



Hik-ProConnect Portal

User Manual

Legal Information

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

About this Manual

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

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

Trademarks

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

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

Disclaimer

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

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




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

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

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

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

Contents

Chapter 1 Introduction	1
1.1 Target Audience	1
1.2 Entities in Hik-ProConnect	2
1.3 Running Environment	2
1.4 Region Availability for Hik-ProConnect Functions	3
1.4.1 Functions Only Available in Certain Regions	3
1.4.2 Regions Only With Support for Free Functions	4
Chapter 2 Account Management	6
2.1 Register an Installer Admin Account	7
2.2 Manage Company Information	9
2.3 Authenticate Account	10
2.4 Manage Role and Permission	11
2.5 Invite Employee	13
2.6 Accept Invitation and Register Installer Account	14
2.7 Set Account Information	14
Chapter 3 Login	16
Chapter 4 Hik-ProConnect Portal Overview	18
Chapter 5 Site Management	24
5.1 Site Page Overview	24
5.2 Add New Site	25
5.3 Add Existing Site	27
5.4 Assign Site to Installer	28
5.5 Invite Site Owner	28
5.6 Apply for Site Authorization from Site Owner	30
Chapter 6 Device Management	32
6.1 Batch Configure Devices on LAN	32

6.1.1 Batch Activate Devices and Assign IP Addresses for Them	34
6.1.2 Batch Link Channels to NVR	35
6.1.3 Create Template for Setting Parameters	37
6.1.4 Batch Set Parameters for Devices via Template	37
6.2 Add Device	39
6.2.1 Add Device(s) after Batch Configuring Them	40
6.2.2 Add Detected Online Device	41
6.2.3 Add Device by Hik-Connect (P2P)	45
6.2.4 Add Devices by IP Address or Domain Name	47
6.2.5 Add Devices in a Batch	49
6.2.6 Add Devices Without Support for the Hik-Connect Service	51
6.3 Manage Device Permission	53
6.3.1 Apply for Device Permission	53
6.3.2 Release the Permission for Devices	54
6.4 Migrate Devices from Hik-Connect Account	54
6.5 Linkage Rule and Exception Rule	59
6.5.1 Add Linkage Rule	59
6.5.2 Add Exception Rule	68
6.5.3 Enable Device to Send Notifications	71
6.6 Reset Device Password	72
6.7 Manage Security Control Panel	74
6.7.1 Control AX Pro	74
6.7.2 Configure AX Pro	76
6.7.3 Batch Arm/Disarm AX Pro	77
6.7.4 Batch Configure AX Pro	80
6.8 View Video	83
6.8.1 View Live Video	84
6.8.2 Play Back Video Footage	84

6.9 Other Management	85
6.9.1 Upgrade Device Firmware	85
6.9.2 Unbind a Device from Its Current Account	86
6.9.3 Configure DDNS for Devices	86
6.9.4 Remote Configuration	87
Chapter 7 Value-Added Services	89
7.1 Health Monitoring Service	89
7.1.1 Purchase Health Monitoring Service	90
7.1.2 Activate the Health Monitoring Service for Devices	92
7.1.3 Manage Your Health Monitoring Service	95
7.2 Access and Attendance Service	97
7.2.1 Flow Chart for Setting Access & Attendance Service	98
7.2.2 Add Access and Attendance System	99
7.3 Cloud Storage Service	100
7.3.1 Flow Chart	100
7.3.2 Purchase Cloud Storage Service	104
7.3.3 Set Cloud Storage for Box	105
7.3.4 Set Cloud Storage for Cloud Storage DVR	108
7.3.5 Network Test	110
7.3.6 Activate or Renew Service for a Channel	111
7.3.7 View Cloud Storage Details	113
7.4 People Counting Service	113
7.4.1 Flow Chart for Setting People Counting Service	113
7.4.2 Activate People Counting Service for Channels	115
7.4.3 Add a Group for People Counting	115
7.5 Temperature Screening Service	118
7.5.1 Flow Chart for Setting Temperature Screening Service	119
7.5.2 Activate Temperature Screening Service for Channels	120

7.6 Alarm Receiving Center (ARC) Service	122
7.7 Co-Branding	123
Chapter 8 Health Monitoring	125
8.1 View Status of Devices in All Sites	125
8.2 View Status of Devices in a Specific Site	130
8.3 Send Report Regularly	133
8.4 Network Topology	134
8.5 Exception Center	138
Chapter 9 Search Operation Log	140
Chapter 10 Tools	141

Chapter 1 Introduction

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

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

Table 1-1 Client Description

Client	Description
Hik-ProConnect Portal	Portal for Installer Admin and Installers logging into Hik-ProConnect to manage the security business, including permission and employees management, site management, devices management, and devices health monitoring, etc.
Hik-ProConnect Mobile Client	Mobile Client for Installer Admin and Installers logging into Hik-ProConnect to manage site, apply for site information management permission from end user, manage and configure the devices, etc.
Hik-Connect Mobile Client	Mobile Client for end users to manage their devices, accept the Installer's invitation as the site owner, approve the Installer's application of site information management permission, etc.
Hik-Connect Portal	Portal for your customers to manage their employees' access level and attendance after you set an attendance system for them via the Hik-ProConnect Portal.

1.1 Target Audience

This manual provides the Installer Admin and Installer with the essential information and instructions about how to use Hik-ProConnect 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 authentication permission from end user, manage and configure the devices belonging to the site, and check the device health status for further maintenance, etc.

1.2 Entities in Hik-ProConnect

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

- **Installer Admin:** The Installer Admin has full access to Hik-ProConnect functions.
- **Installer:** Installers are "sub-account" to the Installer Admin and are controlled by permission for what they can do. For example, they can only manage the sites that are assigned to them.



Note

Installer account is unavailable 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:** 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 he/she 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 Installer transfers ownership of the Site to the end user, the end user becomes the Site Owner who is the holder of the site. Installer can also apply for site authorization permission 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

Internet Explorer 11 (32-bit and 64-bit) and above, and versions of Firefox (32-bit and 64-bit) and Chrome (32-bit and 64-bit) released in the latest half year.

1.4 Region Availability for Hik-ProConnect Functions

Hik-ProConnect offers both free functions and value-added functions that cost certain fees. You can purchase certain services in the Service Market of Hik-ProConnect 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-ProConnect 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
<u>Health Monitoring Service</u>	Only linkage rule.  Note Linkage rule is unavailable in the United States and Canada.
<u>Cloud Storage Service</u>	All functions contained in the service.
<u>Temperature Screening Service</u>	All functions contained in the service.
<u>Access and Attendance Service</u>	All functions contained in the service.
<u>Alarm Receiving Center (ARC) Service</u>	All functions contained in the service.
Employee Account Add-On	All functions contained in the service.

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	<ul style="list-style-type: none"> • <u>Register an Installer Admin Account</u> • <u>Manage Company Information</u> • <u>Set Account Information</u>
Site Management	<ul style="list-style-type: none"> • <u>Add New Site</u> • <u>Add Existing Site</u> • <u>Invite Site Owner</u> • <u>Apply for Site Authorization from Site Owner</u>
Device Management	<ul style="list-style-type: none"> • Add Device <ul style="list-style-type: none"> ◦ <u>Add Detected Online Device</u> ◦ <u>Add Device by Hik-Connect (P2P)</u> ◦ <u>Add Devices by IP Address or Domain Name</u> ◦ <u>Add Devices in a Batch</u> • <u>Apply for Device Permission</u> • <u>Release the Permission for Devices</u> • <u>Migrate Devices from Hik-Connect Account</u> • <u>Enable Device to Send Notifications</u> • <u>Upgrade Device Firmware</u> • <u>Configure DDNS for Devices</u> • Manage AX Pro Security Control Panel <ul style="list-style-type: none"> ◦ <u>Control AX Pro</u> ◦ <u>Configure AX Pro</u> ◦ <u>Batch Arm/Disarm AX Pro</u> • <u>Remote Configuration</u> • <u>Reset Device Password</u> • <u>Unbind a Device from Its Current Account</u>
Video	<ul style="list-style-type: none"> • <u>View Live Video</u> • <u>Play Back Video Footage</u>
Log	<u>Search Operation Log</u>
Tool	<u>Tools</u>

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

Installer Admin

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

Installer

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

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

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



Figure 2-1 Flow Chart of Account Management

- **Register an Installer Admin Account:** The surveillance installation company should first register an Installer Admin account before accessing any functions of Hik-ProConnect. For details, refer to **Register an Installer Admin Account**.

Note

If entering authentication code is required when you register Installer Admin account, you need to complete your company information after log in to the account. For details, see **Manage Company Information**.

For some countries and regions, entering authentication code is not required in registration.

- **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-ProConnect.

Steps



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

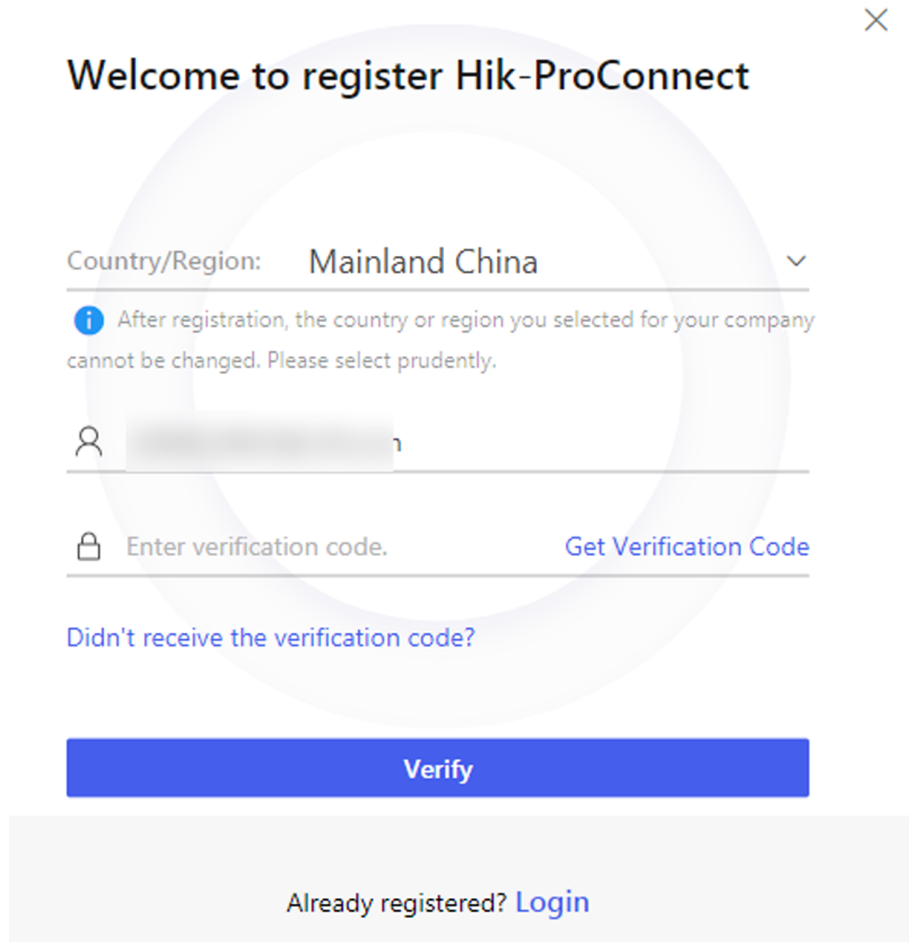
1. In the address bar of the web browser, enter <https://www.hik-proconnect.com> .

The Login page of Hik-ProConnect will show.

2. In the Login page, enter the email account, and then click **Login/Register**.



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



Welcome to register Hik-ProConnect

Country/Region: Mainland China

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

Enter verification code. [Get Verification Code](#)

[Didn't receive the verification code?](#)

Verify

Already registered? [Login](#)

Figure 2-2 Register an Installer Admin Account

3. Click **Verify to verify the account.**

Note

- If you don't enter the verification code within the required time, click **Get Again** to get the verification code again.
- If you fail to get the verification code, click **Didn't receive the verification code?** for failure reasons.

4. Create a password for your account.

Note

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

5. Enter other required information such as your phone number, company name, address, and city.

- 6. Optional:** Enter the authentication code which is used for authenticating that you are a professional installer.



Note

- The authentication code should contain 10 digits. Follow the instruction on the interface to get the authentication code.
- If the authentication code is optional (based on the country/region where you locate), you can leave it empty and authenticate your Installer Admin account later. For details about authenticating your account, refer to **Authenticate Account** .

-
- 7. Optional:** Check **I would like to receive newsletters about new product introduction, service introduction, and questionnaires from Hikvision. I understand that at any time I can unsubscribe.** to subscribe.

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

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

- 9.** Click **Enter Hik-ProConnect** to finish registration and log into Hik-ProConnect.



Note

When logging into Hik-ProConnect, you need to select your identity. If your identity is **End User** or **IT Operation Personnel**, it is recommended that you download and use the Hik-Connect Mobile Client.

What to do next

After registering an Installer Admin account and logging into Hik-ProConnect with this account, you need to complete the information of your company. For details, refer to **Manage Company Information** .

2.2 Manage Company Information

If you have not entered an authentication code when registering the Installer Admin account, you can manage and edit your company information.

Steps

Note

- If you have entered an authentication code when registering an Installer Admin account, you need to submit your company information (such as company name and address) immediately, and the company information cannot be edited once submitted.
 - You can link your Installer Admin account to a distributor via the Hik-ProConnect Mobile Client to get support and help from the distributor. For details, see *Hik-ProConnect Mobile Client User Manual*.
-

1. Go to **Company** → **Company Information** .
 2. Enter the name of your company.
 3. Enter other information of your company, such as postal code, phone number, email, and user type.
-

Note

The country or region cannot be changed after you save the company information.

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.
-

2.3 Authenticate Account

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

Note

You can skip this section if you have already entered the authentication code when registering an Installer Admin account.

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 the Hikvision or distributor first and then enter the authentication code to authenticate your account.

1. Enter **Company** → **Company Information** page, and click **Authenticate Now** to enter account authentication page.
2. (Optional) If you have no authentication code, click **Get Authentication Code**, and 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 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 distributor by your own email box.
-
3. After you get the authentication code, enter the authentication code on 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.

1. Enter **Company** → **Company Information** page, and click **Authenticate Now** to enter account authentication page.
2. (Optional) Edit the company information, such as company name, address, and city if needed.
3. Select your identity type from the drop-down list.
4. Enter the VAT Number of your company.
5. (Optional) Click **+** to upload the picture of your business card.
6. Enter the distributor if you have bought Hikvision products.
7. Click **Authenticate Now**. The application information will be sent. After your application is approved, you will complete the account authentication.

2.4 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 him/her. Or you can give a predefined role to an employee without creating one. An employee can have only one role.

Steps

Note

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

1. Click **Company → Role and Permission** to display all the roles.

2. Add a role.

- 1) On the Home page, click **Company → Role and Permission → 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, inviting site owner, applying for site authorization, searching sites, managing devices in the site (adding, deleting, editing, upgrading), applying for device permission, and health monitoring. No more than 18 employees can be assigned with this permission.

Manage Assigned Site

Managing site(s) assigned to the employee, including editing site, inviting site owner, 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.

2.5 Invite Employee

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

Steps



Note

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

1. Open the Add Employee panel.

- On the Home page, click **Company → Employee → Add Employee**.
- On the Home page, click **Company → Role and Permission → Add Employee** in the Operation column.

2. **Optional:** Click **Add Role** to create a new role.



Note

See **Manage Role and Permission** for details about role.

3. Enter the email of the to-be-invited employee.

4. Select a role for the employee. See **Manage Role and Permission** for details about managing a role.

The permissions of the role will be displayed.

5. 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.

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

2.6 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-ProConnect.
2. Click the button or the link in the email to open the Installer Registration page.
3. In the registration page, set the password of your account and confirm the password.



Note

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

-
4. Enter the employee's name and phone number.
 5. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in these agreements.
 6. Click **Register**.

Result

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

2.7 Set Account Information

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

On the Home page, click the name at the upper-right corner and select **Account Settings**.

Set Basic Information

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

Click  to set the profile of the current account.

Change Password


Change the password of the current account.



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 .
2. Enter a new email address in the **New Email** field.
3. Click **Get Verification Code**.
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.



- 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) under the current account, you cannot delete it.
-

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.

Chapter 3 Login

After login 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-proconnect.com>** .

The login page of Hik-ProConnect will show.

2. Select a country or region where the account locates from the drop-down list below the Hik-ProConnect logo.
3. Enter the registered email and password.
4. **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.

5. Click **Login**.



Note

- For a newly registered user or a user who has registered an account before, if you have entered authentication code on the registration page, you should complete company authentication information when logging in to the platform, including occupation, detailed company address (including street, state/province/region, and city), and company phone number.
 - If you have registered an account before and did not enter the authentication code on the register page, you should enter the company name to complete company authentication information when logging in to the platform.
-

By default, you will enter the site list page.

Chapter 4 Hik-ProConnect Portal Overview

Hik-ProConnect Portal is a B/S portal of Hik-ProConnect platform. The surveillance installation company can register an Installer Admin account on Hik-ProConnect, 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-ProConnect via the web browser and the Home page of Hik-ProConnect Portal will show.

Main Modules

The Hik-ProConnect Portal is divided into several main modules. You can access these modules via the navigation panel on the left.



Note



You can click  or  to pin or unpin the navigation panel on the left of the Portal.

Table 4-1 Main Modules of Hik-ProConnect Portal

Module	Description
Home	On the Home page, you can view the overview of your Sites, managed devices, received exceptions, and other quick entries such as frequently used functions, recently visited Sites, wizard, documentations, etc.
Batch Configure Device	Including batch activating devices, batch adding channels to NVR or DVR, and batch setting device parameters. For details, refer to <u>Batch Configure Devices on LAN</u> .
Site	A Site represents a physical location where devices are installed and through which the Installer Admin/Installer can manage the devices.
Health Monitoring	There are two parts in the Health Monitoring module: <ul style="list-style-type: none">• Health Status: 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.
Company	The Company module deals with all the management and administration aspects of a single installation company. It contains the following five parts:

Hik-ProConnect Portal User Manual

Module	Description
	<ul style="list-style-type: none"> • Company Information: You can manage your company information. • Co-Branding: Enable to display the company logo on the Hik-Connect Mobile Client for brand promotion to the end users. • 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. • 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. • Operation Log: View the operation logs of your accounts and Sites in the current company.
Business	<ul style="list-style-type: none"> • Service Market: Hik-ProConnect provides value-added services and you purchase these service packages or renew them. • 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.
Tools	Hik-ProConnect provides some online tools to improve your work efficiency.
Tutorial Center	View video tutorials to learn more about Hik-ProConnect.

Home Page Introduction

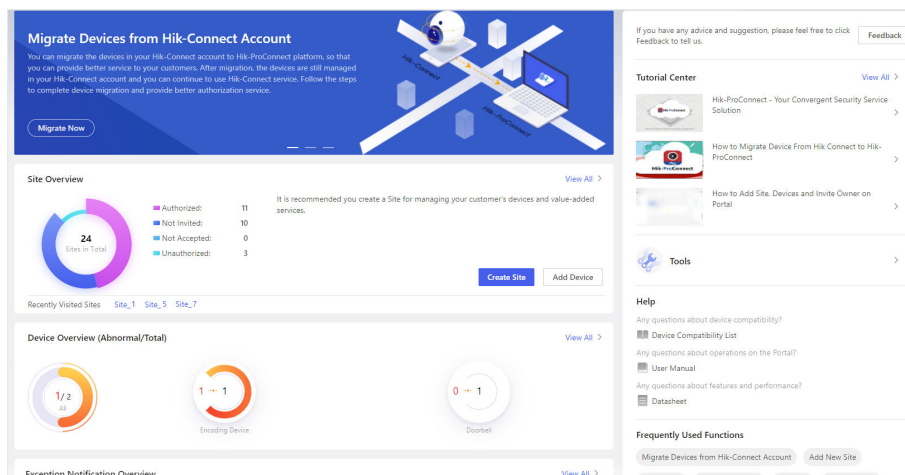







Figure 4-1 Home Page

Table 4-2 Home Page Description


Name	Introduction
Banner	<p>There are some banners, showing the key features, functions, and important information of Hik-ProConnect.</p> <p> Note</p> <p>You can inform your end users to download or update the Hik-Connect Mobile Client (V 4.15.0 or later) by sending the QR code or download link to them.</p>
Site Overview	<p>You can view the total number of Sites and the corresponding number of Sites in different status which include:</p> <ul style="list-style-type: none"> • Authorized: The number of Sites which are authorized to Installers. • Not Invited: The number of Sites for which no Site owners are invited. • Not Accepted: The number of Sites of which the Site owners' invitations are not accepted. • Unauthorized: The number of Sites which have handed over to customers (i.e., the end users) but not get authorization from customers. <p> Note</p> <p>You can click View All to enter Site list page and view all the added Sites in details. For more about Site management, refer to <u>Site Management</u> .</p> <p>You can view the five Recently Visited Sites. Click a Site name to enter Site details page.</p> <p>You can click Create Site to add a new Site. For details, refer to <u>Add New Site</u> .</p> <p>You can click Add Device to add a device. For details, refer to <u>Add Device</u> .</p>
Exception Notification Overview	<p>You can view the number of received exceptions and the proportions of each type of the exceptions.</p> <p>Hover the cursor to the pie chart to view the detailed proportions and amount.</p>

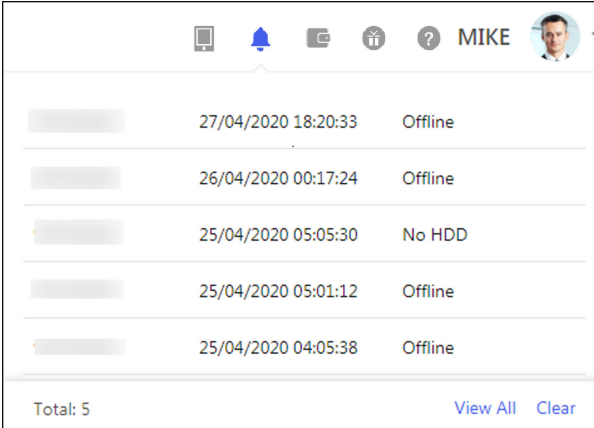
Name	Introduction
	 Note <ul style="list-style-type: none"> To receive exception notifications, you need to configure the recipient when setting the exception rule. For details, refer to Add Exception Rule. The number of exceptions you view here may not be the same as that in Exception Center. You can click View All to enter Exception Center to check the received exceptions. For detailed instructions about Exception Center, refer to Exception Center.
Device Overview	<p>You can view the number of abnormal devices and total devices, including devices overall and each device type respectively.</p>  Note <p>You can click > to enter Health Status to check the device health status details. For detailed instructions about Health Status, refer to View Status of Devices in All Sites and View Status of Devices in a Specific Site.</p>
More Value-Added Services	<p>You can set related service (such as cloud storage service and temperature screening) for devices after adding them to Sites.</p> <p>Click Set on the upper right side, and select a Site in the list to enter the Site details page.</p>
Tutorial Center	<p>You can view video tutorials to learn more about Hik-ProConnect and the proper ways of using the platform.</p> <p>Click a video to open a webpage and start playing the video. Click View All to view all the videos in Tutorial Center.</p>
Tools	<p>You can use some online tools to improve your work efficiency.</p> <p>Click Tools to view all the provided tools.</p>
Frequently Used Functions	<p>You can view the functions which you have used frequently.</p> <p>Click these icons to perform these functions quickly if needed.</p>

Download Hik-ProConnect Mobile Client

On the Home page, click  at the upper-right corner and scan the QR code to download Hik-ProConnect Mobile Client.

View Recently Received Exceptions

When the Portal receives a notification of exception, a window will pop up at the upper-right corner, showing the exception details. You can click  (the number indicates the number of unread messages) at the upper-right corner to view the exception received by the Portal recently.



Device ID	Timestamp	Status
[REDACTED]	27/04/2020 18:20:33	Offline
[REDACTED]	26/04/2020 00:17:24	Offline
[REDACTED]	25/04/2020 05:05:30	No HDD
[REDACTED]	25/04/2020 05:01:12	Offline
[REDACTED]	25/04/2020 04:05:38	Offline


Total: 5 [View All](#) [Clear](#)

Figure 4-2 Recently Received Exceptions


You can click **Clear** to clear the records displayed in this window. You can still check these exceptions in Exception Center.

Click **View All** to enter the Exception Center to view all the exceptions received by the Portal. For details, refer to [Exception Center](#).

Business

On the Home page, click  at the upper-right corner and select **Service Package** or **Order** to view the service details and the orders of your account.

Trial Period

On the Home page, click  at the upper-right corner to view the trial period of your account.




Note

You have the free trial for all features before one specific date. After that, you need to purchase some features if needed.

Submit Feedback

If you have any questions or suggestions about the system, you can submit feedback to us. There are three methods to access the Feedback window:


- Click your user name at the upper-right corner of the Home page, and select **Feedback**.
- Click **Feedback** on the right side of the Home page.
- Click  floating on the Home page.

Select a type for your feedback and then enter your suggestions and questions 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 an conclusion.

Click **Submit** to submit your feedback to us.


Subscribe to/Unsubscribe from Newsletters

For Installer Admin, if you didn't subscribe to newsletters when account registration, you can click the name at the upper-right corner and select **Subscribe to Newsletters**, or click  icon floating on the Home page to subscribe to the newsletters about Hik-ProConnect. After subscription, we will send emails about latest product introduction, service introduction, questionnaires and special offers, to the email address which is used for your account registration. You can unsubscribe at any time in the **About** page. After unsubscription, you will not receive any newsletters emails from us.

About



On the Home page, click the name at the upper-right corner and select **About**. You can view the version of the current system, and read the agreements, including terms of service, privacy policy, and open source license. After subscribing to the newsletters, you can unsubscribe here at any time. After unsubscription, you will not receive any newsletter emails from us.

View User Manual, Datasheet or Device Compatibility List

On the Home page, click  near the name at the upper-right corner and click **User Manual** to open the user manual of the Hik-ProConnect Portal. You can also click **User Manual**, or **Datasheet**, or **Device Compatibility List** at the lower-right corner of the Home page to open the user manual, or datasheet,, or device compatibility list. You can enter keywords to search the information you want in the user manual, or datasheet, or device compatibility list for instructions, specification details, or device model.

Wizard

We provide you a wizard which guides you through the process of configurations and operations. There are two ways to open the wizard:

- On the Home page, click  near the name at the upper-right corner and click **Wizard**.
- Or click  icon floating on the Home page.

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.

Logout

On the Home page, click the name at the upper-right corner and select **Log Out** to log out of the current account and return to the login page.

Chapter 5 Site Management

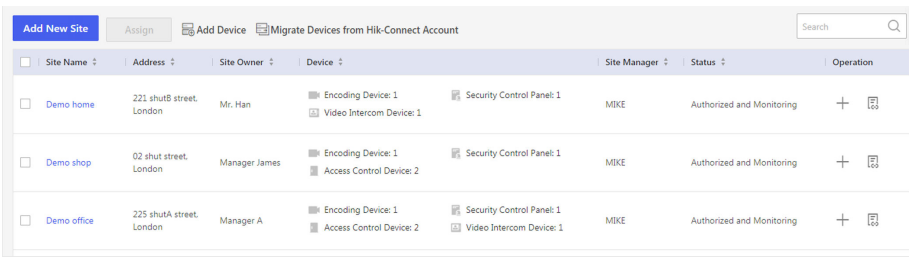
A site can be regarded as an area or location with actual time zone and address, such as the end user's home, office, etc. The Installer can add the authorized devices of end user to the site and uses the site to manage and configure the devices remotely.

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

5.1 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, inviting site owner, assigning site, migrating devices from Hik-Connect Account, etc.

Click **Site** tab to enter Site page.



Site Name	Address	Site Owner	Device	Site Manager	Status	Operation
<input type="checkbox"/> Demo home	221 shutB street, London	Mr. Han	Encoding Device: 1 Video Intercom Device: 1	Security Control Panel: 1 MIKE	Authorized and Monitoring	+
<input type="checkbox"/> Demo shop	02 shut street, London	Manager James	Encoding Device: 1 Access Control Device: 2	Security Control Panel: 1 MIKE	Authorized and Monitoring	+
<input type="checkbox"/> Demo office	225 shutA street, London	Manager A	Encoding Device: 1 Access Control Device: 2 Video Intercom Device: 1	Security Control Panel: 1 MIKE	Authorized and Monitoring	+

Figure 5-1 Site Page

There are different status for the sites in site list.

Not Invited

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

Not Registered

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

Not Accepted

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

Invited, Not Authorized

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

Authorized and Monitoring

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

Note

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

Table 5-1 Supported Operations in Different Status

Supported Operations	Not Invited	Not Accepted Not Registered	Invited, Not Authorized	Authorized and Monitoring
Search Site	√	√	√	√
Assign Site	√	√	√	√
Invite Site Owner	√	√	×	×
Manage Device	√	√	×	√
Edit Site	√	√	×	√
Delete Site	√	√	√	√
Apply for Authorization	×	×	√	×

Note

- See **Add Device** for details about add devices to the site.
 - See **Migrate Devices from Hik-Connect Account** for details about how to migrate devices from Hik-Connect account to Hik-ProConnect.
-

5.2 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 new Site.

Steps

1. Click **Site** tab on Home page to enter Site page.
 2. Click **Add New Site** and select **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

- 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. Click **OK** to add a new Site to the list.

6. **Optional:** According to the Site's status and authorization, perform one of the following operations.



Note

For more details about supported operations in different Site status, refer to [Site Page 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 right area on Site Details page, click to edit the Site name, Site address, city, state/province/region, and whether check Sync Time & Time Zone to Device or not.
Delete Site	Hover the cursor over ... on Operation column and click to delete the Site.
Invite Site Owner	For the Site in the status of Not Invited , click on Operation column on Site page or click Invite on Site Details page to invite an end user as the owner of the Site.



Note

For more details, refer to [Invite Site Owner](#).

Manage Device	For the Site in the status of Not Invited , Not Registered , Not 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, applying for live view or configuration permission, adding linkage rule, adding exception rule, etc.
----------------------	---



Note

For more details, refer to [Device Management](#).

5.3 Add Existing Site

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

Steps

1. Click **Site** tab on Home page to enter Site page.
2. Click **Add New Site** and select **Existing Site**.

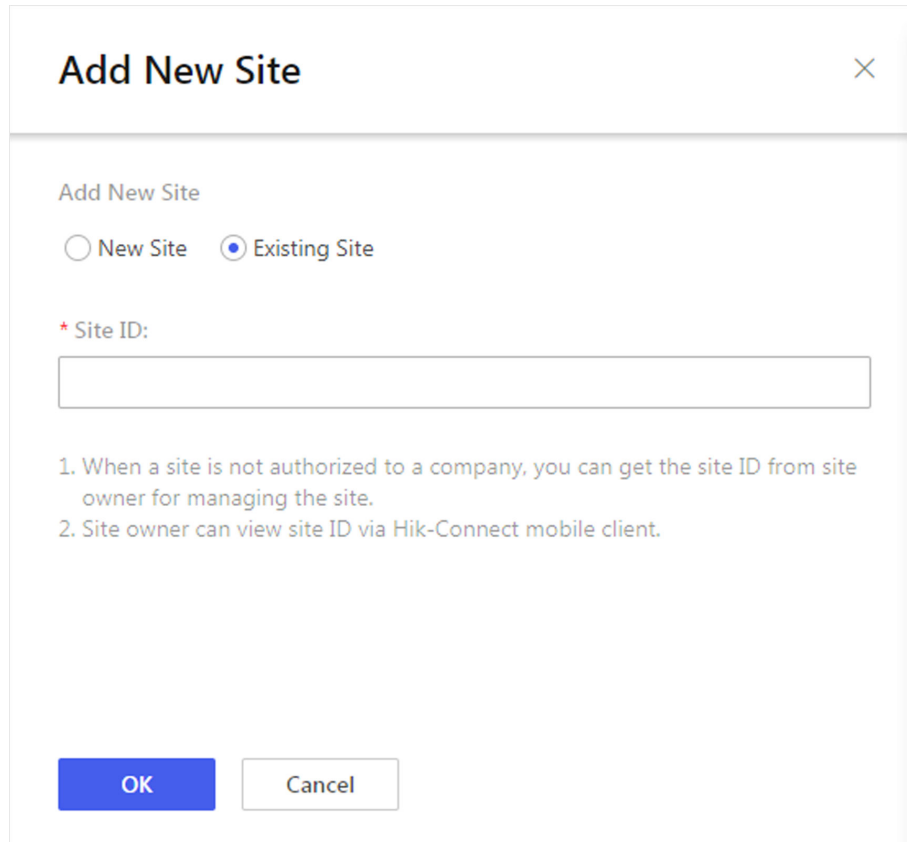


Figure 5-2 Add Existing Site

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. 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.

5.4 Assign Site to Installer

The Installer Admin or the Installers with assigning site permission can assign a site to the specified Installer as site manager responsible for configurations of the devices in the site.

Before You Start

Make sure you have the permission of assigning site.

Steps

1. Click **Site** tab on Home page to enter Site page.
2. Select a site for assignment.
3. Click **Assign**.
4. Select an Installer as site manager.
5. Click **OK**.

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


5.5 Invite Site Owner

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

Before You Start


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

Steps

1. Click **Site** tab on Home page to enter Site page.
2. Select a Site for invitation.
3. Enter Invite Site Owner page.
 - Select a Site and click  on Operation column.
 - Click the Site name to enter Site Details page and click **Invite**.
4. **Optional:** Check **Allow Me to Disable Hik-Connect Service**.

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

Note

You can go to the **Device** tab to disable Hik-Connect service for one device or all devices in this Site by clicking  or setting **Hik-Connect Service** switch to off. You can also delete the devices from the your customer's Hik-Connect account without her/his authorization.

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

Note

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

Site Information Management

The authorization for the permission of managing Site information.

Configuration

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

Live View

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

Playback

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

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

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

Note

- If the Access & Attendance system provided by Hikvision has been added to the Site and activated, the check-box will appear on the Invite Site Owner page.
 - If the Access & Attendance service is provided by a third-party manufacturer, the check-box will be **Allow ### System to Access** or **Allow Third-Party Access & Attendance System to Access**. ### here refers to the name of the third-party manufacturer.
-
9. Enter the remarks, such as the reason of the invitation, which the invitee can view when he/she receives the invitation via Hik-Connect Mobile Client.
 10. Click **OK** to send the invitation.
-

- The invitee will receive the invitation email or message in email box or via short message with a download link of Hik-Connect Mobile Client. The invitee can download or open Hik-Connect Mobile Client via the link.
- If the invitee has not registered a Hik-Connect account, he/she needs to register a Hik-Connect account first. After registering the account and accepting the invitation via Hik-Connect Mobile Client, the end user will become the Site Owner.

Note

Please inform your end users to download or update the Hik-Connect Mobile Client (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 Hik-Connect Mobile Client, but not added and managed in the Site, after the end user accepts the invitation and becomes the Site Owner, he/she can authorize the permissions about these devices to the Installer.

11. Optional: Before the your customer accepts the invitation, click **Invite Again** to send invitation again.


Note

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

5.6 Apply for Site Authorization from Site Owner

When the Site (no permission selected when inviting Site Owner) has been handed over to Site Owner, and then there are maintenance requirements for the devices in the Site, the Installer needs to send an application to Site Owner for the authorization. After the authorization is approved, the Installer can get the permission to manage and configure the devices of the Site. Besides, 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. Click **Site** on Home page to enter Site page.
2. Select a Site.
3. 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**.
4. 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-ProConnect, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; these accounts will be deleted after the Installer deletes the AX Pro from Hik-ProConnect. If you edit an Installer's login password, the password for logging in to the AX Pro by this account will also change.
- After authorizing a Site with AX Pro to an Installer, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; besides, the account with the permission of managing all Sites will also become the account of the AX Pro.
- If an Installer hands over the Site with this AX Pro to an end user, the end user's Hik-Connect account will also become an account of the AX Pro, while the Installer's account will be deleted from the AX Pro. This is also applicable to an Installer Admin.
- For more details about operations on Hik-Connect Mobile Client, refer to the User Manual of Hik-Connect Mobile Client.

5. 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-ProConnect Service function enabled when handing over to Installer, discarding authorization is not supported.

Chapter 6 Device Management

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



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

6.1 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-ProConnect 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.



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

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

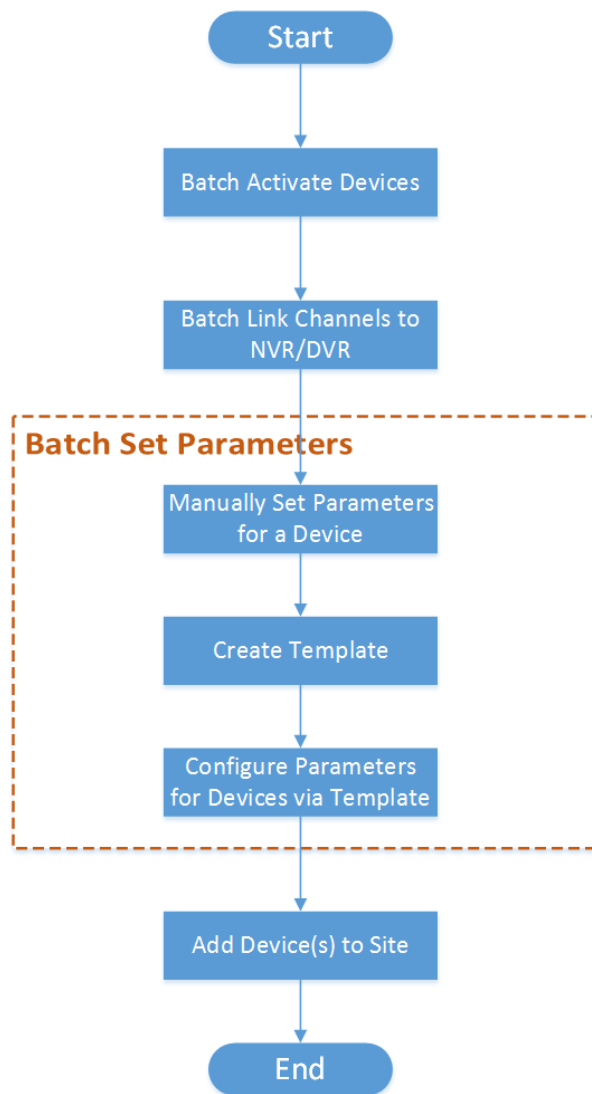


Figure 6-1 Flow Chart

Table 6-1 Flow Chart Description

Step	Sub-step	Description
Batch Activate Devices	N/A	Batch activate online devices on the same Local Area Network (LAN) with the PC on which the Hik-ProConnect Portal runs, and assign IP addresses for the activated devices. See <u>Batch Activate Devices and Assign IP Addresses for Them</u> 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 <u>Batch Link Channels to NVR</u> for details.

Step	Sub-step	Description
Batch Set Device Parameters	Manually Set Parameters for a Device	Select an activated device and set its parameters manually. See 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.


6.1.1 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  **Batch Device Configuration** to enter the batch device configuration page.

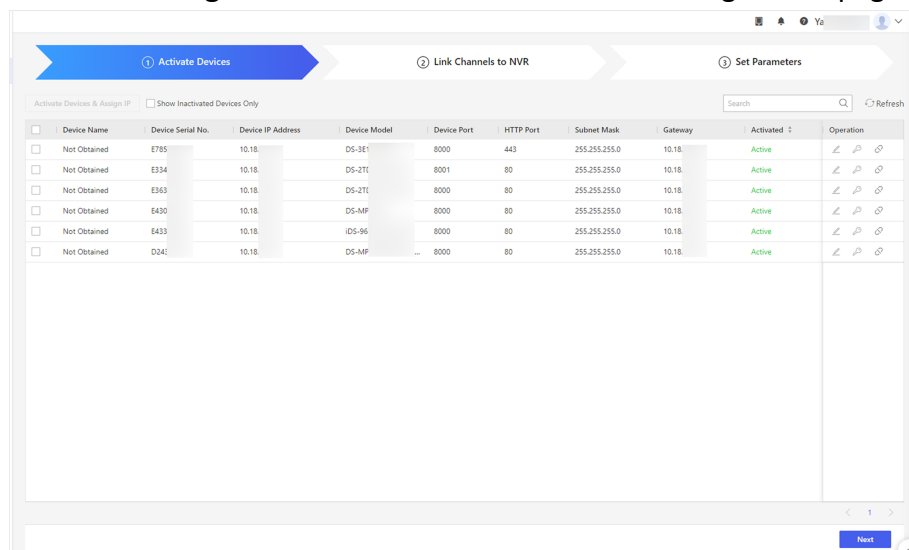


Figure 6-2 Batch Device Configuration

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 as required.

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. For details, refer to [**Batch Link Channels to NVR**](#).

6.1.2 Batch Link Channels to NVR

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

Before You Start

Make sure you have activated the NVR and network cameras. See [**Batch Activate Devices and Assign IP Addresses for Them**](#) for details.

Steps



Note

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

1. On the Link Channel page, select an NVR 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.

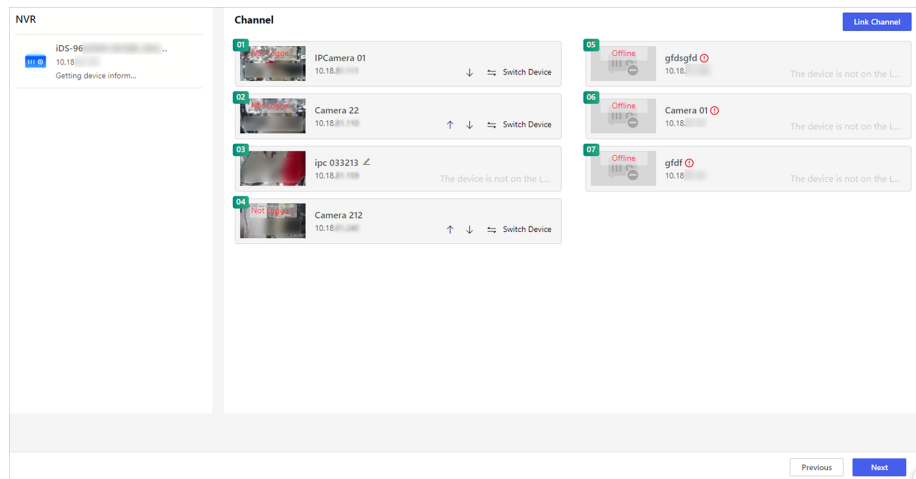



Figure 6-3 Channels on the Same LAN

 **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.

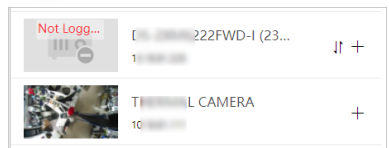






Figure 6-4 Available Channels

5. Click **+** to link the device.

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

- | | |
|------------------------------|--|
| Edit NVR/Channel Name | Click  to edit the NVR/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.

6.1.3 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 other devices.

Before You Start

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

Steps

1. 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**.

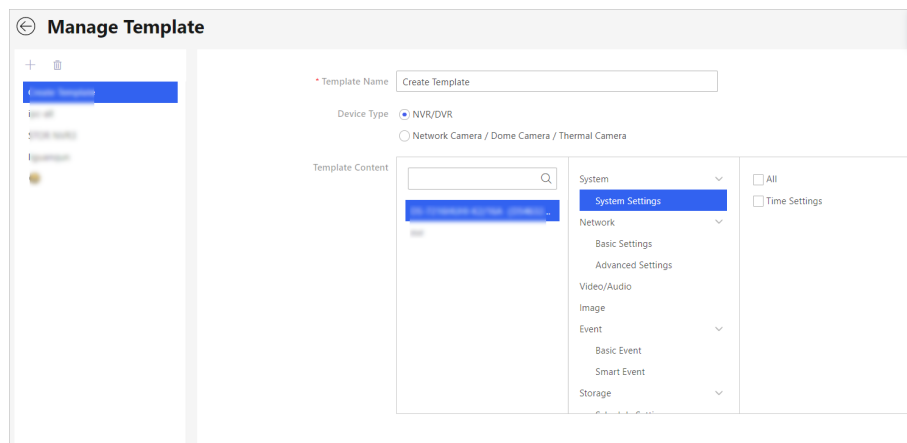



Figure 6-5 Add Template

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

6.1.4 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**.
- 2. Select a template.

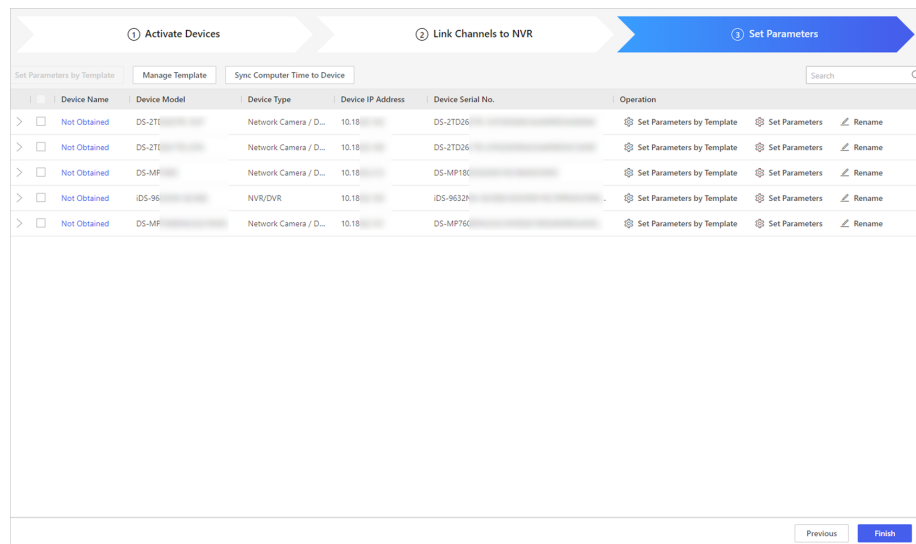


Figure 6-6 Set Parameters

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

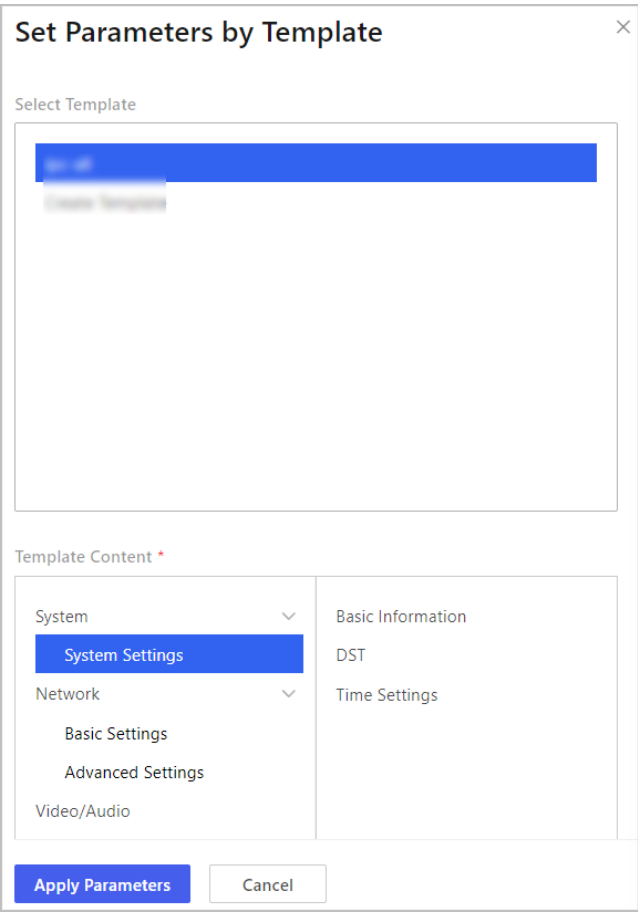


Figure 6-7 Set Parameters by Template

The application process and application results will be displayed.

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

Add Device to Site	Add devices to Sites. See <i>Add Device</i> for details.
Manage Template	Click Manage Template to add new template or delete template. See <i>Create Template for Setting Parameters</i> 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 .


6.2 Add Device

Hik-ProConnect accesses devices by two modes: Hik-Connect (P2P) and Device IP Address/Domain Name. The former provides securer data communication (between Hik-ProConnect 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 6-2 Device Adding Methods

Access Mode	Device Adding Method
Hik-Connect (P2P)	<ul style="list-style-type: none">• <u>Add Detected Online Device</u>• <u>Add Device by Hik-Connect (P2P)</u>• <u>Add Devices Without Support for the Hik-Connect Service</u> <div> 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.</div>
Device IP Address/Domain Name	<ul style="list-style-type: none">• <u>Add Devices by IP Address or Domain Name</u>• <u>Add Devices in a Batch</u>

6.2.1 Add Device(s) after Batch Configuring Them

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

Perform one of the following two ways to enter the Add Device page.

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

 **Note**

For details about batch configuration devices, refer to **Batch Configure Devices on LAN**

- In the Home page, click **Add Device**.

Select **Online Device**, **Hik-Connect (P2P)**, **IP/Domain** or **Batch Import** 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, store, etc.

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 in the page. For more details, refer to [**Add Device**](#).

6.2.2 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.
-


Click **Site** on the left to show the site list. And then enter the Online Device page in one of the following two ways before adding online devices.

- Click **+** in the Operation column of the site list and then select **Online Device**.
- Click the site name to enter the site details page, and then go to **Device → Add Device → Online Device**.

The device(s) connected to the same LAN with the Portal will be displayed on the device list on the Online Device page. 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 **Add**. Perform part or all of the following 4 steps based on the status of the selected devices before you can add them.

Table 6-3 Step Description








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


 **Note**

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

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

Table 6-4 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 <ul style="list-style-type: none">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 is not supported if the site is authorized.
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 configuration) are unavailable if the device is not compatible with the Hik-ProConnect. For devices incompatible with the Hik-ProConnect, you need to upgrade them. <ol style="list-style-type: none">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-ProConnect cannot recognize a device's type after you add it, you can manually set a device type for it. Click Set Device

Operation	Description
	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 <u>Unbind a Device from Its Current Account</u> .

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-ProConnect, 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 successfully, 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.
-



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


6.2.3 Add Device by Hik-Connect (P2P)

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

Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers.
- Make sure the device has been activated and connected to Hik-Connect service.

Steps

1. Click **Site** on the left to show the site list.
 2. Open the Manual Adding page.
 - Click  in the Operation column of the site list and then select **Manual Adding**.
 - Click the site name to enter the site details page, and then go to **Device → Add Device → Manual Adding**.
 3. Select **Hik-Connect (P2P)** as the adding mode.
 4. Enter the device serial number and device verification code.
-



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-ProConnect will start detecting whether the device firmware version is compatible with the Hik-ProConnect. Some functions (including health monitoring, linkage, and remote configuration) cannot be used if the device is not compatible with the Hik-ProConnect. Firmware version detection will not happen if a site is authorized. For devices incompatible with the Hik-ProConnect, 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-ProConnect, you will be able to log into the AX Pro by your Hik-ProConnect account (i.e., Installer account or Installer Admin account) to configure and manage the device; if you delete the AX Pro device from Hik-ProConnect, you can no longer log into the AX Pro device by your Hik-ProConnect account.
 - After your customer authorizes a Site with AX Pro devices to you, you can log into these AX Pro devices by your Hik-ProConnect account to configure and manage the device. In this case, if you are an Installer, the Installer Admin can also log into these AX Pro devices by her/his Hik-ProConnect account; if you are the Installer Admin, your employees (i.e., Installers) have no permission to log into these devices by their Hik-ProConnect accounts.
 - After you hand over a Site with AX Pro devices to your customer, your customer will be able to log into these devices by her/his Hik-Connect account, and you will no longer have the permission to log into these devices by your Hik-ProConnect account.
8. **Optional:** Perform the following operations if required 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.


Upgrade Device	Refer to <u>Upgrade Device Firmware</u> .
Set Type for Unknown Device	If the Hik-ProConnect cannot recognize a device's type after you add it, you can manually set a device type for it. 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 Hik-ProConnect Box and cloud storage DVR, you can click **Cloud Storage Service** to configure Cloud Storage settings. See [Set Cloud Storage for Box](#) and [Set Cloud Storage for Cloud Storage DVR](#) for details.

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

Before You Start

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

Steps



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 Hik-Connect \(P2P\)](#).
 - 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. Click **Site** on the left to show the site list.

2. Open the Manual Adding page.

- Click + in the Operation column of the site list and then select **Manual Adding**.
- Click the site name to enter the site details page, and then go to **Device → Add Device → Manual Adding**.

3. Select **IP/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.

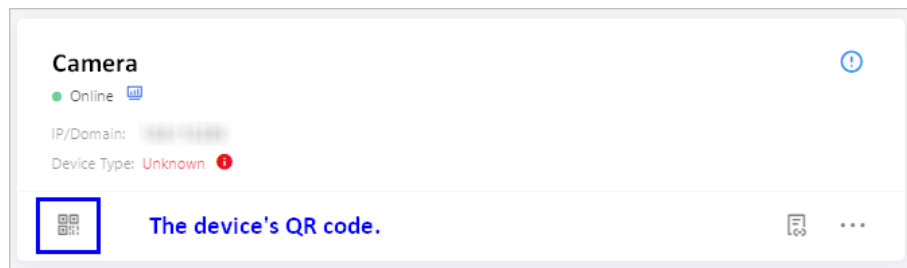






Figure 6-8 The QR Code of the Added Device

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

Operations	Description
Encrypt Device QR Code	<p>It is highly recommended that you encrypt the device QR code for security reasons.</p> <ol style="list-style-type: none"> 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	<p>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.</p> <p>Select a device, and click  →  to edit the device's name, IP address/domain name, port number, user name, and password.</p>
Set Type for Unknown Device	<p>If the Hik-ProConnect cannot recognize a device's type after you add it, you can manually set a device type for it. Click Set Device Type and select a device type from the drop-down list. You can edit it again after the selection.</p>

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.

6.2.5 Add Devices in a Batch

You can add multiple devices to the client in a batch 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 Hik-Connect \(P2P\)](#)**.
 - Only encoding devices mapped in WAN support this function.
-

1. Click **Site** on the left to show the site list.
2. Open the Manual Adding page.
 - Click  in the Operation column of the site list and then select **Manual Adding**.
 - Click the site name to enter the site details page, and then go to **Device** → **Add Device** → **Manual Adding**.
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-ProConnect.

7. Perform the following operations after adding the devices if you need.

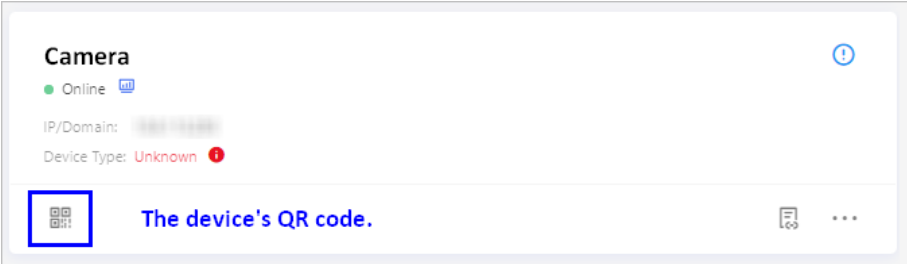













Figure 6-9 The QR Code of Added Device

Operations	Description
Encrypt Device QR Code	<p>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.</p> <p>a. Click  to display the QR code.</p> <p>b. Enter a password to encrypt the QR code, and then click Save.</p>
Activate Health Monitoring Service	<p>Hover the cursor onto  on the device card on the site details page, and then click Activate Service.</p> <hr/> <div> Note</div> <ul style="list-style-type: none">For details about how to activate the health monitoring service, see <i>Activate the Health Monitoring Service for Devices</i> .For details about Health Monitoring service, see <i>Health Monitoring Service</i> .
View and Edit Device Information	<p>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.</p> <p>Select a device, and click     to edit the device's name, IP address/domain name, port number, user name, and password.</p>
Set Type for Unknown Device	<p>If the Hik-ProConnect cannot recognize a device's type after you add it, you can manually set a device type for it. Click Set Device Type and select a device type from the drop-down list. You can edit it again after the selection.</p>
Delete Device	<p>Click     .</p>

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-ProConnect, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; these accounts will be deleted after the Installer deletes the AX Pro from Hik-ProConnect. If you edit an Installer's login password, the password for logging in to the AX Pro by this account will also change.
 - After authorizing a site with AX Pro to an Installer, the Installer and Installer Admin's accounts will become the accounts of the AX Pro; besides, the account with the permission of managing all sites will also become the account of the AX Pro.
 - If an Installer hands over the site with this AX Pro to an end user, the end user's Hik-Connect account will also become an account of the AX Pro, while the Installer's account will be deleted from the AX Pro. This is also applicable to an Installer Admin.
 - Deleting device is not supported if the site is authorized (except for devices added by IP/Domain).
-

6.2.6 Add Devices Without Support for the Hik-Connect Service

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

Before You Start

Make sure that you have added Hik-ProConnect Boxes to Hik-ProConnect. For details, see [**Add Device by Hik-Connect \(P2P\)**](#) 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-ProConnect Device Compatibility List*.
 - The proxied devices do not support features including ARC service, access & attendance service, temperature screening service, people counting service, and ISAPI alarm. For the proxied encoding device, in addition to the above-mentioned features, linkage rule is not supported as well.
-

1. In the left navigation, click **Site** to enter the site list page, and then click the name of a Site with Hik-ProConnect Boxes added.

You enter the site details page.

- 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.

Add Device

☒ Select Hik-ProConnect Box
 Devices will be added to: DS-6700
☒ Add To-Be-Proxied Devices
 Remaining Devices That Can Be Proxied: 14
☐ Enable Proxy for Channels
 Remaining Channels That Can Be Proxied: 1

The network condition determines whether you can connect an online device to the Hik-ProConnect Box.


Device Type	Device Model	Device Serial No.	Device IP Address	Device Port
<input type="checkbox"/> Encoding Device	DS-9600	66001	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-9620	D8123	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-9610	75380	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-9630	12352	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-7700	E0253	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-9620	E9418	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-9660	56792	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-7630	54218	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-7600	F5031	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-9600	A9877	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-9660	65033	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-7610	C7772	192.168.1.10	8000
<input type="checkbox"/> Encoding Device	DS-7610	P2015	192.168.1.10	8000
<input type="checkbox"/> Encoding Device	DS-9660	E5635	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-7600	P2015	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-9660	12352	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-7600	D6525	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-7200	F9762	10.15.10.10	8000
<input type="checkbox"/> Encoding Device	DS-7616N-12/16P	D46509948	10.15.98.75	8000

Figure 6-10 Add To-Be-Proxied Devices

- Add devices in one of the following two ways.

Table 6-5 Add Devices

Way	Description
Online Device	Add devices on the same LAN with the Portal. <ol style="list-style-type: none"> Select devices, and then click Next. 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. Click Next.
Manual Adding	Add a device manually. <ol style="list-style-type: none"> Click Add Device. In the Manual Adding window, select the target Site, and then enter the device IP address and device port No. Click OK and the device will be displayed in the device list. 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.

4. 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).
5. Click **Next**.
6. 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**.
7. Click **Complete**.
8. **Optional:** View the proxy information on the device details page of the Hik-ProConnect Box.

Related Information Add Device

6.3 Manage Device Permission

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

6.3.1 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).

6.3.2 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**.
-

6.4 Migrate Devices from Hik-Connect Account

You can migrate the devices in your Hik-Connect account to the Hik-ProConnect account. After migration, 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 migrate devices from Hik-Connect account to Hik-Connect.

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

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



Figure 6-11 Migrate Devices from Hik-Connect Account to Hik-ProConnect

There are three ways for you to open the Hik-Connect Device Migration window.

- On the Home page, click the name at the upper-right corner and select **Hik-Connect Device Migration**.
- On the Home page, click **Migrate Devices from Hik-Connect Account** in the **Frequently Used Functions**.
- On the Site page, click **Migrate Devices from Hik-Connect Account** on the top of the Site list.

Log into Hik-Connect Account

Firstly, you need to log into your Hik-Connect account.

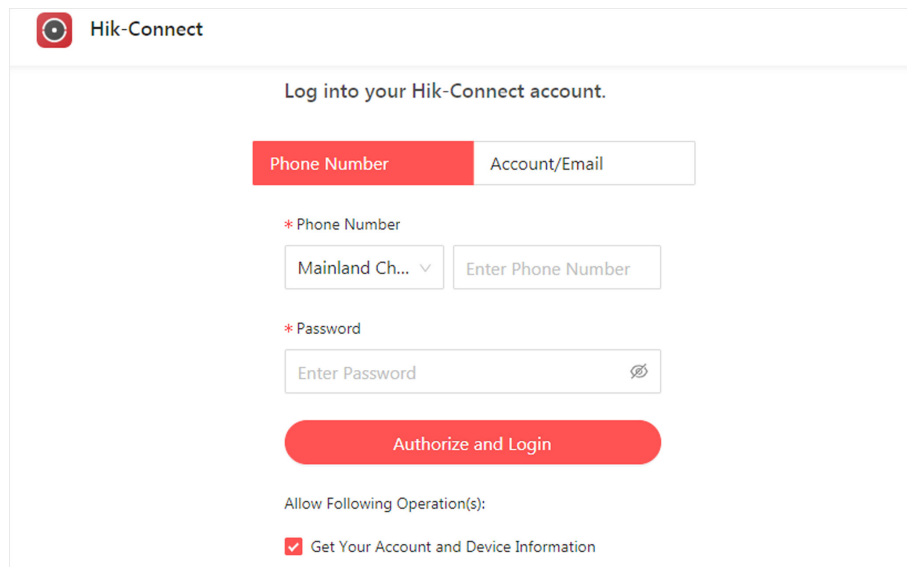


Figure 6-12 Log into Hik-Connect Account

Click **Log into Hik-Connect** to open the login page. You can log into your Hik-Connect account by phone number or user name (or email address).

Check **Get Your Account and Device Information** to allow Hik-ProConnect to get these information, and then click **Authorize and Login** to log into your Hik-Connect account.

Select Device for Migration

Secondly, you need to select the devices for migration.

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. The devices which have been added to Hik-ProConnect already will not be displayed here.

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 migrate to Hik-ProConnect, and click **Next**.

Configure Site for My Devices

Thirdly, you need to set the Site information in Hik-ProConnect for your devices to be migrated. 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.

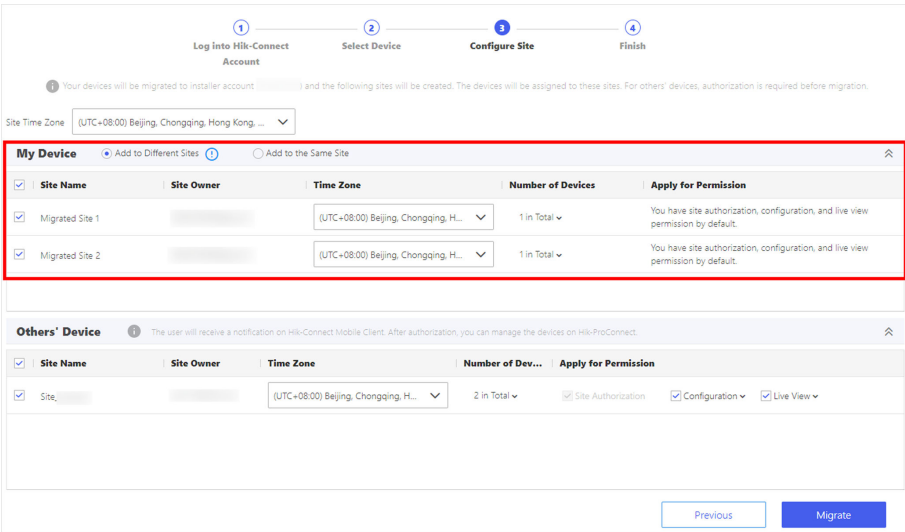


Figure 6-14 Configure Site for My Devices

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 migration, 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-ProConnect and set the device permission for the devices shared to you.

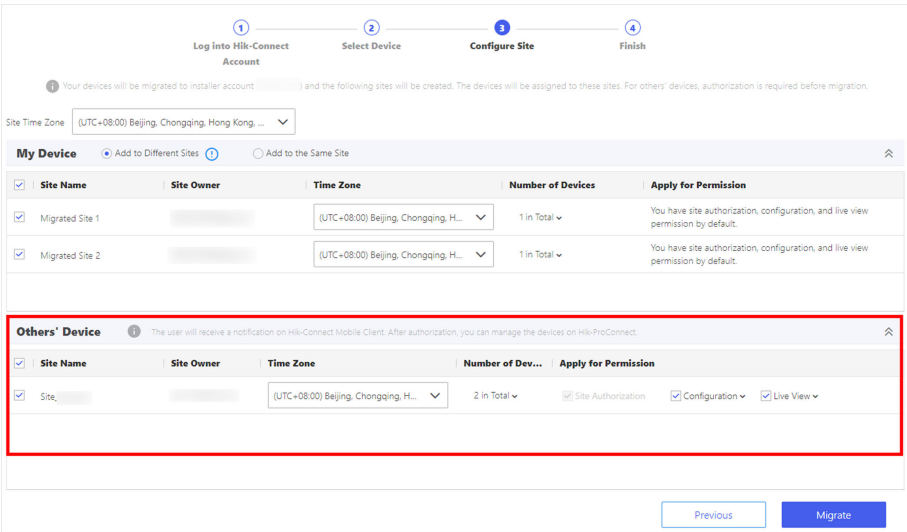


Figure 6-15 Configure Site and Permissions for Others' Devices

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 migration, the customers will receive a notification on Hik-Connect Mobile Client. After authorization by the customers, you can manage the devices on Hik-ProConnect.

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 Migration

Finally, start device migration. After setting the Sites and device permissions, select the devices in the My Devices and Others' Devices list, and click **Migrate** to start migration. 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 migrated successfully. Click **Continue** to select other devices for migration, or click **Finish and View** to view the devices migrated after creating Sites in the Site list.

6.5 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.

6.5.1 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 device A), Linked Resources (resource B, resource C, resource D...), Linkage Actions (actions of resource B, resource C, resource D...), and Linkage Schedule (the scheduled time during which the linkage is activated). The linkages can be used for purposes such as notifying security personnel, upgrading security level, and saving evidence, when specific events happen.

The picture below shows the process of the linkage.

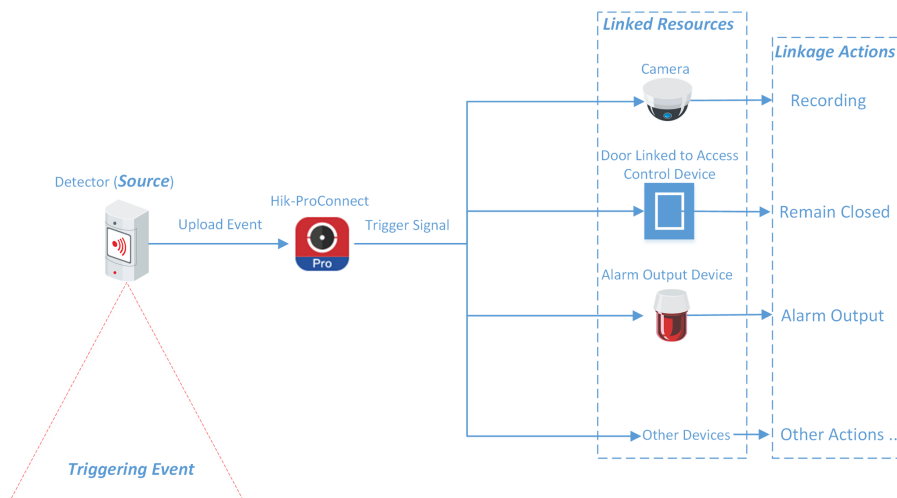


Figure 6-16 Linkage

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. Click  **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 6-6 Available Triggering Events for Different Resource Types

Resource	Triggering Event
Camera	<ul style="list-style-type: none">• Motion Detection• Face Detection• Intrusion• Line Crossing Detection
Access Control Device	<ul style="list-style-type: none">• Tampering Alarm
Door Linked to Access Control Device	<ul style="list-style-type: none">• Door Opened Abnormally• Tampering Alarm
Door Station	<ul style="list-style-type: none">• Calling
Area of Security Control Panel	<ul style="list-style-type: none">• Away Arming• Disarmed• Stay Arming• Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm.
Zone (Detector) Linked to Security Control Panel	<ul style="list-style-type: none">• Alarm, such as Triggering Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm.
Doorbell	<ul style="list-style-type: none">• Calling• PIR Detection

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 6-7 Linkage Action Description

Linked Resource	Linkage Action	Description
Camera (Channel)	Capture	The camera will capture a picture when the Triggering Event is detected.
	Recording	<p>The camera will record video footage when the Triggering Event is detected.</p> <p> Note</p> <p>The recorded video footage starts from 5 s before the detection of the Triggering Event, and lasts 30 s.</p>
	Call Preset	<p>Select a preset from the Preset drop-down list to specify it as the preset which will be called when the Triggering Event is detected.</p> <p>A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. By calling a preset, the PTZ camera will move to the predefined image position.</p> <p> Note</p> <p>Make sure you have configured presets for the PTZ camera. For details, see the user manual of the PTZ camera.</p>
	Call Patrol	<p>Select a patrol from the Patrol drop-down list to specify it as the patrol which will be called when the Triggering Event is detected.</p> <p>A patrol is a predefined PTZ movement path consisted of a series of key points (i.e., presets) that have their own designated sequence. By calling a patrol, the PTZ camera will travels to all the key points in set speed so as to provide a dynamic view.</p>

Linked Resource	Linkage Action	Description
		 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 to 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 to 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.




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***](#).



- 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 list below) of linkage rule.

Before You Start

Make sure you have the permission for the configuration of the devices. Or you need to apply for the permissions first. For details about applying for permission, see [***Apply for Device Permission***](#).

Table 6-8 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. Click  **Site** to enter the site list page.
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 hover the cursor onto the **Forced Entry Alarm** template in the Linkage Template section and click the appeared **Create by Template**.
 - 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, and click **External Linkage Rule** → **Add External Linkage Rule** and then select the **Forced Entry Alarm** template from the left side of the Add Linkage Rule panel.

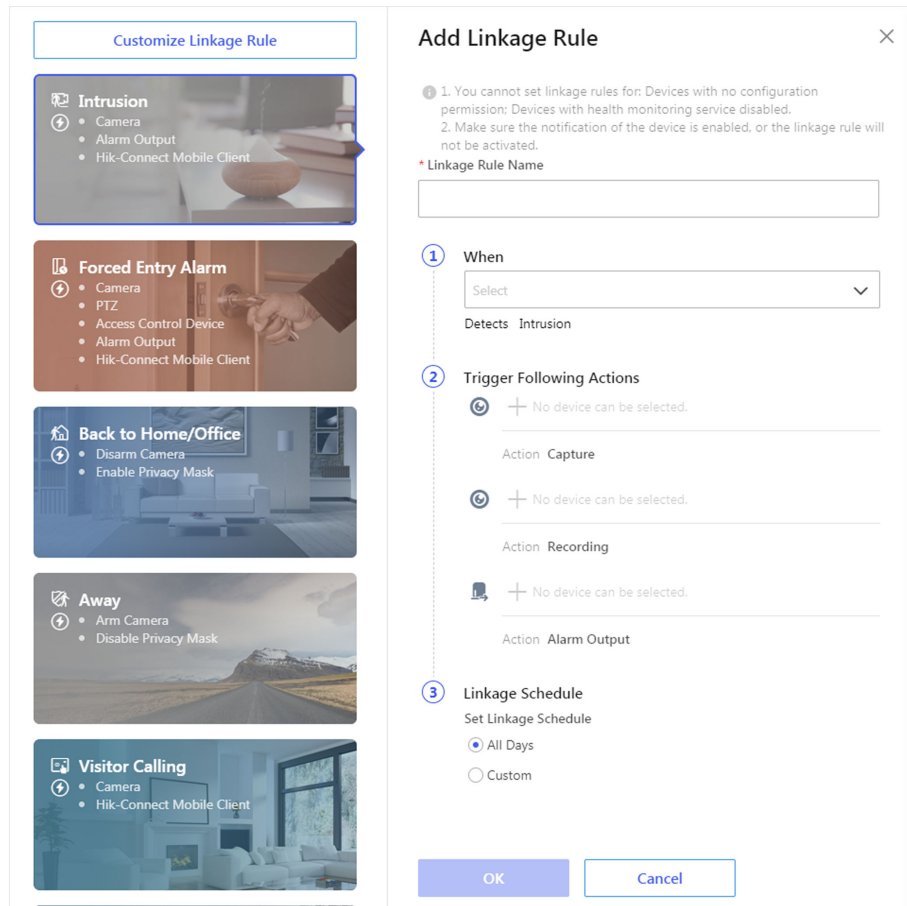


Figure 6-17 Add Linkage Rule by Template

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 6-7](#).

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.

6.5.2 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-ProConnect to notify the specified Installer about this exception. Currently, the exceptions include two types: device exceptions and channel exceptions.

Before You Start

- Make sure you have the permission for configuration of the device. 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

1. Enter **Site** module.
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 encoding devices, all the cameras will be displayed. 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 .

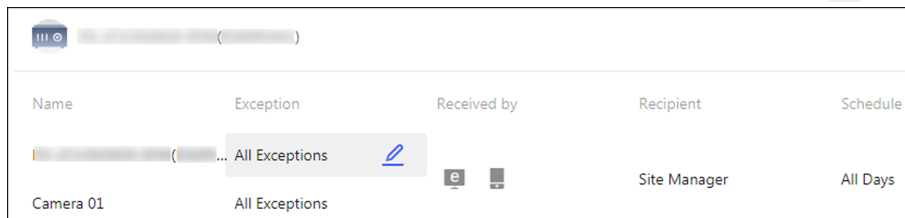


Figure 6-18 Edit Exception


- 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 how to receive the notification.

- 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** .

Mobile Client

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

Email

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

3) 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.

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 Days

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.

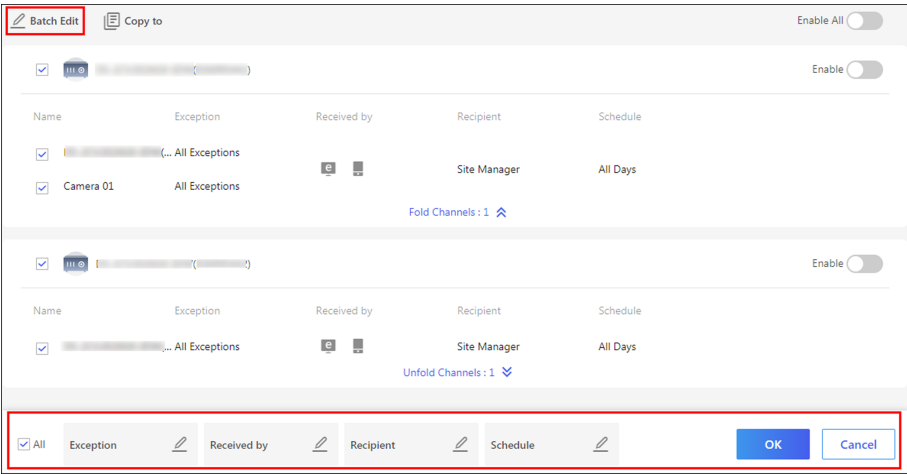


Figure 6-19 Batch Set/Edit Exception Rules

- 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 at the upper-right cornet 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.


6.5.3 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-ProConnect system and the Hik-Connect Mobile Client, which is the prerequisite to trigger the linkage actions and exception rules defined in the Source-device-related linkage rule(s) and exception rule(s) respectively.

Steps

Note

The device should support this functionality.

1. Click  **Site** to enter the site list page.
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.
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-ProConnect 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.
-

6.6 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 and resetting password onsite.



Note

- Resetting password via the Hik-ProConnect platform is not supported by every device type/model. For example, AX PRO does not support this function.
 - Make sure that the device is authorized by the Site Owner to you before resetting device password. For details, see **[Apply for Site Authorization from Site Owner](#)**.
-

Click **Site** and enter the site where the device locates.

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.

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.

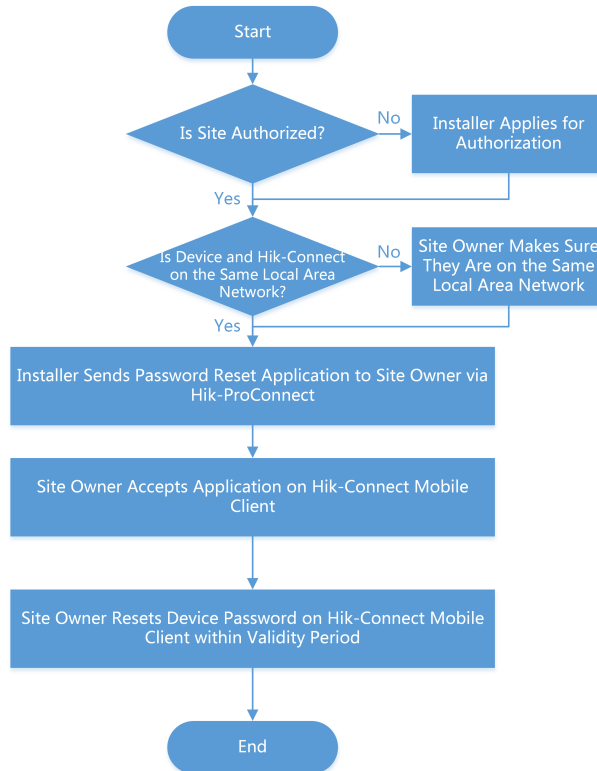


Figure 6-20 Flow Chart of Resetting Device Password Offsite

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

Note

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

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

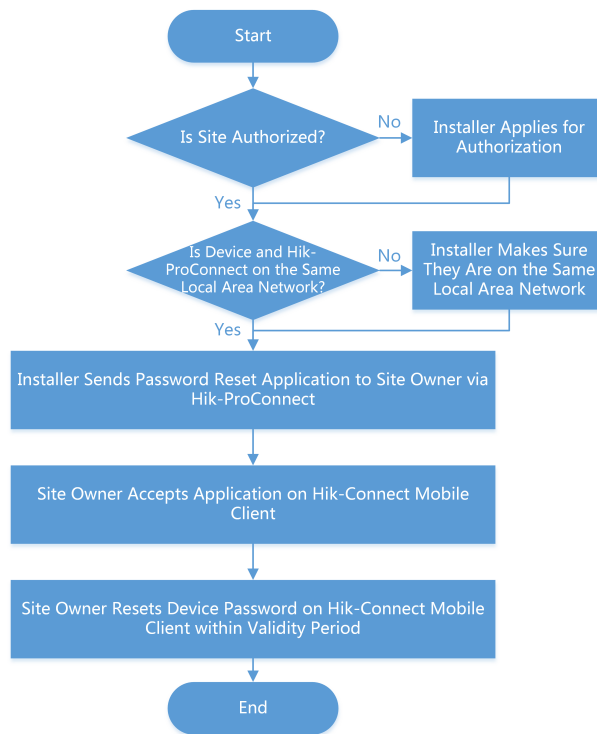


Figure 6-21 Flow Chart of Resetting Device Password Onsite


6.7 Manage Security Control Panel

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






Note

- The following chapter introduces functionality supported by AX Pro security control panel (hereinafter referred to as "AX Pro device"), 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 ***Alarm Receiving Center (ARC) Service*** , ***Health Monitoring*** , ***Linkage Rule and Exception Rule*** , and ***Remote Configuration*** respectively.
-

6.7.1 Control AX Pro

You can perform operations including arming/disarming area, clearing alarm, and bypassing zone. Click  **Site** to enter the site list page, and then click the name of a Site to enter site details page.

Click the AX 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  .
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  .
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.
Bypass Zone	Select the Device tab. Select a zone (i.e., detector) and turn on the Bypass switch to bypass the zone.

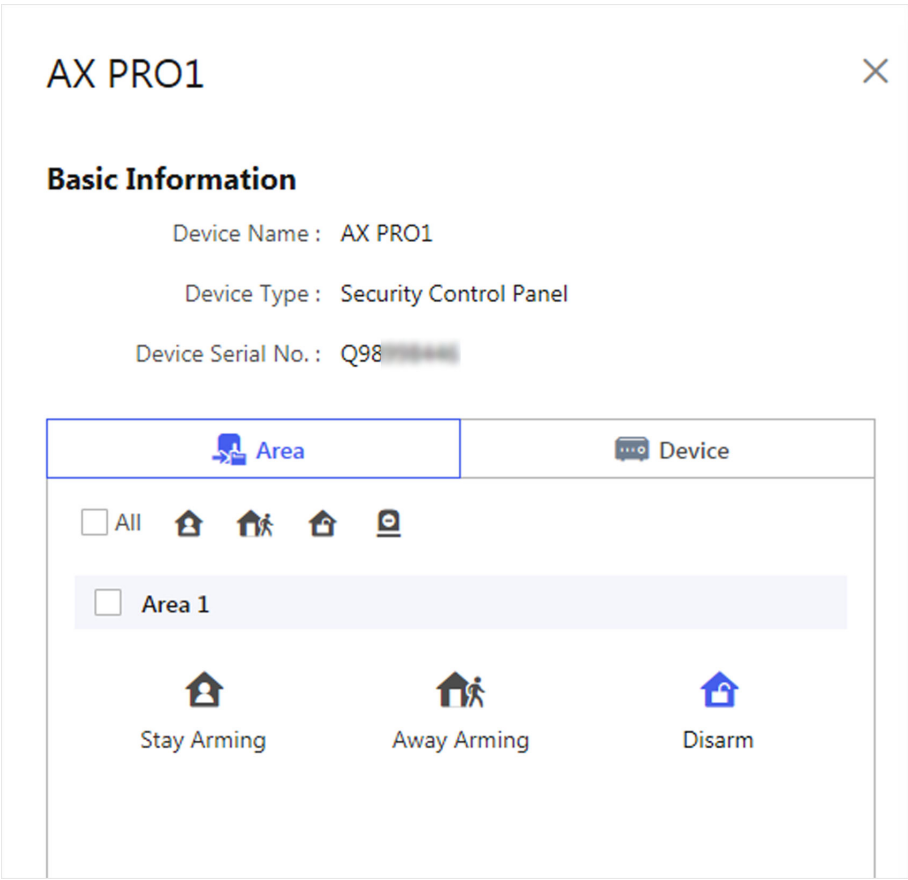


Figure 6-22 Operation Panel of AX Pro

6.7.2 Configure AX Pro

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

Click **Site** to enter the site list page, and then click the name of a site to enter site details page.

Remotely Configure AX 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.

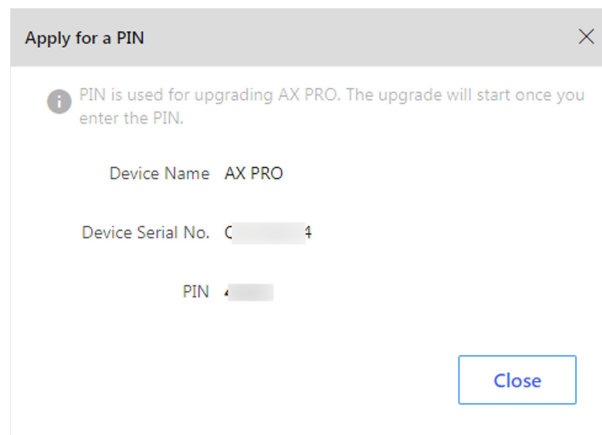


Figure 6-23 Apply for a PIN

Switch Language

You can click **• • • → ⇌ Language** and set the device language.



Note

A PIN code is required for switching language.

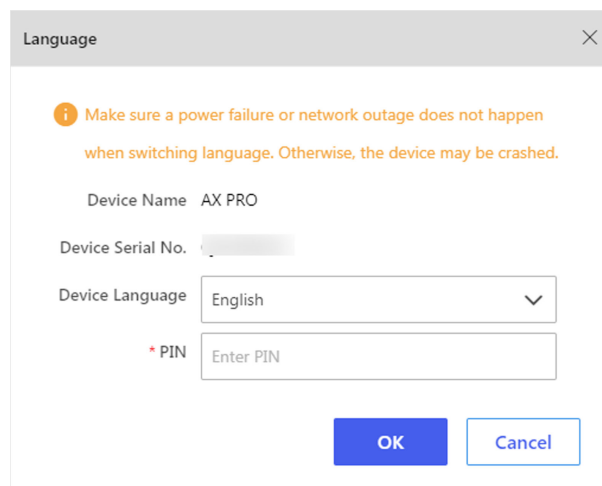


Figure 6-24 Language Window

6.7.3 Batch Arm/Disarm AX Pro

You can batch arm or disarm multiple AX Pro devices in various Sites by grouping the devices. For example, you can batch disarm all devices in several Sites of your customer, or even among different customers, when you are checking the devices on the spot, so that the devices will not issue an alarm.

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

Steps

Note

This function is available in Spain only.

1. Click **Site** on navigation panel.
2. Click **Batch Arm/Disarm**.

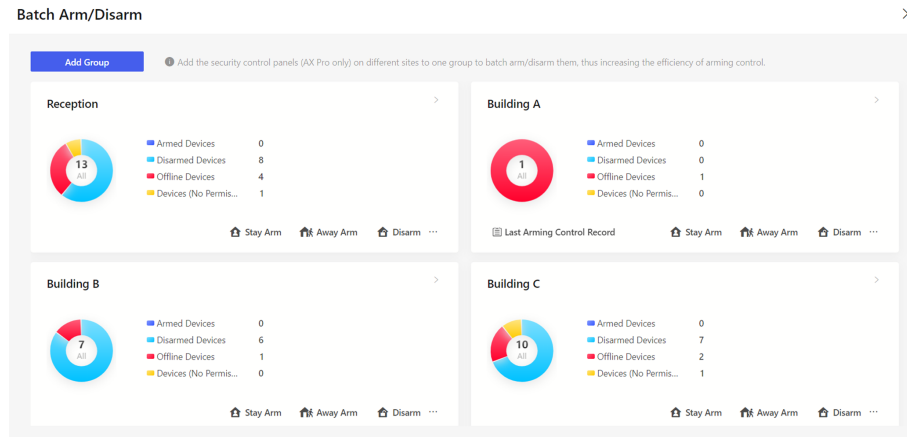


Figure 6-25 Batch Arm/Disarm Page

3. Click **Add Group**.
4. Create a name for the group.
5. 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.
6. Click **OK**.

Add Group for Batch Arming Control

Group security control panels to batch arm/disarm them by group.

* Group Name

Building 1

* Select Device

+ Add

Delete

<div></div>	Device Name	Site
<div></div>	AX PRO	k
<div></div>	AX PRO	k
<div></div>	AX PRO	k
<div></div>	AX PRO	k
<div></div>	AX PRO	k
<div></div>	AX PRO	A
<div></div>	AX PRO	A
<div></div>	AX PRO	A
<div></div>	AX PRO	A
<div></div>	AX PRO	A

OK

Cancel

Figure 6-26 Add Group for Batch Arming Control

7. 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.

i

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.

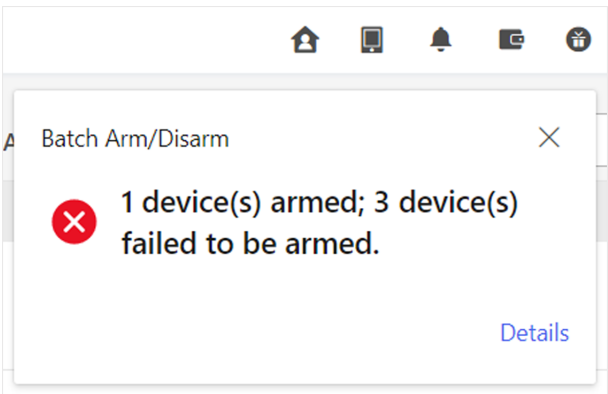


Figure 6-27 Pop-Up Notice

- You will also be notified on the Mobile Client when the arming/disarming process is completed.

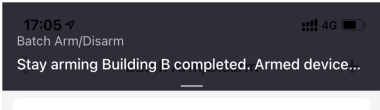


Figure 6-28 Notice on the Mobile Client

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.

6.7.4 Batch Configure AX Pro

You can batch configure parameters for the added AX Pro devices by creating template(s) in the platform.

Note

- Only AX Pro devices of Version 1.1.0 and later are supported.
- The function is only supported in certain countries and regions.

Create a Template

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

1. On the navigation panel, click **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 6 holiday groups.

Panel Alarm Duration

The time duration of the panel alarm.

Alarm Receiving Center

Protocol Type

Select **ADM-CID**, **SIA-DCS**, ***SIA-DCS**, ***ADM-CID**, or **CVS-IP** 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. On the left navigation panel of the Home page, click **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 **Add 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.

6.8 View Video

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

6.8.1 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 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.
-


6.8.2 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.

6.9 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.

6.9.1 Upgrade Device Firmware

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-ProConnect.

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 Box, and cloud storage DVR.
 - 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 Hik-Connect \(P2P\)**](#) for details.
-

1. Click a site name to enter the site details page.
2. 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 outage does not happen during the upgrade.
- You can enable EN50131 Compliant mode on device configuration page via a Web Client. See device user manual for details.



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.

6.9.2 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 Service** when handing over a Site to your customer, you cannot unbind the devices added to this Site. For details about Site handover, see [***Invite Site Owner***](#) .

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.


6.9.3 Configure DDNS for Devices

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

Steps

Note

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

1. Click **Site** tab on Home page 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**.


6.9.4 Remote Configuration

You can remotely configure online devices such as doorbells, encoding devices, and security control panels.



Note

- Only site managers can remotely configure a device. See **Assign Site to Installer** for details about how to assign Sites to Installers and thereby making the Installers be site managers.
- For encoding devices and security control devices, if the device is NOT on the same LAN with the Portal, some features (such as device account management, enabling Hik-Connect, and restoring device) will be unavailable.

Click **Site** to enter the Site List page, and then click the name of a Site to enter the site details page. And then click **Device** tab to show devices added to the Site. And then click  to open the remote configuration page of a device and set parameters of the device.

 **Note**

- See the device user manual for details about how to configure a device.
- If you have changed device parameters by other software or clients (such as device web page, Hik-ProConnect 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.

Table 6-9 Additional Information

Device Type	Additional Information
NVR	When an NVR is added by Hik-Connect (P2P), you can remotely configure network cameras connected to the NVR.
Security Control Panel	<ul style="list-style-type: none">• If the security control device is on the same LAN with the Portal, you need to enter the user name and password before accessing the remote configuration page.• If an AX Hub device or AX Hybrid device is not on the same LAN with the Portal, and the EN50131 Compliant mode is enabled for the device, you need to enter password of the device for verification first. After verification, you can access the configuration page of the device by entering the setter password of the device.

Chapter 7 Value-Added Services

Hik-ProConnect provides multiple value-added services for you to better serve your customers, including the health monitoring service, access and attendance service, cloud storage service, people counting service, temperature screening service, alarm receiving center 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 details, refer to the after sales or local distributor.

7.1 Health Monitoring Service

Hik-ProConnect 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-ProConnect, 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 7-1 Differences Between Free Package and Health Monitoring Package

Functionality	Free Package	Health Monitoring Package
Adding Devices	<ul style="list-style-type: none">SupportedManageable Devices: 1024	<ul style="list-style-type: none">SupportedManageable Devices: More than 1024 based on the package you purchase.
Site & Device		
Applying for Authorization		
Viewing Device Online Status		
Remote Configuration		

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	Manageable Employees: 4
Role/Permission Management	Not Supported	Supported
Searching Operation Logs of Employees	Not Supported	Supported

7.1.1 Purchase Health Monitoring Service

You can purchase the health monitoring service in two ways. The first way is to purchase service packages online in the Service Market in Hik-ProConnect. The second way is to purchase a service key from the local distributor offline first, and then purchase the service 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. In the left navigation, click **Business → Service Market** to enter 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 **Purchase by Service Key** to purchase the service.

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

All Device Monthly Package

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

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

All Device Monthly Package * 20

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

All Device Monthly Package * 100

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

All Device Annual Package

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

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

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

All Device Annual Package * 20

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

All Device Annual Package * 100

100 All 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 Annual 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 **Business → **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***](#) .

7.1.2 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-ProConnect, 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: Go to **Business** → **My Service** → **All Services** , and then click **Activate Health Monitoring Service**.

- Choice 2: Go to **Business → 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 Hik-Connect \(P2P\)**](#) for details.

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

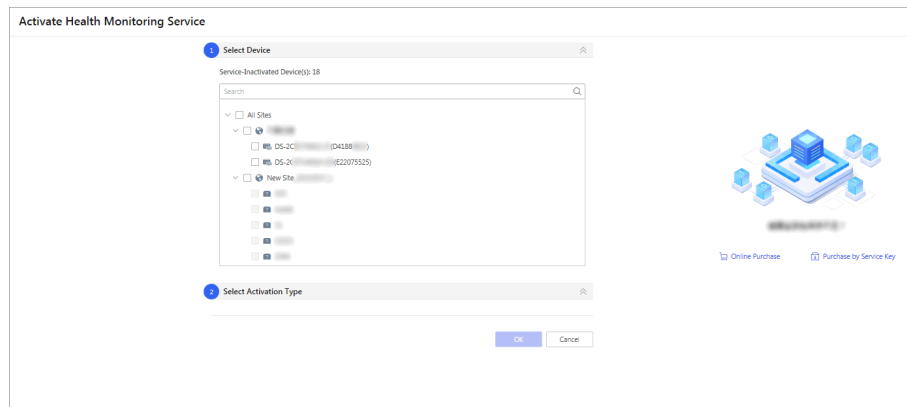


Figure 7-1 Figure 1: Select Devices to Activate Health Monitoring Service

The screenshot shows a dialog box titled "Activate Health Monitoring Service" with a close button (X) in the top right corner. Inside the dialog, there is a section for "Available Package" with a link "Online Purchase" in blue. Below this, there are four package options in a 2x2 grid:

Package Name	Count
All Device Monthly Package	83
Network Camera Monthly Package	0
All Device Annual Package	20040
Network Camera Annual Package	0

Below the packages, there is a "Select Type" section with two radio buttons. The first radio button is selected and labeled "All Device Monthly Package", with a dropdown menu showing the value "3". Below this, it says "Activate 3 month(s) of health monitoring service for each device." The second radio button is labeled "All Device Annual Package" with a dropdown menu showing the value "0".

At the bottom, there is an "Auto Renewal" toggle switch, which is currently turned off. Below the toggle, it says: "The health monitoring service will be automatically renewed using the same type of service packages that you have purchased."

At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (white).

Figure 7-2 Figure 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 7-36** 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 **Purchase 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**.

5. **Optional:** Go to the site details page, and then click a device with the service activated to show the device details panel, and then perform the following operations if needed.

Renew the Service Click **Renew** to renew the service for the device.

Transfer the Service 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 **Auto Renewal** to Open the Auto Renew window, switch on **Auto Renewal**, and then select a type of service packages for auto renewal.

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

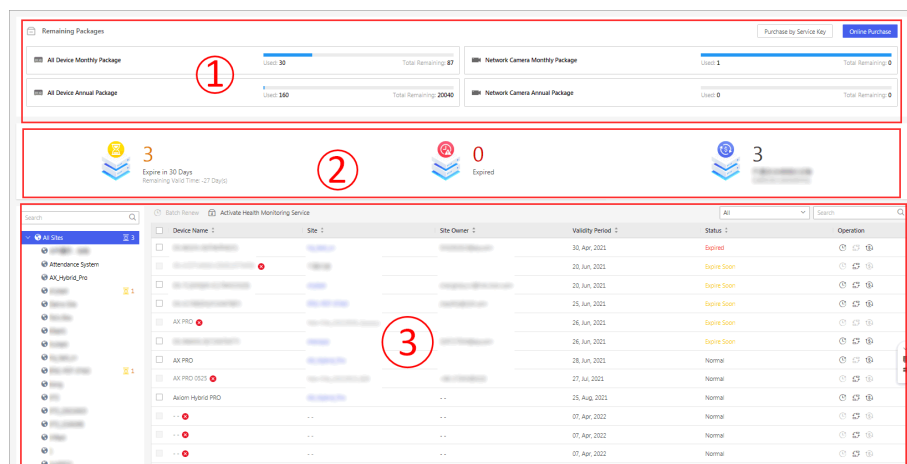

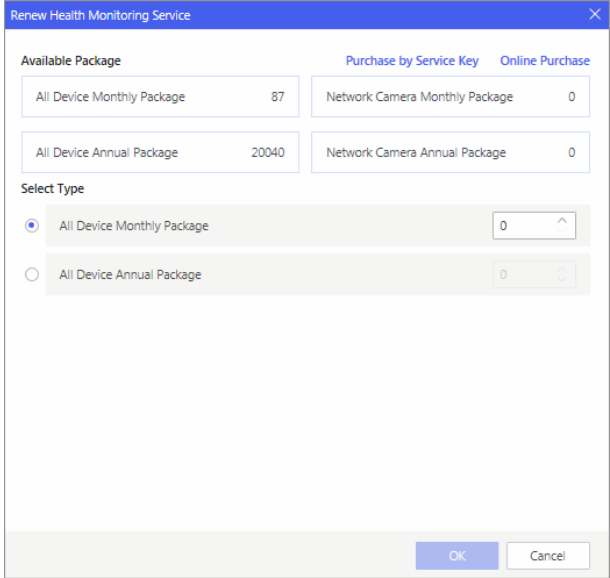




Figure 7-3 Manage Your Health Monitoring Service

On the page, the following features are available.

Table 7-2 Available Features

Area No.	Feature	Description
1	View Remaining Packages & Purchase More	View used number and remaining number of each type of health monitoring packages. Click Purchase by Service Key or Online Purchase to purchase more packages. For details, see <u>Purchase Health Monitoring Service</u> .
2	View Expiration and Auto Renewal Information	<ul style="list-style-type: none"> • 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.
3	Activate Service	Click Activate Health Monitoring Service to activate the health monitoring service for specific devices. For details, see <u>Activate the Health Monitoring Service for Devices</u> .
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 <u>Activate the Health Monitoring Service for Devices</u> 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 <u>Activate the Health Monitoring Service for Devices</u> for details.

Area No.	Feature	Description
		 <p>Figure 7-4 Renew</p>
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.

7.2 Access and Attendance Service

Access & Attendance provides an all-in-one solution for access control and attendance management in various businesses. You can create Access & 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 Access & Attendance system. With Hik-Connect Mobile Client V4.13.0 or later, the employees can control doors and check attendance records on their mobile phones.

Note

The Access and 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.

7.2.1 Flow Chart for Setting Access & Attendance Service

The flow chart below shows the recommended process for setting Access & Attendance service.

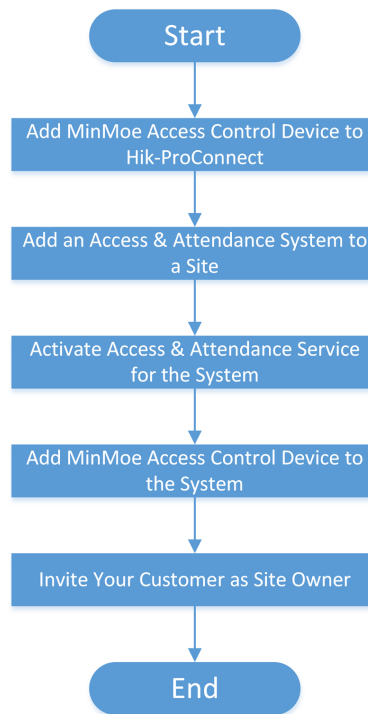



Figure 7-5 Flow Chart

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

Table 7-3 Flow Chart Description

Step	Description
Add MinMoe Access Control Devices to Hik-ProConnect	Add MinMoe access control devices to Site(s) which owned by a same customer. For details about adding devices to Hik-ProConnect, see <i>Add Device</i> and its sections.
Add an Access & Attendance System to a Site	Add an Access & Attendance system to a specific Site. The Access & Attendance system is used for grouping and managing

Step	Description
	MinMoe access control devices. For details about adding the system, see <u>Add Access and Attendance System</u> .
Activate Access & Attendance Service	Activate the Access & Attendance service for the system. For details, see <u>Add Access and Attendance System</u>
Add Access & Attendance Devices to the System	Add MinMoe access control devices to the system. For details, see <u>Add Access and Attendance System</u> .
Invite Your Customer as Site Owner	<p>After completing the required configurations, invite your customer as the Site Owner so as to hand over the Site to her/him. For details, see <u>Invite Site Owner</u> .</p> <p> Note</p> <p>When your customer accept the invitation and approving activating the Access and Attendance service on the Hik-Connect Mobile Client (V 4.15.0 or later), he/she will be able to set access levels and attendance rules for her/his employees via the Hik-Connect Portal (http://www.hik-connect.com) And her/his employees will be able to use the Hik-Connect Mobile Client to check their attendance records.</p>

7.2.2 Add Access and Attendance System

You can add an Access & Attendance system for a Site to set up the basic attendance management environment for the Site Owner.

Steps

1. Click **Site** tab on the navigation panel.
2. Select the Site where you want to add the Access & Attendance system.
3. Select the **Access & Attendance** tab.
4. Click **Add Access & Attendance System**.
5. Create a name for the system.
6. Click **OK**.
7. Activate Access & Attendance service for the Site.
8. Click **Add Device** or **Edit** to add access control devices to the Access & Attendance system.
 - 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 **Access & Attendance** for the devices.

What to do next

Hand over the Site to the Site Owner and inform the Site Owner to accept Access & Attendance service permission application. See instructions in [***Invite Site Owner***](#) .

7.3 Cloud Storage Service

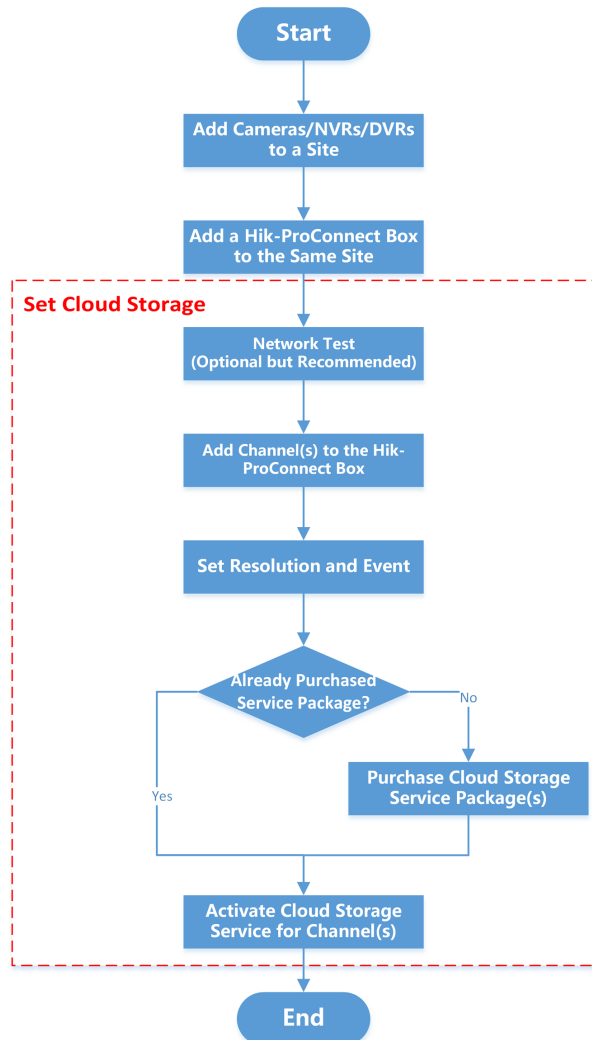
Hik-ProConnect offers cloud storage solution for the event-related video footage, which refers to the video footage recorded when a pre-defined event is detected by the channel of an encoding device.

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 or 30 days on the cloud, basing on the types of the cloud storage service packages purchased from the service market.

7.3.1 Flow Chart

The flow charts below shows the recommended procedures for using cloud storage service by Hik-ProConnect box and cloud storage DVR.



Flow Chart for Hik-ProConnect Box



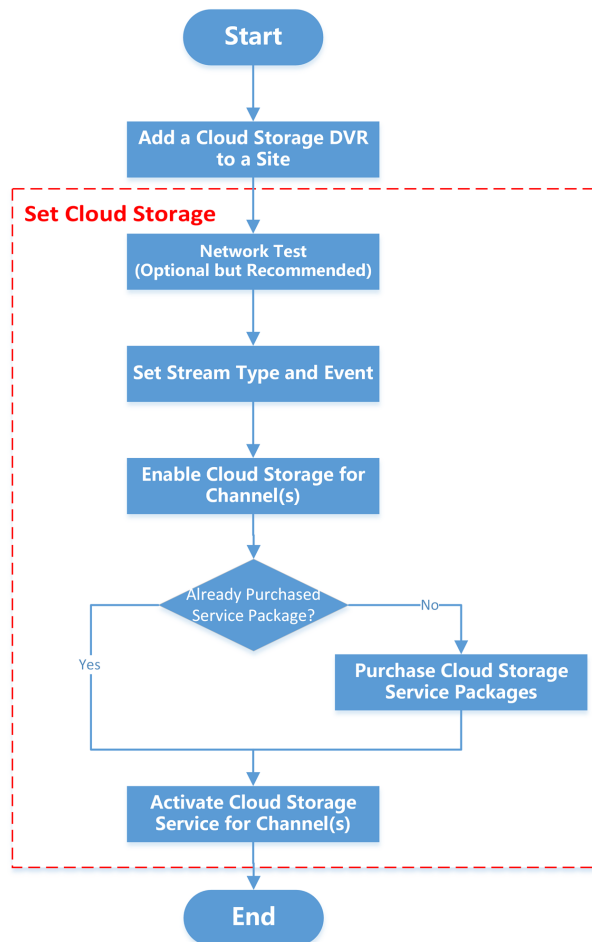
The following table shows the description for each procedure of the flow chart.

Table 7-4 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 Hik-Connect (P2P) , Add Devices in a Batch , and Add Detected Online Device .


Procedure	Description
	 Note For the Hik-ProConnect box added by IP/Domain name, cloud storage service is not supported.
Set Cloud Storage	<p>Set cloud storage for the Hik-ProConnect. See <u>Set Cloud Storage for Box</u> for details.</p> <p>The following list shows the descriptions of the sub-procedures.</p> <ul style="list-style-type: none"> • Network Test: Test your network condition to get the recommended settings for cloud storage. See <u>Network Test</u> 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 <u>Purchase Cloud Storage Service</u> for details.  Note You can also purchase service packages by service key. Consult the distributor to get the service key. <ul style="list-style-type: none"> • 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 <u>Activate or Renew Service for a Channel</u> for details.


Flow Chart for Cloud Storage DVR



The following table shows the description for each procedure of the flow chart.

Table 7-5 Flow Chart Description

Procedure	Description
Add a Cloud Storage DVR to a Site	<p>Add a cloud storage DVR to a site by Hik-Connect (P2P). For details, see <u>Add Device by Hik-Connect (P2P)</u> , <u>Add Devices in a Batch</u> , and <u>Add Detected Online Device</u> .</p> <p> Note</p> <p>For the cloud storage DVR added by IP/Domain Name, cloud storage service is not supported.</p>
Set Cloud Storage	<p>Set cloud storage for the cloud storage DVR. For details, see <u>Set Cloud Storage for Cloud Storage DVR</u> .</p> <p>The following list shows the descriptions of the sub-procedures.</p>

Procedure	Description
	<ul style="list-style-type: none"> • 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 cloud storage DVR. • 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. <p> Note</p> <p>You can also purchase service packages by service key. Consult the distributor to get the service key.</p> <ul style="list-style-type: none"> • 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.

7.3.2 Purchase Cloud Storage Service

You should purchase the cloud storage service in the service market before using it.

Before You Start

Make sure you have the permission to manage service package and order.

Steps

1. On the home page, click **Business → Service Market** to enter the service market page.
2. In the Cloud Service area, click **Online Purchase** to enter purchasing page.

You can view four types of cloud storage service packages and their corresponding prices.

3. 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.
- **7-Day** and **30-Day** refer to the retention periods 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 the 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.

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



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:** Click **Business → My Service → Cloud Storage Details** to view the service package(s) you have purchased in the list.

7.3.3 Set Cloud Storage for 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 Hik-Connect (P2P)** , **Add Devices in a Batch** , 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 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.

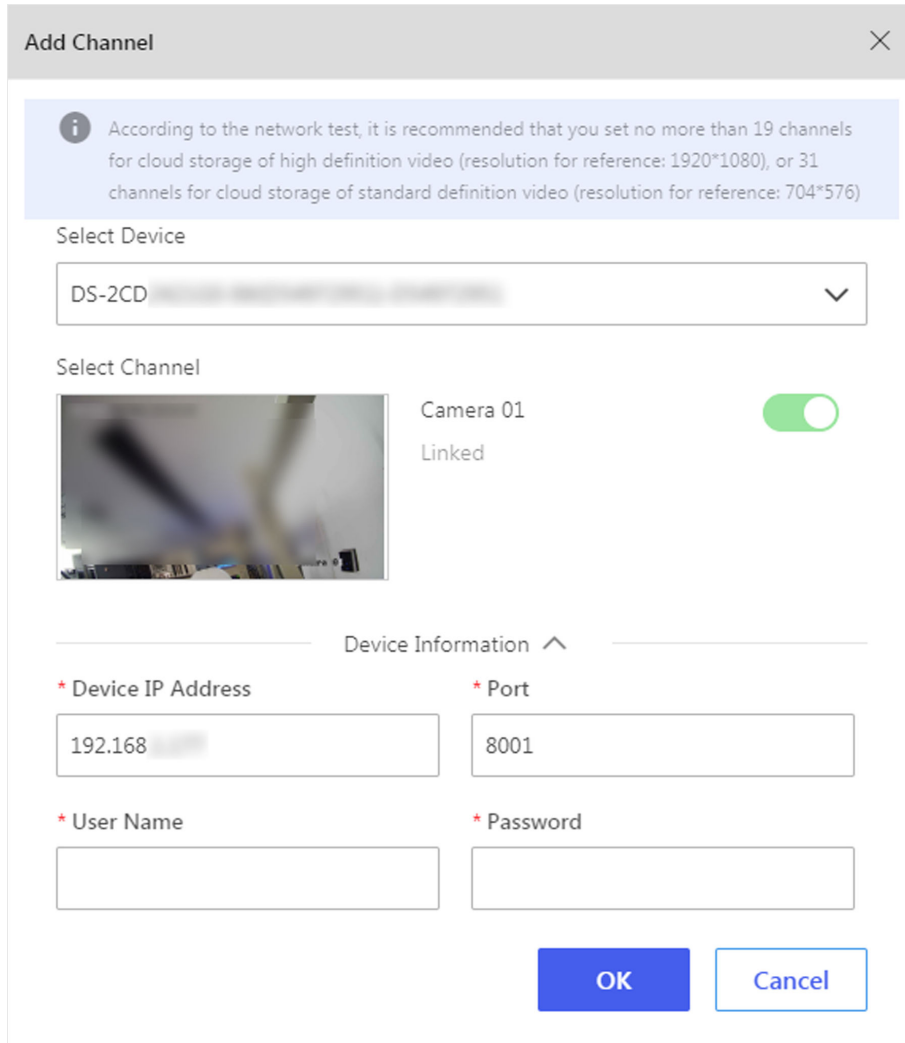


Figure 7-6 Add Channel Window

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.

- 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 enter the Cloud Storage Settings page, which displays the channel(s) already added to the Hik-ProConnect Box.

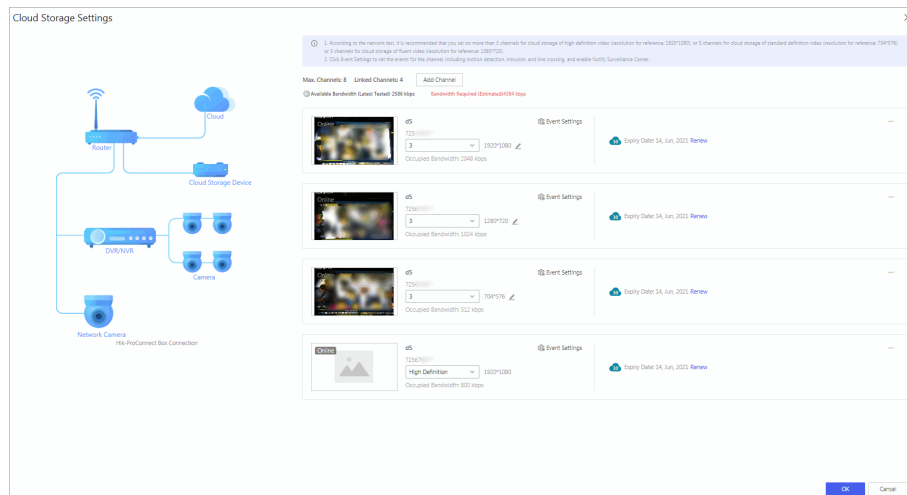



Figure 7-7 Cloud Storage Settings Page

5. Set resolution of the footage to be uploaded to the cloud.
 - Choice 1: 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).

- Choice 2: 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**.

7.3.4 Set Cloud Storage for Cloud Storage DVR

When you complete adding a cloud storage DVR to a site, the result page will show the entry for setting cloud storage. You can skip the settings, 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 DVR's channels, and activating cloud storage service for the channels. When you complete all these settings, the cloud storage DVR will be able to upload event-related video footage from its linked channels to the cloud.

Steps



Note

If you skip the cloud storage settings when completing adding the cloud storage DVR, you can click the device in the device list to open its settings panel to set cloud storage for it later.

1. Add a cloud storage DVR to a site by Hik-Connect (P2P).

Note

- For details about adding cloud storage DVR, see [Add Device by Hik-Connect \(P2P\)](#) , [Add Devices in a Batch](#) , or [Add Detected Online Device](#) .
- If you add the cloud storage DVR 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 cloud storage DVR 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.



If it is the first time you enable cloud storage for a channel of the cloud storage DVR, the cloud storage 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.



For details about how to activate the service, see [***Activate or Renew Service for a Channel***](#) .

The cloud storage DVR will automatically reboot. After that, the event related video footage of the channel will be uploaded to the cloud.



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 cloud storage DVR in the device list to open its settings panel, and then click **Edit** to edit the settings of its channels.




If you turn off **Cloud Storage** for all of its channels, the cloud storage DVR will automatically reboot itself.

7.3.5 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.



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.

7.3.6 Activate or Renew Service for a Channel

On the cloud storage service page, you can view the cloud storage details of different channels of a cloud storage device. If cloud storage service is not activated for a certain channel, you should activate the service before using it. For an activated service that will expire soon or has expired, you can renew the service for this 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-ProConnect 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. On the home page, click **Site** to enter the site list page.
2. Click a site to enter its site details page.
3. Select **Cloud Storage Service** tab.
4. Enter the Activate/Renew Cloud Storage Service window.
 - When you have not activated the service for any channel in the site, click **Activate Cloud Storage Service**, select an online device in the list, enable **Cloud Storage** and click **Activate Service**.
 - When you have already activated the service for one or more channels in the site, click **Activate Service** to activate the service for a certain channel, or click **Renew Service** to renew the service for a certain channel.

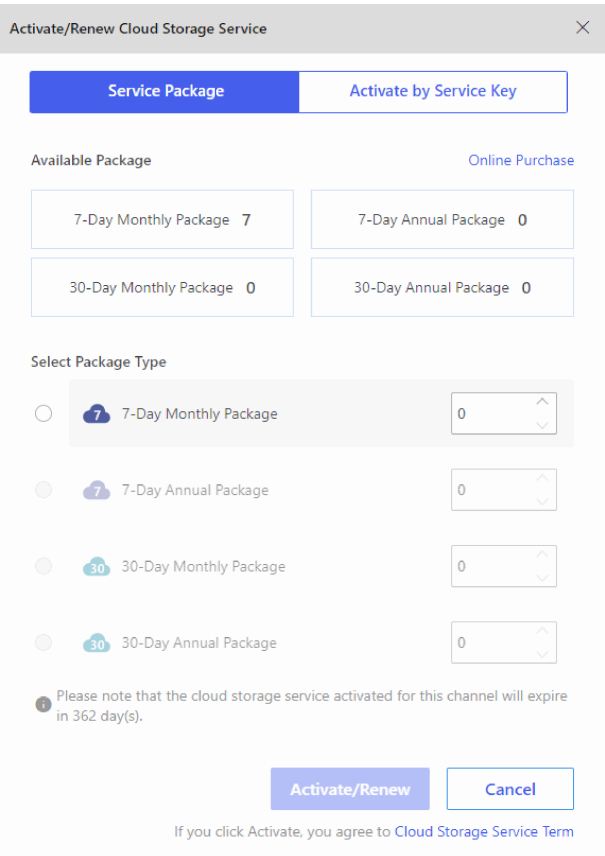



Figure 7-8 Activate/Renew Cloud Storage Service

 **Note**

You can view the available packages which you have purchased. You can also click **Online Purchase** to purchased more packages if needed. For details, refer to **Purchase Cloud Storage Service** .

5. Activate or renew the cloud storage service for a channel.
- Click **Service Package**, check a package type, and click  (or manually enter a number) to define the number of package.
 - Click **Activate by Service Key**, and enter the 16-digit service key.

 **Note**

You can consult the distributor to get the service key.

6. Click **Activate/Renew** to finish activating or renewing the cloud storage service.
- After activating or renewing the service, you can view the package type and expiry date of the service in each channel.


7.3.7 View Cloud Storage Details

You can view the cloud storage details including the type(s) and the number of the service packages that you have purchased and used, and the details (such as the expiry date and status) of service activated for different channels of cloud storage devices. Also, you can perform more operations such as renewing the service for further use.

You can enter the cloud storage details page via the following two methods:

- On the home page, click **Business → My Service → Cloud Storage Details** .
- On the home page, click **Business → My Service → All Services** , select the cloud storage service package and click **Details**.

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 more following operations.

- **Filter:** Click  to filter the channels of cloud storage devices according to the status (expire soon or expired) of cloud storage service.
- **Search:** Enter a keyword (of device name, site name, or site owner name) in the search box to view the service status of channels of a specific device.
- **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***](#) .

7.4 People Counting Service

Hik-ProConnect 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.

7.4.1 Flow Chart for Setting People Counting Service

The flow chart below shows the recommended process for setting people counting service.

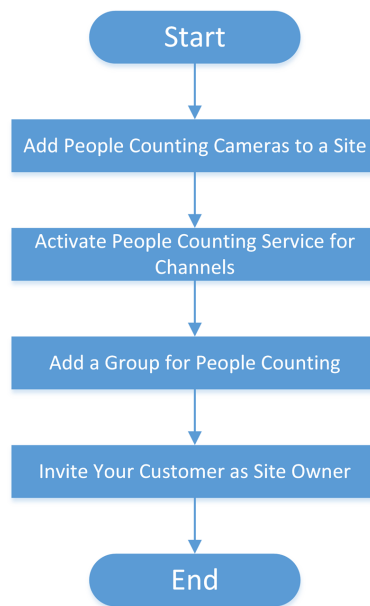



Figure 7-9 Flow Chart

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

Table 7-6 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 <u>Add Device</u> 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 <u>Activate People Counting Service for Channels</u> .
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 <u>Add a Group for People Counting</u> .
Invite Your Customer as Site Owner	<p>After complete the required configurations, invite your customer as the Site Owner so as to hand over the Site to her/him. For details, see <u>Invite Site Owner</u> .</p> <p> Note</p> <p>When your customer accept the invitation 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.</p>



7.4.2 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. Click  **Site** to enter the site list page.
2. Click a site to enter its site details page, and then 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.

7.4.3 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. Click  **Site** to enter the site list 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.

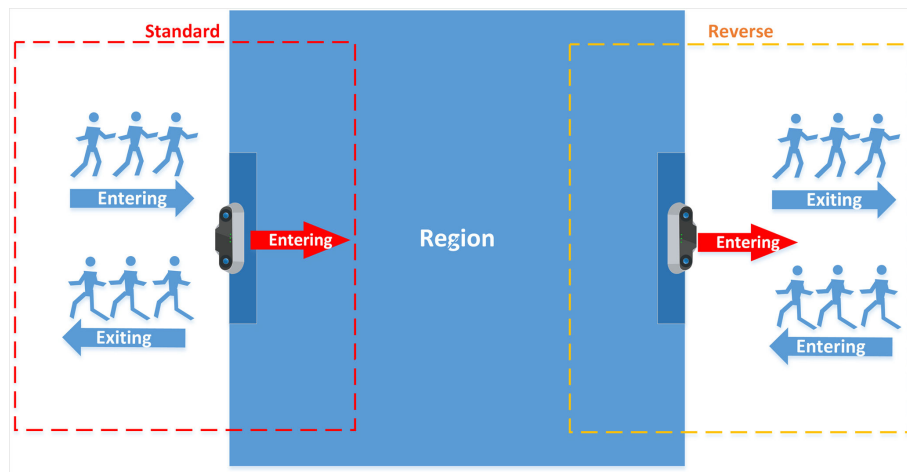


Figure 7-10 Calculation Mode

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.



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.



If you delete a people counting group, the corresponding people counting functionality will also be deleted.

Disable a Specific Group Set  to  to disable the group.



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.



If you disable the group, the people counting related functionality on the Hik-Connect Mobile Client will be unavailable.

7.5 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.



The service is only available in some countries and regions.

7.5.1 Flow Chart for Setting Temperature Screening Service

The flow chart below shows the recommended process for setting temperature screening service.

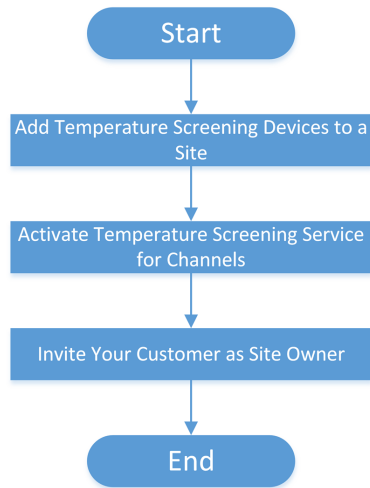



Figure 7-11 Flow Chart

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

Table 7-7 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 .
Invite You Customer as Site Owner	<p>After complete the required configurations, invite your customer as the Site Owner so as to hand over the Site to her/him. For details, see Invite Site Owner.</p> <p> Note</p> <p>When your customer accept the invitation 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.</p>

7.5.2 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. Click  **Site** to enter the site list 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-ProConnect 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.



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-ProConnect 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.



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.





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 Functionality of All Devices

Click **Disable All** to disable all temperature screening 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.

7.6 Alarm Receiving Center (ARC) Service

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

Steps

 **Note**

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

1. Click **Site** on the navigation panel to enter the site list page.
 2. Select a Site to enter the site details page, and then select **ARC Service**.
 3. Click **Select ARC** to display the Select Authorized ARC panel.
-

 **Note**

On the panel, you can view details of each ARC, including company name, logo, country, 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 ARC service will be displayed.

Note

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 ARC service for a specific device.

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

7. **Optional:** If you have enabled ARC service for an AX device in the previous step and the device is accessed to ARC via Hik IP Receiver Pro, click the device in the device list to open the configuration panel, and then set the way to connect the device to Hik IP Receiver Pro.

Note

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

Ways to Connect to Hik IP Receiver Pro

Connect Directly or by Hik-ProConnect Server

When the two connections are both available, direct connection will be used in priority, i.e., the device will be connected to Hik IP Receiver Pro directly. When direct connection is abnormal, the device will be linked to Hik IP Receiver Pro by Hik-ProConnect server. If direct connection is restored, the way will automatically switch back to direct connection. Such a mechanism ensures the stability of data transmission from the device to the ARC.

Connect by Hik-ProConnect Server

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

Note

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

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.

7.7 Co-Branding

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

Note

You can get the co-branding service for free after purchasing the annual type of health monitoring packages (including All Device Annual Package and Network Camera Annual Package) for the first time. For details about how to purchase health monitoring packages, see [***Purchase Health Monitoring Service***](#) .

On the Home page, click **Company → Co-Branding** . Switch **Co-Branding** to on, 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.

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). 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 8 Health Monitoring

The portal provides the Health Monitoring module for managing the resources. There are two sub-modules in the Health Monitoring module.

- The **Health Status** module provides near-real-time information about the status of the devices added to the sites. And 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 maintenance of the devices managed on the Hik-ProConnect platform as a whole, helps you locate the source of exceptions and determine methods for troubleshooting in time, thereby contributing to the smooth running of these devices.



Note

For Installer, you can only view the status information of the devices on the Site which has been assigned to you. For Installer Admin, you can view the status information of the devices on all Sites.

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



Note

For Installer, you can only view the exceptions of the devices in the site which has been assigned to you. For Installer Admin, you can view the exceptions of the devices in all sites.

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 Type

Encoding Device	Refer to <i>Encoding Device</i> .
Access Control Device	Refer to <i>Access Control Device</i> .
Security Control Device	Refer to <i>Security Control Device</i> .
Video Intercom Device	Refer to <i>Video Intercom Device</i> .
Doorbell	Refer to <i>Doorbell</i> .

Hik-ProConnect Box	Refer to <i>Hik-ProConnect Box</i> .
Network Switch	Refer to <i>Network Switch</i> .

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 if video loss occurs.


Offline Camera

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

You can perform the following operations.

- Hover the cursor over the device name to view its device type and device version.
- Click  in the Operation column to remotely configure the device parameters. For details, see the device user manual.
- Click **Refresh** to inspect all the encoding devices in all sites.
- Check **Abnormal Only** to display the abnormal devices only.
- Check **Display Authorized Device Only** to display the devices of which configuration permission has been authorized to you.
- Click  to show the cameras linked to the device, and then you can view the online/offline status of each camera.
- Click  to show the HDD information of the DVR, including self-inspection evaluation result, overall evaluation result, running status, running time, HDD temperature, and S.M.A.R.T 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.
- Click  in the Operation column to inspect the selected encoding device manually.
- 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*** .
-
-  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**](#) .
-

Access Control Device

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

- Hover the cursor over the device name to view its device type and device version.
 - Click  to inspect access control devices.
 - Check **Abnormal Only** to let the page only display the abnormal devices.
 - Check **Display Authorized Device Only** to display the devices whose configuration permission has been authorized to you.
 - 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.
 - Click  in the Operation column to inspect the selected access control device manually.
 -  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**](#) .


Security Control 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.

- Hover the cursor over the device name to view its device type and device version.
 - Click  in the Operation column to remotely configure the device parameters. For details, see the device user manual.
-

Note




Remote configuration is not supported if the device is armed.

- Click  to inspect access control devices.
 - Check **Abnormal Only** to let the page only display the abnormal devices.
 - Check **Display Authorized Device Only** to let the page only display the devices whose configuration permission has been authorized to you.
-

- 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 Firmware](#) .
-  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](#) .

- Click  to view the status of the zones and peripheral devices linked to the security control panel.
You can hover the cursor over a specific zone to view its detailed exceptions.
- 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.
- Click  in the Operation column to inspect the selected security control device manually.

Video Intercom Device

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

You can perform the following operations.

- Hover the cursor over the device name to view its device type and device version.
- Click **Refresh** to inspect the video intercom devices.
- Click  in the Operation column to inspect the selected device manually.
-  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](#) .


Doorbell

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

You can perform the following operations.


- Hover the cursor over the device name to view its device type and device version.
- Click  to inspect access control devices
- Check **Abnormal Only** to display the abnormal devices only.
- Check **Display Authorized Device Only** to display the devices whose configuration permission has been authorized to you only.
- Click  in the Operation column to remotely configure parameters of the device. For details, see the user manual of the device.
- Click  in the Operation column to inspect the selected encoding device manually.
- 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](#).
-
-  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](#).



- 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 Firmware](#).
-

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.

Click  to view the basic information (e.g., device serial number and device model) and the detailed list of online and offline channels (cameras).




You can also perform the following operations:


- Click  in the Operation column to remotely configure parameters of the device. For details, see the user manual of the device.
- Click  in the Operation column to inspect the 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:

- Click  in the Operation column to inspect the device manually.
- Click  in the Operation column to reboot the network switch remotely.
- Click  in the Operation column to view the topology of this switch. For details about topology, refer to [Network Topology](#).

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.

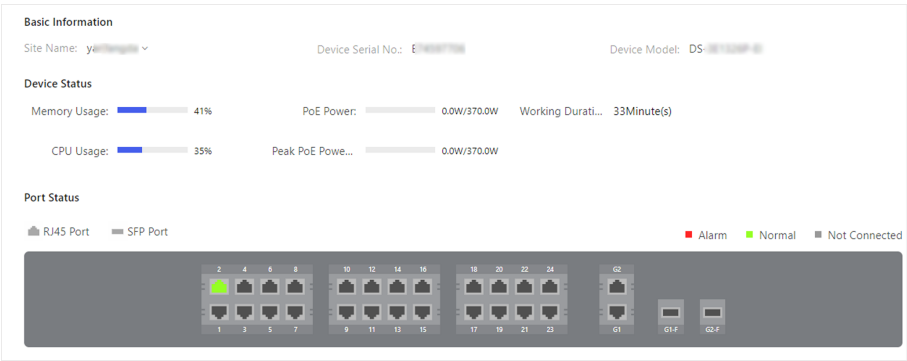


Figure 8-1 Switch Details

Hover the cursor onto the switch picture to view the enlarged picture of the ports.
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 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 Abnormal Only to display the abnormal device(s) only. Check Display Authorized Device Only to display the device(s) of which configuration permission has been authorized to you only.
Upgrade Device Firmware	If there are security control panel(s) available for upgrade, a number in red will be displayed on Upgrade showing the number of upgradable device(s). In this case, you can click Upgrade and select the upgradable device(s), and then click Upgrade to upgrade the select one(s).



Note

For details, see [**Upgrade Device Firmware**](#) .

Diagnose Devices of the Site

Click **Health Check** to open the Health Check window, and then 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 also 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.

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.

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 a schedule to let the platform generate device health check report and send it to your email addresses automatically, so that you can get regular updates on important devices and compare the reports of each period.

Before You Start

Make sure you have activated Health Monitoring Package.

Steps

1. On the navigation panel, click **Health Monitoring** → **Send Report Regularly**.

Note

- All Sites available for this feature are shown on the page automatically.
- The platform only supports automatically sending health check report on the encoding devices and AX Pro security control panels in authorized Sites.
- Sites that do not contain the above-mentioned types of devices or are not authorized to you will NOT be shown.

2. Enter editing mode to configure report settings.

- To configure the report settings for one Site, click **Edit** of the Site.
- To batch configure report settings for multiple Sites, click **Batch Configure** and then select the Sites that you want to configure.

3. Configure report settings.

Device

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

Schedule

Specify the frequency, date, and time of sending the report. You can set the frequency to 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 the language of your report. Currently, you can select English or Spanish.

4. Enable the settings.

- To enable the settings for one Site, switch on **Enable** of 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.

8.4 Network Topology

If you have added network switch(es) to a site and connected devices to the network switch(es), you can view these devices' network topology. Network topology displays network links between devices and shows the link exceptions and abnormal devices, helping you to locate 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 configuration permission, see [***Apply for Device Permission***](#) .
- If you have not activated the health monitoring service for the network switch, some topology functions (e.g., viewing device status on the topology) will be unavailable. For details about activating the health monitoring service for devices, see [***Activate the Health Monitoring Service for Devices***](#) .

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

- On the navigation panel, click **Site**, 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 Health Monitoring service for the network switch, you can enter the network topology page in this way only.



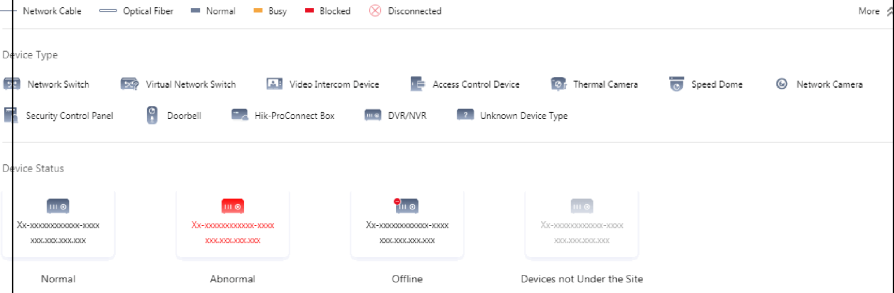



- In the navigation panel, click **Health Monitoring → Health Status** , select **All Sites** from the site list, and then select **Network Switch**, and then click  in the Operation column in the network switch list.
- On the navigation panel, click **Health Monitoring → Health Status** , select a site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

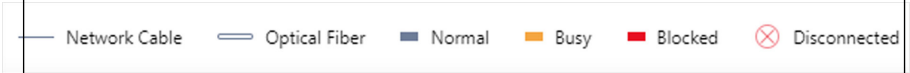







Figure 8-2 Network Topology

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

Table 8-2 Available Operations

Operation	Description
View Legend	<p>You can click  next to More to view the legends (see the figure below).</p>  <p style="text-align: center;">Figure 8-3 Legend</p>
Edit Root Node	<p>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.</p>  <p style="text-align: center;">Figure 8-4 Edit Root Node</p>
Refresh Topology	<p>Click Refresh to refresh the topology structure.</p> <p> Note The device status will not be refreshed.</p>
Display in Cards	<p>If you want to view more device status information by a glimpse of all the devices connected to the network switch(es), click Display in Cards to display device information in cards.</p>
Move Network Topology	<p>Drag the network topology to move it.</p>

Operation	Description
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 to the display window. You can click ☒ in the upper left corner to display 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 your current cursor location on the topology.
Search Devices in Topology	You can enter a 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	<p>You can view link information based on the legends shown in the figure below.</p>  <p>Figure 8-5 Link Information Legend</p>
View Link Details	You can hover the cursor over a specific link to view its details, such as upstream, downstream, port name, and port status.
Apply for Configuration Permission	<p>If you don't have configuration permission for 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.</p> <p> Note</p> <p>If you don't have the permission, the position of the device in the network topology might be incorrect.</p>
View Network Switch Details and Control It	<p>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.</p> <p>You can also perform operations such as rebooting the network switch and restarting port. For details, see <u>Network Switch View Status of Devices in a Specific Site</u> .</p>

Operation	Description
	 Note You cannot view details of a virtual network switch.
View Other Device's Details and Configure It	<p>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 information about it, including basic information (e.g., device model) and device status (e.g., network status). You can also click  to configure device parameters.</p> <p> Note</p> <ul style="list-style-type: none">• 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 NOT added to the same site with the network switch, its displayed serial number will be randomly generated virtual serial number. And you cannot view its information.

8.5 Exception Center

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

 **Note**

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

Click **Health Monitoring → Exception Center** to enter the Exception Center page as follows.

Schedule	Site Name	Source	Exception Type	Site Owner	Received by
24. May. 2021 11:20:55	Win	IPCamera 02	Offline	with	
24. May. 2021 10:32:35	Win	IPCamera 02	Online	with	
24. May. 2021 10:32:35	Win	IPCamera 02	Offline	with	
21. May. 2021 20:06:58	Win	Camera 07	Offline	with	
21. May. 2021 20:05:43	Win	Camera 09	Offline	with	
21. May. 2021 20:01:29	axj	Camera 08	Lid Opened	com	
21. May. 2021 15:21:13	Win	Camera 13	Offline	with	
21. May. 2021 15:21:13	Win	Camera 07	Offline	with	
21. May. 2021 15:21:13	Win	Camera 09	Offline	with	
21. May. 2021 15:21:12	Win	Camera 04	Offline	with	
21. May. 2021 15:21:12	Win	Camera 10	Offline	with	
21. May. 2021 15:21:12	Win	Camera 08	Offline	with	
21. May. 2021 15:21:12	Win	Camera 15	Offline	with	

Figure 8-6 Exception Center

Check Exception Details

Perform the following steps to filter the exceptions according to 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. Select the exception types that you want to check. The exception types include device exception and channel exception.

You can set the **Auto-Update** switch to on 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).

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** at 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.

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.

Click **Company → 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.



Name	Employee's Email	Client	Site	Operation Target	Operation Content	Schedule
lulu	81@qq.com	Portal	--	--	Login Succeeded	7, Nov, 2020 10:57:45
ddc	.test1@sina.com	Portal	--	--	Login Succeeded	7, Nov, 2020 10:51:30
p h	75@qq.com	Portal	hucong	1260	Adding Device Succeeded	7, Nov, 2020 10:35:35
p h	75@qq.com	Portal	--	--	Login Succeeded	7, Nov, 2020 10:32:17
lulu	81@qq.com	Portal	--	--	Login Succeeded	6, Nov, 2020 23:55:57
lulu	81@qq.com	Portal	--	--	Login Succeeded	6, Nov, 2020 23:35:56
lulu	81@qq.com	Portal	83	D418	Remove Device from Health Monitoring Package Succeeded	6, Nov, 2020 21:41:26
lulu	81@qq.com	Portal	83	D418	Deleting Device Succeeded	6, Nov, 2020 21:41:25
lulu	81@qq.com	Portal	83	D418	Adding Device Succeeded	6, Nov, 2020 21:40:58
lulu	81@qq.com	Portal	--	--	Login Succeeded	6, Nov, 2020 21:39:36
lulu	81@qq.com	Portal	--	--	Login Succeeded	6, Nov, 2020 20:48:06
lulu	81@qq.com	Portal	83	D418	Deleting Device Succeeded	6, Nov, 2020 20:43:49
lulu	81@qq.com	Portal	83	D418	Adding Device Succeeded	6, Nov, 2020 20:43:12

Total 5976 Record(s) 20 / 299 Go

Figure 9-1 Search Operation Logs

Chapter 10 Tools

Hik-ProConnect provides tools, such as disk calculator and NVR channel calculator, to help you improve your work efficiency.

On the Home page, click  **Tools** or  **Tools** to enter your tools page.

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.

