If your DVR/NVR does not support cloud storage, you should use a Hik-ProConnect box to help the DVR/NVR upload footage to the cloud, and the flow chart is the same as that for the Hik-ProConnect box.

Flow Chart for Hik-ProConnect Box



The following table shows the description for each procedure of the flow chart.

Table 15-5 Flow Chart Description

Procedure	Description
Add Cameras/NVRs/DVRs to a Site	Add cameras, NVRs, or DVRs to a site. For details, see ***Add Device*** .
Add a Hik-ProConnect Box to the Same Site	Add a Hik-ProConnect box to the same site by Hik-Connect (P2P). For details, see ***Add Device by Entering Serial No.*** , ***Batch Add Devices*** , and ***Add Detected Online Device*** . **Note** For the Hik-ProConnect box added by IP/Domain name, cloud storage service is not supported.
Set Cloud Storage	Set cloud storage for the Hik-Partner Pro. See ***Set Cloud Storage for Hik-ProConnect Box*** for details. The following list shows the descriptions of the sub-procedures. • Network Test: Test your network condition to get the recommended settings for cloud storage. See ***Network Test*** for details. • Add Channel(s) to the Hik-ProConnect Box: Add channel(s) to the Hik-ProConnect box to allow the latter to get video footage data from the channel(s). • Set Resolution and Event: Set resolution for the channels, and set the event(s) that will trigger the channel to record related video footage. • Purchase Cloud Storage Service Package(s): Purchase cloud storage service packages from the service market. See ***Purchase Cloud Storage Service*** for details. **Note** You can also activate service packages by service key. Consult the distributor to get the service key. • Activate Cloud Storage Service for Channel(s): Activate cloud storage service for specific channel(s) using the purchased cloud storage service package(s) or service key. See ***Activate or Renew Service for a Channel*** for details.

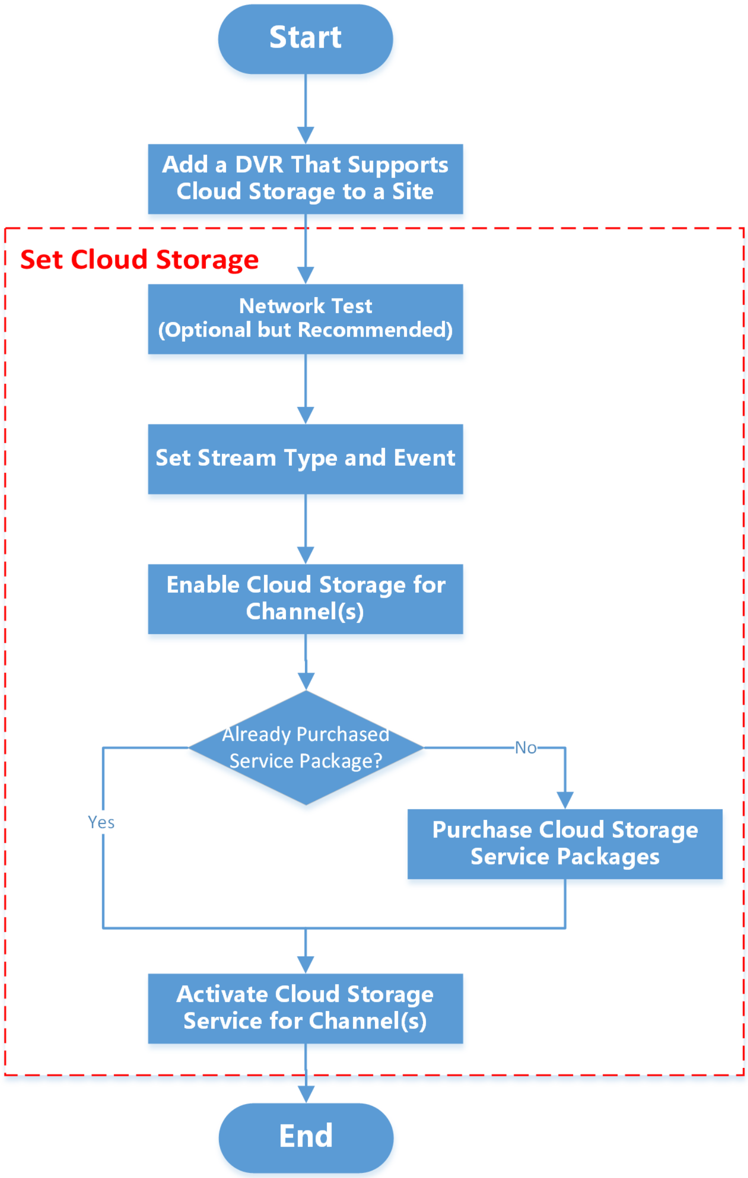


Figure 15-8 Flow Chart for DVR That Supports Cloud Storage

The following table shows the description for each procedure of the flow chart.

Table 15-6 Flow Chart Description

Procedure	Description
Add a DVR That Supports Cloud Storage to a Site	Add a DVR that supports cloud storage to a site by Hik-Connect (P2P). For details, see ***Add Device by Entering Serial No.*** , ***Batch Add Devices*** , and ***Add Detected Online Device*** .

Procedure	Description
	Note If the DVR that supports cloud storage is added by IP/Domain Name, cloud storage service is not supported.
Set Cloud Storage	Set cloud storage for the DVR that supports cloud storage. For details, see ***Set Cloud Storage for DVR*** . The following list shows the descriptions of the sub-procedures. • Network Test: Test your network condition to get the recommended settings for cloud storage. See ***Network Test*** for details. • Enable Cloud Storage for Channel(s): Enable cloud storage for the channel(s) of the DVR that supports cloud storage. • Set Stream Type and Event: Set stream type (main-stream or sub-stream) for the channel(s). And set event(s) that will trigger the channel to record related video footage. • Purchase Cloud Storage Service Package(s): Purchase cloud storage service packages from the service market. See ***Purchase Cloud Storage Service*** for details. **Note** You can also activate service packages by service key. Consult the distributor to get the service key. • Activate Cloud Storage Service for Channel(s): Activate cloud storage service for specific channel(s) using the purchased cloud storage service package(s) or service key. See ***Activate or Renew Service for a Channel*** for details.

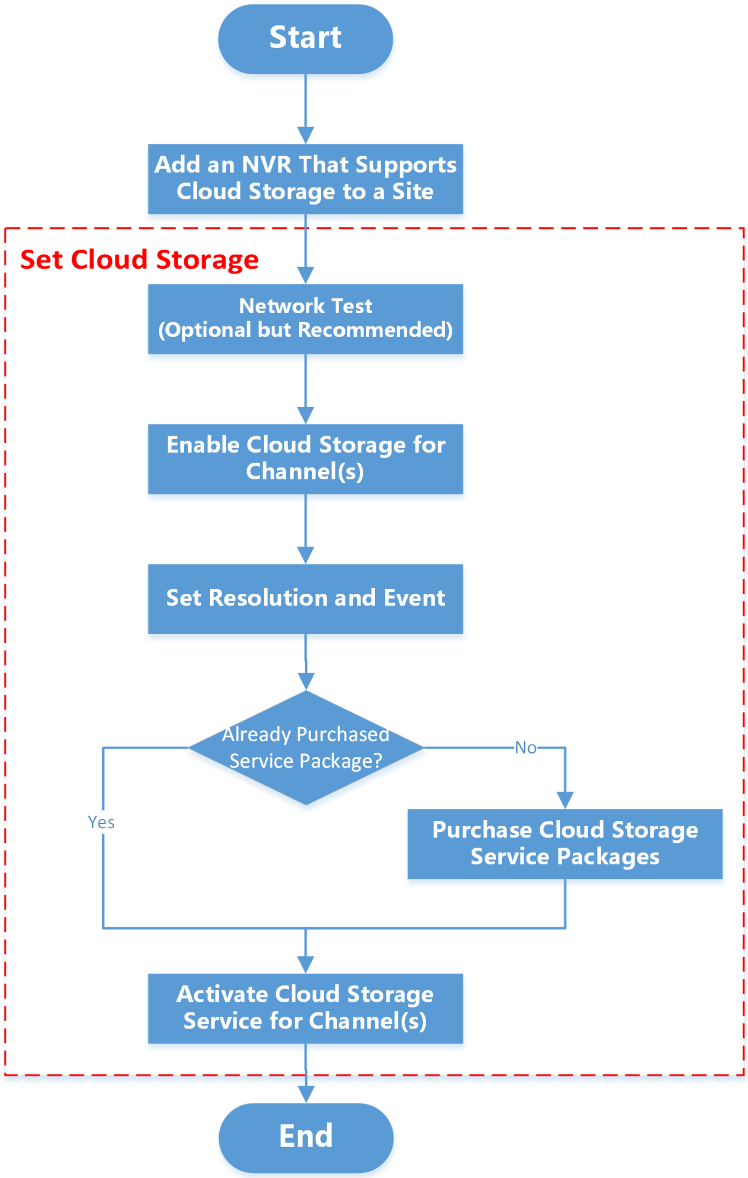


Figure 15-9 Flow Chart for NVR That Supports Cloud Storage

The following table shows the description for each procedure of the flow chart.

Table 15-7 Flow Chart Description

Procedure	Description
Add an NVR That Supports Cloud Storage to a Site	Add an NVR that supports cloud storage to a site by Hik-Connect (P2P). For details, see ***Add Device by Entering Serial No.*** , ***Batch Add Devices*** , and ***Add Detected Online Device*** .

Procedure	Description
	Note If the NVR that supports cloud storage is added by IP/Domain Name, cloud storage service is not supported.
Set Cloud Storage	Set cloud storage for the NVR that supports cloud storage. For details, see ***How to enable cloud storage for an NVR that supports cloud storage?*** . The following list shows the descriptions of the sub-procedures. • Network Test: Test your network condition to get the recommended settings for cloud storage. See ***Network Test*** for details. • Enable Cloud Storage for Channel(s): Enable cloud storage for the channel(s) of the NVR that supports cloud storage. **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 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. • Set Resolution and Event: Set resolution for the channels, and set the event(s) that will trigger the channel to record related video footage. • Purchase Cloud Storage Service Package(s): Purchase cloud storage service packages from the service market. See ***Purchase Cloud Storage Service*** for details.

Procedure	Description
	Note You can also activate service packages by service key. Consult the distributor to get the service key. • Activate Cloud Storage Service for Channel(s): Activate cloud storage service for specific channel(s) using the purchased cloud storage service package(s) or service key. See ***Activate or Renew Service for a Channel*** for details.

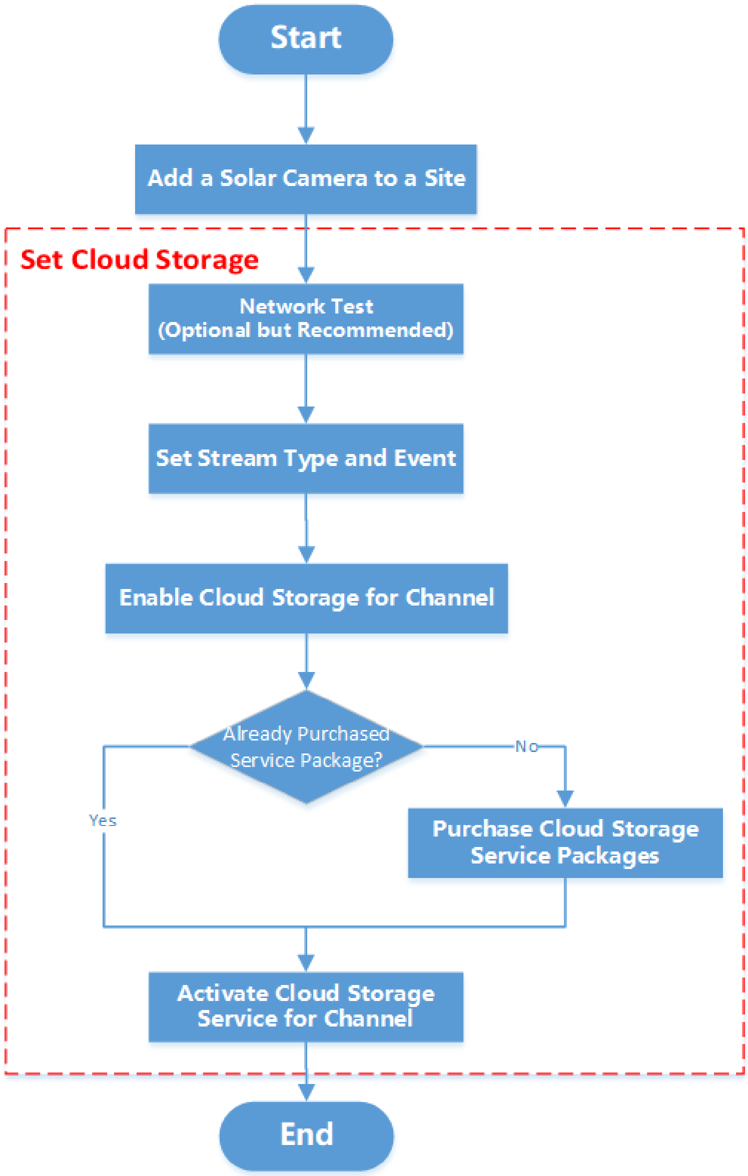


Figure 15-10 Flow Chart for Solar Camera

The following table shows the description for each procedure of the flow chart.

Table 15-8 Flow Chart Description

Procedure	Description
Add a Solar Camera to a Site	Add a solar camera to a site by Hik-Connect (P2P). For details, see ***Add Device by Entering Serial No.*** , ***Batch Add Devices*** , and ***Add Detected Online Device*** .

Procedure	Description
	Note If the solar camera is added by IP address / domain name, cloud storage service is not supported.
Set Cloud Storage	Set cloud storage for the solar camera. For details, see ***Set Cloud Storage for Solar Camera*** . The following list shows the descriptions of the sub-procedures. • Network Test: Test your network condition to get the recommended settings for cloud storage. See ***Network Test*** for details. • Set Stream Type and Event: Set stream type (main stream or sub-stream) for the channel. And set the event that will trigger the channel to record related video footage. **Note** Currently only motion detection is supported. • Enable Cloud Storage for Channel: Enable cloud storage for the channel of the solar camera. • Purchase Cloud Storage Service Package(s): Purchase cloud storage service packages from the service market. See ***Purchase Cloud Storage Service*** for details. **Note** You can also activate service packages by service key. Consult the distributor to get the service key. • Activate Cloud Storage Service for Channel: Activate cloud storage service for the channel using the purchased cloud storage service package(s). See ***Activate or Renew Service for a Channel*** for details.

15.4.2 Purchase Cloud Storage Service

There are seven types of cloud storage service packages, namely, 7-Day Monthly Package, 7-Day Annual Package, 30-Day Monthly Package, 30-Day Annual Package, 90-Day Annual Package, 180-Day Annual Package, and 365-Day Annual Package. You should purchase the cloud storage service from the service market before using it.

Before You Start

The cloud storage service is available for purchase only if your company is authenticated.

Steps

1. Go to the Service Market page.
2. Click **Cloud Storage** under **Value-Added Services**.
3. In the Cloud Storage area, click **Online Purchase** to enter the purchasing page.

   You can view the seven types of cloud storage service packages and their corresponding prices.
4. Click or manually enter a number to define the number of the packages to be purchased.

   Note

   - You can purchase one or more packages at a time. The validity period of the service is one year after purchase, and thus you should activate the service within the validity period.
   - The number before "Day" (e.g. 7-Day, 30-Day, 90-Day, etc.) refers to the retention period of the event-related video footage on the cloud. **Monthly** and **Annual** refer to how long the service will last after activation.

   Example

   For example, if you select **7-Day Monthly Package**, the video footage can be saved on the cloud storage for 7 days, and it will be covered by new video footage from the 8th day. After activation, the service will last for a month.

   The selected service package(s) will be displayed on the right side of the page.
5. Click to enter the VAT number, and click to confirm.

   Note

   The VAT number entered here will be displayed in the payment receipt.
6. Select **Credit/Debit Cards** as the payment method.
7. Click **Checkout** to enter the payment page and finish the payment.
8. **Optional:** Click **Service → My Service → Cloud Storage Service** to view the service package(s) you have purchased.

15.4.3 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 click 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 click the device in the device list to open its settings panel to set cloud storage for it later.

1. Add a Hik-ProConnect box to a site by Hik-Connect (P2P).

Note

- For details about adding the Hik-ProConnect box, see ***Add Device by Entering Serial No.*** , ***Batch Add Devices*** , or ***Add Detected Online Device*** .
- If you add the Hik-ProConnect box by IP/Domain name, its cloud storage functionality will be unavailable.

When you complete adding the device, the entry for setting cloud storage will be displayed on the adding result page.
2. Click **Cloud Storage Settings** to start setting cloud storage parameters.

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

Note

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

The Add Channel window will pop up.

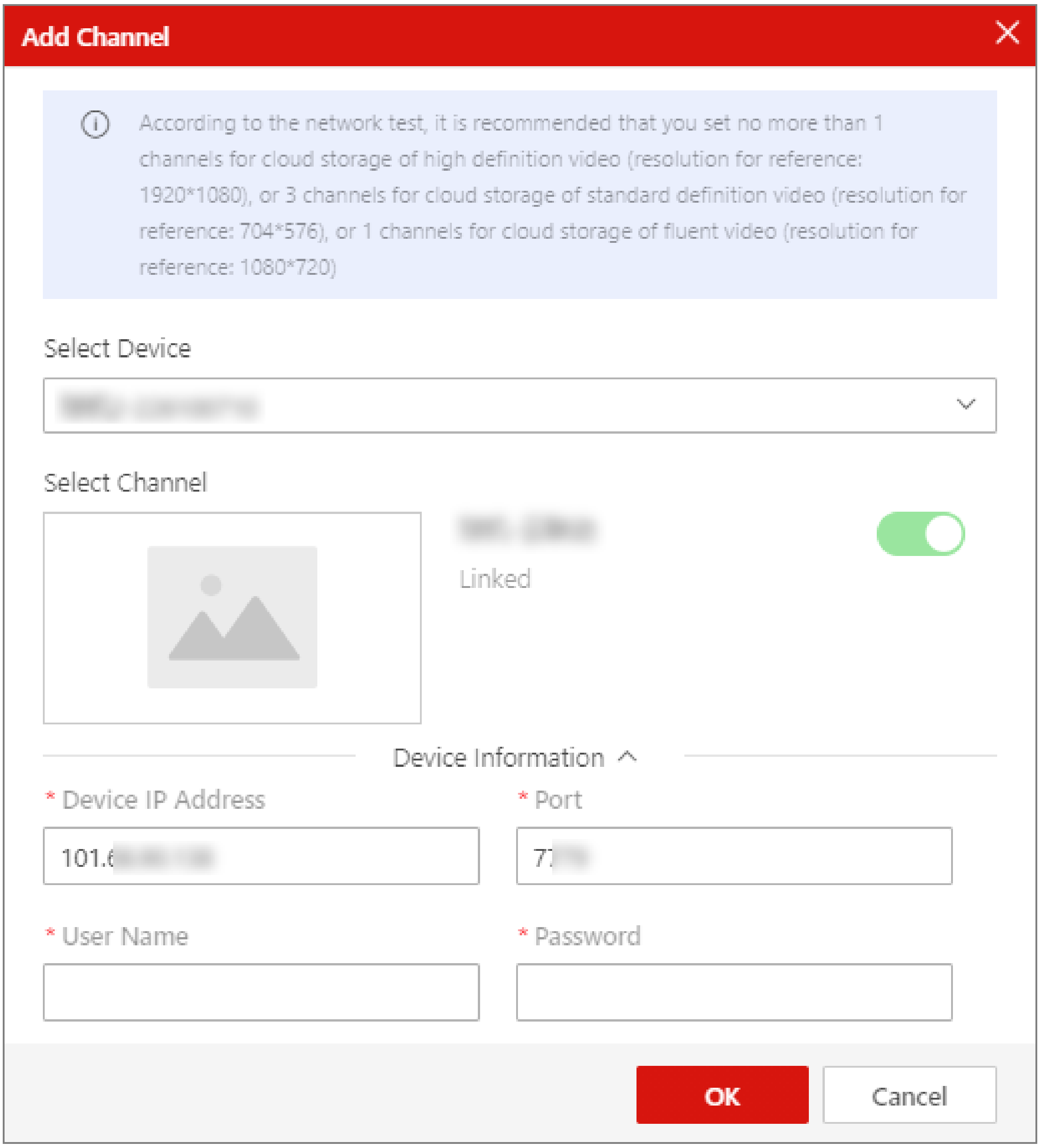


Figure 15-11 Add Channel Window

4. Add channel(s) to Hik-ProConnect box to enable cloud storage functionality for them.

1) Select a device (e.g., NVR and network camera) from the drop-down list on the Add Channel window.

The channels of the device will be displayed. And you can click **Device Information** to view or edit the device information, including device IP address, port No., device user name, and password.

Note

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

2) Turn on the switch(es) to add specific channel(s) to the Hik-ProConnect box so as to enable their cloud storage functionality.
3) Enter the information of the device to which the channel belongs, including IP address, port No., user name, and password.
4) Click **OK**.

You will enter the Cloud Storage Settings page, which displays the channel(s) already added to the Hik-ProConnect box.

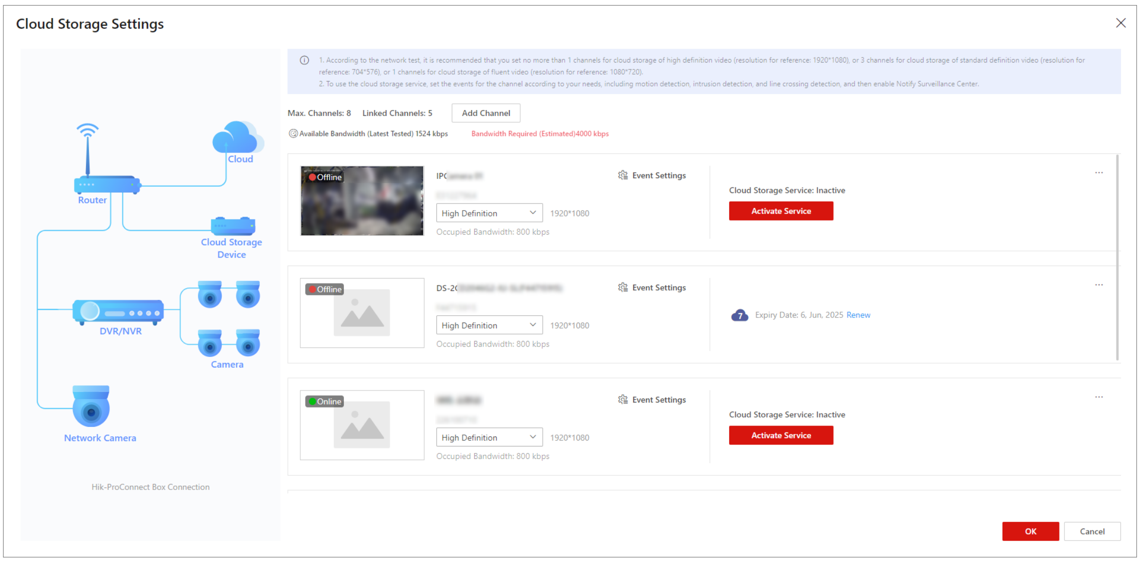


Figure 15-12 Cloud Storage Settings Page

5. Set resolution of the footage to be uploaded to the cloud.
   - Select **Standard Definition** or **High Definition** from the drop-down list according to the recommended resolution displayed on the Cloud Storage Settings page (if you have done network test).

   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).

   - Click , and then select a resolution (1080P, 720P, 4CIF, or CIF) from the drop-down list in the pop-up window, and then set the bit rate according to the recommendation shown on the pop-up window.
6. Click **Event Settings** to set the event(s) that will trigger video recording action of the channel.

Note

The events that support such a trigger include motion detection, intrusion, and line crossing. For the settings of different events are similar, here we only briefly introduce how to set motion detection. For details about settings of other events, see the user manual of the channel (camera).

Enable Motion Detection

Turn on the switch to enable motion detection.

Area Settings

Tap **Draw Area** to draw an area on the image, and then drag the slider to set the sensitivity of motion 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 checked, otherwise the channel will not record event-related video footage even if the event is detected.

7. **Optional:** Edit or delete a specific channel.

Edit a Channel	Click ••• → ⇌ to edit the settings of the channel.
Delete a Channel	Click ••• → 🗑 to delete the channel.

8. Click **Activate** to activate cloud storage service for the channel.

Note

For details about how to activate the service, see ***Activate or Renew Service for a Channel*** .

The event related video footage of the channel will be uploaded to the cloud.

9. **Optional:** Click ••• → ⇌ to switch channel to use the activated service.
10. Click **Finish**.

15.4.4 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 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 then select the **Cloud Storage** tab. Click **Enable Cloud Storage Service** to set up cloud storage for the NVR and its channels.

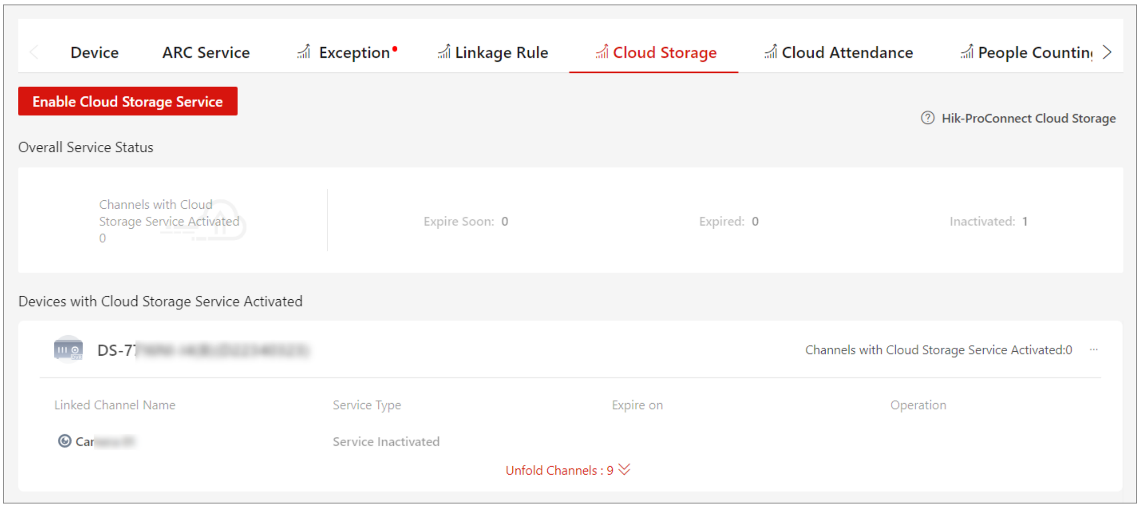


Figure 15-13 Cloud Storage

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

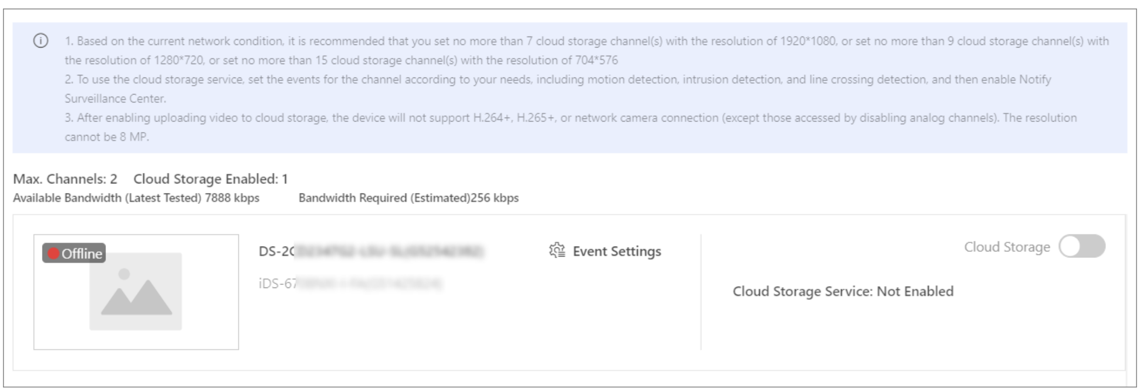


Figure 15-14 Cloud Storage Settings

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 information on the video resolution, event settings, and service activation.

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 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.

15.4.5 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, but it is recommended that you click the entry to start the settings, including network test (optional), event settings, stream type 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 DVR upload footage to the cloud. See details in ***Set Cloud Storage for Hik-ProConnect Box*** .
- If you skip the cloud storage settings when completing adding the DVR that supports cloud storage, you can click the device in the device list to open its settings panel to set cloud storage for it later.

1. Add a DVR that supports cloud storage to a site by Hik-Connect (P2P).

   Note

   - For details about adding a DVR that supports cloud storage, see ***Add Device by Entering Serial No.*** , ***Batch Add Devices*** , or ***Add Detected Online Device*** .
   - If you add the DVR that supports cloud storage by IP/Domain name, its cloud storage functionality will be unavailable.

   When you completes adding the device, the entry for setting cloud storage will be displayed on the adding result page.
2. Click **Cloud Storage Settings** to start setting cloud storage parameters.

   You enter the Network Test page.
3. **Optional:** Click **Start** to test the network performance if the network bandwidth is limited, and then click **Next** when the test completes.

Note

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

You enter the Cloud Storage Settings page, on which all the channels of the DVR that supports cloud storage are displayed.

4. Select **Main Stream** or **Sub Stream** from the drop-down list as the stream type for the channel.

Note

The video definition of main stream and sub stream are displayed below the drop-down list. 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).

5. Click **Event Settings** to set the events that will trigger video recording action of the channel.

Note

The events that support such a trigger include motion detection, intrusion, and line crossing. For the settings of different events are similar, here we only briefly introduce how to set motion detection. For details about settings of other events, see the user manual of the channel (camera).

Enable Motion Detection

Turn on the switch to enable motion detection.

Area Settings

Tap **Draw Area** to draw an area on the image, and then drag the slider to set the sensitivity of motion 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 checked, otherwise the channel will not record video footage even if the event is detected.

6. Turn on **Cloud Storage** to enable cloud storage functionality for the channel.

Note

If it is the first time you enable cloud storage for a channel of the DVR that supports cloud storage, the DVR will be automatically rebooted. Please wait patiently until it completes rebooting and then open its settings panel to complete the steps below.

7. Click **Activate** to activate cloud storage service for the channel.

Note

For details about how to activate the service, see ***Activate or Renew Service for a Channel*** .

The DVR that supports cloud storage will automatically reboot. After that, the event related video footage of the channel will be uploaded to the cloud.

Note

When cloud storage service is activated for the channel, you cannot turn off **Cloud Storage** for the channel by default.

8. Click **Finish**.
9. **Optional:** Click the DVR that supports cloud storage in the device list to open its settings panel, and then click **Edit** to edit the settings of its channels.

Note

If you turn off **Cloud Storage** for all of its channels, the DVR that supports cloud storage will automatically reboot itself.

15.4.6 Set Cloud Storage for Solar Camera

You can enable and set up cloud storage for a solar camera when adding the solar camera to a site. When you complete the settings, the solar camera will be able to upload event-related footage of its channel to the cloud.

Steps

Note

- If you skip the cloud storage settings when adding a solar camera, you can go to the site to which the solar camera is added to set cloud storage for it later.
- For a complete list of supported solar camera models, refer to the *Hik-Partner Pro Compatibility List*.

1. Add a solar camera to a site by Hik-Connect (P2P).

Note

- For details about adding solar cameras, see ***Add Device by Entering Serial No.*** , ***Batch Add Devices*** , or ***Add Detected Online Device*** .
- If the solar camera is added by IP address / domain name, its cloud storage functionality will be unavailable.

When you complete adding the solar camera, the entry for setting cloud storage will be displayed on the adding result page.

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

A pop-up window indicating the time remaining for waking up the solar camera will appear before entering the Cloud Storage Settings page, on which the channel of the solar camera is displayed.

3. **Optional:** On the Network Test page, click **Start** to test the network performance if the network bandwidth is limited, and then click **Next** when the test completes.

Note

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

4. Select **Main Stream** or **Sub-Stream** from the drop-down list as the stream type for the channel.

Note

The video definition of main stream and sub-stream are displayed next to the drop-down list.

5. Click **Event Settings** to set the event that will trigger the video recording action of the channel.

Note

Currently only motion detection is supported by solar cameras.

Enable Motion Detection

Turn on the switch to enable motion detection.

Area Settings

Tap **Draw Area** to draw an area on the image, and then drag the slider to set the sensitivity of motion 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 checked, otherwise the channel will not record video footage even if the event is detected.

6. Switch on **Cloud Storage** to enable cloud storage for the channel.
7. Click **Activate Service** to activate cloud storage service for the channel.

Note

- For details about how to activate the service, see ***Activate or Renew Service for a Channel*** .
- After the cloud storage service is activated for the channel, you will not be able to disable cloud storage for the channel.

8. Click **Finish**.

The event-related video footage of the channel will be uploaded to the cloud.

15.4.7 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.

Note

It takes about one minute to test the network.

You can click the cloud storage device in the device list to open the device settings panel, and then click → **Start** to start network test.

15.4.8 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*** .

Steps

Note

For a device which doesn't 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. Go to the Customer Site page.
2. Click a site to enter the site details page.
3. Select the **Cloud Storage** tab.
4. Open the Activate / Renew Cloud Storage Service window.
   - If cloud storage service is not enabled for any of the channels of the cloud storage device, click **Enable Cloud Storage Service** first, select an online device from the list, enable **Cloud Storage** for a device channel, and click **Activate Service**.
   - If a cloud storage device has at least one channel with cloud storage service enabled, its linked channels and their service status will be displayed on the page. In the Operation column of a channel, click **Activate Service** to activate the service for the channel, or click **Renew Service** to renew the service for the channel.

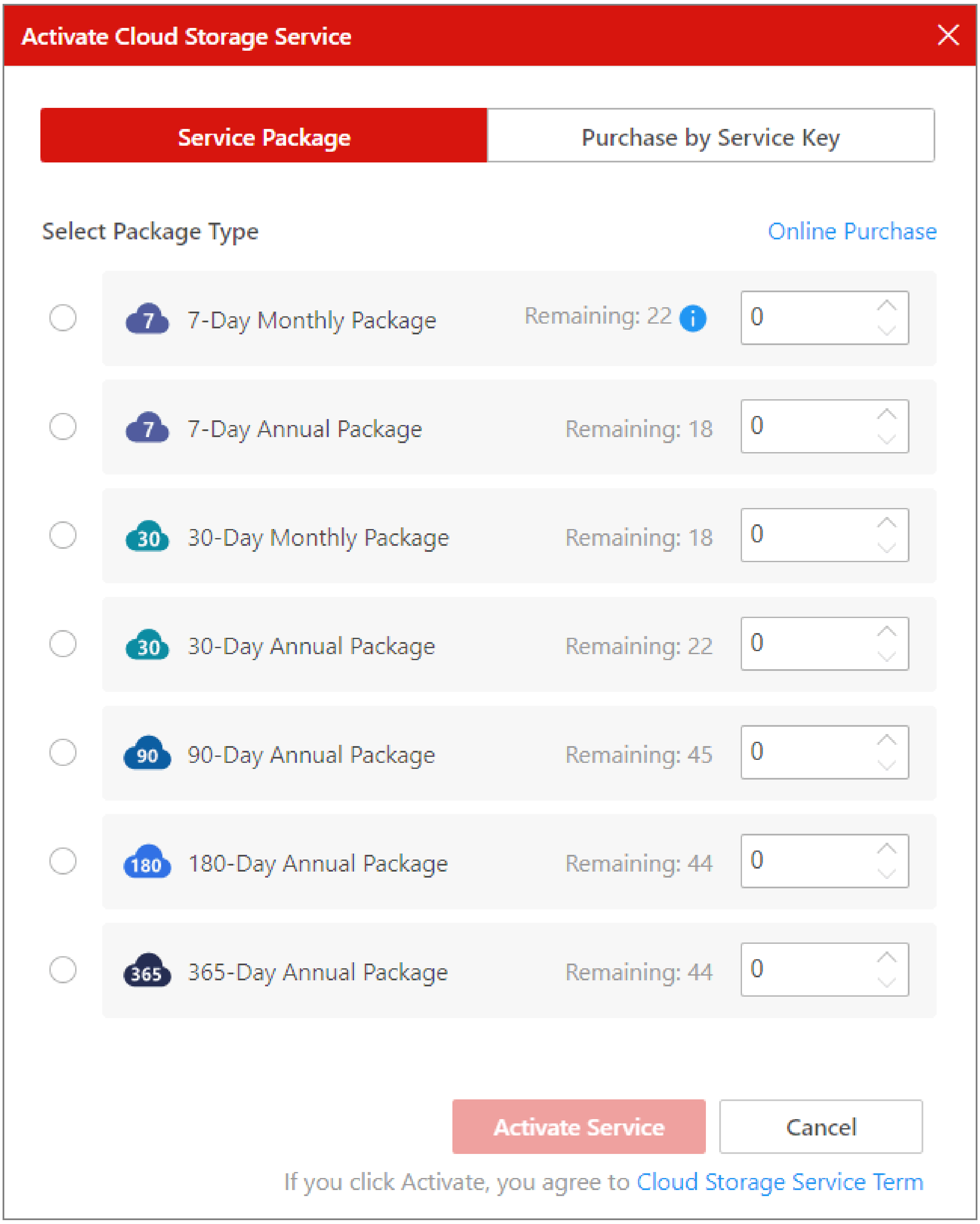


Figure 15-15 Activate Cloud Storage Service Window

Note

You can view the available packages which you have purchased. You can also click **Online Purchase** to purchase more packages if needed. For details, refer to ***Purchase Cloud Storage Service*** .

5. Activate or renew the cloud storage service for the channel.
   - Click **Service Package**, select a package type, and click ^ (or manually enter a number) to set the number of package(s) to be used.
   - Click **Activate by Service Key**, and enter the 16-character service key.

   Note

   You can consult the distributor to get the service key.

6. Finish activating or renewing the cloud storage service.
   - For activating cloud storage service, click **Activate Service**.
   - For renewing cloud storage service, click **Renew**.

   After activating or renewing the service, you can view the package type and expiry date of the service activated for each channel.

15.4.9 View Cloud Storage Details

You can view details of the cloud storage service, including the number of used and remaining service packages and the details (such as the expiry date and status) of service activated for channels of the cloud storage devices. You can also perform operations such as renewing the service for further use.

You can enter the cloud storage details page via the following two methods:

- On the navigation pane, select **Site & Device → Service → My Service → Cloud Storage Service** .
- On the navigation pane, select **Site & Device → Service → My Service → All Services** , find the cloud storage service block, and click **Details**.

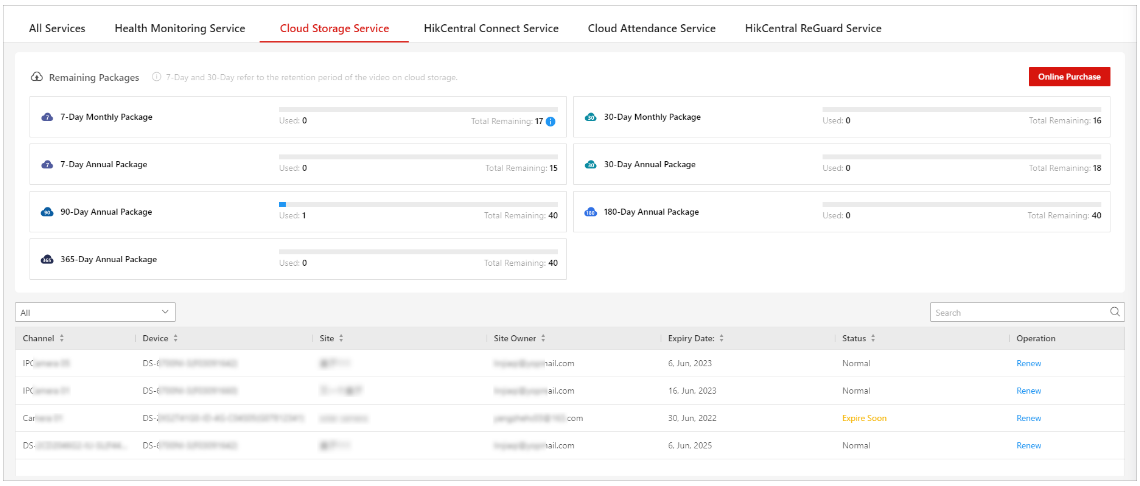


Figure 15-16 Cloud Storage Service Details Page

On the cloud storage details page, you can have an overall view of the cloud storage service packages that you have purchased and used, view the status of the service activated for different channels, and perform the following operations if needed.

- **Filter:** Click ⌄ to filter the channels of cloud storage devices according to the service status (expire soon or expired).
- **Search:** Enter a keyword (name of device, site, or site owner) in the search box to search for and view the service status of specific channels.
- **Purchase Cloud Storage Service Package:** Click **Online Purchase** on the upper right corner of the page to purchase more cloud storage service packages as needed. For details, refer to ***Purchase Cloud Storage Service*** .
- **Renew Cloud Storage Service:** For the service that will expire soon, click **Renew** to renew the cloud storage service. For details, refer to ***Activate or Renew Service for a Channel*** .

15.5 HCC Services

HCC services refer to the enterprise-user services offered by the HikCentral Connect (HCC) system, which provides a Video Security as a Service (VSaaS) solution for enterprise users. By subscribing to the HCC services (e.g., video management service, on-board monitoring service, access control service, video intercom service, and alarm detection service), the enterprise users can manage resources remotely, perform video-based monitoring, handle alarms, locate and track vehicles, control doors, manage calls, and so on.

See the following sections for more information about HCC services.

- ***Relationship Between Hik-Partner Pro and HCC***
- ***Introduction to the Services of HCC***
- ***HCC System User Types***
- ***Clients for Accessing HCC***

Relationship Between Hik-Partner Pro and HCC

HCC systems can be created on Hik-Partner Pro by installers like you and handed over to an enterprise user of HCC. To hand over a system, an email containing a super user account and an initial password will be sent to your customer for logging in to the HCC system. If there are devices added to the HCC system, the devices will be handed over together with the system. Refer to ***Create HCC Systems*** and ***Hand Over an HCC System and Devices*** for details.

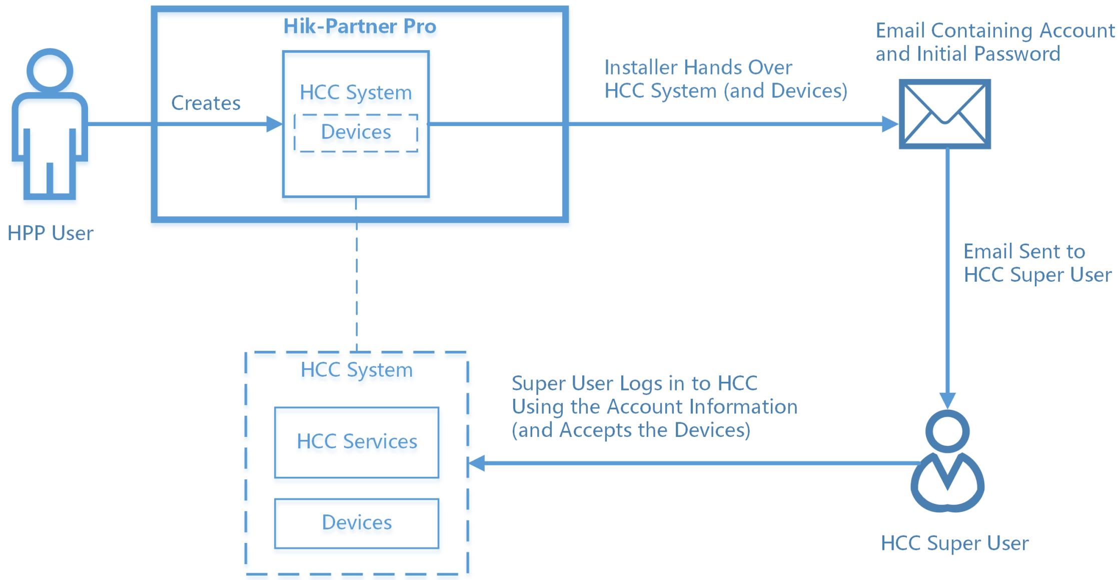


Figure 15-17 How an HCC System Is Created on Hik-Partner Pro and Handed Over

HCC systems can also be created by the self-registered HCC users themselves and added to Hik-Partner Pro for installers like you to purchase/activate value-added services for them via account linking. To complete the account linking process, HCC super users will need to give their account information (i.e., email address of the system owner) to you, and you can then send an account linking request to them using the information. Refer to ***Link with HCC Account*** for details.

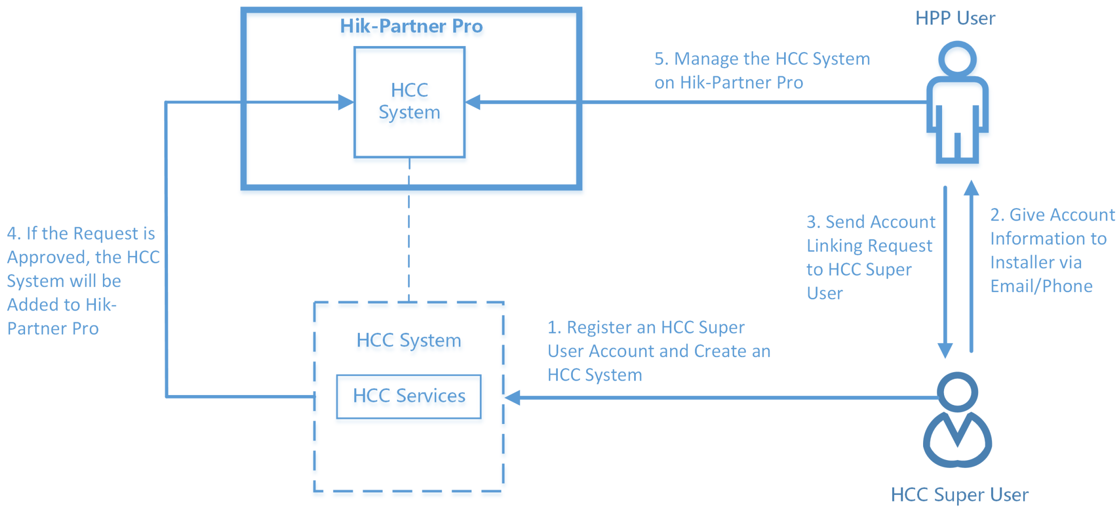


Figure 15-18 How an HCC System Is Created and Added to Hik-Partner Pro

Introduction to the Services of HCC

Table 15-9 Services of HCC

Service	Description
Video Management Service	The video management service provides video monitoring features such as live view, playback, and cloud storage. Your customers can enjoy the following perks: • Easy-to-use Portal and Mobile Client for centralized management of video resources. • Centralized monitoring anywhere anytime via the live view in 64-window division mode. • Convenient evidence search via simultaneous playback of up to 16 channels. • Receiving multiple types of alarm notifications and handling/marking important ones. • Flexible creation of sub accounts for different persons such as operators and IT managers. • Convenient event backtrack via detailed logs.
On-Board Monitoring Service	The on-board monitoring service provides features such as vehicle management, real-time vehicle locating, and driving monitoring. Your customers can enjoy the following perks: • Easy-to-use Portal and Mobile Client for centralized management of vehicles after connecting them to the cloud. • Viewing real-time locations of vehicles via GPS positioning.

Service	Description
	• Live view and playback via cameras mounted in/on vehicles. • Playing back vehicle tracks and viewing related footage. • Flexible creation of sub accounts for different persons such as operators and IT managers.
Access Control Service	The access control service provides features such as access level management, person management, access record search, and remote door controls. Your customers can enjoy the following perks: • Connecting to access control devices and managing events. • Convenient person management, access level management, and device management. • Remote door control and door opening via Bluetooth.
Video Intercom Service	The video intercom service provides features such as housing management, call answering and management, and temporary pass management. Your customers can enjoy the following perks: • Connecting to video intercom devices (e.g., door stations), and managing the devices (e.g., adding, deleting, editing, and searching for devices, and upgrading firmware). • Cloud-based solution which supports video calling from video intercom devices to the Mobile Client without being limited by the wiring or network. • Connecting to video intercom devices and managing events, including viewing history events and alarm configurations for video intercom events. • Making video calls from door stations and receiving the calls via Mobile Client. • 6 self-service users can be added to each room for using functions on the Mobile Client.
Alarm Detection Service	The alarm detection service provides features such as real-time monitoring of partition (area) status and resource arming controls. Your customers can enjoy the following perks: • Professional security services with the use of security control devices. • Multiple ways of arming/disarming partitions (areas). • Assigning different operation permissions for better teamwork. • Handling alarms from partitions (areas) and zones directly on the map. • Linkage between alarms and videos for you to check the situation in time. • Features for maintenance which help you to manage alarm detection systems easily.

HCC System User Types

Table 15-10 User Types

User Type	Description
Super User	The enterprise user who accepts a ready-to-use HCC system handed over from installers like you or self-registers an HCC account and plays the role of the initial administrator of HCC. The super user has full access to the resources and features of HCC.
Normal User	All other users of HCC except the super user.

Clients for Accessing HCC

Table 15-11 Portal and Mobile Client

Client	Description
Portal	Portal for users to log in to HCC to manage resources and perform related configurations and operations. All features of the five types of services (except for those related to call answering and the self-service features) are available on the Portal.
Mobile Client	Mobile Client for users to log in to HCC to use more lightweight features of the five types of services, such as live view, playback, driving monitoring, remote door controls, person/resident management, and arming control of security control partitions (areas) or zones. It is also for self-service users (e.g., employees, residents, etc.) to use self-service features such as door opening via mobile credentials, call answering and management, temporary pass management, etc.

15.5.1 Purchase HCC Services

In the service market, you can either purchase HCC service packages online or activate the services by entering service keys purchased from local distributors offline.

Before You Start
Make sure that the HCC service is available in your country/region.

Steps

Note

Activating the service by service key is only supported in some countries and regions. Contact a local distributor for details.

1. Go to **Site & Device → Service → Service Market** .
2. In the Value-Added Services area, click **HikCentral Connect Service**.
3. Click **Online Purchase**.

   Note

   If your country/region supports activating by service key and you have purchased a service key from a distributor, you can also click **Activate by Service Key** to get the service packages.
4. Set the number of the service packages to be purchased.

   Note

   - The access control service and video intercom service are offered in annual packages only. The other services (video management, on-board monitoring, and alarm detection) are offered in both monthly and annual packages.
   - You can also purchase cloud storage service packages along with the video management service packages for enabling cloud storage service for your video management channels. To do so, check the checkbox displayed under each type of video management service packages and set the number of each type of packages according to your needs.
   - The number set for each type of service packages and the total price (tax included) will be displayed on the right under **Currently Selected** for you to confirm before checkout.
5. Enter your VAT number, or check whether your previously entered VAT number is correct and edit it if needed.

   Note

   The VAT number entered here will be displayed on the payment receipt.
6. Click **Checkout** to enter the payment page and complete your payment.

   Note

   The payment method is selected as Credit/Debit Cards by default.
7. **Optional:** Go to **Site & Device → Service → My Service → HikCentral Connect Service** to view your HCC service packages and manage them.

   Note

   For more details, refer to ***Manage Your HCC Services*** .

15.5.2 Activate HCC Services for HCC System

As the service provider of your customers, you can activate services for HCC systems created by you or added to your system via account linking.

Before You Start

- Make sure that the HCC service is available in your country/region.
- Make sure you have created an HCC system or your account is linked with an HCC account.

Steps

1. Go to **Site & Device → Site & HCC → HikCentral Connect** , and click a system name to enter the system details page.
2. If a service is not yet activated for the system, you can click **Activate Service** to enter the Activate HikCentral Connect Service page.

   Note

   You can also enter this page via the HCC system list in My Service. For details, refer to ***Manage Your HCC Services*** .
3. Click the service to be activated to expand the activation details pane.
4. Set the number of resources to be activated, and select the length of activation.

   The activation details will be displayed below in Current Activation Status as a green bar visualizing the total number of resources to be added and the length of activation. The message below tell you how many packages are required for activating the resources selected above; if the remaining service packages are insufficient, it will tell you how many more packages are needed.

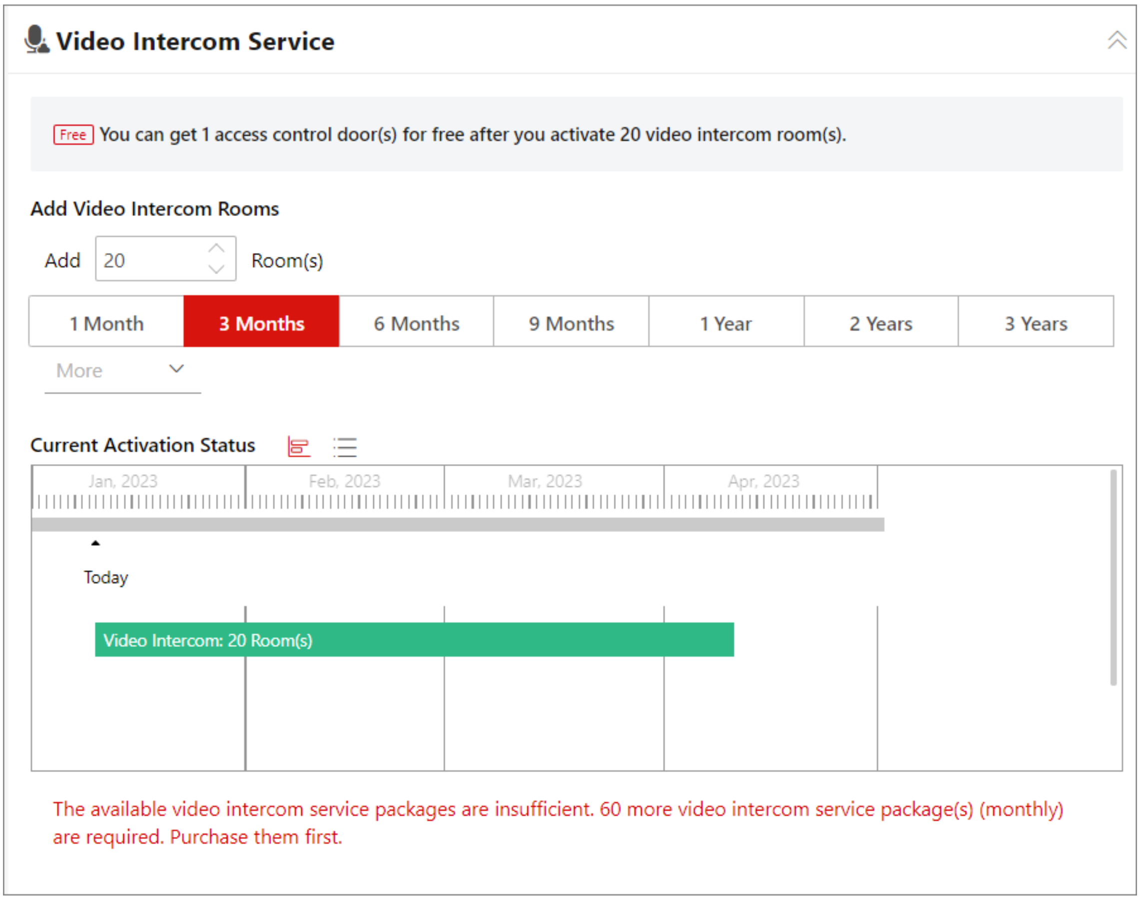


Figure 15-19 Activate Video Intercom Service

5. Click **Confirm** on the right pane to complete the service activation.

Note

If the remaining service packages are insufficient, the button will become **Purchase and Activate**, and you can click it to purchase the required packages directly online.

6. **Optional:** After activating services, go to **Site & Device → Service → My Service → HikCentral Connect Service** to manage them if needed.

Note

For details, refer to ***Manage Your HCC Services*** .

15.5.3 Manage Your HCC Services

In My Service, you can manage your HCC services, including the video management service, on-board monitoring service, access control service, video intercom service, and alarm detection service.

Note

Make sure that the HCC service is available in your country/region.

You can go to the HikCentral Connect service details page by clicking **Site & Device → Service → My Service → HikCentral Connect Service** .

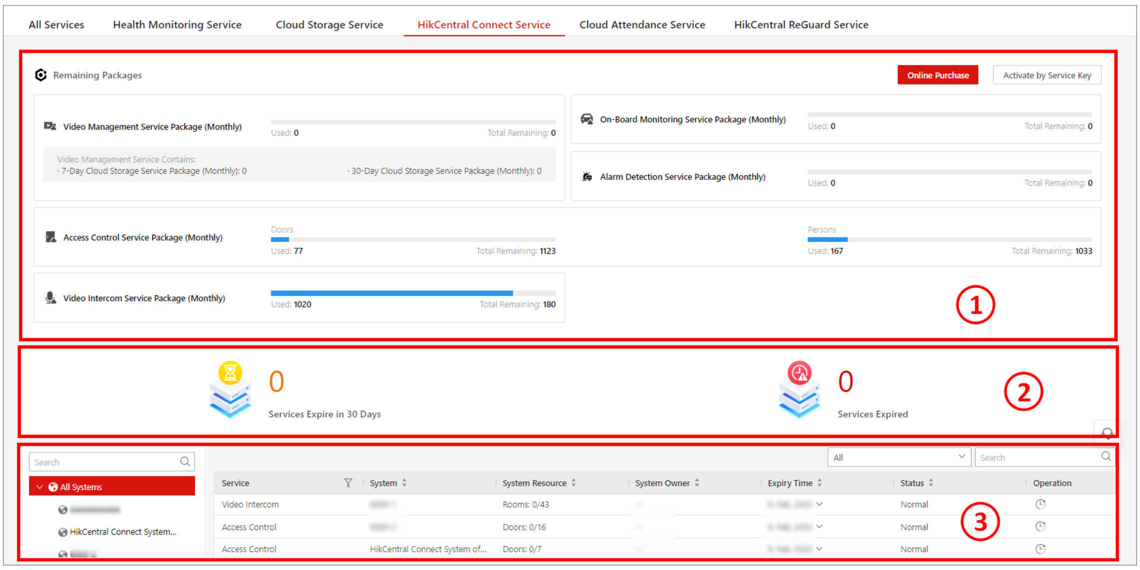


Figure 15-20 Manage Your HCC Services

On the page, you can perform the following operations as needed.

Table 15-12 Supported Operations

No.	Operation	Description
1	Check Remaining Packages & Purchase More	You can check the number of used and remaining packages for each service. If needed, click **Online Purchase** or **Activate by Service Key** on the top right to purchase more packages. For details, see ***Purchase HCC Services*** .
2	View Overall Package Expiration Status	You can view the overall number of services that are going to expire within 30 days and those that have already expired. Click a number to view details of these services in the list below.
3	Filter by System or Search by Keyword	Service details are displayed for all systems by default. You can select a specific system from the system list on the left to check service activation details for that system only.

No.	Operation	Description
		You can also search for systems by entering keywords in the search box.
	Filter Services by Type or Expiration Status	For each system, you can click by the Service column to filter its services by service type or filter by selecting a status (e.g., Services Expire in 30 Days, Expired) from the drop-down list.
	Activate Service	You can click in the Operation column of a service to activate the service for the corresponding HCC system. For details, see ***Activate HCC Services for HCC System*** .

15.5.4 Create HCC Systems

On the Hik-Partner Pro Portal, you can create HCC systems which contain the video management service, on-board monitoring service, alarm detection service, access control service, and video intercom service. After you hand an HCC system over to a customer, the customer becomes the system owner and can log in to HCC with the given account and use the above-mentioned services to manage devices and perform monitoring tasks. You can still monitor the HCC system on the Hik-Partner Pro Portal, including the capacity and the status of the services activated for the system.

Before You Start

Make sure that the HCC service is available in your country/region.

Steps

Note

HCC systems can also be created by the self-registered HCC users themselves. To add their self-created HCC systems to Hik-Partner Pro and offer them value-added services, you need to link with their self-registered accounts. Refer to ***Link with HCC Account*** for more details.

1. Go to **Site & Device → Site & HCC → HikCentral Connect** .
2. Click **Create HikCentral Connect System** to open the Create HikCentral Connect System pane.

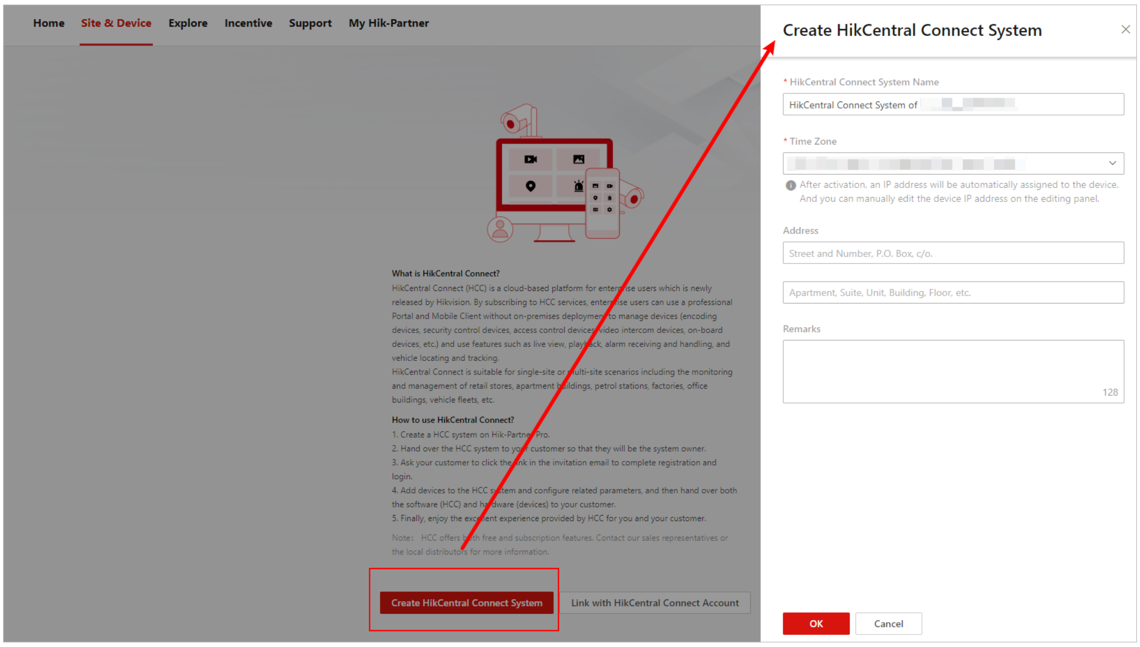


Figure 15-21 Create HikCentral Connect System

3. Create a name for the HCC system.
4. Select a time zone for the HCC system.
5. **Optional:** Enter the address of your customer.
6. **Optional:** Enter the remarks.
7. Click **OK**.
8. **Optional:** Perform the following operations as needed.

View System Details	Click the name of an HCC system to view its details, including the validity period of the video management service, on-board monitoring service, access control service, video intercom service, and alarm detection service, whether the system has been handed over, etc.
Hand Over System	Click in the Operation column to hand over a system, or click the name of an HCC system to enter its details page and click **Hand Over** on the right. Refer to ***Hand Over an HCC System and Devices*** for details.
Delete System(s)	Select system(s), and click **Delete** to delete the selected system(s).
Upgrade Service Plan	Select a system, click a service, and click **Upgrade to Trial Plan** to upgrade the plan of the service to trial plan.
Activate Service	Select a system, click a service, and click **Activate Service** to active the service for your customer so that they can enjoy the perks.

15.5.5 Add Devices to an HCC System

You can add devices to an HCC system before handing it over to a customer.

Note

- Make sure that the HCC service is available in your country/region.
- The systems created by HCC users themselves and added to Hik-Partner Pro via account linking do not support the device adding.

You can add devices to an HCC system via one of the three following ways:

- ***Add Devices on HCC System List Page***
- ***Add Devices on HCC System Details Page***
- ***Add Devices After You Finish On-Site Config***

After entering the Add Device page, refer to the hints displayed on the right of the page or the step descriptions in ***Add Detected Online Device*** and ***Add Device by Entering Serial No.*** respectively for details about adding devices. You can create a new HCC system or select an existing HCC system (not handed over) for adding devices to.

Refer to ***Device Status and Further Operations*** for more details about the status of added devices and what operations you can further perform.

Add Devices on HCC System List Page

Go to **Site & Device → Site & HCC → HikCentral Connect** and click **Add Device** at the top.

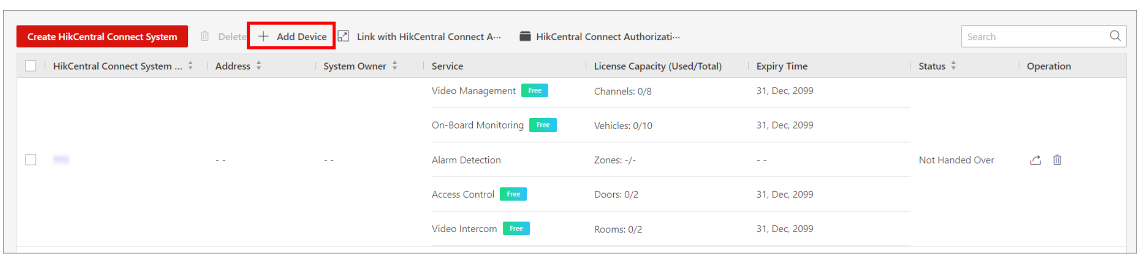


Figure 15-22 Add Devices on HCC System List Page

Add Devices on HCC System Details Page

Go to **Site & Device → Site & HCC → HikCentral Connect** and click the name of an HCC system to enter its details page. If there are no devices added to the system, you can click **Add Device** below the descriptions of each service.

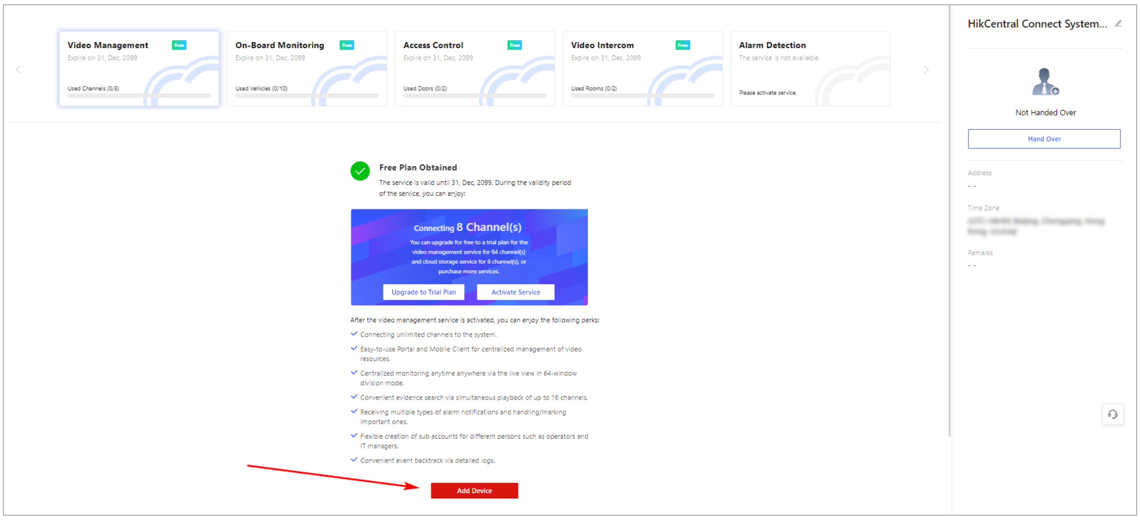


Figure 15-23 Add Devices on HCC System Details Page (First Time Adding)

If you have added devices to the system before and want to add more, click **Add Device** next to **Hand Over Now** to add more devices before handing these over.

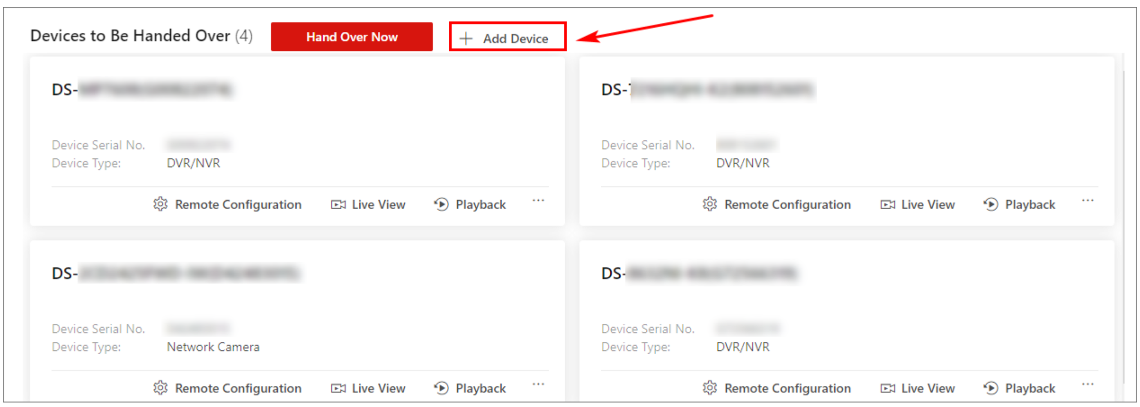


Figure 15-24 Add Devices on HCC System Details Page (Add More)

Add Devices After You Finish On-Site Config

After batch configuring devices via On-Site Config (refer to ***Batch Configure Devices on LAN*** for details), click **Add Device** on the prompt window to enter the Add Device page.

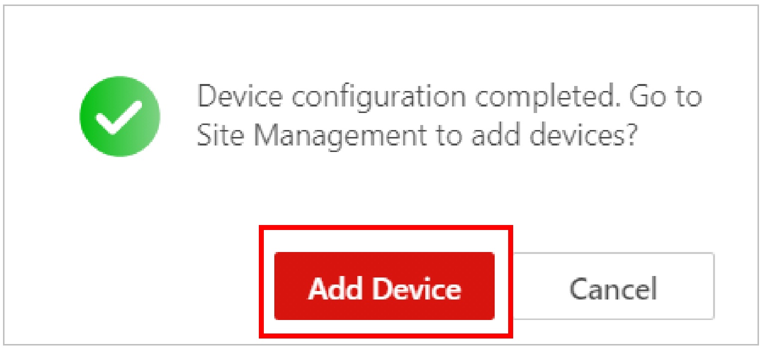


Figure 15-25 Prompt Window After Finishing On-Site Config

Device Status and Further Operations

After the devices are added via one of the above ways, you can click **Hand Over Now** to hand over the devices right away to a customer along with the HCC system, or click **Continue Adding Devices** to add more. The added devices will be displayed on the details page of the HCC system below the service plan details.

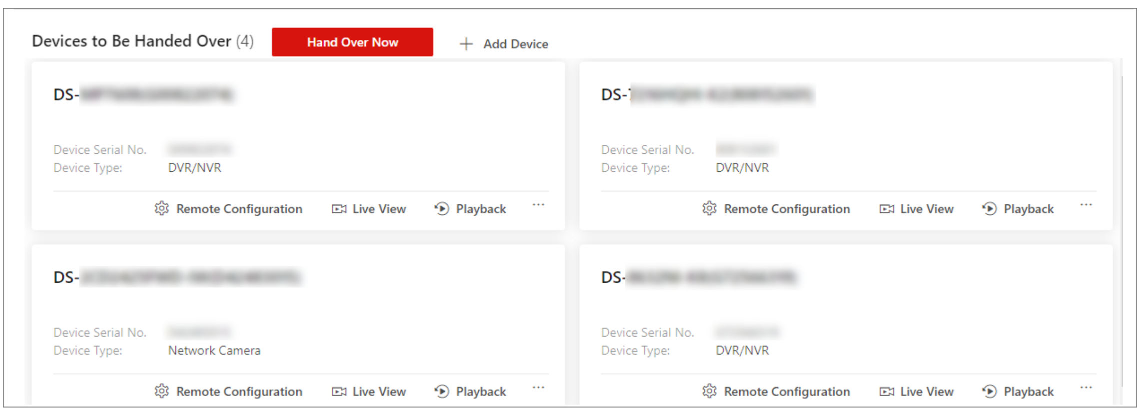


Figure 15-26 Device List of an HCC System

If the system is not handed over to a customer, the devices will be in the "to be handed over" status, and you can perform operations such as remote device configuration, deleting devices, and editing the device names.

Once you have initiated a handover attempt, the status of the devices will be changed to "to be accepted". For devices to be accepted, you can only view the device list and cannot perform any other operations.

The devices handed over successfully (i.e., accepted by your customer on HCC) will not be displayed on Hik-Partner Pro anymore. Those failed to be handed over will be shown on the page for you to check and notify your customer of the (partial) handover failure.

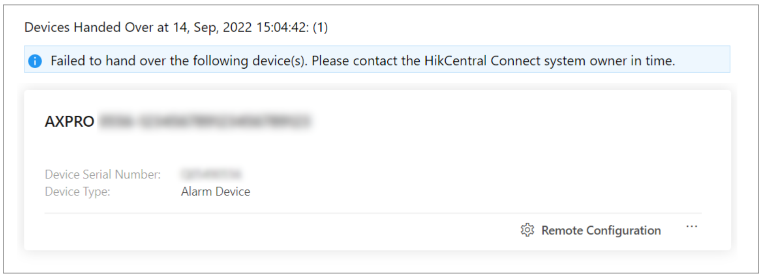


Figure 15-27 Device(s) Failed to Be Handed Over

15.5.6 Link with HCC Account

You can link with the self-registered users of HCC, or HCC users whose systems are created by other Hik-Partner Pro users, to add their HCC systems to your Hik-Partner Pro and offer value-added services for them.

Note

Make sure that the HCC service is available in your country/region.

The self-registered HCC users can create an HCC system on their own and start using the video management service, on-boarding monitoring service, access control service, and video intercom service of HCC on free service plans. However, if they want to use the alarm detection service or enjoy the service features without limitations, they need to link with service providers like you to purchase/activate the services for them.

To complete the linking process, you can go to **Site & Device → Site & HCC → HikCentral Connect** , click **Link with HikCentral Connect Account** at the top, and enter the account information (i.e., email address) given by the self-registered users for you to send them the account linking request.

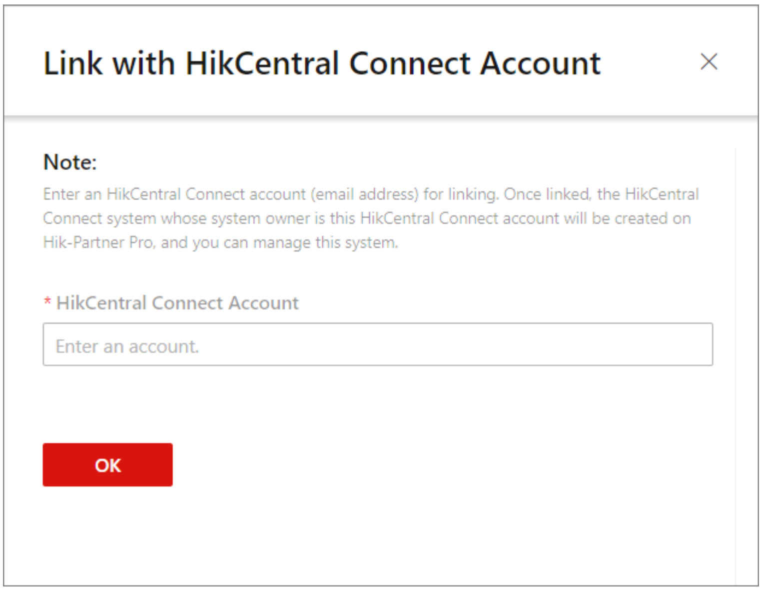


Figure 15-28 Link with HikCentral Connect Account

After a linking request is approved, the HCC system whose system owner is this HCC account will be added to your HikCentral Connect system management page for you to manage, such as performing service plan upgrades and service activations.

Note

- An HCC account can only be linked with one service provider at a time. If your customer has already linked with another service provider, you can still send a linking request. After the request is approved, you can start managing your customer's HCC system and the services already activated by the previous service provider will not take up your service package inventory.
- For linking with an HCC account (system) created by another service provider, once your customer approves your linking request, the HCC system is deleted from the other service provider's Hik-Partner Pro account and added to yours.

15.5.7 Hand Over an HCC System and Devices

After you create an HCC system, you can hand it over to a customer together with the devices added to it. As a result, the customer becomes the system owner and is able to use the services of HCC (i.e., video management, on-board monitoring, access control, video intercom, and alarm detection service) to manage the corresponding devices and perform monitoring tasks. You can still monitor the HCC system on Hik-Partner Pro after the system handover.

Before You Start

Make sure that the HCC service is available in your country/region.

Steps

Note

The systems added to Hik-Partner Pro via account linking do not support device adding and handover.

1. Go to **Site & Device → Site & HCC → HikCentral Connect** .
2. Choose from the followings to start the handover process.
   - Click in the Operation column of a system to be handed over.
   - Click the name of an HCC system to enter its details page. On the page, click **Hand Over** on the system details pane, or click **Hand Over Now** next to **Devices to Be Handed Over** (if there are devices added to the system).
   - Click **Hand Over Now** on the success page after you add devices to an HCC system. For details about adding devices to an HCC system, refer to ***Add Devices to an HCC System*** .

   A window may pop up to remind you that you will not be able to add devices to the system after handing it over to your customer.

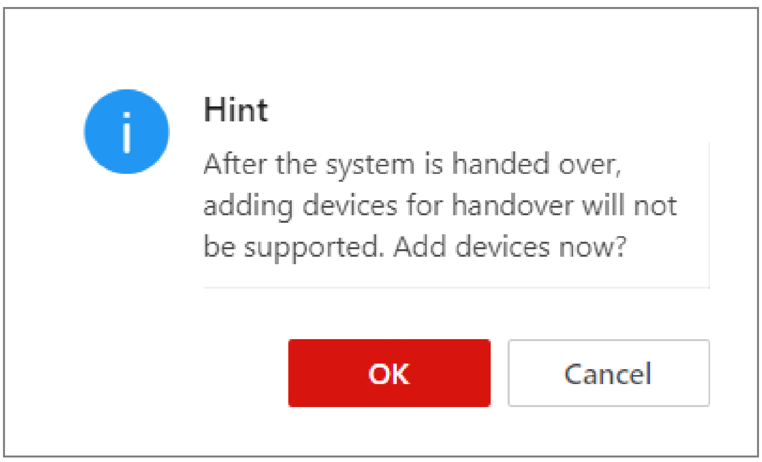


Figure 15-29 Device Adding Reminder for System Handover

3. **Optional:** On the pop-up window, click **OK** to go to the device adding page to add devices, or click **Cancel** to proceed with the handover process.
4. On the Hand Over System pane, enter the email address, first name, and last name of your customer.

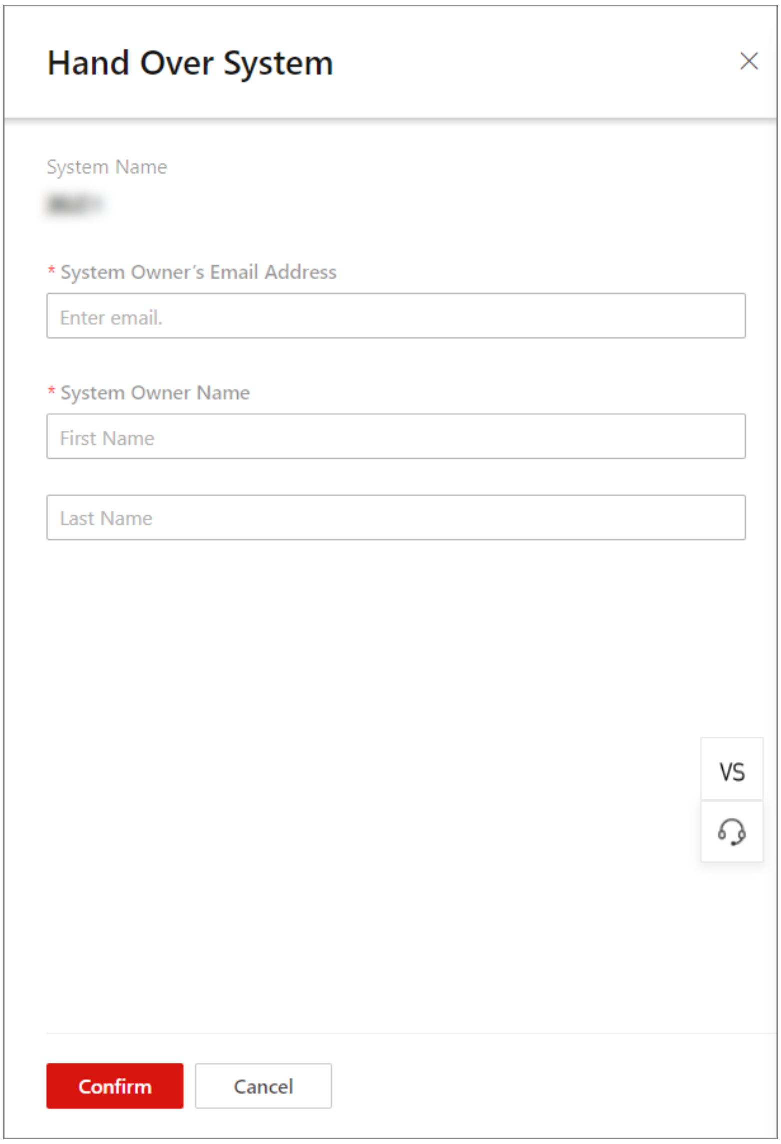


Figure 15-30 Hand Over System

5. Click **Confirm**.

   The status of the system and the devices added to it (if any) will be changed to "to be accepted". An email will be sent to your customer to provide them the account information. After successfully logging in to their system, your customer will receive another email notifying them of the device handover attempt.
6. **Optional:** Contact the customer to log in to the HCC system and accept the devices.

15.5.8 HCC Authorization Code

You can access your customers' HCC systems using the authorization code created by them on HCC to provide them maintenance services within a set period of time.

Note

Make sure that the HCC service is available in your country/region.

If your customer needs maintenance services from you, they can create an authorization code on HCC for you to access their HCC system directly without the need to log in using their account name and password.

To do so, you can go to **Site & Device → Site & HCC → HikCentral Connect** , click **HikCentral Connect Authorization Code** at the top, and enter the authorization code given to you by your customer. To access their HCC system, confirm that the system information (system name and account information) displayed after you enter the code is correct and click **Access HikCentral Connect**.

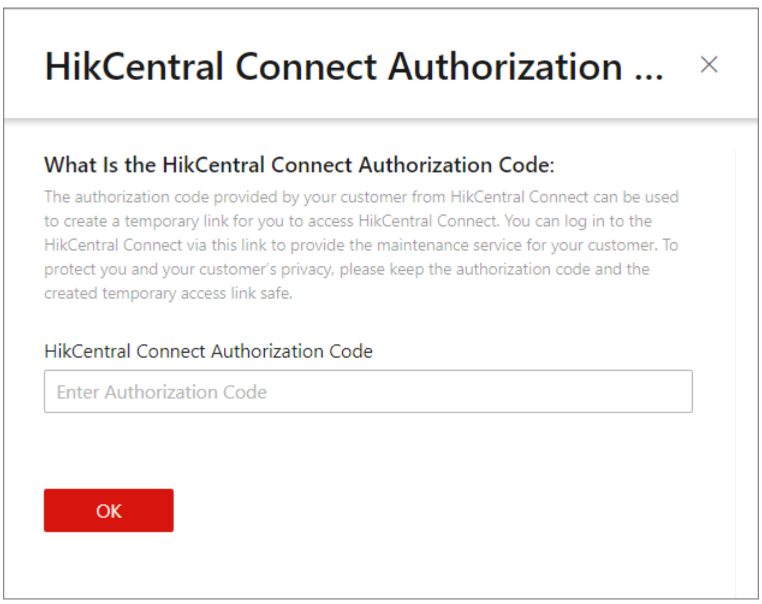


Figure 15-31 Enter HikCentral Connect Authorization Code

15.6 People Counting Service

Hik-Partner Pro offers people counting service to help your customers to resolve issues related to people flow control. After adding people counting cameras to specific Sites managed via this platform and activating this service for your customers, you can integrate people counting capabilities to of these cameras with the platform so as to monitor in real time the people densities of specific areas in these Sites. These cameras will count people entering, exiting, or passing by the areas, and analyze whether people densities of these areas reach the upper-limits. This is useful for certain commercial and health protection scenarios, such as limiting the customer traffic of a shopping mall during the promotion period.

Note

People density here refers to the amount of people staying within a limited area at the same time.

15.6.1 Flow Chart for Setting People Counting Service

The flow chart below shows the recommended process for setting people counting service.

Figure 15-32 Flow Chart

The table below shows the description of each step and the link to corresponding section.

Table 15-13 Flow Chart Description

Step	Description
Add People Counting Cameras to a Site	Add people counting cameras (i.e., the cameras with people counting capability) to a specific Site. For details about adding devices, see ***Add Device*** and its sections.
Activate People Counting Service for Channels	Activate people counting service for specific channels of the added people counting cameras. For details, see ***Activate People Counting Service for Channels*** .

Step	Description
Add a Group for People Counting	Add a group to define people counting rules, such as calculation mode and maximum allowed people in the area. For details, see ***Add a Group for People Counting*** .
Hand Over Site to Your Customer	After complete the required configurations, hand over the site to your customer, so they will be the site owner. For details, see ***Hand Over Site*** . **Note** When your customer accept the site handover on the Hik-Connect Mobile Client, he/she will be able to access the people counting functionality of the people counting cameras via the Mobile Client.

15.6.2 Activate People Counting Service for Channels

If the end user needs to use people counting related functionality on Hik-Connect, you should activate people counting service for channels of the people counting cameras first.

Before You Start

- Make sure you have added people counting cameras to the target site. For details, see ***Add Device***
- Make sure you have the permission for device configuration. Or you should apply for the permissions first. For details, see ***Apply for Device Permission*** .

Steps

1. Go to the Customer Site page.
2. Click a site to enter its site details page, and the select **People Counting** tab.

   The people counting cameras will be displayed in the Device area.
3. Click › to open the device panel.

   The channel(s) of the device will be displayed on the panel.
4. Click **Activate** to open the Activate People Counting Service window.
5. Enter the user name and password of the admin account of the device.
6. Click **OK** to activate people counting service for the channel.

15.6.3 Add a Group for People Counting

A people counting group refers to a group of people counting cameras mounted in a certain region. A people counting group defines two elements, namely, the boarder of the region (i.e., the cameras added to the group) and the maximum amount of people allowed to stay in the region.

The cameras added to the group will detect the entering and exiting persons and at the same time calculate related data. In this way, the platform will be able to determine if the amount of persons staying in the region has reached the maximum allowed value, and meanwhile send related data to the Hik-Connect Mobile Client, which will display in real time the number of persons staying in the region and the remaining quota for entering the region. This allows the end users to use Hik-Connect to remotely monitor the people density of the region and take corresponding measures in time. The function is useful in various scenarios in which people flow of a certain region requires to be limited. For example, assume that your customer is the manager of a supermarket, when a contact-transmission disease outbreaks, you can set the people counting cameras at the entrance and exit of the supermarket as a people counting group and enable it, thus allowing your customer to respond timely based on the data on Hik-Connect so as to lower the risk of infection for the customers in the supermarket.

Before You Start

- Make sure you have configuration permission for the people counting cameras. Or you should apply for the permissions first. For details about applying for permission, see ***Apply for Device Permission***
- Make sure you have enabled people counting service for channels. For details, see ***Activate People Counting Service for Channels*** .
- Make sure people counting settings (e.g., entering direction) has been configured on the camera. For details, see the user manual of the camera.

Steps

Note

See *Hik-Connect Mobile Client User Manual* for details about how to view related people counting data on the Hik-Connect Mobile Client.

1. Go to the Customer Site page.
2. Click a site to enter its site details page, and the select **People Counting** tab.
3. Click **Add Group** to open the Add Group panel.
4. Set the required information.

   Group Name

   Create a name for the people counting group.

   For example, if you need to count the customer flow in the first floor of a shopping mall, you can name the group as "1st Floor".

   Select Channel

   Click **Add** and then select channel(s) to add the selected one(s) to the group.

Note

- Only the channel(s) that have been enabled the people counting service can be selected.
- Up to 16 channels can be added to one people counting group.
- You can add a channel to up to 16 people counting groups.

Calculation Mode

Set the calculation mode for each selected channel.

Standard

Count the amount of the people entered detected by the camera as the amount of people entering the region and count exited as exiting the region. Select this mode when the direction of entering configured on the camera is the same with the actual entering direction.

Note

See the picture below for reference, in which the blue arrows represent the actual entering and exiting direction of the people, while the red arrows represent the entering direction configured on the camera.

Reverse

Count the amount of people entered detected by the camera as the amount of people exiting the region and count exited as entering the region. Select this mode when the direction of entering configured on the camera is opposite to the actual calculation direction.

Note

See the picture below for reference, in which the blue arrows represent the actual entering and exiting direction of the people, while the red arrows represent the entering direction configured on the camera.

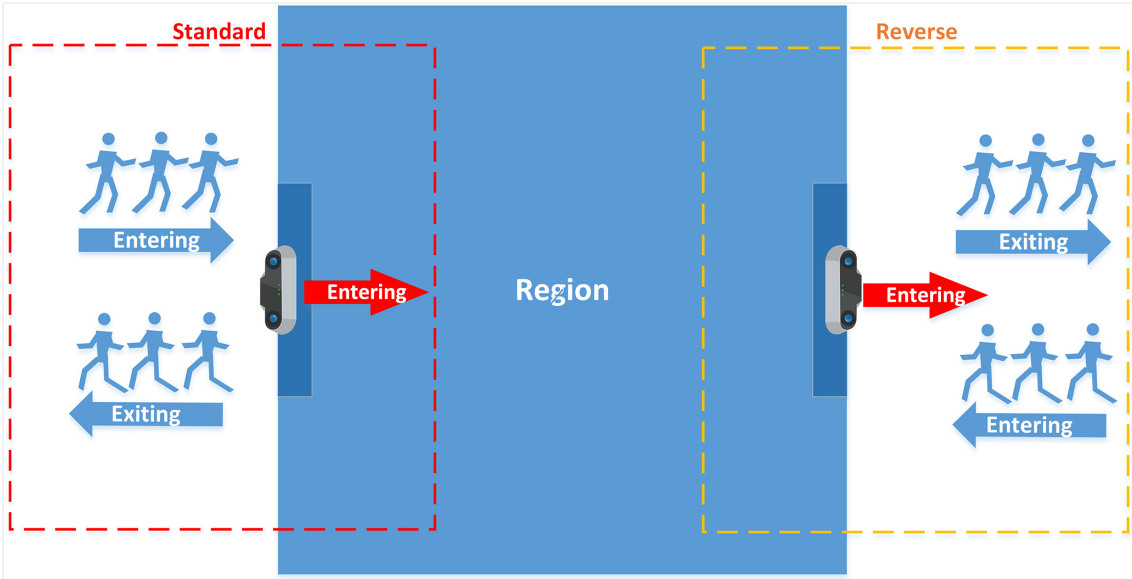


Figure 15-33 Calculation Mode

Max. People Allowed

Define the maximum amount of people (range: 1 to 100,000) allowed to stay in a specific region at the same time.

Push Alarm to Hik-Connect If Max. People Reached

After enabled, an alarm notification will be pushed to the Hik-Connect Mobile Client if **Max. People Allowed** is reached.

Note

Please notify the end user that he/she should keep the Notification functionality of the Hik-Connect Mobile Client enabled, or he/she will not receive this alarm notification on the Mobile Client. For details about enabling the Notification functionality on Hik-Connect, see *Hik-Connect Mobile Client User Manual*.

5. Click **OK**.

The people counting group will be displayed on the **People Counting** tab and it is enabled by default. And the end user will be able to view corresponding people counting data on Hik-Connect Mobile Client.

Note

You can add up to 16 people counting groups to a site.

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

Edit Group	Hover the cursor onto and then click to edit the group.
Delete Group	Hover the cursor onto and then click to delete the group.

	Note If you delete a people counting group, the corresponding people counting functionality will also be deleted.
Disable a Specific Group	Set the toggle from on to off to disable the group. **Note** If you disable the group, the people counting related functionality on the Hik-Connect Mobile Client will be unavailable.
Batch Enable/ Disable Groups	Click **Enable All** or **Disable All** to enable or disable all groups respectively. **Note** If you disable the group, the people counting related functionality on the Hik-Connect Mobile Client will be unavailable.

15.7 Temperature Screening Service

Temperature Screening service provides contact-less skin-surface temperature measurement and facial mask detection in real time. You can activate this service for your customers, such as the manager of a retail store or the administrator of a school campus, so that they can view the screening results on their mobile phone via Hik-Connect Mobile Client.

Note

The service is only available in some countries and regions.

15.7.1 Flow Chart for Setting Temperature Screening Service

The flow chart below shows the recommended process for setting temperature screening service.

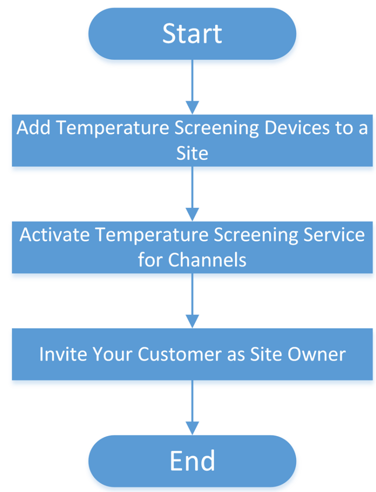


Figure 15-34 Flow Chart

The table below shows the description of each step and the link to corresponding section.

Table 15-14 Flow Chart Description

Step	Description
Add Temperature Screening Devices to a Site	Add temperature screening devices (i.e., the devices with temperature screening capability) to a specific Site. For details about adding devices, see ***Add Device*** and its sections.
Activate Temperature Screening Service to Channels	Activate temperature screening service to specific channels of the added temperature screening devices. For details, see ***Activate Temperature Screening Service for Channels*** .
Hand Over Site to Your Customer	After complete the required configurations, hand over the site to your customer, so they will be the site owner. For details, see ***Hand Over Site*** . **Note** When your customer accept the site handover on the Hik-Connect Mobile Client, he/she will be able to access the temperature screening functionality of the temperature screening devices via the Mobile Client.

15.7.2 Activate Temperature Screening Service for Channels

If you have added devices that support temperature screening to the platform, you need to activate temperature screening service for the channels of these devices and then set temperature screening parameters for each channel. After that, the temperature screening functionality of these devices will be available and the Site Owner will be able to view the skin-surface temperature of the persons appeared in the live view of the channels on the Hik-Connect Mobile Client. Optimally, you can also enable the channels to push abnormal temperature alarm to Hik-Connect, upload captured pictures of the person whose temperature is abnormal to Hik-Connect, detect if the persons wear masks, and upload the no-mask alarm to Hik-Connect.

Before You Start

Make sure you have added devices that support temperature screening to the target Site.

Steps

Note

Temperature screening related functionality are not available in some countries and regions.

1. Go to the Customer Site page.
2. Click a Site to enter its site details page, and then select **Temperature Screening** tab.

   Only the devices that support temperature screening will be displayed.
3. Click > to open the channel panel.

   The channel(s) of the device will be displayed.
4. Click **Activate** to open the Activate Temperature Screening Service window.
5. Enter the user name and password of the admin account of the device.
6. Click **OK** to activate temperature screening service for the channel.
7. Set temperature screening parameters.
   1) Click **Settings** to set the temperature screening parameters.

   Temperature Threshold

   For the channel of a temperature screening camera, set a temperature as the threshold for triggering abnormal temperature alarm if the detected skin-surface temperature is higher than the threshold.

   For the channel of a face recognition terminal, define a temperature range as the range of normal skin-surface temperatures. An abnormal temperature alarm will be triggered if the detected skin-surface temperature is NOT within the range.

   Mask Detection

   After enabled, the temperature screening device will detect if the persons wear masks.

   Store Temperature Screening Information

   After enabled, the temperature screening information will be uploaded to the Hik-Partner Pro platform.

   If disabled, the platform and the Hik-Connect Mobile Client will be unable to receive temperature screening information from temperature screening devices, including abnormal temperature alarm, normal temperature records, no-mask alarm, as well as the captured face pictures of the persons with abnormal skin-surface temperature.

Push Alarm to Hik-Connect If Abnormal Temp. Detected

After enabled, abnormal temperature alarms will be pushed to the Hik-Connect Mobile Client if abnormal skin-surface temperatures are detected.

Note

Please notify the end user that he/she should keep the Notification functionality of the Hik-Connect Mobile Client enabled, or he/she will not receive this alarm notification on the Mobile Client. For details about enabling the Notification functionality on Hik-Connect, see *Hik-Connect Mobile Client User Manual*.

Save Normal Temperature Records

Save normal temperature records on the Hik-Partner Pro platform.

Upload Captured Pictures

After enabled, the temperature screening device will capture the face picture of the person whose skin-surface temperature is abnormal and upload the captured picture to the platform.

Note

If disabled, the end user will be unable to view the captured picture on the Hik-Connect Mobile Client.

Push Alarm to Hik-Connect If Wearing No Mask Detected

After enabled, if a person who wears no mask is detected, an alarm about it will be pushed to the Hik-Connect Mobile Client.

Note

Please notify the end user that he/she should keep the Notification functionality of the Hik-Connect Mobile Client enabled, or he/she will not receive this alarm notification on the Mobile Client. For details about enabling the Notification functionality on Hik-Connect, see *Hik-Connect Mobile Client User Manual*.

2) Click **OK**.

8. **Optional:** Perform the following operations if required.

Disable Temperature Screening Functionality of a Specific Device	Set to to disable the temperature screening functionality of the device. **Note** If disabled, the end user will NOT be able to use the temperature screening functionality of the device on the Hik-Connect Mobile Client.
Disable Temperature Screening	Click **Disable All** to disable all temperature screening functionality of all devices.

Functionality of All Devices	**Note** If disabled, the end user will NOT be able to use the temperature screening functionality of these devices on the Hik-Connect Mobile Client.

15.8 Alarm Receiving Center (ARC) Service

Alarm Receiving Centers (ARC) is a facility that receives and responds to alarms from systems of companies, schools, factories, etc., for the security purpose. It is made up of a specially trained team who can react quickly when an alarm occurs. Hik-Partner Pro offers multiple ARCs, which can provide 24/7 remote alarm receiving service for customers.

If your company is a professional ARC, you can add your company to the Alarm Receiving Center (ARC) list. After that, all the other Hik-Partner Pro users can be your potential customers. They can select your company as the ARC for their customers. This can promote the brand awareness of your company and provide great possibility for your company to expand business.

The diagram below shows the overall process of how an installer can enable the ARC service for the installer's customer.

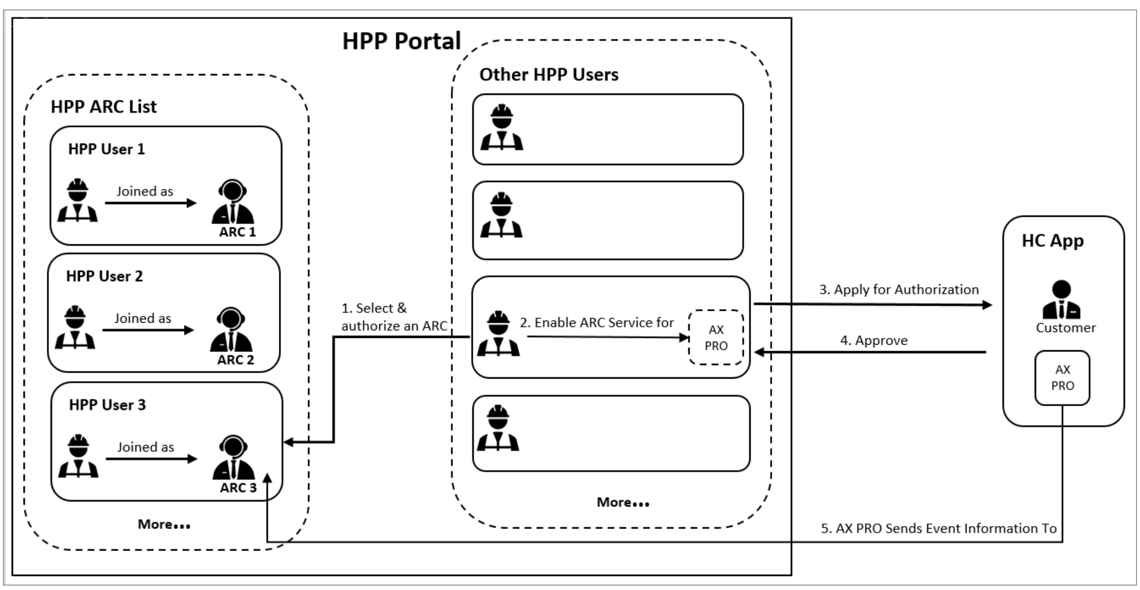


Figure 15-35 Overall Process of Enabling ARC Service

In the diagram:

- HPC represents Hik-Partner Pro and HC represents Hik-Connect.
- "Joined as" indicates that a Hik-Partner Pro user has been authenticated as a user who runs/ manages a professional ARC. Once authenticated, this ARC will be listed in the ARC list of Hik-

Partner Pro. For details about how to apply for "joining as ARC", see ***Add Your Company to the ARC List*** .

- For more information about the five procedures (marked with red digits in the diagram), see ***Enable ARC Service for Devices*** .
- AX PRO represents the AX PRO security control panel. Here we take this device as a example.

Note

ARC service is only supported by the devices added by Hik-Connect (P2P). The supported device types include the camera and NVR manufactured by Hikvision, and AX PRO/Hub/Hybrid security control panel.

15.8.1 Add Your Company to the ARC List

You can add your company to the Alarm Receiving Center (ARC) list to enable your company to provide alarm receiving services to other Hik-Partner Pro users. After adding your company to the ARC list, all the Hik-Partner Pro users can view the company information and determine whether to connect the encoding devices and/or alarm devices managed by them to the ARC of your company. This can greatly increase brand awareness of your company and bring more customers to you.

Before You Start

- Make sure the type of your company is ARC. For details, refer to ***Manage Company Information*** . If the type of your company is not ARC, you will be reminded of changing the type to ARC first on the page of joining as ARC.
- Make sure you have the permission for managing company information. If you do not have the permission, contact the Installer Admin.

Steps

1. Find the entry of joining as ARC.

Note

There are three entries.

- Go to the Customer Site page, select a site from the list, select the **ARC Service** tab, and then click **Join as ARC** in the upper-right corner.

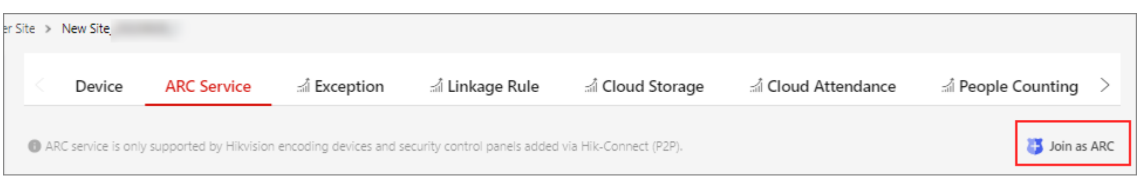


Figure 15-36 The First Entry

- Go to the Customer Site page, select a site from the list, select the **ARC Service** tab, click **Select ARC** to open the Select ARC for Authorization panel, and then click **Join as ARC**.

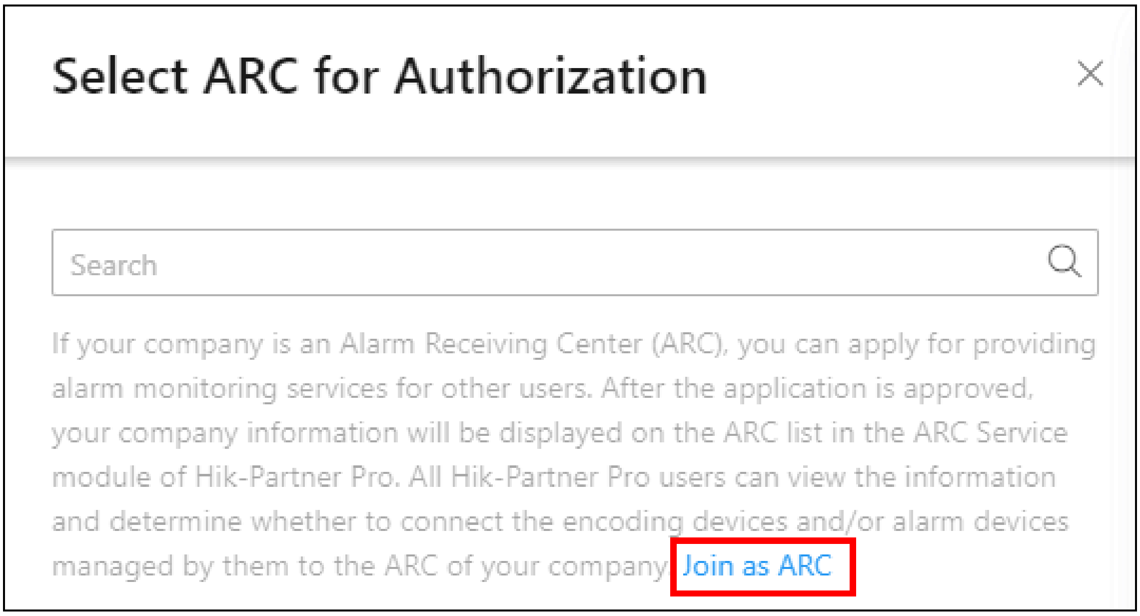


Figure 15-37 The Second Entry

- Click **Company → Company Information** to enter the company information page, click **Apply Now** in the Add Your Company to ARC List area.

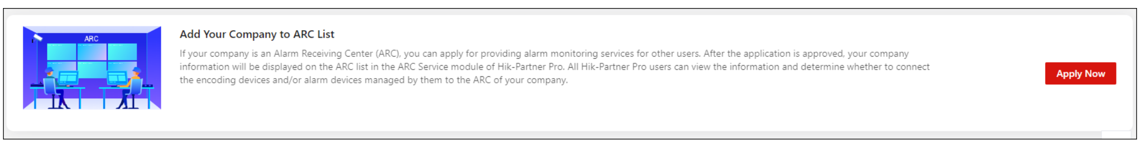


Figure 15-38 The Third Entry

You will enter the introduction page of applying for ARC and can read the detailed steps about how to apply for ARC.

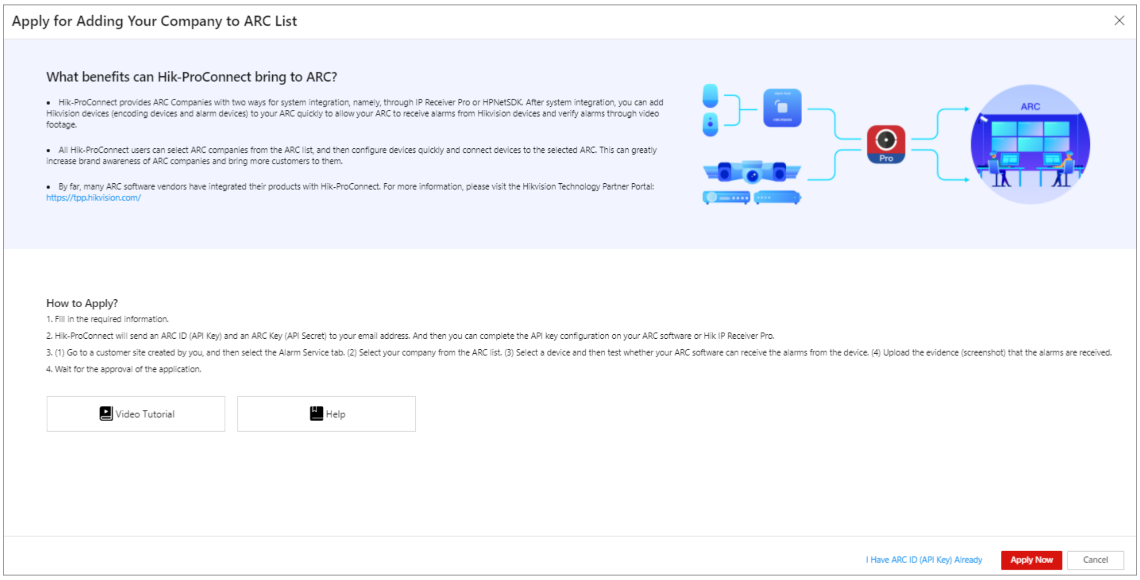


Figure 15-39 The Introduction Page of Applying for ARC

2. If your company has not been authenticated, click **Company Authentication → Authenticate Now** to authenticate your company.

Note

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

---

3. If your company has been authenticated, click **Apply Now** to enter the following page.

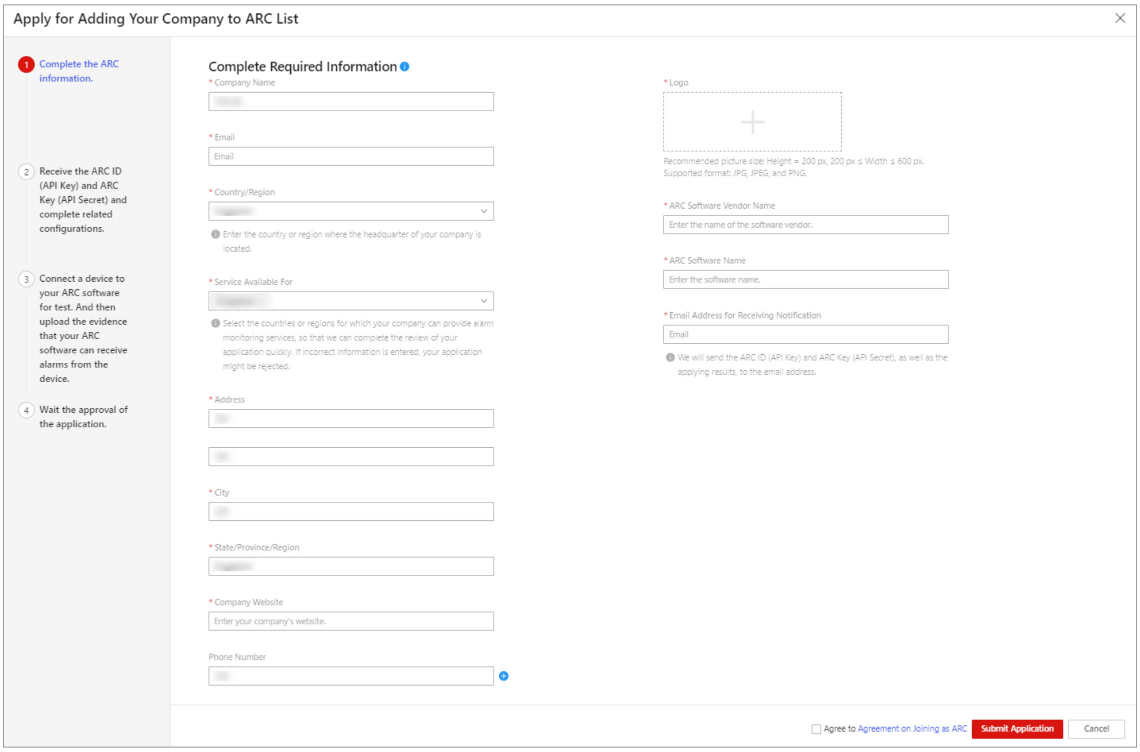


Figure 15-40 Fill In Information

4. Enter or edit the required company information such as the email address.
5. Read **Agreement on Joining as ARC** carefully and check **Agree to Agreement on Joining as ARC** in the down-right corner.
6. Click **Submit Application**.

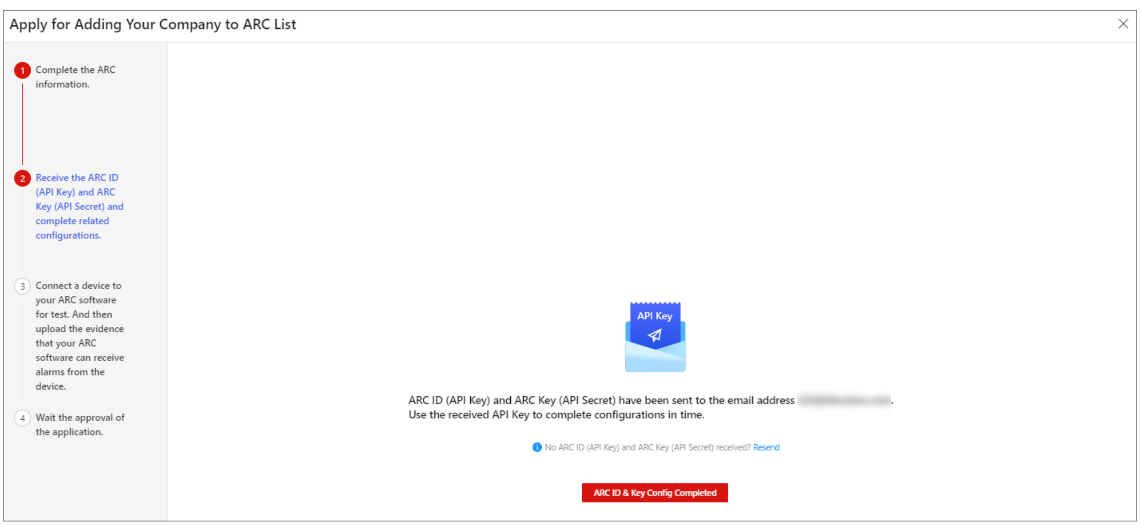


Figure 15-41 ARC ID & Key Sent

Note

You will receive an email containing the ARC ID (API Key) and ARC Key (API Secret). If receiving failed, you can click **Resend** to resend the ARC ID and ARC Key to your email address. Then, you can complete the ARC ID and ARC Key configuration on your ARC software (software used by your company for receiving alarms) or Hik IP Receiver Pro. If you have any questions about the ARC ID and ARC Key configuration, refer to **Agreement on Joining as ARC** and find the email for getting help.

7. Click **ARC ID & Key Config Completed** to enter the next page.
8. Authorize a device, and then upload the evidence (up to 2 pictures) that your ARC software can receive alarms from the device.

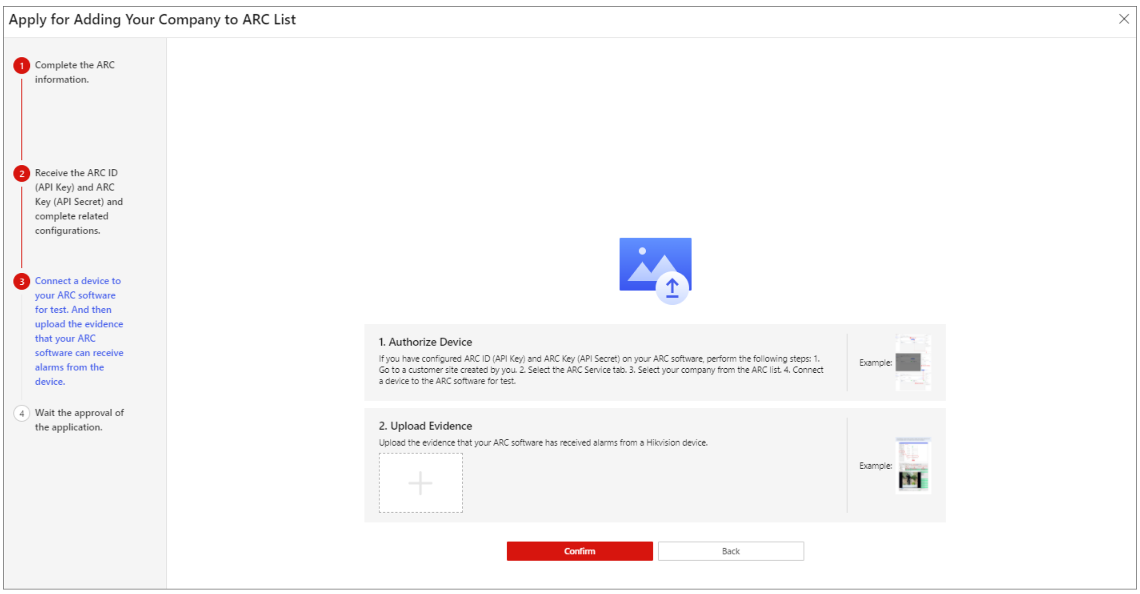


Figure 15-42 Authorize Device & Upload Evidence

Note

You can click the pictures on the right side to view the examples. Also, you can refer to ***Enable ARC Service for Devices*** for details about authorizing devices.

9. Click **Confirm** to enter the application approval page.

Note

Wait for the approval of your application. If the application is approved, your company information (e.g., brand logo) will be displayed on the ARC list. If the approval failed (e.g., you have entered the wrong company information), you should click **Edit ARC Info** to edit your ARC information.

15.8.2 Enable ARC Service for Devices

You can authorize a site to an ARC, and then enable the 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.

Steps

Note

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

1. Enter the Site list page.
   - Go to **Site & HCC → Customer Site** .
   - Go to **Customer Site** (if HikCentral Connect is not available in your country or region).
2. Select a Site to enter the site details page, and then select **ARC Service**.
3. Click **Select ARC** to display the Select ARC for Authorization pane.

   Note

   On the pane, you can view the details of each ARC, including the company name, logo, country/region, location, contacts, and official website.
4. **Optional:** Click the official website of the ARC to view more information about it.
5. Select an ARC, and click **Authorize**.

   The device(s) available for enabling the ARC service will be displayed, and an email will be sent to the ARC's **Email Address for Receiving Notification** to notify them, with the user account, device serial No., device model, and your company information.

   Note

   The ARC service is only supported by Hikvision encoding devices and AX security control panel (including AX PRO, AX Hub, and AX Hybrid) added by Hik-Connect (P2P).
6. Switch on to enable the ARC service for a specific device.

   The events detected by the device and the device exceptions will be sent to the ARC.
7. **Optional:** If you have enabled the ARC service for an AX device in the previous step and the device is accessed to the ARC via Hik IP Receiver Pro, click the device in the device list to open the configuration pane, 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 types of connection 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 byHik-Partner Pro server constantly.

Note

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

8. **Optional:** Click **Deauthorize** to deauthorize the ARC.

Note

- After you deauthorize the ARC, the ARC service for all devices on the Site will be automatically disabled.
- Once you deauthorize the ARC, an email will be sent to the ARC's **Email Address for Receiving Notification** to notify them, with the user account, device serial No., device model, and your company information.

15.9 HikCentral ReGuard Service

HikCentral ReGuard (hereinafter referred to as HCRG) services are the value-added services offered by the HCRG. HCRG provides a security management solution that helps its users (i.e., service providers) with alarm receiving and handling.

Note

- The HCRG services are not supported in some countries/regions. For details about the supported countries/regions, contact the local distributors or after-sales.
- HCRG service-related features (i.e., purchase, activation, and service management) are only supported on the Hik-Partner Pro Portal.

1. The HCRG user (usually the Remote Monitoring Center, or RMC, who provides the alarm receiving and handling services) registers and becomes a Hik-Partner Pro user to purchase HCRG services and generate an HCRG key on Hik-Partner Pro.
2. The HCRG user logs in to HCRG to activate the HCRG services by using the key.
3. After activation, the HCRG user can create work orders on HCRG and assign the work orders to an installation company from Hik-Partner Pro by specifying the Installer Admin account of the company, and can also use other HCRG services.

Note

All installers with the Manage Assigned Site permission in the company will receive the work order notifications, and those who are to handle the work orders will go to the sites to install the devices according to the address and customer information on the work orders.

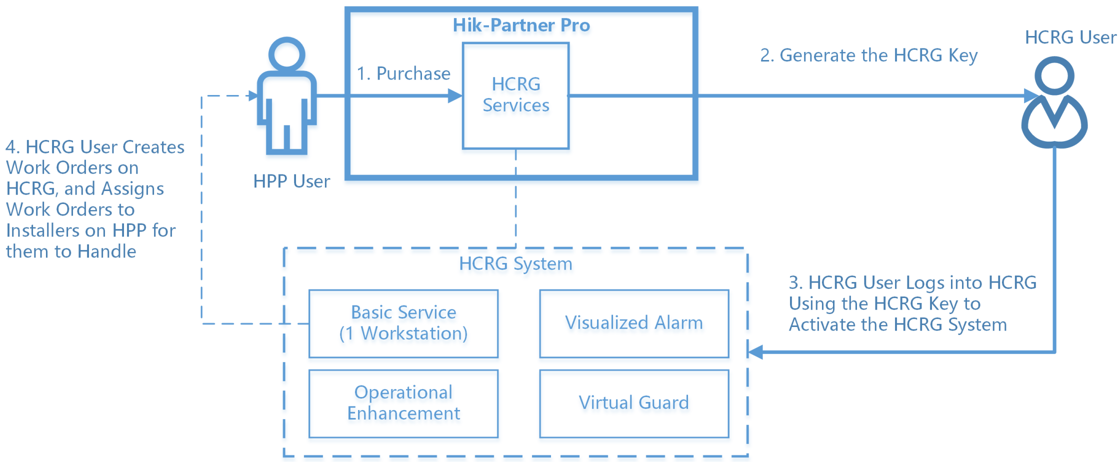


Figure 15-43 How HCRG Services Are Used

15.9.1 Purchase HikCentral ReGuard Service

In the service market, you can purchase HCRG services by entering service keys purchased from local distributors offline.

Before You Start

Make sure you have completed account authentication before you can purchase HCRG services. For details, see ***Authenticate Account*** .

Steps

Note

Online purchase is currently not supported.

1. Go to the service purchase page.
   - Go to **Site & Device → Service → Service Market → HikCentral ReGuard Service** .

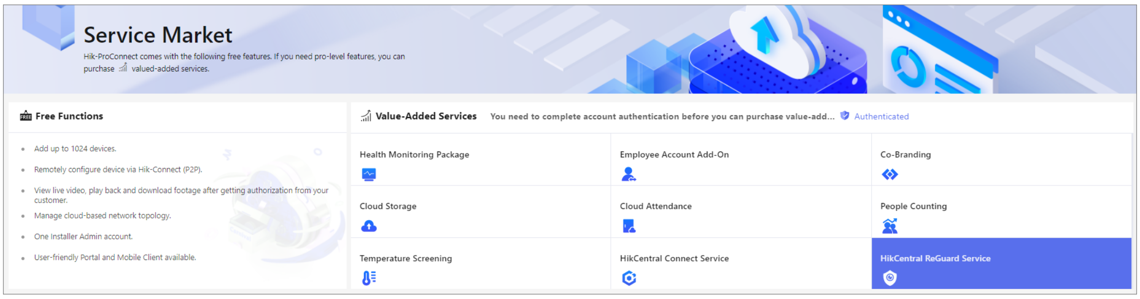


Figure 15-44 HCRG Services in Service Market

- Go to **Site & Device → Service → My Service → HikCentral ReGuard Service** .

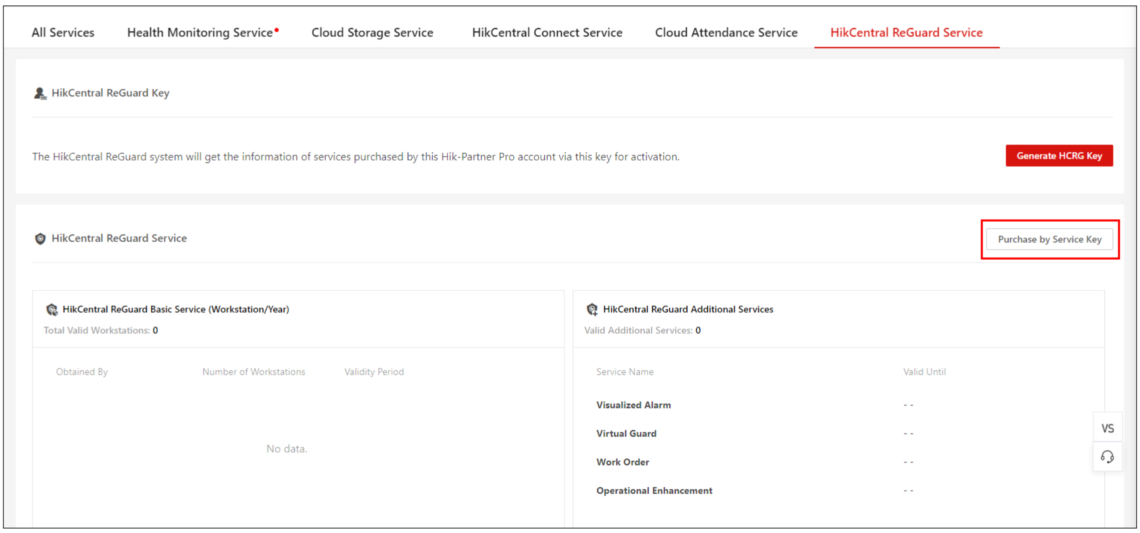


Figure 15-45 The Second Entry

2. Click **Activate by Service Key**.
3. Enter the service key purchased from local distributors offline.
4. Click **OK**.

What to do next

Generate an HCRG key for activating the HCRG system. See details in ***Generate HikCentral ReGuard Key*** .

15.9.2 Generate HikCentral ReGuard Key

After HCRG services are purchased by service key, you can generate an HCRG key for activating the HCRG system. The generated key will be sent to the email address of the Installer Admin and is also displayed in My Service. HCRG users can log in to HCRG with the key to activate the HCRG system.

Before You Start

Make sure you have purchased HCRG services by service key. See details in ***Purchase HikCentral ReGuard Service*** .

Steps

1. Go to **Site & Device → Service → My Service → HikCentral ReGuard Service** .

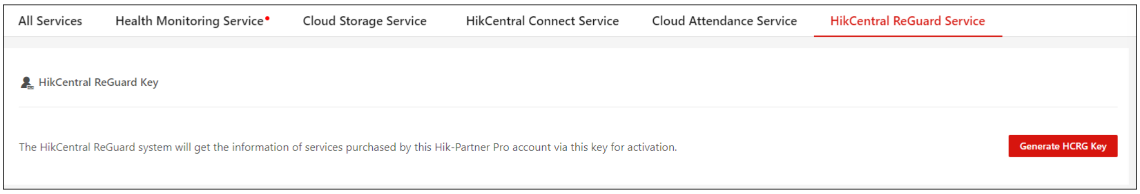


Figure 15-46 HikCentral ReGuard Service

2. Click **Generate HCRG Key**.

   The generated HCRG key is displayed and automatically sent to the email address of the Installer Admin. You can click / to hide/display the generated HCRG key.

What to do next

- Log in to HCRG with the key to activate the HCRG system. See details in *HikCentral ReGuard Web Client User Manual*.
- Manage HikCentral ReGuard services. See details in ***Manage HikCentral ReGuard Services*** .

15.9.3 Manage HikCentral ReGuard Services

After purchasing and activating HCRG services, you can monitor the real-time status of HCRG services on Hik-Partner Pro, including the total number of valid workstations, the number of valid additional services, the number of services expiring within 30 days, and the number of expired services.

Go to **Site & Device → Service → My Service → HikCentral ReGuard Service** .

Basic Service (1 Workstation/ Year)	You can view the total number of valid workstations and their detailed information, including the person who obtains the workstations, the number of workstations obtained by the person, and the validity period.
Additional Services	You can view the total number of valid additional services and for each service, you can view the validity period.
Service Filtering	You can view the total number of services expiring within 30 days and total number of expired services. By selecting the service type (**All Services**, **Workstation**, **Visualized Alarm**, **Virtual Guard**, or **Operational Enhancement**)

	and service status (**All Statuses**, **Expires in 30 Days**, **Expired**, or **Not Expired**), you can filter the service information.

15.10 Co-Branding

This feature helps improve the visibility of your brand, products, and services. It allows your customers to view some basic information of your company via Hik-Connect Mobile Client. You can purchase and enable this service as needed.

Note

- 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 get the co-branding service for free for one year after authenticating your account and adding 3 devices via P2P. See details in ***Authenticate Account*** and ***Add Device by Entering Serial No.*** .

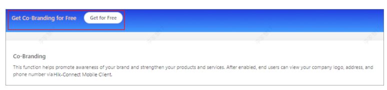


Figure 15-47 Entrance for Getting Free Co-Branding

- 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 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. For details about how to purchase health monitoring packages, see ***Purchase Health Monitoring Service*** .

15.10.1 Purchase Co-Branding

In the service market, you can either purchase co-branding service packages online or activate them by entering service keys purchased from local distributors offline.

Note

- Make sure you get your company authenticated. For details, see ***Authenticate Account*** .
- In some countries/regions, you can get the co-branding service for free for one year after authenticating your account and adding 3 devices via P2P (see details in ***Add Device by Entering Serial No.***).
- Purchasing co-branding services online is supported only in some countries/areas. Contact a local distributor for details.

Go to **Service → Service Market → Company Management** . In the Co-Branding area, purchase the service packages online or activate the services by service keys.

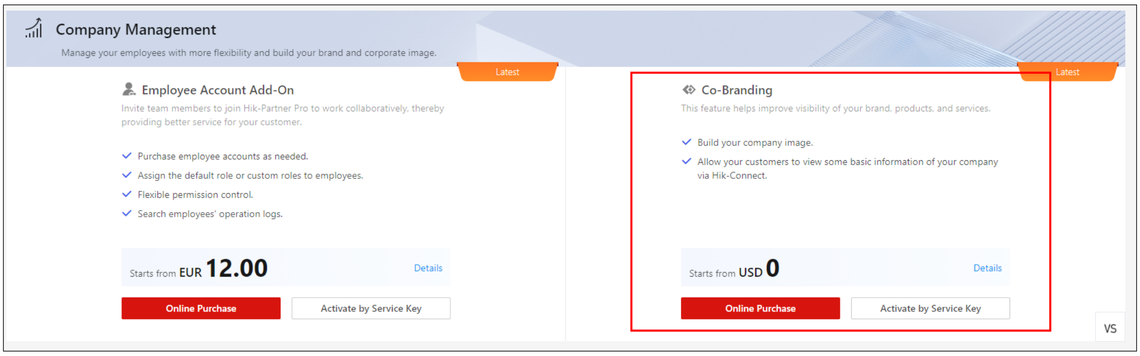


Figure 15-48 Company Management

Online Purchase	1. Click **Online Purchase**. 2. Specify the amount which determines the validity period, enter your VAT number, and select the payment method. 3. Click **Checkout** to enter the payment page and complete your payment.
Activate by Service Key	1. Click **Activate by Service Key** if your country/region supports activating services by service keys and you have purchased a service key from a distributor. 2. Enter the service key. 3. Click **OK**.

15.10.2 Enable 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.

Note

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.

Go to **Company Management → Co-Branding** . Switch on **Service Status**, and then hover the cursor onto the Logo area to show the **Edit** button. And finally click **Edit** to upload your company logo. After you edit the logo, the latest logo will be updated to the Company Information page.

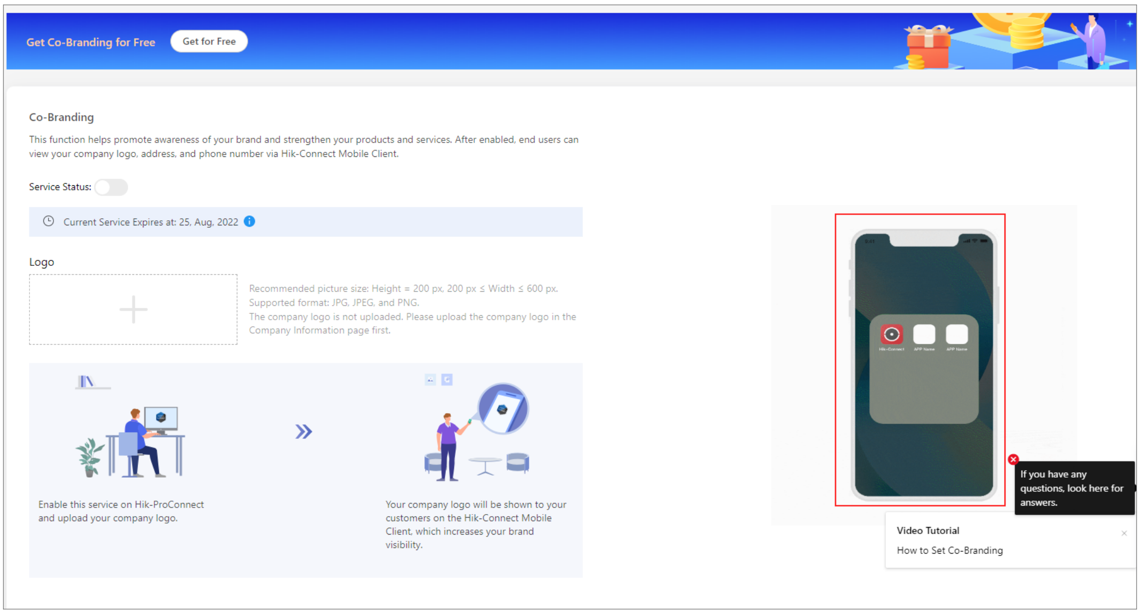


Figure 15-49 How Your Company Logo Will Be Shown to Your Customers

Note

- To ensure the co-branding service works on the Hik-Connect Mobile Client, please ask your customers to update the 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 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 16 Tools

Hik-Partner Pro provides tools, such as disk calculator and NVR channel calculator, to help you improve your work efficiency.

On the Hik-Partner Pro page, click **Tools** on the left pane to enter your tools page.

Batch Configuration

The tool is used to batch configure devices on LAN.
See ***Batch Configure Devices on LAN*** for details.

Batch Upgrade

The tool is used to detect whether the firmware of devices on LAN need to be upgraded and batch upgrade the firmware of the devices.
See ***Batch Upgrade Devices on LAN*** for details.

Search for Important Firmware Update

The tool is used to check whether the firmware of your device needs to be updated and download the relevant firmware package for the update.

Disk Calculator

The tool is used to calculate the recording time and recording space by setting related parameters.

NVR Channel Calculator

The tool is used to calculate the number of network cameras that can be connected to the NVR by setting the related parameters.

Focal Length Calculator

The tool is used to calculate focal length and object distance by setting related parameters such as sensor size. You can view the recommended data by the tool.

Bandwidth Calculator

The tool is used to calculate the required bandwidth of a network camera or NVR by setting parameters such as channel number and resolution.

Maintenance Quotation

The tool is used to create quotations for after-sales maintenance, which can help installers standardize the service process, improve customer satisfaction, and expand business.
See ***Create a Maintenance Quotation*** for details.

Chapter 17 Compensation

For distributors who keep a supply of products from Hikvision at a fixed price in advance, but later sell products at a lower price due to getting project support, you may apply for compensation online. After a compensation application is approved, the compensation amount may be issued to your e-wallet, or you may be compensated by credit notes against receivables or free items.

Note

This feature is only available to authenticated channel partners.

17.1 Apply for Compensation

You can apply for compensation for projects that are either submitted by you or shared to you. Projects that support the submission of a compensation application should be in Closed Won status and the date of closing should be within three months.

Before You Start

Make sure there is at least one closed project (either submitted by you or shared to you) that is in Close Won status and the date of closing is within three months from now.

Steps

1. Go to **Incentive → Compensation** and select **Projects waiting for application**.

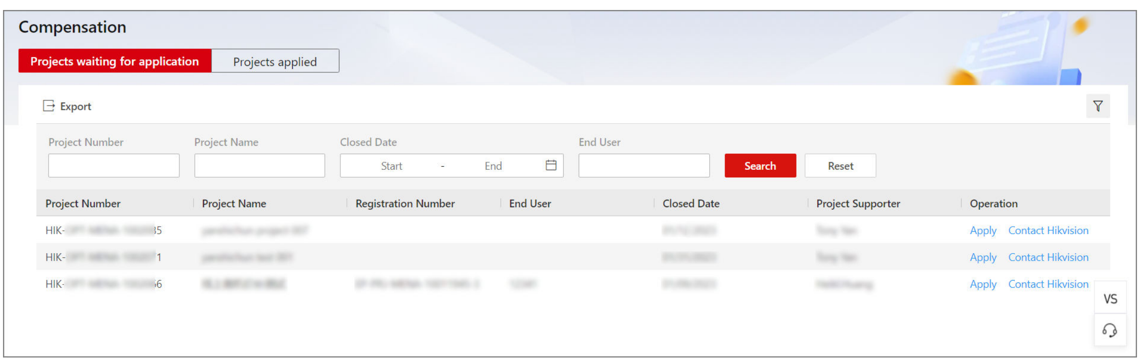


Figure 17-1 Projects Waiting for Compensation Application

2. **Optional:** Click **Contact Hikvision** in the Operation column of a project to contact the project supporter (i.e., Hikvision sales representative) if you have any questions or there is something you would like to tell them before applying.

   Note

   An email will be sent to the project supporter. The message you entered for the previous time will be kept for you to edit and resubmit if needed.

3. Click **Apply** in the Operation column of a project to enter the Input Price Information page.

Note

A window will pop up showing you the Compensation Policy. If needed, you can check the box next to **No more reminder** before clicking **Continue** to skip this part for next time you click **Apply**. You can always review the Compensation Policy again at any time before you submit applications.

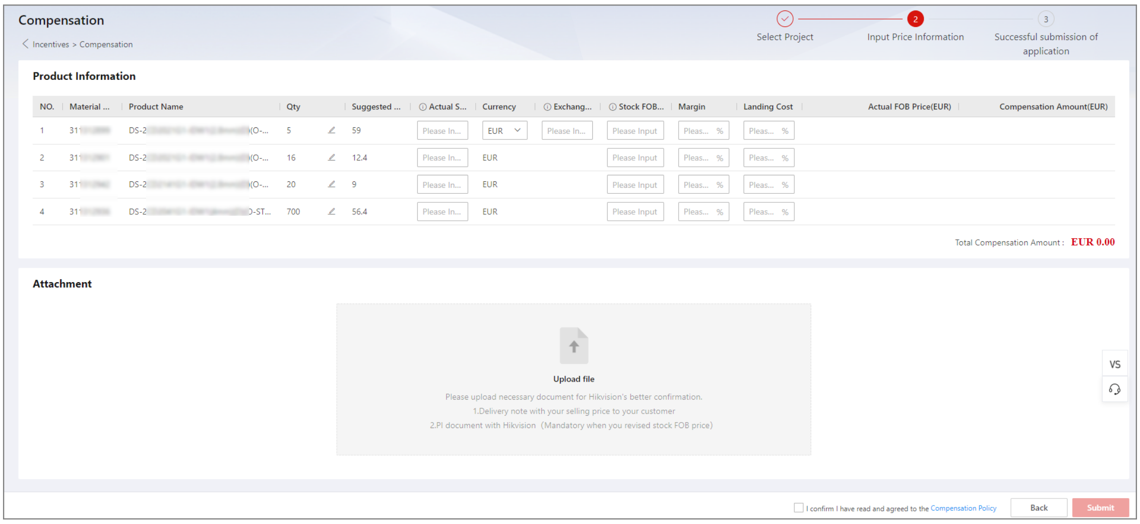


Figure 17-2 Compensation Application

4. In the Product Information field, enter or edit the following price related information accordingly for each product.

Actual Sales Price

If the currency of the actual transaction is different from that of the suggested sales price, enter this field according to your actual situation. Otherwise, the actual sales price should be the same as the suggested sales price.

Currency

Select the currency of the actual transaction. The selection of the first row will be applied to all the rows below.

Exchange Rate

If the currency of the actual transaction is different from that of the suggested sales price, enter the currency exchange rate at the time of the transaction. The value entered for the first row will be applied to all the rows below.

Note

If the currency are the same, exchange rate will be set to 1 and cannot be edited.

Stock FOB Price

Revise this field if you find a price displayed is incorrect.

Note

You have to upload a PI document as the proof attachment below if you have edited this field.

Margin

Enter the handling fee of a transaction as a percentage (%).

Landing Cost

Enter the total landed cost for a product as a percentage (%).

The compensation amount will be calculated automatically based on the price information you enter.

5. **Optional:** Upload the appropriate attachments (e.g., delivery notes with actual sales prices, PI documents, etc.) according to your actual situation to make it easier to get your application approved.

Note

If you have revised the stock FOB price for a product above, uploading a PI document is required here. Otherwise your application will be rejected.

6. Read the Compensation Policy, check the box for confirming policy agreement, and click **Submit**.

A window will pop up for you to confirm the submission. After clicking **Confirm**, you will land on the successful submission page with relevant details of your application such as the application number, project number, and the total compensation amount.

Note

If your application is failed to be submitted, please contact Hikvision. A failed submission will be saved in Draft status for you to edit and resubmit later.

What to do next

For further operations, refer to ***View and Handle Submitted Compensation Applications*** .

17.2 View and Handle Submitted Compensation Applications

After submitting a compensation application, you can track the status of your application, search for submitted applications by project number, status, application date, and application number, and perform operations on applications according to its current status.

Go to **Incentive → Compensation** and select **Projects applied**.

For each submitted application, you can check the application number, the latest date of submission, the total compensation amount, the related project number, and the current status of the application. If an application is rejected, you can also view the latest remarks for the application.

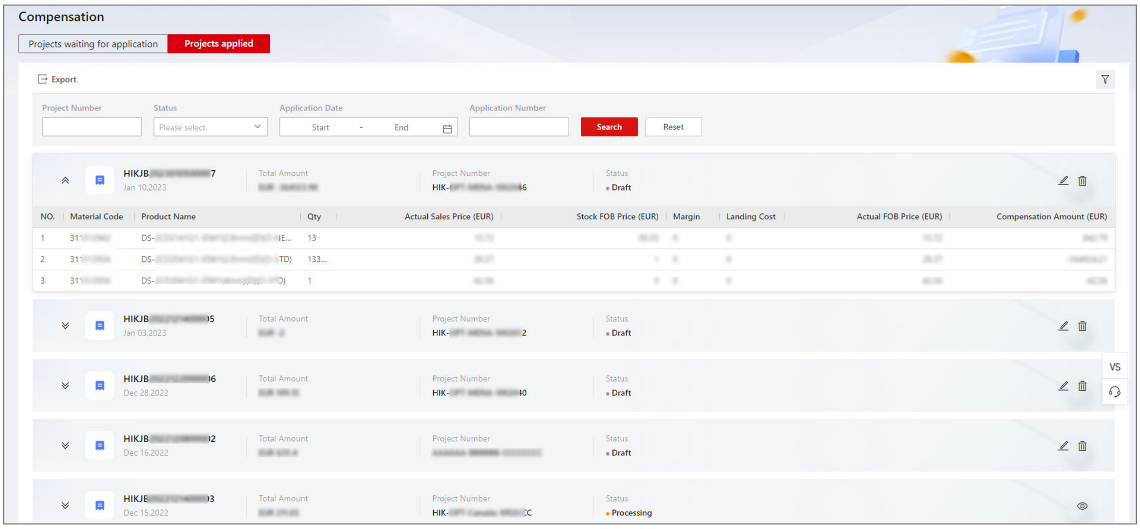


Figure 17-3 View Submitted Compensation Applications

Perform the following operations as needed.

Operation	Description
Filter Applications by Status	You can filter applications by selecting status(es) from the drop-down list. The four possible statuses are as follows: • **Draft**: The application has failed to be submitted. Information entered for the latest submission will be saved for you to edit and resubmit if needed. • **Processing**: The application has been submitted successfully and is currently under review. • **Rejected**: The application has been reviewed by a Hikvision sales representative and is rejected. You can view remarks for your application, make changes to it, and resubmit if needed. • **Completed**: The application is approved. You will be compensated by one of the following methods: compensation amount issued to your e-wallet, credit notes, or free items.
Search for Applications	You can search for applications by entering the project/application number or specifying a range for the application date.

Operation	Description
Edit Application	Click to edit an application. **Note** You can only edit applications in Draft or Rejected status.
Delete Application	Click to delete an application. **Note** You can only delete applications in Draft or Rejected status.
View Application Details	• Click to expand the detailed product and price information of an application. • Click an application number (in the format "HIKJB+yyyymmdd+xxxxx") to enter the application details page, which displays the basic information, product and price related information, attachments, and operation history of the application.
Export Application Details	Click **Export** to save details of all applications to the local PC as an Excel file. Each product of every application will be saved to a row in the file.

Chapter 18 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 **Incentive → Partner Program** , and click 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 18-1 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. Click **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.

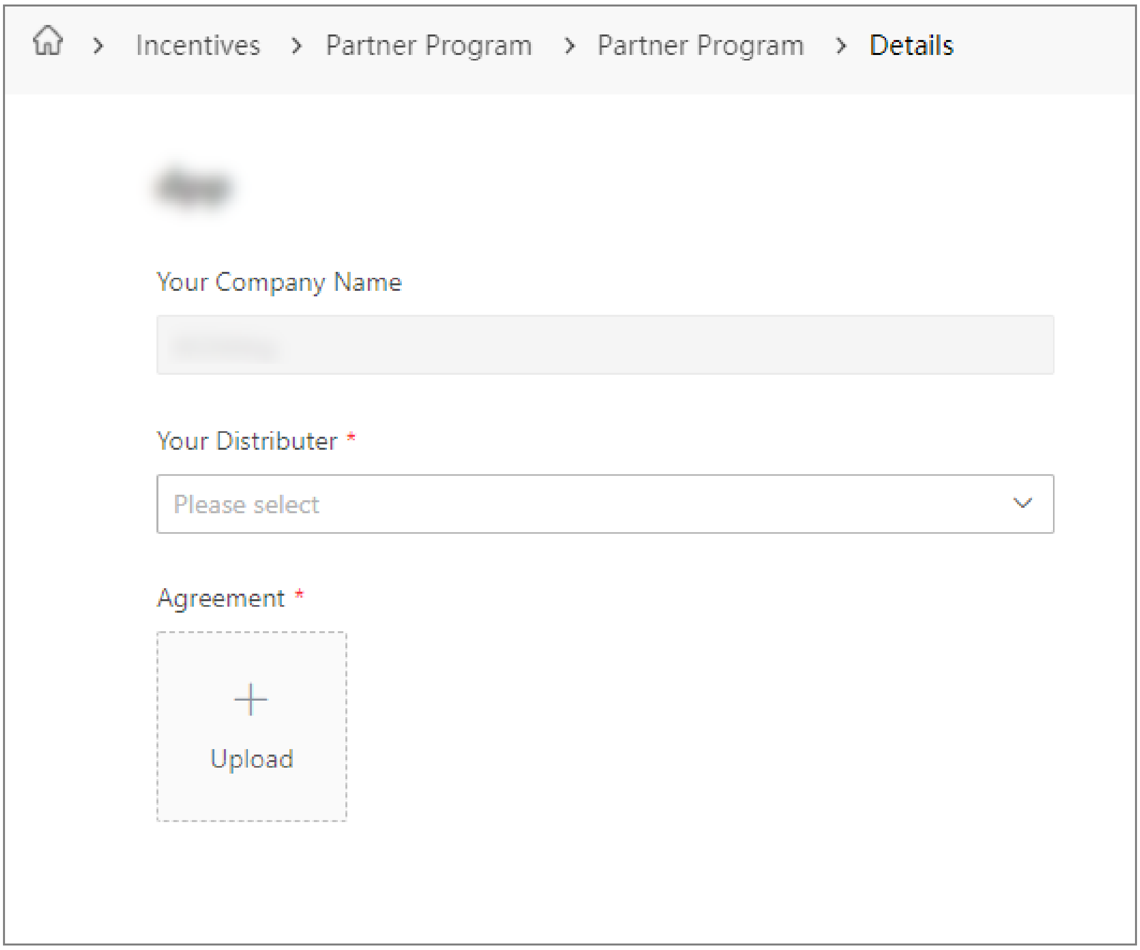


Figure 18-2 Application Page (Contract Agreement Already Signed Offline)

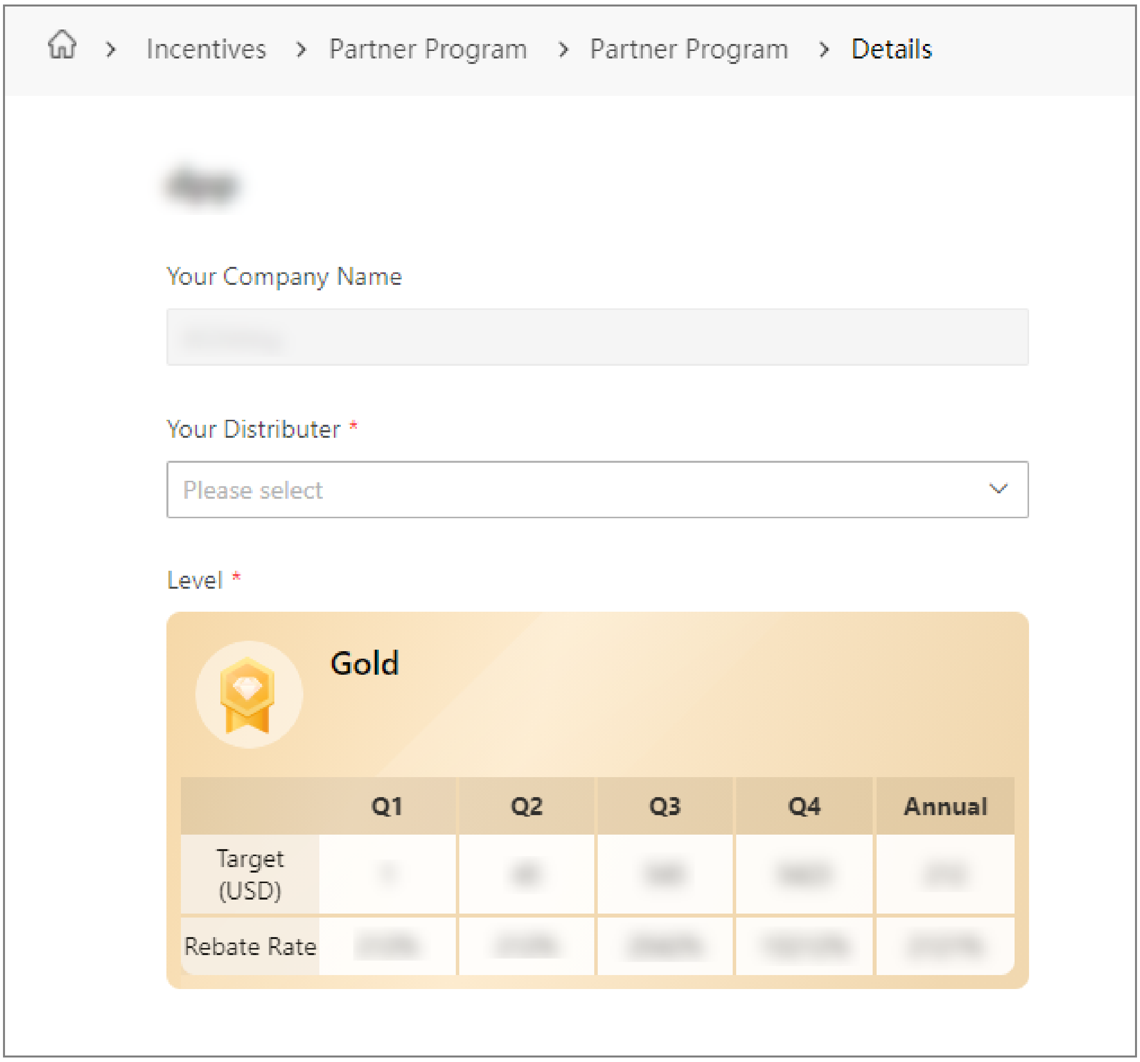


Figure 18-3 Application Page (Contract Agreement Not Signed)

Click **Submit** 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 click **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 click **Submit**.
- 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 **Incentive → Partner Program → My Certificate** .

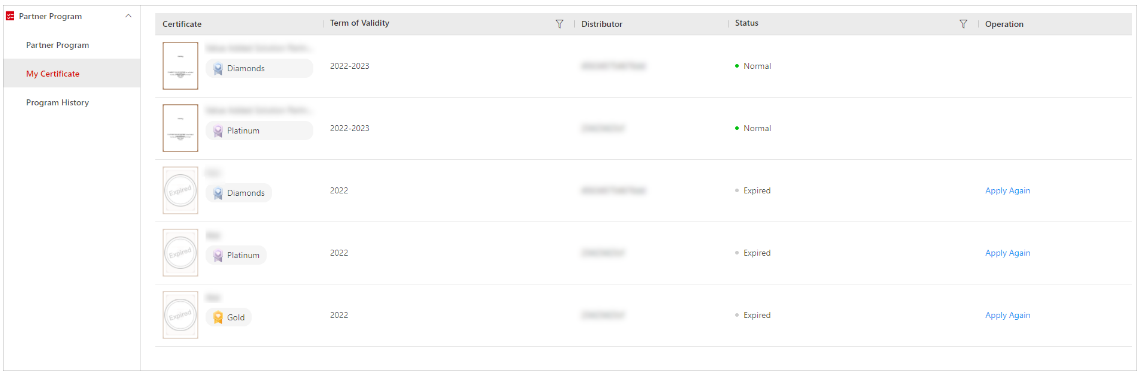


Figure 18-4 My Certificate

On the certificate list, you can view the program certificate name, certificate thumbnail, level, term of validity, distributor, and status (normal or expired).

Click beside the **Term of Validity** and/or **Status** to filter the certificates.

Click **Apply Again** in the Operation column to apply for the partner program of which your certificate has expired.

Click the certificate thumbnail or name to enter the Certificate Details page. You can download the certificate and 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 **Incentive → Partner Program → Program History** .

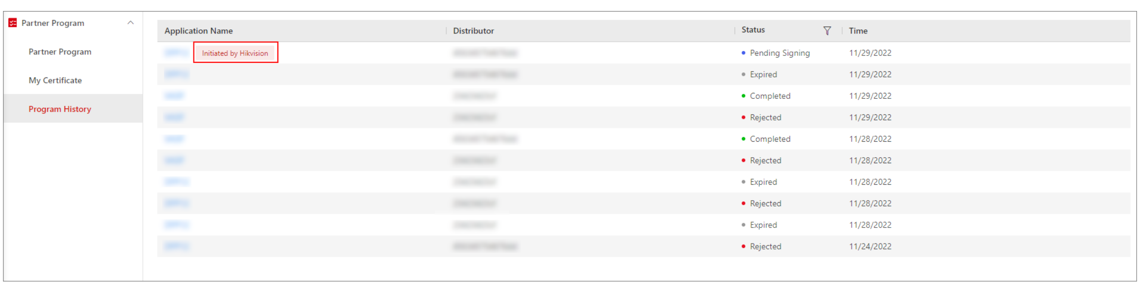


Figure 18-5 Program History

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.

Click an application record to enter the Details page. 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**, click **Sign** on the right bottom of the Details page to sign the agreement online.

Chapter 19 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 Account*** .

Enter the Rewards Store page.

- Click **Check In to Earn Points/My Points** in the upper-right corner to enter the Rewards Store.
- Click **Incentive → Rewards Store** to enter the Rewards Store.

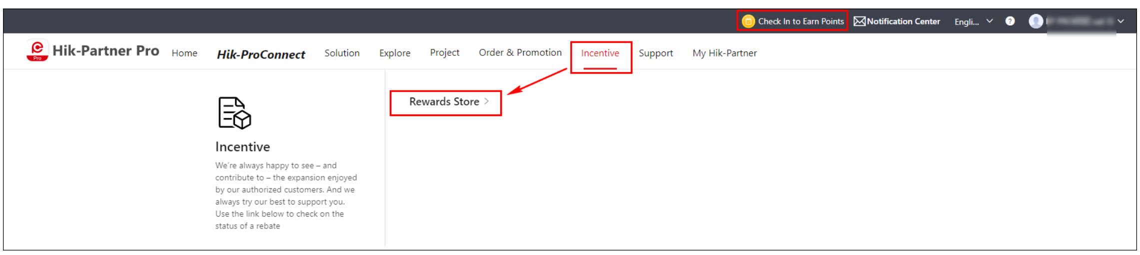


Figure 19-1 How to Enter the Rewards Store Page

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

Table 19-1 Available Information/Operations for the Installer Admin / Installers

Information/Operation	Installer Admin	Installer
Total Points Available	√ View company total points.	√ View personal total points.
Points History	√ 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 staff member are available.	√ Only the Installer's own records are available.

Information/Operation	Installer Admin	Installer
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	√	×
Lucky Draw	√ Only supported in some countries/regions.	×

Note

- Distributors can go to **My Hik-Partner → Gifts Verify** to verify the gifts redeemed offline and export the records.
- 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.

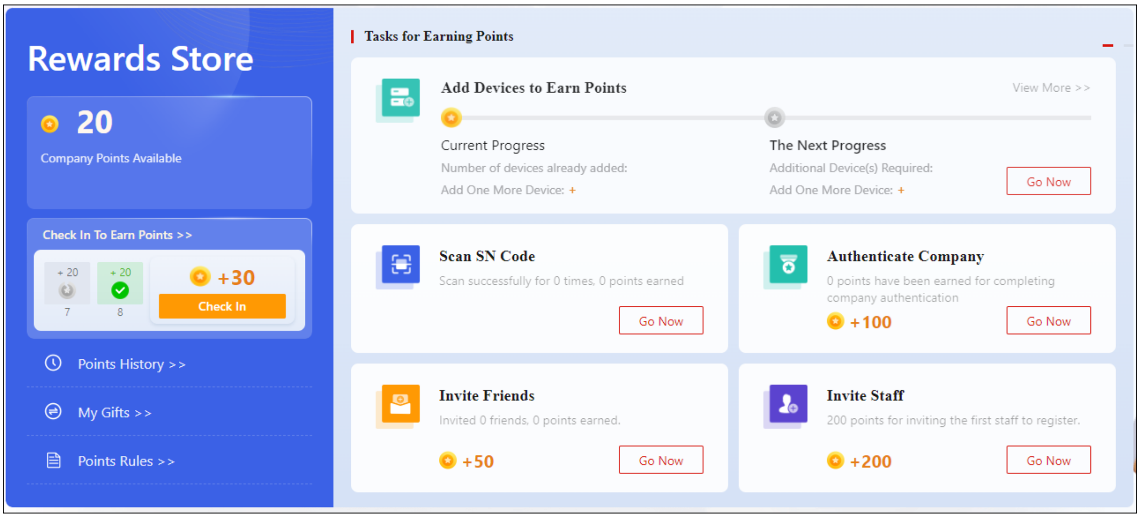


Figure 19-2 Rewards Store Page for Installer Admin

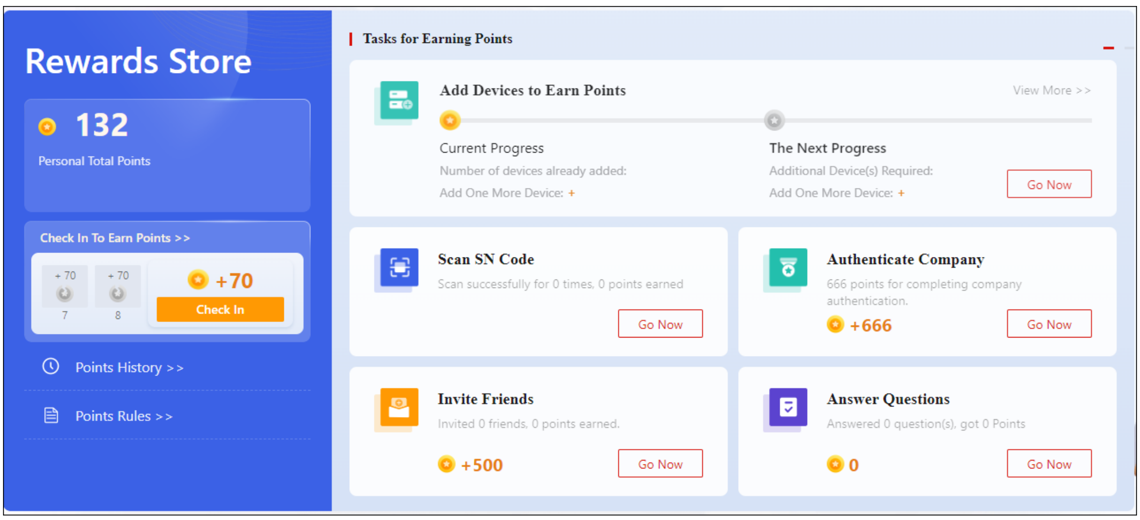


Figure 19-3 Rewards Store Page for Installers

Chapter 20 Rebate

For authenticated channel partners, they can view the rebates they earn from successfully promoting services (i.e., health monitoring service and cloud storage service) of Hik-Partner Pro to their customers, including installers and secondary distributors. Here we will introduce the process and the calculation method of earning rebates.

Note

This function is only available to some users in some countries/regions. For details, please contact Hikvision.

20.1 Generate Authentication Code

For some countries or regions, authenticated channel partners can generate authentication codes for installers and secondary distributors to complete the company authentications on Hik-Partner Pro, and then they can have chances to earn rebates.

Note

Contact the local Hikvision branch for details about whether the country or region supports generating authentication codes on Hik-Partner Pro.

Go to **My Hik-Partner → Rebate → Authentication Code** .

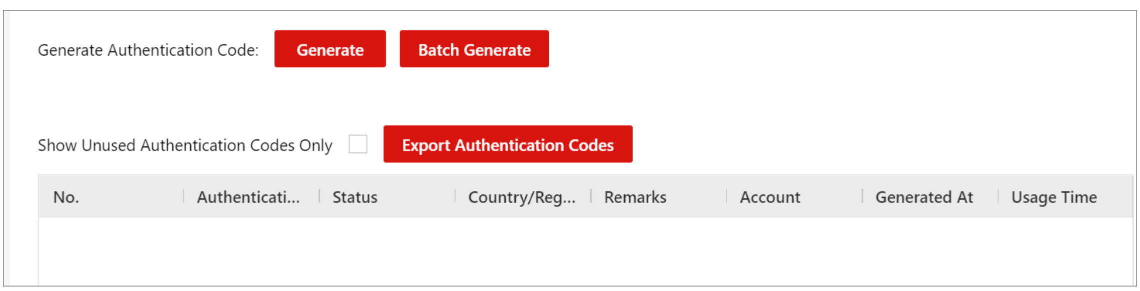


Figure 20-1 Generate Authentication Code

Generate an Authentication Code

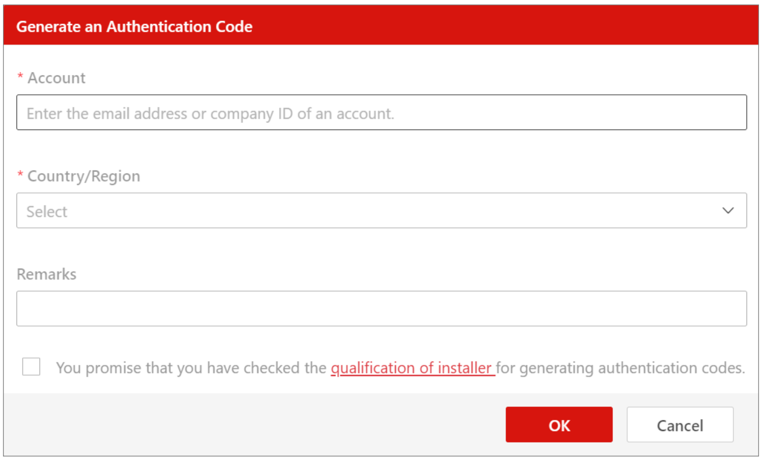


Figure 20-2 Generate an Authentication Code

1. Click **Generate** to open the Generate an Authentication Code window.
2. Enter the information about account (email address or company ID) and select the country/ region of the installer or secondary distributor for whom you generate the authentication code.
3. Check **You promise that you have checked the qualification of installer for generating authentication codes.** and click **OK**.
   The generated authentication code will be displayed on the Authentication Code page.

Batch Generate Authentication Codes

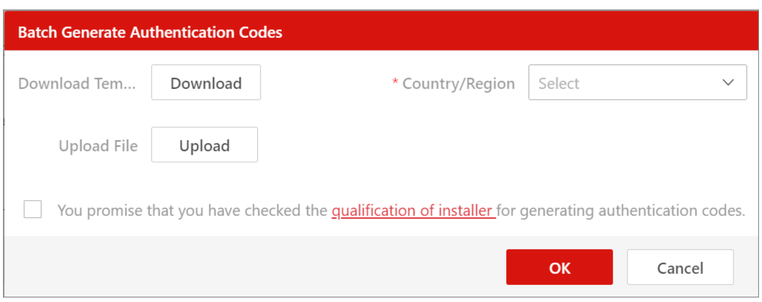


Figure 20-3 Batch Generate Authentication Codes

1. Click **Batch Generate** to open the Batch Generate Authentication Codes window.
2. Click **Download** to download the template and fill in the information about accounts of the installer or secondary distributor for whom you generate authentication codes.
3. Click **Upload** to upload the filled-in template file.
4. Select the country/region for the accounts you uploaded.

Note

You can only batch generate authentication codes for accounts in the same country or region each time.

5. Check **You promise that you have checked the qualification of installer for generating authentication codes.** and click **OK**.
   The generated authentication codes will be listed on the Authentication Code page.

Export Authentication Codes

Click **Export Authentication Codes** to export the generated authentication codes and send to the installer or secondary distributor.
You can also check **Show Unused Authentication Codes Only** to export the authentication codes that are not used.

20.2 The Process of Earning Rebates

The process of earning rebates varies basing on whether the country or region supports generating the authentication codes.

Process for Countries and Regions Which Support Generating Authentication Codes

Note

Contact the local Hikvision branch for details about whether the country or region supports generating authentication codes on Hik-Partner Pro.

1. The authenticated channel partner introduces and promotes services to an installer or secondary distributor when selling Hikvision devices.
2. The authenticated channel partner goes to **My Hik-Partner → Rebate → Authentication Code** on the Hik-Partner Pro Portal and generates an authentication code for the installer or secondary distributor.

   Note

   For details about generating authentication codes, refer to ***Generate Authentication Code*** .
3. The installer or secondary distributor authenticates their company by entering authentication codes.

   Note

   For details about how to authenticate the company, refer to ***Authenticate Account*** .
4. The installer or secondary distributor activates services for devices via Hik-Partner Pro after their company authentication is completed.

Note

For details about how to activate services for devices, refer to ***Activate the Health Monitoring Service for Devices*** and ***Activate or Renew Service for a Channel*** .

5. Hik-Partner Pro calculates monthly rebate amount based on resources with service(s) activated in the last month for the authenticated channel partner.

Note

If a service has been activated for a resource before, the resource will NOT be included in statistics. The authenticated channel partner can go to **My Hik-Partner → Rebate → Rebate Settings** to view the calculation rules. And for more details, refer to ***The Way to Calculate Rebate Amount*** .

6. The authenticated channel partner gets the rebate amount in the form of a credit note.

Note

The authenticated channel partner can go to **My Hik-Partner → Rebate → Rebate Details** to view the information about the rebates they earned. See ***View Rebate Details*** for details.

Process for Other Counties and Regions

1. The authenticated channel partner introduces and promotes services to an installer or secondary distributor when selling Hikvision devices.
2. The installer or secondary distributor activates services for devices via Hik-Partner Pro.

Note

For details about how to activate services for devices, refer to ***Activate the Health Monitoring Service for Devices*** and ***Activate or Renew Service for a Channel*** .

3. Hik-Partner Pro calculates monthly rebate amount based on resources with service(s) activated in the last month for the authenticated channel partner.

Note

If a service has been activated for a resource before, the resource will NOT be included in statistics. The authenticated channel partner can go to **My Hik-Partner → Rebate → Rebate Settings** to view the calculation rules. Refer to ***The Way to Calculate Rebate Amount*** for details.

4. The authenticated channel partner gets the rebate amount in the form of a credit note.

Note

The authenticated channel partner can go to **My Hik-Partner → Rebate → Rebate Details** to view the information about the rebates they earned. See ***View Rebate Details*** for details.

20.3 The Way to Calculate Rebate Amount

Here we introduce the four elements that determine the rebate amount, and the formula for calculating the rebate amount.

Go to **My Hik-Partner → Rebate → Rebate Settings** to view the calculation rules.

Elements that Determine the Rebate Amount

Four elements determine the earned rebate amount, including:

- Number of Resources Contributed to Rebates
- Unit Price
- Rebate Rate
- Calculation Type

Table 20-1 Element Description

Element	Description
Number of Resources Contributed to Rebates	The number of resources which have contributed to rebates. To be a resource contributed to rebates, 1) it should belong to an authenticated channel partner; 2) it should have been added to Hik-Partner Pro and the health monitoring service or cloud storage service should have been activated for it. **Note** • For the health monitoring service, "resource" refers to devices. • For the cloud storage service, "resource" refers to the channels linked to Hik-ProConnect box.
Unit Price	• For the health monitoring service, the unit price refers to the monthly service fee per device. • For the cloud storage service, the unit price refers to the monthly service fee per channel. **Note** For example, assume that a customer spent 288 US dollars to purchase a 7-Day Annual Package (a type of cloud storage service package; the "7-Day" means the videos uploaded to the cloud will be retained for 7 days; the "Annual" means the service lasts for 12 months) and activated it for two channels, the unit price in this case would be the result of 288/2/12, that is, 12 dollars.

Element	Description
Rebate Rate	Fixed rebate rate or tiered rebate rate, depending on the marketing strategy for the country or region. For the tiered rebate rate, the authenticated channel partner can get a higher rebate rate when the number of resources with service activated reaches a certain threshold.
Calculation Type	One of two calculation types is used for calculating the rebate amount, that is, **Combined** or **Separated**, depending on the marketing strategy for the country or region. • **Combined**: ◦ For calculating the rebate amount related to the health monitoring service, the rebate rate(s) for different device types are the same, be it fixed or tiered rebate rate. ◦ For calculating the rebate amount related to the cloud storage service, the rebate rate for different types of service packages are the same, be it fixed or tiered rebate rate. • **Separated**: ◦ For calculating rebate amount related to the health monitoring service, the rebate rate for network cameras and other device types can be different. Other device types include the NVR/DVR, security control device, access control device, video intercom device, etc. ◦ For calculating rebates related to the cloud storage service, the rebate rate for different types of service packages can be different.

Formula for Calculating the Rebate Amount

The formula for calculating rebate amount is shown below:
Number of New Resources Contributed to Rebates in Current Month × Unit Price × Rebate Rate = Rebate Amount for Current Month

Note

The platform will calculate the rebate amount of the previous month on the 1st day (fixed) of each month.

Example

Calculate the Rebate Amount of the Current Month
Assume that in the current month:

- Customer A purchased a 7-day annual package (price: 288 US dollars) and activated it for 8 channels linked to a Hik-ProConnect box; Customer B purchased a 30-day annual package (price: 600 US dollars) and activated it for 4 channels linked to a Hik-ProConnect box.
- The Calculation Type used in the country or region is **Separated**.
- Tiered rebate rate is used for calculation in the country or region:
  - First Tier: a rebate rate of 10% for the first 4 channels activated with the 7-day annual package; a rebate rate of 20% for the first 2 channels activated with the 30-day annual package.
  - Second Tier: a rebate rate of 30% for all other channels activated with the 7-day annual package; a rebate rate of 40% for all other channels activated with 30-day annual package.

In this case, for the 7-day annual package, the unit price would be: (288/12)/8 = 3 US dollars; For 30-day annual package, (600/12)/4 = 12.5 US dollars, so we can calculate the rebate amount as: 4 × 3 × 10% +4 × 3 × 30% + 2 × 12.5 × 20% + 2 × 12.5 × 40% = 19.8 US dollars.

20.4 View Rebate Details

After authenticated channel partners promote the health monitoring service or cloud storage service to their customers (i.e., installers and secondary distributors), if customers activate two services for devices added to Hik-Partner Pro or channels linked to a Hik-ProConnect box, authenticated channel partners will earn a certain rebate amount and they can view the details of their rebates.

Note

You can view the rebates of the current month after the calculation day of the next month. For example, if the calculation day of the month is set to 15th, you can view the rebates of July on 16th, August.

Go to **My Hik-Partner → Rebate → Rebate Details → Health Monitoring Related/Cloud Storage Related** .

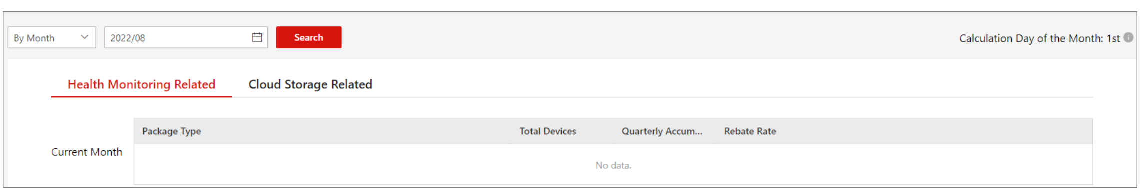


Figure 20-4 Rebate Details

Select **By Month** or **By Quarter** from the drop-down list on the top left, select a corresponding period, and click **Search** to search for rebate related data.

20.5 View Bill of Sale

Authenticated channel partners can filter their bills of sale to check the information related to the devices sold to customers (i.e., installers or secondary distributors). The information includes the device serial No., device model, purchaser name, and purchaser type. By setting the purchaser type to **Secondary Distributor**, authenticated channel partners can transfer rebates related to specific devices to the secondary distributors.

Go to **My Hik-Partner → Rebate → Bill of Sale** .

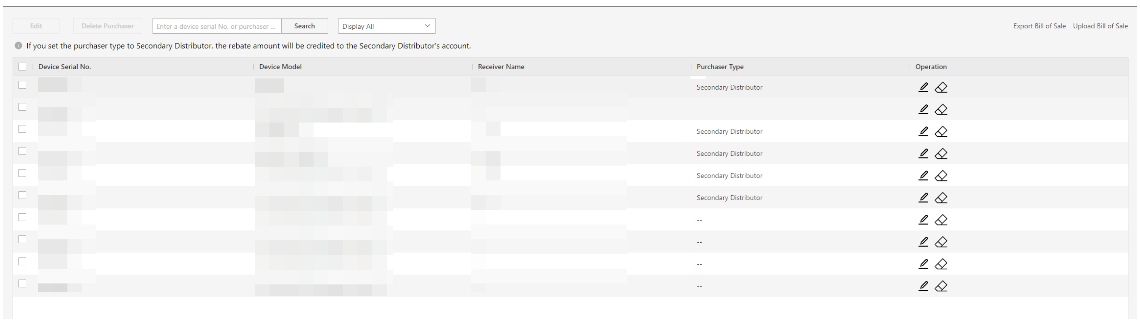


Figure 20-5 Bill of Sale Page

Note

If the bill of sale is uploaded before the calculation day, the related rebates will be credited to the amount of the previous month. If the bill of sale is uploaded on or after the calculation day, the related rebates will be credited to the current month.

Filter Bills of Sale

- Enter a device serial No. or purchaser name to filter.
- Set one of the following conditions to filter.

Display All

All bills of sale will be displayed.

Display Secondary Distributor Only

Only the devices purchased by secondary distributors will be displayed.

Display Installer Only

Only the devices purchased by installers will be displayed.

Export Bills of Sale

Click **Export Bill of Sale** and select **Export All Bills of Sale** or **Export Filtered Bills of Sale** to export the data as needed.

Transfer Ownership of Future Rebates

If the purchaser of specific devices is a secondary distributor, the authenticated channel partner can transfer the ownership of future rebates related to these devices to the secondary distributor. Once the ownership is transferred, the previously calculated rebates are still owned by the Authenticated channel partner, the secondary distributor starts owning rebates related to these devices from the next month.

The authenticated channel partner can transfer the ownership in the following three methods.

Transfer Ownership of Future Rebates Related to a Device to a Secondary Distributor

1. On the Bill of Sale page, select a device and click in the Operation column.

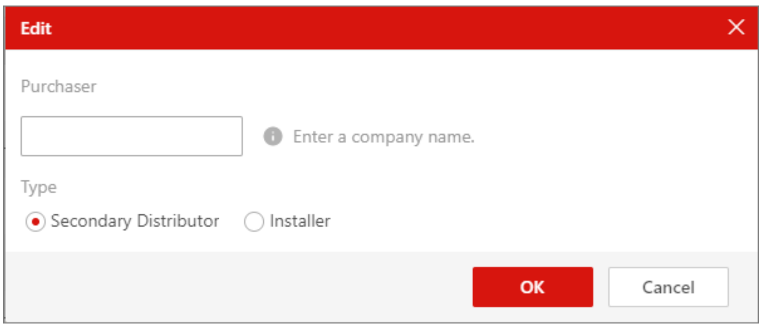


Figure 20-6 Transfer Rebates

2. Enter the purchaser name.
3. Select **Secondary Distributor** as the purchaser type.
4. Click **OK**.

Batch Transfer Ownership of Future Rebates Related to Multiple Devices to a Secondary Distributor

1. On the Bill of Sale page, select all devices and click **Edit**.
2. Enter the purchaser name.
3. Select **Secondary Distributor** as the purchaser type.
4. Click **OK**.

Transfer Ownership of Future Rebates Related to Multiple Devices to Multiple Secondary Distributors

1. On the Bill of Sale page, click **Upload Bill of Sale**.

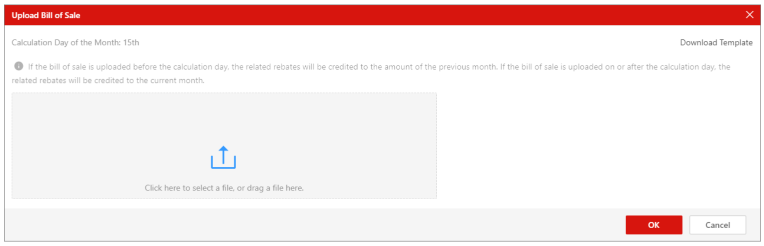


Figure 20-7 Upload Bill of Sale

2. Click **Download Template** and fill the required information (e.g., fill **Secondary Distributor** in the Purchaser Type column) in the template.
3. Click on the Upload Bill of Sale window to upload the filled-in template file.
4. Click **OK**.

UD31423N