# Hik-ProConnect Portal (for Europe)

## User Manual

# Legal Information

## About this Manual

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

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

## Trademarks

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

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

## Disclaimer

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

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

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE 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. |
| ℹ **Note** | Provides additional information to emphasize or supplement important points of the main text. |

# Contents

# Chapter 1 Introduction

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

Hik-ProConnect provides different ways/clients for Installers or end users to access the platform or manage resources.

- **Hik-ProConnect Portal:** Portal for Installer Admin and Installers logging into Hik-ProConnect to manage the security business, including permission and employees management, site management, devices management, and devices health monitoring, etc.
- **Hik-ProConnect Mobile Client:** Mobile Client for Installer Admin and Installers logging into Hik-ProConnect to manage site, apply for site information management permission from end user, manage and configure the devices, etc.
- **Hik-Connect Mobile Client:** Mobile Client for end users to manage their devices, accept the Installer's invitation as the site owner, approve the Installer's application of site information management permission, etc.

## 1.1 Target Audience

This manual provides the Installer 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) that 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.
- 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.
- 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$^{TM}$ 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.

# Chapter 2 Account Management

There are two types of accounts: Installer Admin and Installer. Each company has only one Installer Admin but can have multiple Installers.

**Installer Admin**

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

**Installer**

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

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

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

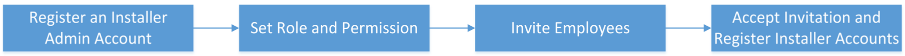

Register an Installer Admin Account
Set Role and Permission
Invite Employees
Accept Invitation and Register Installer Accounts

**Figure 2-1 Flow Chart of Account Management for Countries and Regions**

- **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 surveillance installation company should first register an Installer Admin account before accessing any functions of Hik-ProConnect.

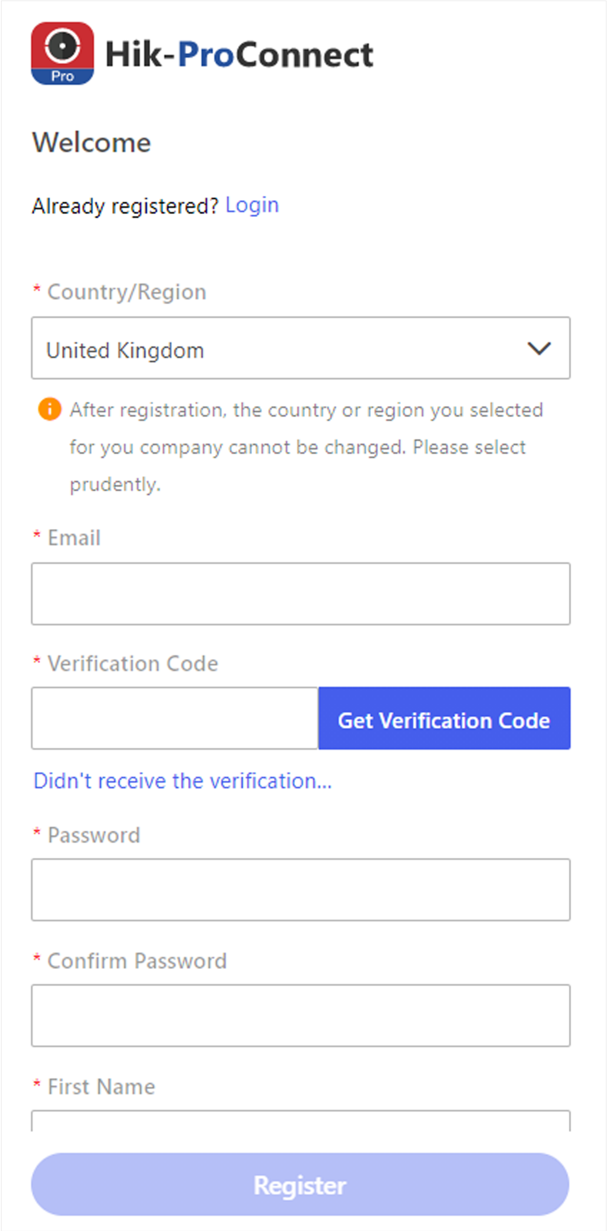
**Steps**

**Note**

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, click **Register for Free**.



Hik-ProConnect

Welcome

Already registered? Login

* Country/Region

United Kingdom

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

* Email

* Verification Code

Get Verification Code

Didn't receive the verification...

* Password

* Confirm Password

* First Name

Register

**Figure 2-2 Register an Installer Admin Account**

3. Select the country or region of your company.

**Note**

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

4. Enter an email address which will be bound with the Installer Admin account after registration.
5. Click **Get Verification Code** to get the verification code.

**Note**

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

An email which contains the verification code will be sent to the email address you entered in the previous step.

6. Enter the verification code you have received.
7. 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.

8. Enter your name and phone number.
9. Enter your company name.
10. **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*** .

11. **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.
12. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in these agreements.
13. Click **Register**.

    A registration confirmation email will be sent to the email address you entered in Step 4.
14. Click **Verify Now** in the email you received.

After verification completed, you enter the login page of Hik-ProConnect.

**Result**

You can log into Hik-ProConnect with this account, invite your employees to register Installer accounts, and perform other operations such as site management, etc.

**What to do next**

After registering an Installer Admin account, you can log into Hik-ProConnect with your account. You need to fill in the information of your company to bind with your account. For details, refer to ***Manage Company Information*** .

## 2.2 Manage Company Information

If you have entered authentication code when registering an Installer Admin account, you need to submit your company information (such as company name and address) for more available functions on the platform.

**Steps**

1. Enter the name of your company.
2. Enter other information of your company, such as address, postal code, phone number, etc.
3. **Optional:** Enter the website of your company if any.
4. Click **Submit**.

   After setting your company's information, you enter the Home page of the Hik-ProConnect Portal.
5. **Optional:** If you want to set VAT number, upload company's log, or edit the other information of your company, perform the following steps.
   1) In the Hik-ProConnect Portal, enter **Company → Company Information** .
   2) Click ✎ at the upper-left corner of the **Company Information** panel.
   3) Edit the information if needed, such as company name, phone number for contact, email for contact, etc.

      **Note**

      The country or region cannot be changed once selected when binding the company information after registration.
   4) **Optional:** Enter or edit VAT number of your company which will be used for qualification verification.
   5) **Optional:** Click **+** to upload a picture of the company's 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 Co-branding function if you didn't set your company's logo.
- After editing the logo, it will be updated to the Co-Branding page, which is for brand promotion to the end users. For details about co-branding settings, refer to ***Co-Branding*** .

6) **Optional:** Enter or edit the description information, which will be displayed on Hik-Connect Mobile Client.
7) Click **Save** to save the changes.

**6.** **Optional:** In the Company Information page, you can view the maximum number of manageable employees, the comparison about the supported functions and manageable devices between basic package and health monitoring package provided by Hik-ProConnect, and when the trial period will end.

**Free Package**

Package with up to 1,024 devices manageable (unlimited during trial period) and basic functions available (including adding devices in a batch, device firmware upgrade, site and device management, applying for site authorization, viewing device online status, remote configuration, and live view).

**Health Monitoring Package**

Package with unlimited manageable devices and advanced functions available (such as health monitoring, exception, linkage, role and permission management, employee management, viewing operation logs, co-branding, etc.).

The health monitoring package is still free during the trial period, and you need to pay for it after your free trial period ends if you still want to access the functions in this package and manage unlimited devices.

## 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 experience the features in Hik-ProConnect first, and authenticate your account later. For the account which is not authenticated, you cannot purchase value-added services. In this section, we introduce how to authenticate your Installer Admin account after registration.

**Note**

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

If you want to authenticate your account, one of the following ways is supported according to 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. (Optional) Click + to upload the picture of your business card.
4. Enter the distributor if you have ever bought Hikvision products.
5. 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**

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**

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.

**Note**

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

### Change Account's Bound Email

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

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

**Note**

- Deleting Installer Admin account is irreversible. The company information and accounts CANNOT be restored once deleted. Back up the required data before deleting the account.
- If there are authorized site(s) 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 verification 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 seven main modules. You can access these modules via the navigation panel on the left.

**Note**

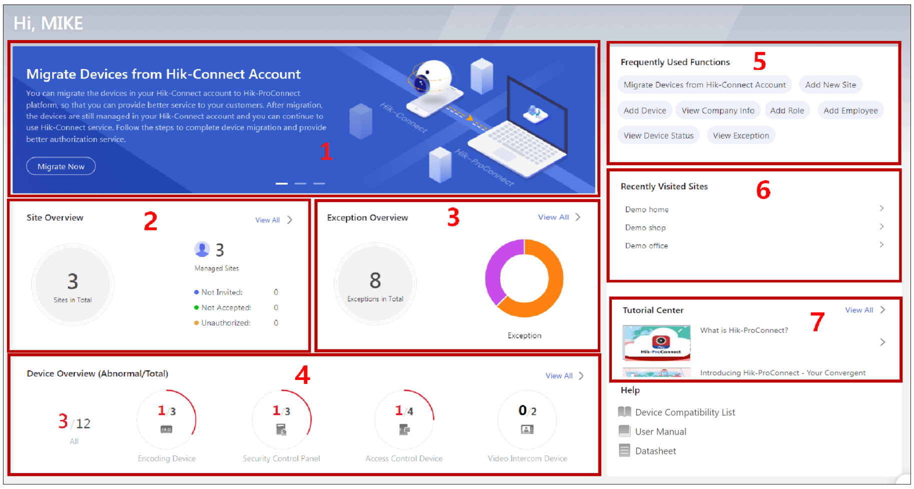
You can click ≡ or ☰ to pin or unpin the navigation panel on the left of the Portal.

**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. |
| 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:<br>• **Health Status:** Installer can view the devices overall, normal, and abnormal status, locate the abnormal devices, and perform troubleshooting quickly.<br>• **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:<br>• **Company Information:** You can manage your company information.<br>• **Co-Branding:** Enable to display the company logo on the Hik-Connect Mobile Client for brand promotion to the end users. |

| Module | Description |
|---|---|
| | • **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.<br>• **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.<br>• **Operation Log:** View the operation logs of your accounts and sites in the current company. |
| Business | • **Service Market:** Hik-ProConnect provides value-added services and you purchase these service packages or renew them.<br>• **My Service:** View all services you purchased and the details, such as free package and cloud storage service package.<br>• **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



Hi, MIKE

Migrate Devices from Hik-Connect Account

You can migrate the devices in your Hik-Connect account to Hik-ProConnect platform, so that you can provide better service to your customers. After migration, the devices are still managed in your Hik-Connect account and you can continue to use Hik-Connect service. Follow the steps to complete device migration and provide better authorization service.

**Figure 4-1 Home Page**

**Table 4-2 Home Page Description**

| No. | Name | Introduction |
|---|---|---|
| 1 | Banner | There are some banners, showing the key features, functions, and important information of Hik-ProConnect.<br>**Note**<br>You can inform your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later) by sending the QR code or download link to them. |
| 2 | Site Overview | You can view the number of sites managed in total. Besides, you can view:<br>• **Not Invited:** The number of sites for which no site owners are invited.<br>• **Not Accepted:** The number of sites of which the site owner invitation are not accepted.<br>• **Unauthorized:** The number of sites which are not authorized to you.<br>**Note**<br>You can click › to enter the site list. For detailed instructions about site management, refer to ***Site Management*** . |
| 3 | Exception Overview | You can view the number of received exceptions and the proportions of each type of the exceptions.<br>Hover the cursor to the pie chart to view the detailed proportions and amount.<br>**Note**<br>You can click **View All Exceptions** to enter **Exception Center** to check the received exceptions. For detailed instructions about Exception Center, refer to ***Exception Center*** . |
| 4 | Device Overview | You can view the number of abnormal devices and total devices, including devices overall and each device type respectively.<br>**Note**<br>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 Specific Site*** . |

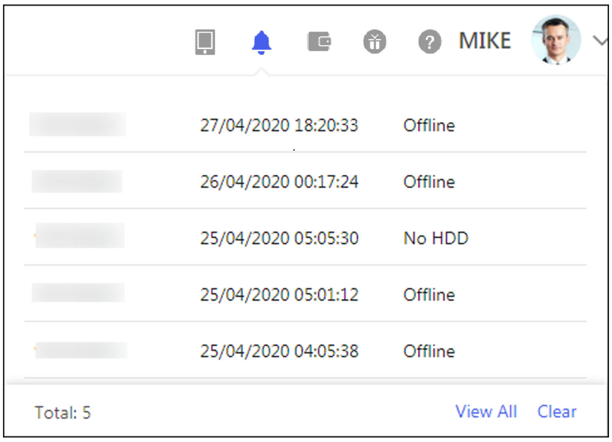
| No. | Name | Introduction |
|---|---|---|
| 5 | Frequently Used Functions | You can view the functions which you have used frequently. Click these icons to perform these functions quickly if needed. |
| 6 | Recently Visited Sites | You can view the five sites which you visited recently.<br>Click the site name to enter the site details page. |
| 7 | Tutorial Center | You can view video tutorials to learn more about Hik-ProConnect and the proper ways of using the platform.<br>Click a video to open a webpage and start playing the video. Click **View All** to view all the videos in Tutorial Center. |

### 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.



| | | |
|---|---|---|
| [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

**Figure 4-2 Recently Received Exceptions**

**Note**

You need to set the device's exception rules first before the Portal can receive the notifications. For details, refer to ***Add Exception Rule*** .

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.
On the Home page, click the name at the upper-right corner and select **Feedback** to open the Feedback window.

Or click icon floating on the Home page to open the Feedback window.
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**, **Datasheet**, or

**Device Compatibility List** at the lower-right corner of the Home page to open the user manual, datasheet, or device compatibility list.

You can enter keywords to search the information you want in the user manual, datasheet, 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 Co-Branding

This function helps promote awareness of your brand and strengthens your products and services. After enabled, end users can view your company logo, address, and phone number via Hik-Connect Mobile Client.

On the Home page, click **Company → Co-Branding** . Switch **Co-Branding** on, and hover the cursor on the Logo area to show the **Edit** button. Click **Edit** to upload your company logo. After editing the logo, it will be updated to the Company Information page.

**Note**

- Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page to them.
- If all the devices of an end user are managed by the same installation company, the installation company's logo will be displayed on the login page and About page of the end user's Hik-Connect account.
- If an end user's devices are managed by different installation companies, he or she can go to the device details page of Hik-Connect account to view the companies' logo and details.

# Chapter 6 Site Management

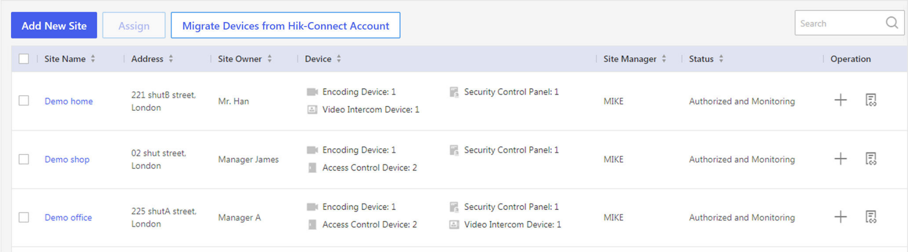
A site can be regarded as an area or location with actual time zone and address, such as the end user's home, office, etc. The Installer can add the authorized devices of end user to the site and uses the site to manage and configure the devices remotely.

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.

## 6.1 Site Page Overview

On the Site page, you can view the sites that are assigned to you (the Installer Admin as well as Installers with Manage All Sites permission can view all the sites of the company), and perform some operations for the sites, such as searching site, adding site, 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 |
|---|---|---|---|---|---|---|---|---|
| □ | Demo home | 221 shutB street, London | Mr. Han | Encoding Device: 1<br>Video Intercom Device: 1 | Security Control Panel: 1 | MIKE | Authorized and Monitoring | + |
| □ | Demo shop | 02 shut street, London | Manager James | Encoding Device: 1<br>Access Control Device: 2 | Security Control Panel: 1 | MIKE | Authorized and Monitoring | + |
| □ | Demo office | 225 shutA street, London | Manager A | Encoding Device: 1<br>Access Control Device: 2 | Security Control Panel: 1<br>Video Intercom Device: 1 | MIKE | Authorized and Monitoring | + |

**Figure 6-1 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 6-1 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 ***Migrate Devices from Hik-Connect Account*** for details about how to migrate devices from Hik-Connect account to Hik-ProConnect.

## 6.2 Add New Site

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

**Before You Start**

Make sure you have the permission of adding 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, site address, city, and state/province/region.

**Note**

You should select the correct time zone where the devices locate and the time zone cannot be changed after the site is added.

4. **Optional:** Check **Sync Time & Time Zone to Device** to synchronize the time and time zone of the site to the devices added to the site.
5. Click **OK** to add a new site to the list.
6. **Optional:** According to the site's status and authorization, perform one of the following operations.

**Note**

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

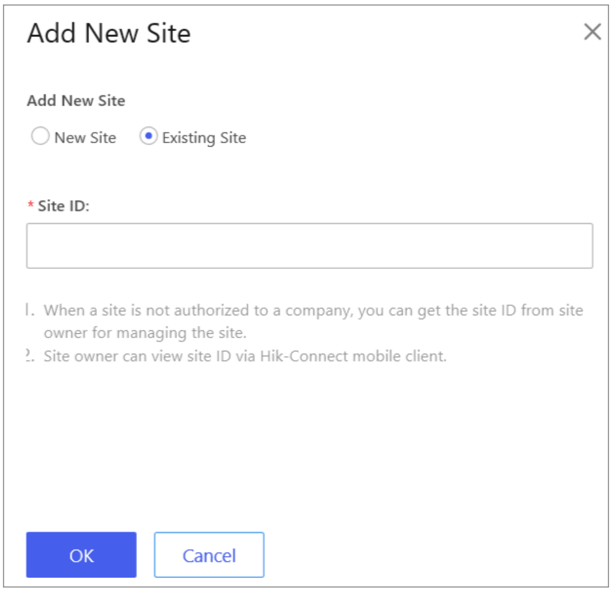
For more details, refer to ***Manage Device*** .

## 6.3 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**.



Add New Site

Add New Site

○ New Site ● Existing Site

* Site ID:

1. When a site is not authorized to a company, you can get the site ID from site owner for managing the site.
2. Site owner can view site ID via Hik-Connect mobile client.

**Figure 6-2 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 (Version 4.7.1 and 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 by the Installer.

## 6.4 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.

## 6.5 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**

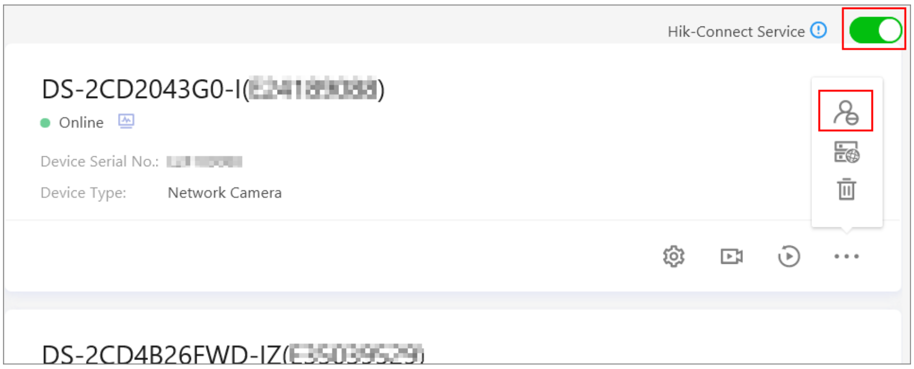
Make sure the site status is **Not Invited** and you have the permission of site management, such as Manage All Sites and Manage Assigned Site.

**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**. Then after handing over the site to end user, you can disable Hik-Connect service for the devices and the end user cannot perform device operations via Hik-Connect Mobile Client.

   **Note**

   When this function is enabled and the site is handed over, if required, you can enter Site Details page and click **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 end user's Hik-Connect account without authorization of end user.



Hik-Connect Service

DS-2CD2043G0-I([redacted])

Online

Device Serial No.: [redacted]

Device Type: Network Camera

DS-2CD4B26FWD-IZ([redacted])

**Figure 6-3 Disable Hik-Connect Service**

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. Enter the remarks, such as the reason of the invitation, which the invitee can view when he/she receives the invitation via Hik-Connect Mobile Client.
9. 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 (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page to them.

- If there are maintenance requirements for the devices added in Hik-Connect Mobile Client, but not added and managed in the site, after the end user accepts the invitation and becomes the Site Owner, he/she can authorize the permissions about these devices to the Installer.

10. **Optional:** Before the end user 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.

## 6.6 Apply for Site Authorization from Site Owner

When the site (no permissions selected when inviting Site Owner) has been handed over to Site Owner, and then there are maintenance requirements for the devices in the site, the Installer needs to send an application to Site Owner for the authorization. After the authorization is approved, the Installer can get the permission to manage and configure the devices of the site. Besides this, the Site Owner can add a device on Hik-Connect Mobile Client and authorize it to the Installer for further management and configuration.

**Steps**

1. Click **Site** tab 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 (Version 4.7.1 and 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.
- For more details about operations on Hik-Connect Mobile Client, refer to the User Manual of Hik-Connect Mobile Client.

5. **Optional:** Click the site name to enter Site Details page and apply for permissions.

# Chapter 7 Manage Device

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 required settings, including remotely configuring device parameters, configuring exception rule, linkage rule, people counting, temperature screening, etc.

**Note**

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

## 7.1 Add Device

Three ways for adding devices to site are provided. 1. Add detected online devices. 2. Add devices by Hik-Connect (P2P). 3. Add a single device or import multiple devices in a batch by device IP address or domain name.

### 7.1.1 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 7-1 Step Description**

| Step | Description |
|---|---|
| Activate Device | If there are inactivated device(s), activate them. See ***Activate Device*** for details.<br>**Note**<br>During activation, Dynamic Host Configuration Protocol (DHCP) will be automatically enabled for allocating IP addresses for the device. After activation, you can click ✎ at the Operation Column of the online device list to manually disable DHCP if required. |
| Enter Device Password | Enter admin password of the device. See ***Enter Device Password*** for details. |
| Automatically Connect to Hik-Connect Service | Connect device(s) to the Hik-Connect service. See ***Connect to Hik-Connect Service*** for details. |
| Automatically Get Device Verification Code | If a device is connected to the Hik-Connect service successfully, the system will automatically get device verification code from device.<br>See ***Get Device Verification Code*** for details. |

**Note**

- 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.

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

**Table 7-2 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.<br>ⓘ **Note**<br>For details, see ***Add Custom Linkage Rule*** . |
| Enable Health Monitoring Service | Turn on Health Monitoring Service switch to enable Health Monitoring service for the device.<br>ⓘ **Note**<br>• Make sure device capacity of the Health Monitoring package you purchased is enough, or this function will be unavailable.<br>• Health Monitoring service is not available in every country and region.<br>• For details about Health Monitoring service, see ***Health Monitoring Service*** . |
| Delete Device | Click ⋯ → 🗑 to delete the device.<br>ⓘ **Note**<br>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.<br>For devices incompatible with the Hik-ProConnect, you need to upgrade them.<br>1. Select **Upgrade to Compatible Version** on the **Upgrade or Not** column, and click **Add and Upgrade**.<br>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 ***Unbind Device from Its Current Account*** . |

### Activate Device

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

**Note**

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

### Enter Device Password

For devices which are activated but not connected to the Hik-Connect service, you should enter its admin password on the pop-up window. The admin password is created when you activate the device.

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

**Note**

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

### Connect to Hik-Connect Service

After entering device admin passwords, the system 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.

### Get Device Verification Code

If a device is connected to the Hik-Connect service successfully, the system will automatically get device verification code from device. If the system failed to get the verification codes from any devices, these devices will show for you 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.

**Note**

For EZVIZ devices, admin password is nor required, and device verification code is required.

## 7.1.2 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.
- The device should have 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.

   **Note**

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

   **Note**

   Hik-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.

**Note**

By default, the **Enable Health Monitoring Service** will be checked and cannot be edited. For devices with health monitoring service disabled, you cannot upgrade device firmware, set linkage rules (the existing linkage rules will be invalid), set and receive exceptions, and check device health status.

7. Click **Add**.

**Note**

- 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.

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

| | |
|---|---|
| **Edit Device Name** | Click the device name to edit it.<br>Or move the cursor to the device and then click ✎ to edit it. |
| **Delete Device** | Click ··· → 🗑 . |
| **Upgrade Device** | Refer to ***Upgrade Device Firmware*** . |
| **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. |

| | |
|---|---|
| **Enable Health Monitoring Service** | Turn on Health Monitoring Service switch to enable Health Monitoring service for the device.<br>**Note**<br>• Make sure device capacity of the Health Monitoring package you purchased is enough, or this function will be unavailable.<br>• Health Monitoring service is not available in every country and region.<br>• For details about Health Monitoring service, see ***Health Monitoring Service*** . |
| **Configure Cloud Storage Service** | For Hik-ProConnect Box and cloud storage DVR, you can click **Cloud Storage Service** to configure Cloud Storage Service. See ***Set Cloud Storage for Hik-ProConnect Box*** and ***Set Cloud Storage for Cloud Storage DVR*** for details. |

**Note**

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

### 7.1.3 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 the Hik-ProConnect by specifying its IP address/domain name, user name, password, etc.

**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**

Only encoding devices mapped in WAN support this function.

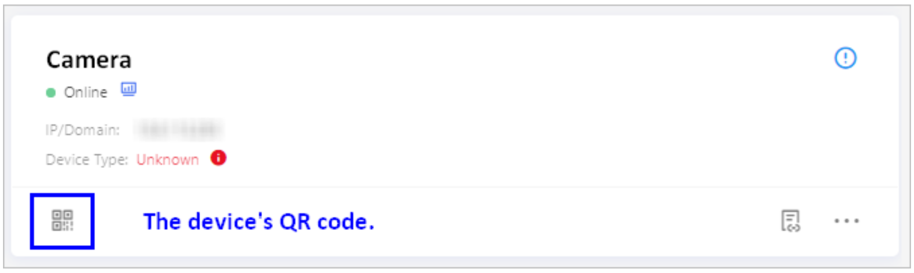
1. Click **Site** on the left to show the site list.
2. Open the Manual Adding page.
   - Click + in the Operation column of the site list and then select **Manual Adding**.
   - Click the site name to enter the site details page, and then go to **Device → Add Device → Manual Adding** .
3. Select **IP/Domain** 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**.
6. **Optional:** Perform the following operations if you need.



Camera

● Online

IP/Domain: [redacted]

Device Type: Unknown

The device's QR code.

**Figure 7-1 The QR Code of the Added Device**

| **Operations** | Description |
|---|---|
| **Encrypt Device QR Code** | A QR code will be generated and displayed in the device information area. If an end user did not add the device to his/her Hik-Connect account, he/she can add it to the Hik-Connect account by scanning this QR code using Hik-Connect Mobile Client.<br>a. Click ▦ to display the QR code.<br>b. Enter a password to encrypt the QR code, and then click **Save**. |
| **View and Edit Device Information** | Click the device's IP address or domain name to view the device basic information. If the device's information changed, or a network exception occurs, you can edit its information accordingly.<br>Select a device, and click • • • → ✎ to edit the device's name, IP address/domain name, port number, user name, and password. |
| **Set Type for Unknown Device** | If the Hik-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. |
| **Enable Health Monitoring Service** | Turn on Health Monitoring Service switch to enable Health Monitoring service for the device. |

| | |
|---|---|
| | **Note**<br>• Make sure device capacity of the Health Monitoring package you purchased is enough, or this function will be unavailable.<br>• Health Monitoring service is not available in every country and region.<br>• For details about Health Monitoring service, see ***Health Monitoring Service*** . |
| **Delete Device** | Click ••• → 🗑 . |

**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 (Version 4.7.1 and 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).

### 7.1.4 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**

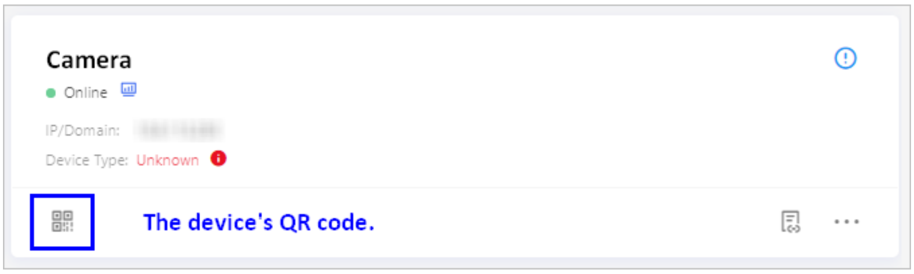
**Note**

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.



The device's QR code.

**Figure 7-2 The QR Code of Added Device**

| **Operations** | Description |
|---|---|
| **Encrypt Device QR Code** | A QR code will be generated and displayed in the device information area. If an end user did not add the device to his/her Hik-Connect account, he/she can add it to the Hik-Connect account by scanning this QR code using Hik-Connect.<br>a. Click ▦ to display the QR code.<br>b. Enter a password to encrypt the QR code, and then click **Save**. |
| **View and Edit Device Information** | Click the device's IP address or domain name to view the device basic information. If the device's information changed, or a network exception occurs, you can edit its information accordingly.<br>Select a device, and click ● ● ● → ✎ to edit the device's name, IP address/domain name, port number, user name, and password. |
| **Set Type for Unknown Device** | If the Hik-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. |
| **Delete Device** | Click ● ● ● → 🗑 . |

**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 (Version 4.7.1 and 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).

## 7.2 Apply for Device Permission

After handing over a site to the end user, if you need to view the live view/recorded videos of devices added to the site or configure the devices added to the site, you can apply for the permission accordingly from the end user.

**Steps**

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

**Note**

You can select **Permanent**, **1 Hour**, **2 Hours**, **4 Hours**, or **8 Hours** as the validity period.

5. **Optional:** Enter the remarks for the permission.
6. Click **Apply** to apply for the permission from end user.

   If the end user approves your application, you will get corresponding permission(s).

## 7.3 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 area, select a permission, and click 🔗 → **OK** to release the permission.

**Note**

- After releasing, the permission will be unavailable for you. You need to apply for it again if needed.
- You do not have to release permission if the permission validity is **Permanent**.

## 7.4 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 meed to migrate devices from Hik-Connect account to Hik-ProConnect.

- **Case 1**: Before using Hik-ProConnect, you managed the devices for the end user by Hik-Connect Mobile Client after the end user 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 end users 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.

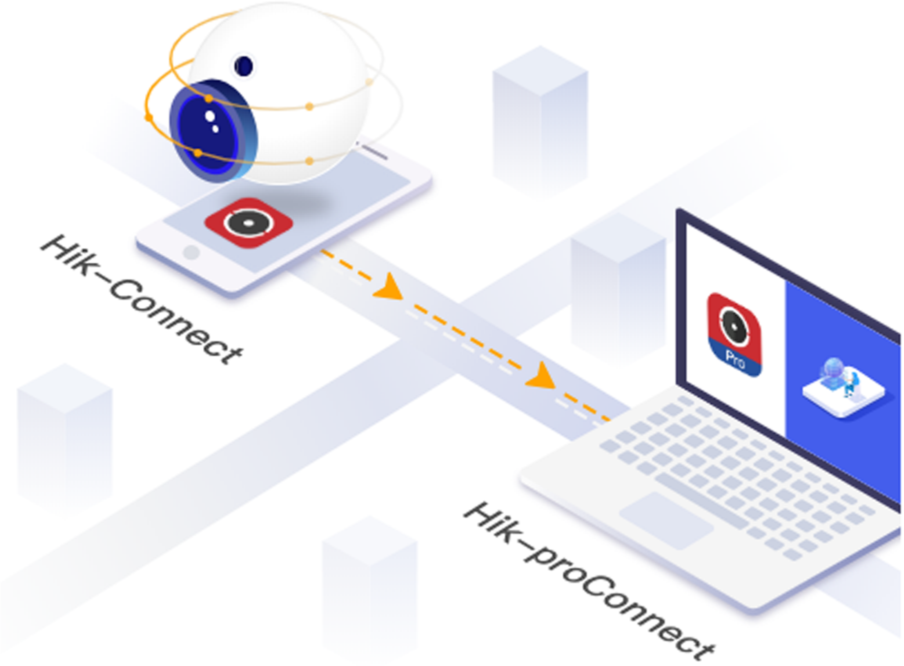


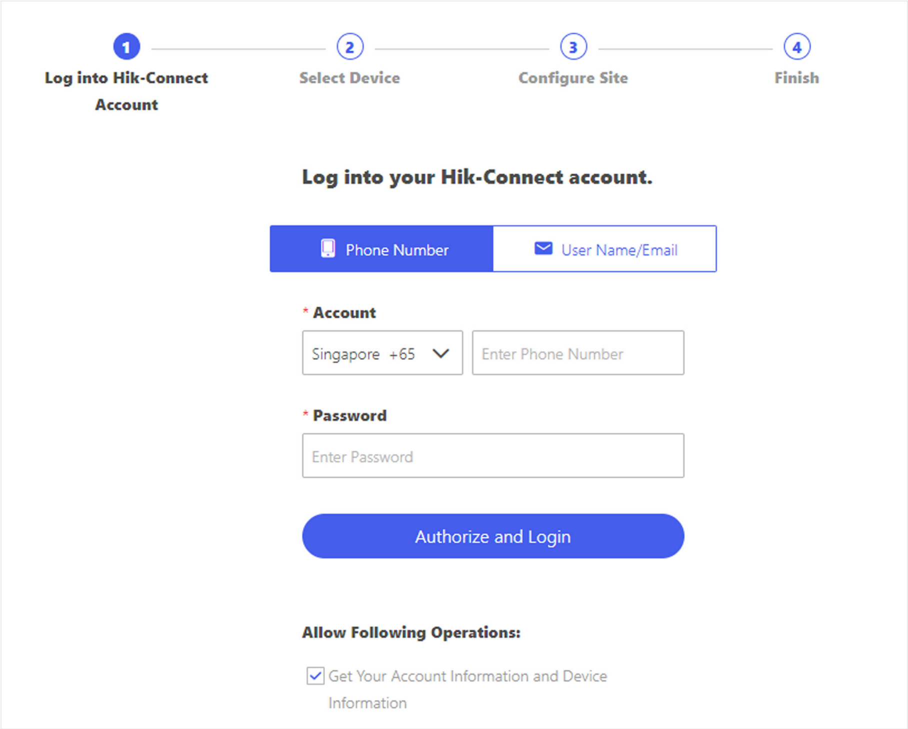
**Figure 7-3 Migrate Devices from Hik-Connect Account to Hik-ProConnect**

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.



Log into your Hik-Connect account.

* Account

Singapore +65 | Enter Phone Number

* Password

Enter Password

Allow Following Operations:

☑ Get Your Account Information and Device Information

Figure 7-4 Log into Hik-Connect Account

You can login by phone number or user name (or email address).

Check **Get Your Account Information and Device Information** to allow Hik-ProConnect to get these information, and 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.

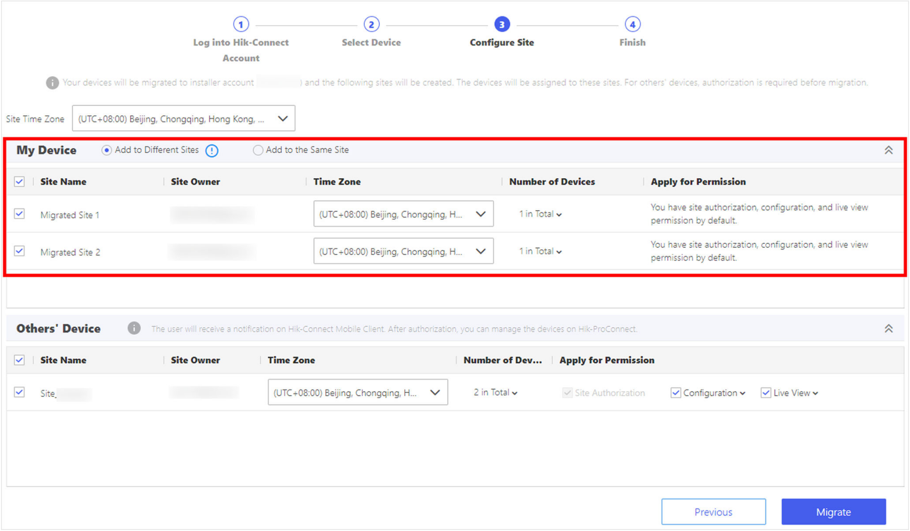
You can filter the devices by selecting **Show All Devices**, **Show My Devices Only** (the devices added to your Hik-Connect account), or **Show Others' Devices Only** (the devices shared to your Hik-Connect account from the end user) in the drop-down list.

Select the devices you want to migrate to the 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.



Your devices will be migrated to installer account [redacted] ) and the following sites will be created. The devices will be assigned to these sites. For others' devices, authorization is required before migration.

Site Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, ...

**My Device** ● Add to Different Sites ○ Add to the Same Site

| ☑ Site Name | Site Owner | Time Zone | Number of Devices | Apply for Permission |
|---|---|---|---|---|
| ☑ Migrated Site 1 | [redacted] | (UTC+08:00) Beijing, Chongqing, H... | 1 in Total | You have site authorization, configuration, and live view permission by default. |
| ☑ Migrated Site 2 | [redacted] | (UTC+08:00) Beijing, Chongqing, H... | 1 in Total | You have site authorization, configuration, and live view permission by default. |

**Others' Device** The user will receive a notification on Hik-Connect Mobile Client. After authorization, you can manage the devices on Hik-ProConnect.

| ☑ Site Name | Site Owner | Time Zone | Number of Dev... | Apply for Permission |
|---|---|---|---|---|
| ☑ Site_[redacted] | [redacted] | (UTC+08:00) Beijing, Chongqing, H... | 2 in Total | ☑ Site Authorization ☑ Configuration ☑ Live View |

Figure 7-5 Configure Site for My Devices

### Add to Different Sites

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

For the devices which have been shared to the end users, the system will automatically create sites by the user names of the end users, and then add the devices to these sites. If there already exists a site the Site Owner of which is the end user, 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

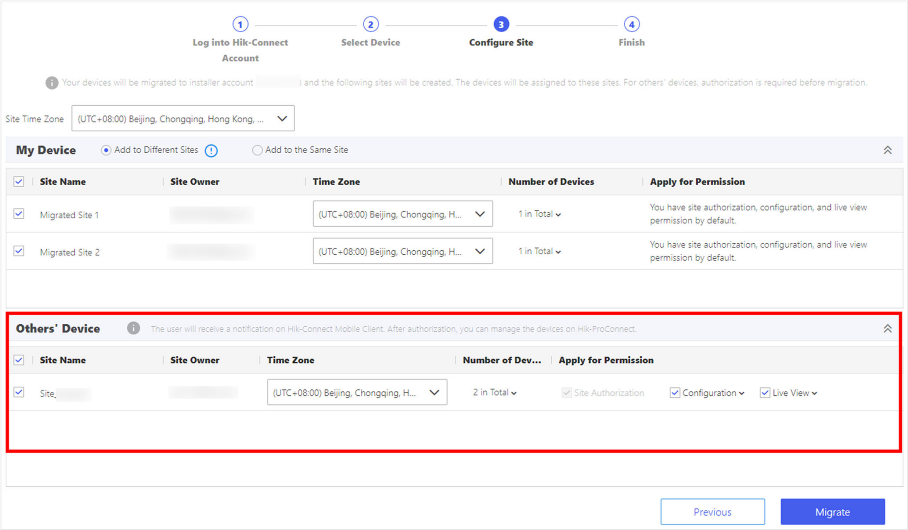
You can also add these devices to the same site. The system will automatically create a site named after your Hik-Connect account user name, and then add all these selected devices to this site.

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.



Your devices will be migrated to installer account [redacted]) and the following sites will be created. The devices will be assigned to these sites. For others' devices, authorization is required before migration.

Site Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, ...

**My Device** ● Add to Different Sites ○ Add to the Same Site

| ☑ Site Name | Site Owner | Time Zone | Number of Devices | Apply for Permission |
|---|---|---|---|---|
| ☑ Migrated Site 1 | [redacted] | (UTC+08:00) Beijing, Chongqing, H... | 1 in Total | You have site authorization, configuration, and live view permission by default. |
| ☑ Migrated Site 2 | [redacted] | (UTC+08:00) Beijing, Chongqing, H... | 1 in Total | You have site authorization, configuration, and live view permission by default. |

**Others' Device** The user will receive a notification on Hik-Connect Mobile Client. After authorization, you can manage the devices on Hik-ProConnect.

| ☑ Site Name | Site Owner | Time Zone | Number of Dev... | Apply for Permission |
|---|---|---|---|---|
| ☑ Site_[redacted] | [redacted] | (UTC+08:00) Beijing, Chongqing, H... | 2 in Total | ☑ Site Authorization ☑ Configuration ☑ Live View |

**Figure 7-6 Configure Site and Permissions for Others' Devices**

For the devices shared to you by others, usually end users, (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 end users, and then add all these selected devices to this site. If there already exists a site the Site Owner of which is the end user, 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 end users for the devices. By default, you will have site authorization permission of the automatically created site(s). After migration, the end users will receive a notification on Hik-Connect Mobile Client. After authorization by the end users, 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 end users in Others' Devices list, the system will send a request to the end users. After the end users 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.

## 7.5 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 pre-defined template or customize a rule to define such a linkage. The rule contains five elements, including Source (resource A), Triggering Event (the event detected by device A), Linked Resources ( resource B, resource C, resource D... ), Linkage Actions (actions of resource B, resource C, resource D... ), as well as Linkage Schedule (the scheduled time during which the linkage is activated). The linkages can be used for purposes such as notifying security personnel, upgrading security level, saving evidence, etc., when specific events happen.

The picture below shows the process of the linkage.

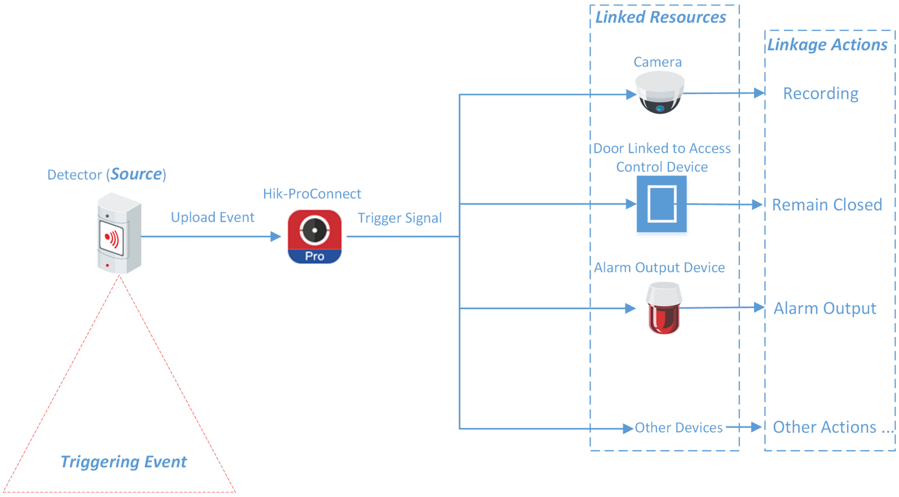


**Figure 7-7 Linkage**

**Example**

Sample Application

Assume that the end user is the manager of a jewelry store, and the store needs to upgrade security level during non-work hours. And the store has been installed with a PIR detector linked to a security control panel, a siren linked to the security control panel, and several network cameras. In this case, you can set a linkage rule for him/her to trigger alarm output and recording in the store when object(s) in motion are detected in the store during non-work hours. The followings should be defined in the linkage rule:

- Source: The PIR detector in the store.
- Triggering Event: Motion detection event.
- Linked Resources: The alarm output (the siren in this case) and the network cameras in the store.
- Linkage Actions:

- For siren: The triggering of the alarm output (i.e., the siren) sends out audible alarm.
- For network cameras: The network cameras starts recording.

- Linkage Schedule: Non-work hours every day.

### 7.5.1 Add Custom Linkage Rule

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

**Steps**

**Note**

- If the trial period of your account expires, the added linkage rule(s) will remain for 3 months but the linkage will not be activated. After 3 months, the linkage rule(s) will be cleared.
- 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 Axiom 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 7-3 Available Triggering Events for Different Resource Types**

| Resource | Triggering Event |
|---|---|
| Camera | • Motion Detection<br>• Face Detection<br>• Intrusion<br>• Line Crossing Detection |
| Access Control Device | • Tampering Alarm |
| Door Linked to Access Control Device | • Door Opened Abnormally<br>• Tampering Alarm |
| Door Station | • Calling |
| Area of Security Control Panel | • Away Arming<br>• Disarmed<br>• Stay Arming<br>• Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm. |
| Zone (Detector) Linked to Security Control Panel | • Alarm, such as Triggering Alarm, such as Instant Zone Alarm, 24-Hour Annunciating Zone Alarm, and Delayed Zone Alarm. |
| Doorbell | • Calling<br>• PIR Detection |

**Linkage**

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

**Note**

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

**Linkage Action**

Select linkage action(s).

**Table 7-4 Linkage Action Description**

| Linked Resource | Linkage Action | Description |
|---|---|---|
| Camera (Channel) | Capture | The camera will capture a picture when the Triggering Event is detected. |
| | Recording | The camera will record video footage when the Triggering Event is detected.<br>**Note**<br>The recorded video footage starts from 5 s before the detection of the Triggering Event, and lasts 30 s. |
| | Call Preset | Select a preset from the Preset drop-down list to specify it as the preset which will be called when the Triggering Event is detected.<br>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.<br>**Note**<br>Make sure you have configured presets for the PTZ camera. For details, see the user manual of the PTZ camera. |
| | Call Patrol | Select a patrol from the Patrol drop-down list to specify it as the patrol which will be called when the Triggering Event is detected.<br>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.<br>**Note**<br>Make sure you have configured patrols for the PTZ camera. For details, see the user manual of the PTZ camera. |

| Linked Resource | Linkage Action | Description |
|---|---|---|
| | Call Pattern | Select a pattern from the Pattern drop-down list tot specify it as the pattern which will be called when the Triggering Event is detected.<br>A pattern is a predefined PTZ movement path with a certain dwell-time configured for a certain position. By calling a pattern, the PTZ camera moves according the predefined path.<br>**Note**<br>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.<br>**Note**<br>Make sure you have configured privacy mask for the camera. For details, see the user manual of the camera. |
| | Disable Privacy Mask | Privacy mask will NOT be displayed on the live images of the camera when the Triggering Event is detected. |
| Alarm Output | Alarm Output | The alarm output of the Linked Resource will be triggered when the Triggering Event is detected. |
| Area of Security Control Panel | Stay Arm | The arming status of the area of the security control panel will switch to Stay when the Triggering Event is detected. |
| | Away Arm | The arming status of the area of the security control panel will switch to Away when the Triggering Event is detected. |
| | Disarm | The area of the security control panel will be disarmed when the Triggering Event is detected. |

| Linked Resource | Linkage Action | Description |
|---|---|---|
| Door Linked to Access Control Device | Open Door | The door related to the access control device will be opened when the Triggering Event is detected. |
| | Remain Open | The door related to the access control device will remain open when the Triggering Event is detected. |
| | Remain Closed | The door related to the access control device will remain closed when the Triggering Event is detected. |
| Door Station | Open Door | The door linked to the door station will be automatically opened when the Triggering Event is detected. |
| Alarm Input | Arm Alarm Input | The alarm input will be armed and hence events related to it will be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected. |
| | Disarm Alarm Input | The alarm input will be disarmed and hence events related to it will NOT be uploaded to the Hik-Connect Mobile Client when the Triggering Event is detected. |

**Linked Resource**

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

**Note**

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

**Note**

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

**Linkage Schedule**

Define the scheduled time during which the linkage is activated.

**All Days**

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

**Custom**

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

**Note**

The date(s) marked blue is selected.

4. Click **OK**.

   The linkage rule will appear on the Linkage Rule list.

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

| | |
|---|---|
| **Edit Linkage Rule** | Click ⋯ → ✎ to edit the linkage rule. |
| **Delete Linkage Rule** | Click ⋯ → 🗑 to delete the linkage rule. |
| **Disable Linkage Rule** | Set ● to ○ to disable the linkage rule. |

**What to do next**

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

**Note**

- If the Notification functionality of the Source is disabled, the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not.
- Please notify the end user after handing over the site to him/her that notification of the Source should be kept enabled on the Hik-Connect Mobile Client, or the Linkage Action will NOT be activated no matter the Triggering Event is detected by Source or not. For details about enabling alarm notification for a specific device or channel, see the *Hik-Connect Mobile Client User Manual*.
- Please notify your end users to download or update the Hik-Connect Mobile Client (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

## 7.5.2 Add Linkage Rule Based on Pre-defined Template

You can use six pre-defined templates to add linkage rules, including Intrusion, Forced Entry Alarm, Back to Home/Office, Away, Visitor Calling, and Perimeter Zone Alarm. Each of the six templates is designed for a typical applications (see the list below) of linkage rule.

**Before You Start**

You should have the permission for the configuration of the devices. Or you should apply for the permissions first. For details about applying for permission, see ***Apply for Device Permission*** .

**Table 7-5 Template Description**

| Template | Description |
|---|---|
| Intrusion | The Intrusion Template: Used for improving security level by triggering the linkage actions including capture, recording, and alarm output, |

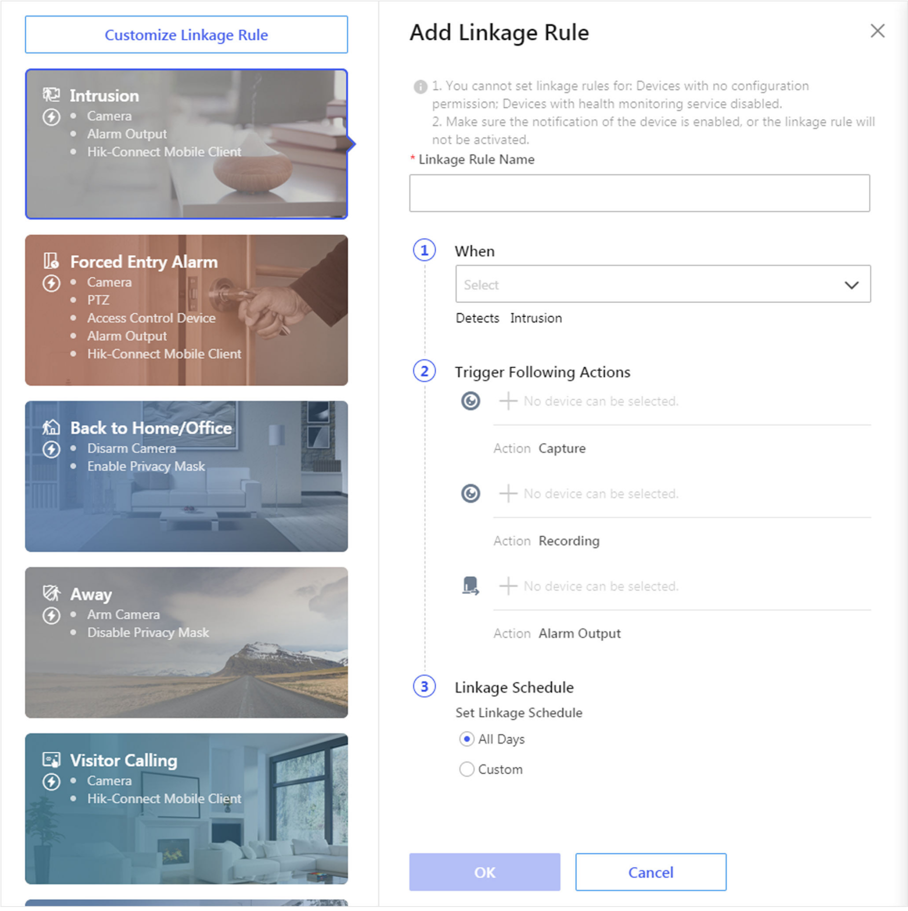
| Template | Description |
|---|---|
| | when the intrusion event (people, vehicles, or other objects enter a pre-defined area) occurs. |
| Forced Entry Alarm | The Forced Entry Alarm Template: Used for improving security level by triggering the linkage actions including capture, recording, remaining door closed, alarm output, and calling preset when line crossing detection (people, vehicles, or other objects cross a pre-defined virtual line) occurs. |
| Back to Home/Office | The Back to Home/Office Template: Used for lowering the security level and enabling privacy protection by triggering the linkage actions including disarming and enabling privacy mask, when you are back to home or office. |
| 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.



Add Linkage Rule

1. You cannot set linkage rules for: Devices with no configuration permission; Devices with health monitoring service disabled.
2. Make sure the notification of the device is enabled, or the linkage rule will not be activated.

* Linkage Rule Name

1 When

Select

Detects Intrusion

2 Trigger Following Actions

No device can be selected.

Action Capture

No device can be selected.

Action Recording

No device can be selected.

Action Alarm Output

3 Linkage Schedule

Set Linkage Schedule

● All Days

○ Custom

**Figure 7-8 Add Linkage Rule by Template**

**3.** Set the required information.

**Linkage Rule Name**

Create a linkage rule name.

**When**

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

**Trigger the Following Actions**

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

**Note**

- You can set only one linkage action.
- For details about the linkage actions, see ***Table 7-4*** .

**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 (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page to them.

### 7.5.3 Video Tutorial

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

## 7.6 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).

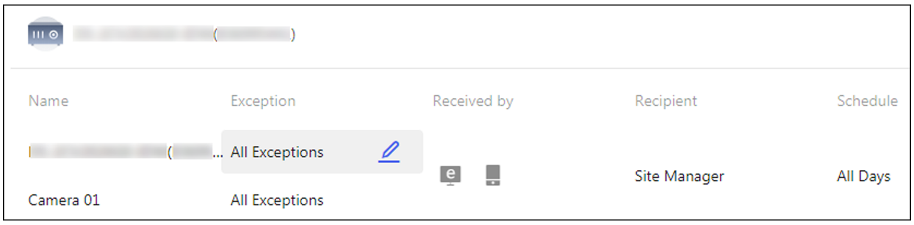
### Steps

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 ✎ .



[redacted]([redacted])

| Name | Exception | Received by | Recipient | Schedule |
|---|---|---|---|---|
| [redacted]([redacted]... | All Exceptions ✎ |  | Site Manager | All Days |
| Camera 01 | All Exceptions |  |  |  |

**Figure 7-9 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.

   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.

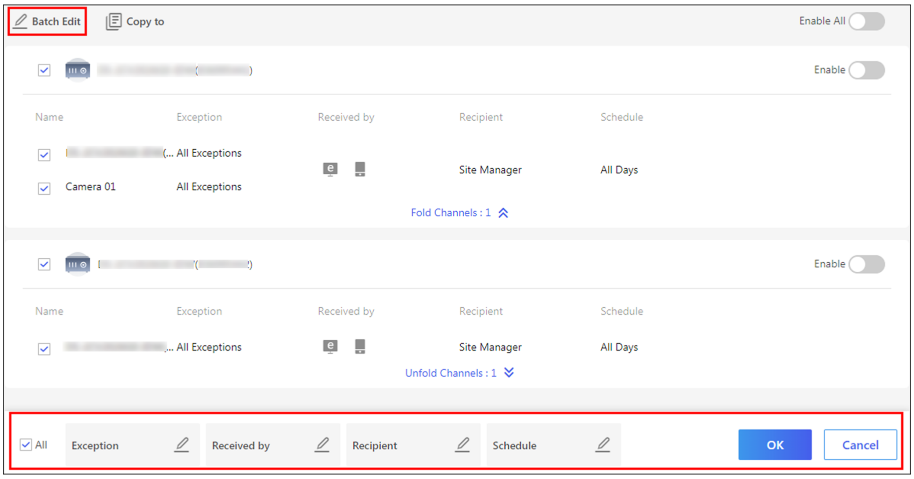
**Custom**

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.



☑ [redacted]

| | Name | Exception | Received by | Recipient | Schedule |
|---|---|---|---|---|---|
| ☑ | [redacted] | All Exceptions | | Site Manager | All Days |
| ☑ | Camera 01 | All Exceptions | | | |

☑ [redacted]

| | Name | Exception | Received by | Recipient | Schedule |
|---|---|---|---|---|---|
| ☑ | [redacted] | All Exceptions | | Site Manager | All Days |

**Figure 7-10 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.

## 7.7 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 (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page to them.

## 7.8 People Counting

The people counting function provided by the people counting camera is used to calculate the number of people entering, exiting, or passing by an area. After adding people counting cameras to the sites of Hik-ProConnect, you can integrate the people counting capabilities of these cameras together to implement real-time monitoring of the people density within a specific region. This is useful for certain commercial and health protection scenarios, such as limiting the customer flow of a shopping mall during the promotion period.

**Note**

- People counting related functionality is not available in specific countries and regions.
- People density here refers to the amount of people staying within a limited region at the same time.

## 7.8.1 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 the select **People Counting** tab.

   The people counting cameras will be displayed in the Device area.
3. Click › to open the device panel.

   The channel(s) of the device will be displayed on the panel.
4. Click **Activate** to open the Activate People Counting Service window.
5. Enter the user name and password of the admin account of the device.
6. Click **OK** to activate people counting service for the channel.

## 7.8.2 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.

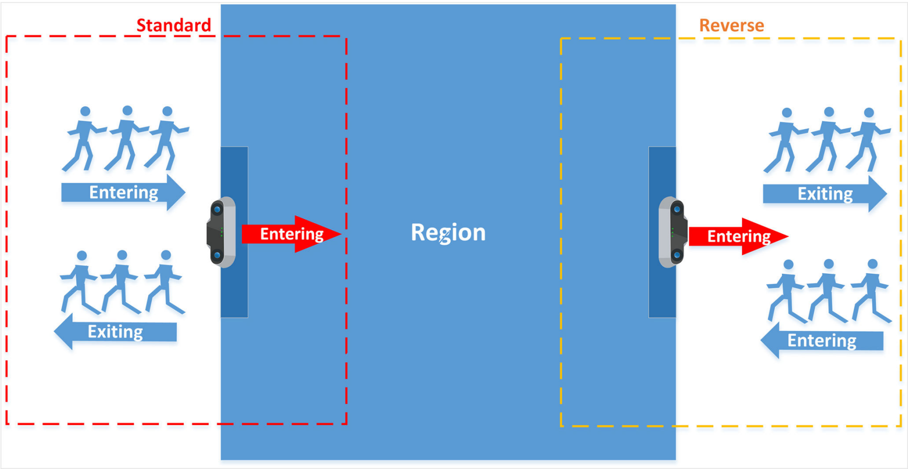


**Figure 7-11 Calculation Mode**

**Max. People Allowed**

Define the maximum amount of people (range: 1 to 100,000) allowed to stay in a specific region at the same time.

**Push Alarm to Hik-Connect If Max. People Reached**

After enabled, an alarm notification will be pushed to the Hik-Connect Mobile Client if **Max. People Allowed** is reached.

**Note**

Please notify the end user that he/she should keep the Notification functionality of the Hik-Connect Mobile Client enabled, or he/she will not receive this alarm notification on the

Mobile Client. For details about enabling the Notification functionality on Hik-Connect, see *Hik-Connect Mobile Client User Manual*.

5. Click **OK**.

   The people counting group will be displayed on the **People Counting** tab and it is enabled by default. And the end user will be able to view corresponding people counting data on Hik-Connect Mobile Client.

   **Note**

   You can add up to 16 people counting groups to a site.

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

   **Edit Group**
   Hover the cursor onto ⋯ and then click ✎ to edit the group.

   **Delete Group**
   Hover the cursor onto ⋯ and then click 🗑 to delete the group.

   **Note**

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

   **Disable a Specific Group**
   Set 🟢 to ⚪ to disable the group.

   **Note**

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

   **Batch Enable/ Disable Groups**
   Click **Enable All** or **Disable All** to enable or disable all groups respectively.

   **Note**

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

## 7.9 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 end user will be able to view the skin-surface temperatures 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 specific 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.

**Note**

Please notify the end user that he/she should keep the Notification functionality of the Hik-Connect Mobile Client enabled, or he/she will not receive this alarm notification on the Mobile Client. For details about enabling the Notification functionality on Hik-Connect, see *Hik-Connect Mobile Client User Manual*.

**Save Normal Temperature Records**

Save normal temperature records on the Hik-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.

**Note**

If disabled, the end user will be unable to view the captured picture on the Hik-Connect Mobile Client.

**Push Alarm to Hik-Connect If Wearing No Mask Detected**

After enabled, if a person who wears no mask is detected, an alarm about it will be pushed to the Hik-Connect Mobile Client.

**Note**

Please notify the end user that he/she should keep the Notification functionality of the Hik-Connect Mobile Client enabled, or he/she will not receive this alarm notification on the Mobile Client. For details about enabling the Notification functionality on Hik-Connect, see *Hik-Connect Mobile Client User Manual*.

2) Click **OK**.

8. **Optional:** Perform the following operations if required.

**Disable Temperature Screening Functionality of a Specific Device**

Set ● to ○ to disable the temperature screening functionality of the device.

**Note**

If disabled, the end user will NOT be able to use the temperature screening functionality of the device on the Hik-Connect Mobile Client.

**Disable Temperature Screening 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.

## 7.10 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.

## 7.11 Unbind 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*** .

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

**Note**

If the device firmware does not support device unbinding, you are required to enter a CAPTCHA code after entering device password.

## 7.12 Reset Device Password

You can reset the password of a device when the Site Owner and the Installer both lost the password.

**Note**

- Resetting password via Hik-ProConnect platform is not supported by every device type/model. For example, AX Pro security control panel 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*** .
- Make sure that the device is on the same local area network with the PC where your Hik-ProConnect Portal runs.

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

Select the device and click ••• → to send a password reset application to the Site Owner.

Refer to the flow chart below for the whole process of resetting the password of a device.

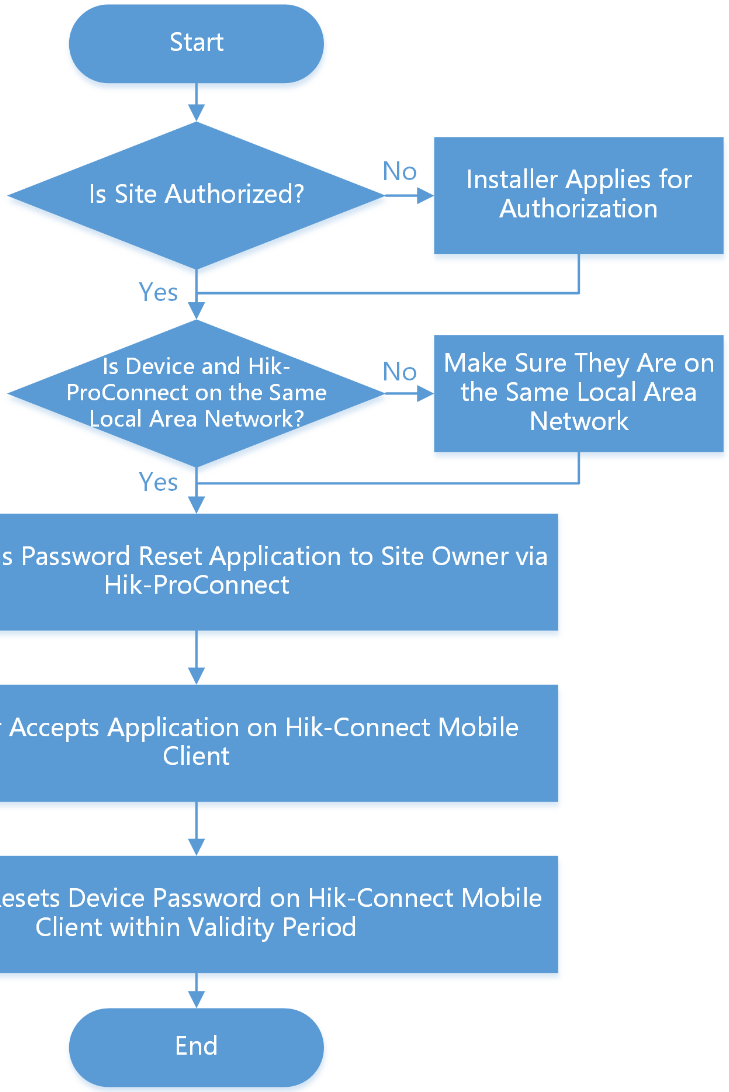

Start
Is Site Authorized?
No
Installer Applies for Authorization
Yes
Is Device and Hik-ProConnect on the Same Local Area Network?
No
Make Sure They Are on the Same Local Area Network
Yes
Installer Sends Password Reset Application to Site Owner via Hik-ProConnect
Site Owner Accepts Application on Hik-Connect Mobile Client
Site Owner Resets Device Password on Hik-Connect Mobile Client within Validity Period
End

**Figure 7-12 Flow Chart of Resetting Device Password**

## 7.13 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**.

## 7.14 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 (Version 4.7.1 and later). You can send the QR code or download link shown in the banner on the Home page to them.
- Make sure the device is online, otherwise the function cannot be used.

## 7.15 View Recorded 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 stored on the device.

**Note**

- Make sure your account has the permission for playback. If you have no permission for playback, 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 are videos stored in the device.

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

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

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

**Note**

Up to four playback windows are supported.

## 7.16 Operate and Configure AX Pro

For AX Pro security control panel, you can perform operations including arming/disarming area, clearing alarm, bypassing zone etc., and remotely configure the control panel on the Portal. You can also apply for PIN (required for upgrading the firmware of AX Pro) and switch the language of AX Pro.

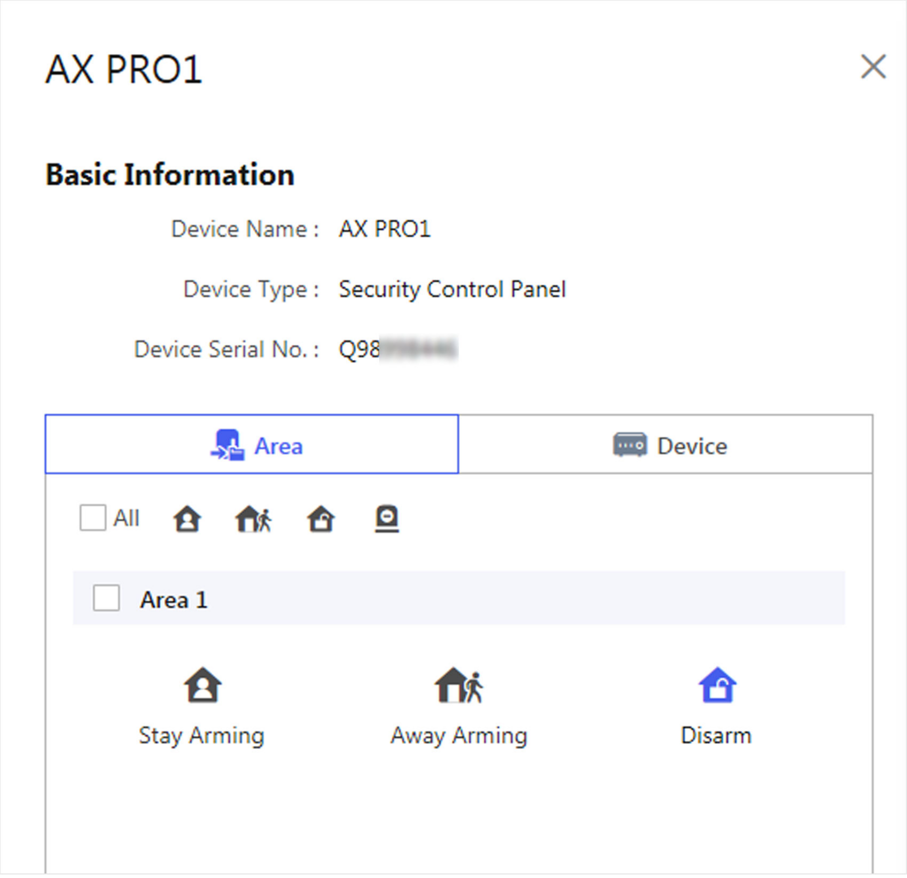
Click 🌐 **Site** to enter the site list page, and then click the name of a site to enter site details page.

### Remotely Operate AX Pro

Click the AX Pro to open the operation panel. And you can perform the following operations.

**Table 7-6 Operation Description**

| Operation | Description |
|---|---|
| Stay Arm a Specific Area | Select the **Area** tab, and then click **Stay Arming** to stay arm the area. |
| Away Arm a Specific Area | Select the **Area** tab and then click **Away Arming**. |
| Disarm a Specific Area | Select the **Area** tab and then click **Disarm**. |
| Stay Arm Multiple Areas | Select the **Area** tab, and then select areas and click 🏠 . |
| Away Arm Multiple Areas | Select the **Area** tab, and then select areas and click 🏃 . |
| Disarm Multiple Areas | Select the **Area** tab, and then select areas and click ⌂ . |
| Clear Alarms of Multiple Areas | Select the **Area** tab, and then select areas and click 🔔 |
| Filter Peripheral Device by Area | Select the **Device** tab, and then click ∨ and select an area to only display the peripheral devices linked to the selected area, or select **All** to display all the peripheral devices linked to all the areas. |
| Bypass Zone | Select the **Device** tab, and then select a zone (i.e., detector) and turn on the **Bypass** switch to bypass the zone. |



AX PRO1

**Basic Information**

Device Name : AX PRO1

Device Type : Security Control Panel

Device Serial No. : Q98[redacted]

Figure 7-13 Operation Panel of AX Pro

### Remotely Configure AX Pro

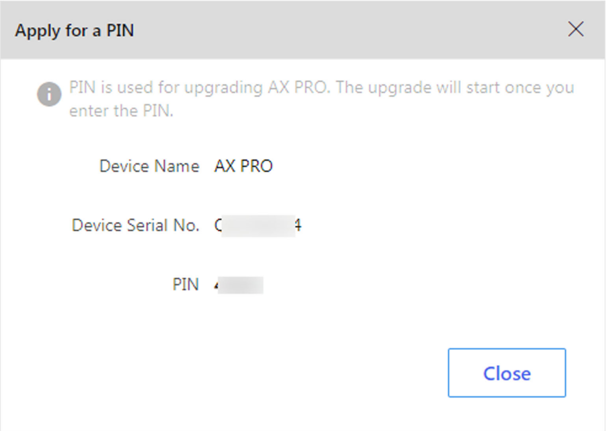
You can click ⚙ to enter the web page of the security control panel to configure the device.

**Note**

For details about security control panel configuration, see the user manual of the device.

### Apply for a PIN

You can click ● ● ● → 🗎 to open the Apply for a PIN window, and then PIN code will be displayed.



PIN is used for upgrading AX PRO. The upgrade will start once you enter the PIN.

Device Name AX PRO

Device Serial No. [redacted]

PIN [redacted]

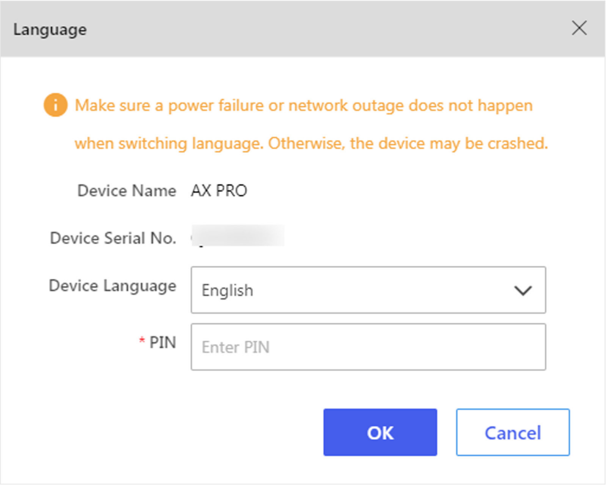
Figure 7-14 Apply for a PIN

### Switch Language

**Note**

You should have applied for a PIN. See ***Apply for a PIN*** for details.

You can click ••• → ⇆ to open the Language window, and then set the device language and enter the PIN.



Make sure a power failure or network outage does not happen when switching language. Otherwise, the device may be crashed.

Device Name AX PRO

Device Serial No. [redacted]

Device Language English

* PIN Enter PIN

Figure 7-15 Language Window

## 7.17 Remote Configuration

You can perform device remote configuration if you need.

**Note**

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

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

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

**Note**

- Only doorbells, encoding devices, indoor stations, and security control panels support remote configuration.
- Make sure the device is online, otherwise the function cannot be used.
- For doorbells, you don't need to enter the device user name and password before accessing the remote configuration page.
- For encoding devices, if you have already entered the device's user name and password when adding it, you do not need to enter these information before remote configuration. For NVR and DVR, operations including rebooting, HDD formatting, and network settings are supported.
- For security control devices:
  - If the security control device is in the same LAN with the Portal, you need to enter the user name and password before accessing the remote configuration page.
  - If the Axiom Hub device and Axiom Hybrid device are not in the same LAN and EN50131 Compliant mode is enabled, you need to enter the devices' admin passwords for verification first. After that, you can enter their remote configuration page after entering password of setter account.
- For encoding devices and security control devices, if the device is not in the same local area network with the Portal, some operations in the remote configuration (such as device account management, enabling Hik-Connect, and restoring device, etc.) are not available.
- See device user manual for details about remote configuration.
- If you have changed device parameters by other software or client (such as device page, Hik-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.

# Chapter 8 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.

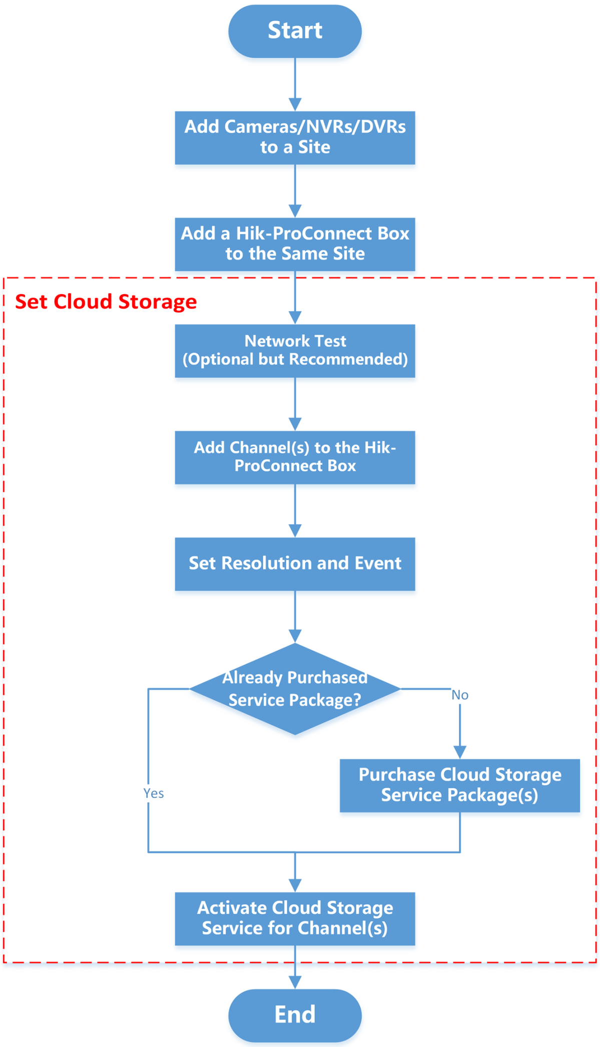
**Note**

The supported cloud storage devices include Hik-ProConnect box and the DVR that supports cloud storage service (hereafter simplified as cloud storage DVR).

## 8.1 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


Start
Add Cameras/NVRs/DVRs to a Site
Add a Hik-ProConnect Box to the Same Site
Set Cloud Storage
Network Test (Optional but Recommended)
Add Channel(s) to the Hik-ProConnect Box
Set Resolution and Event
Already Purchased Service Package?
No
Purchase Cloud Storage Service Package(s)
Yes
Activate Cloud Storage Service for Channel(s)
End

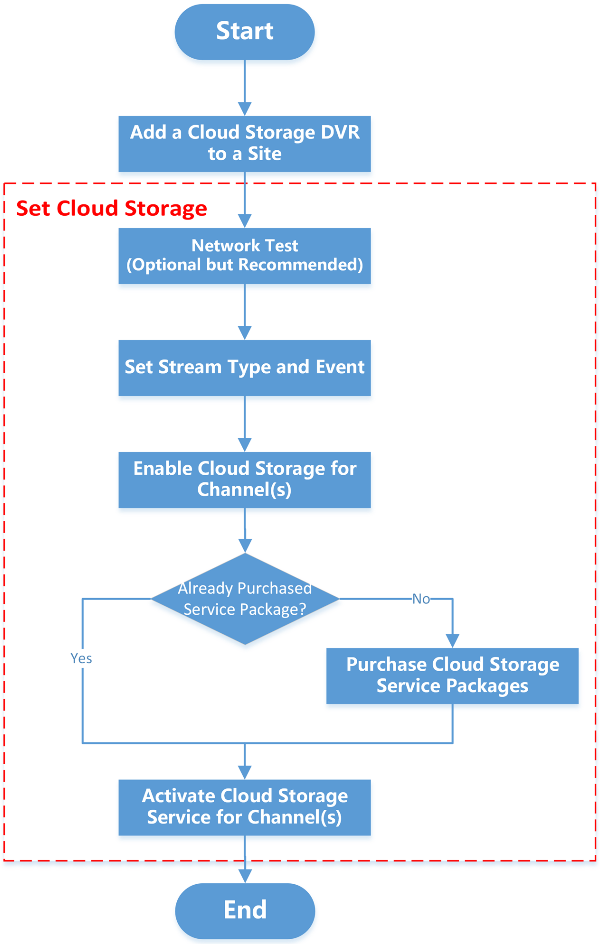
The following table shows the description for each procedure of the flow chart.

**Table 8-1 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**<br>For the Hik-ProConnect box added by IP/Domain name, cloud storage service is not supported. |
| Set Cloud Storage | Set cloud storage for the Hik-ProConnect. See ***Set Cloud Storage for Hik-ProConnect Box*** for details.<br>The following list shows the descriptions of the sub-procedures.<br>• Network Test: Test your network condition to get the recommended settings for cloud storage. See ***Network Test*** for details.<br>• 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).<br>• Set Resolution and Event: Set resolution for the channels, and set the event(s) that will trigger the channel to record related video footage.<br>• Purchase Cloud Storage Service Package(s): Purchase cloud storage service packages from the service market. See ***Purchase Cloud Storage Service*** for details.<br>**Note**<br>You can also purchase service key from the distributor.<br>• 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. |

### Flow Chart for Cloud Storage DVR


Start
Add a Cloud Storage DVR to a Site
Set Cloud Storage
Network Test (Optional but Recommended)
Set Stream Type and Event
Enable Cloud Storage for Channel(s)
Already Purchased Service Package?
No
Yes
Purchase Cloud Storage Service Packages
Activate Cloud Storage Service for Channel(s)
End

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

**Table 8-2 Flow Chart Description**

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

| Procedure | Description |
|---|---|
|  | • Network Test: Test your network condition to get the recommended settings for cloud storage. See ***Network Test*** for details.<br>• Enable Cloud Storage for Channel(s): Enable cloud storage for the channel(s) of the cloud storage DVR.<br>• 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.<br>• Purchase Cloud Storage Service Package(s): Purchase cloud storage service packages from the service market. See ***Purchase Cloud Storage Service*** for details.<br>**Note**<br>You can also purchase service key from the distributor.<br>• 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. |

## 8.2 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.

## 8.3 Set Cloud Storage for Hik-ProConnect Box

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

**Steps**

**Note**

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

1. Add a Hik-ProConnect box to a site by Hik-Connect (P2P).

**Note**

- For details about adding the Hik-ProConnect box, see ***Add Device by 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.

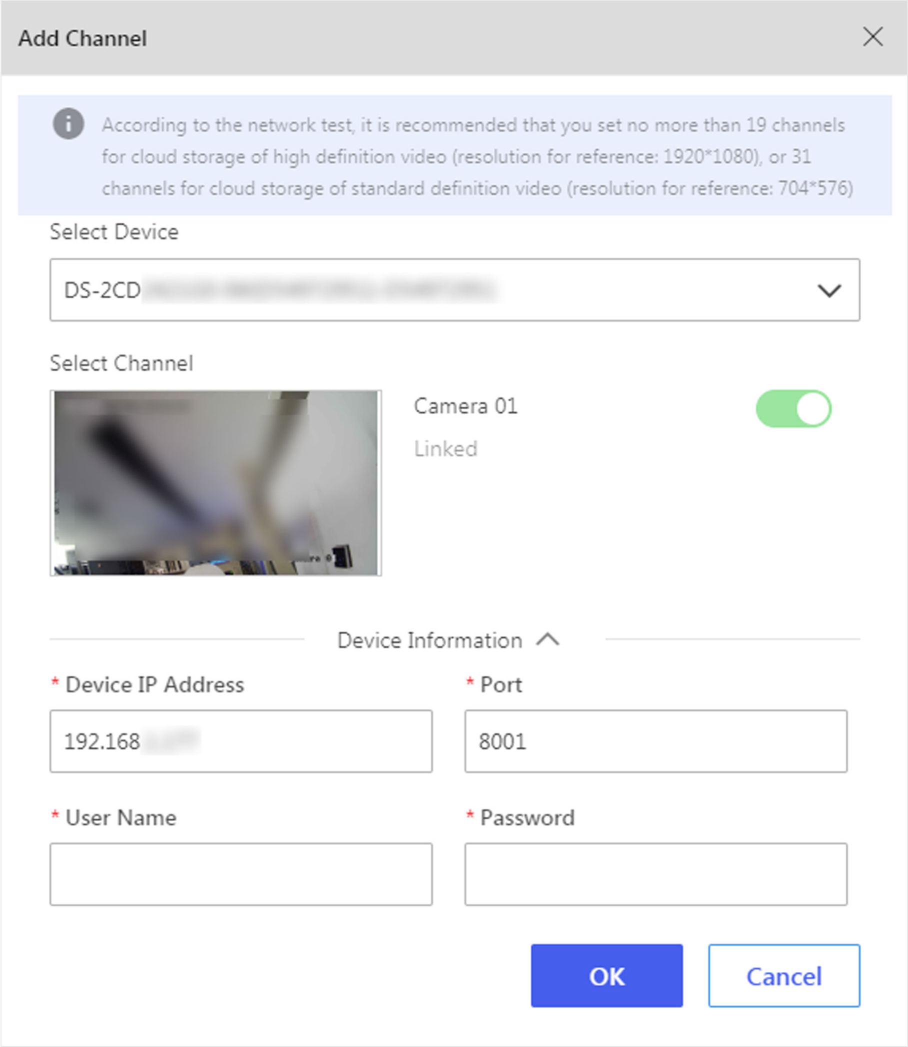
You enter the Network Test page.

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.



Add Channel

According to the network test, it is recommended that you set no more than 19 channels for cloud storage of high definition video (resolution for reference: 1920*1080), or 31 channels for cloud storage of standard definition video (resolution for reference: 704*576)

Select Device

DS-2CD[redacted]

Select Channel

Camera 01

Linked

Device Information

* Device IP Address: 192.168[redacted]

* Port: 8001

* User Name:

* Password:

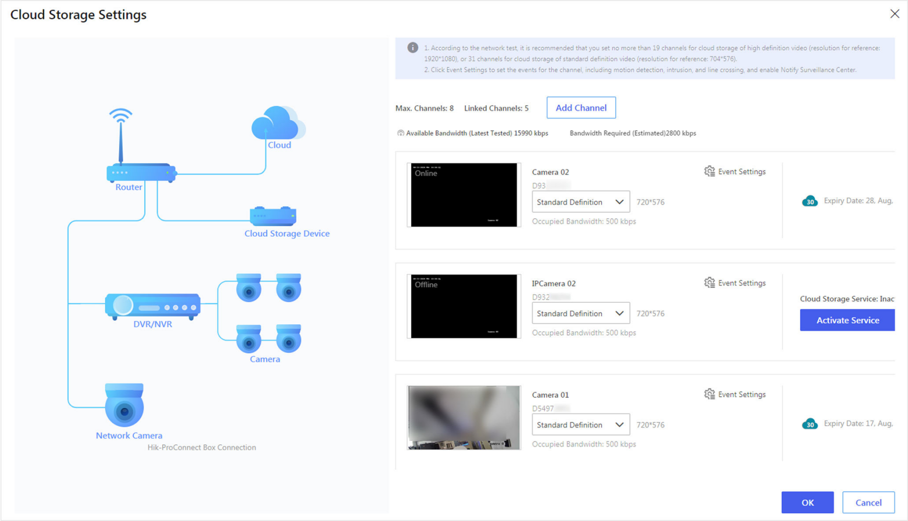
**Figure 8-1 Add Channel Window**

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.


Cloud Storage Settings

1. According to the network test, it is recommended that you set no more than 19 channels for cloud storage of high definition video (resolution for reference: 1920*1080), or 31 channels for cloud storage of standard definition video (resolution for reference: 704*576).
2. Click Event Settings to set the events for the channel, including motion detection, intrusion, and line crossing, and enable Notify Surveillance Center.

Max. Channels: 8 Linked Channels: 5

Available Bandwidth (Latest Tested) 15990 kbps Bandwidth Required (Estimated)2800 kbps

Online
Camera 02
D93
Standard Definition 720*576
Occupied Bandwidth: 500 kbps
Expiry Date: 28, Aug,

Offline
IPCamera 02
D932
Standard Definition 720*576
Occupied Bandwidth: 500 kbps
Cloud Storage Service: Inac

Camera 01
D5497
Standard Definition 720*576
Occupied Bandwidth: 500 kbps
Expiry Date: 17, Aug,

**Figure 8-2 Cloud Storage Settings Page**

5. 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).

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**.

## 8.4 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.

**Note**

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.

**Note**

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.

**Note**

When cloud storage service is activated for the channel, you cannot turn off **Cloud Storage** for the channel by default.

8. Click **Finish**.
9. **Optional:** Click the cloud storage DVR in the device list to open its settings panel, and then click **Edit** to edit the settings of its channels.

**Note**

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

## 8.5 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.

**Note**

It takes about one minute to test the network.

You can click the cloud storage device in the device list to open the device settings panel, and then click → **Start** to start network test.

## 8.6 Activate or Renew Service for a Channel

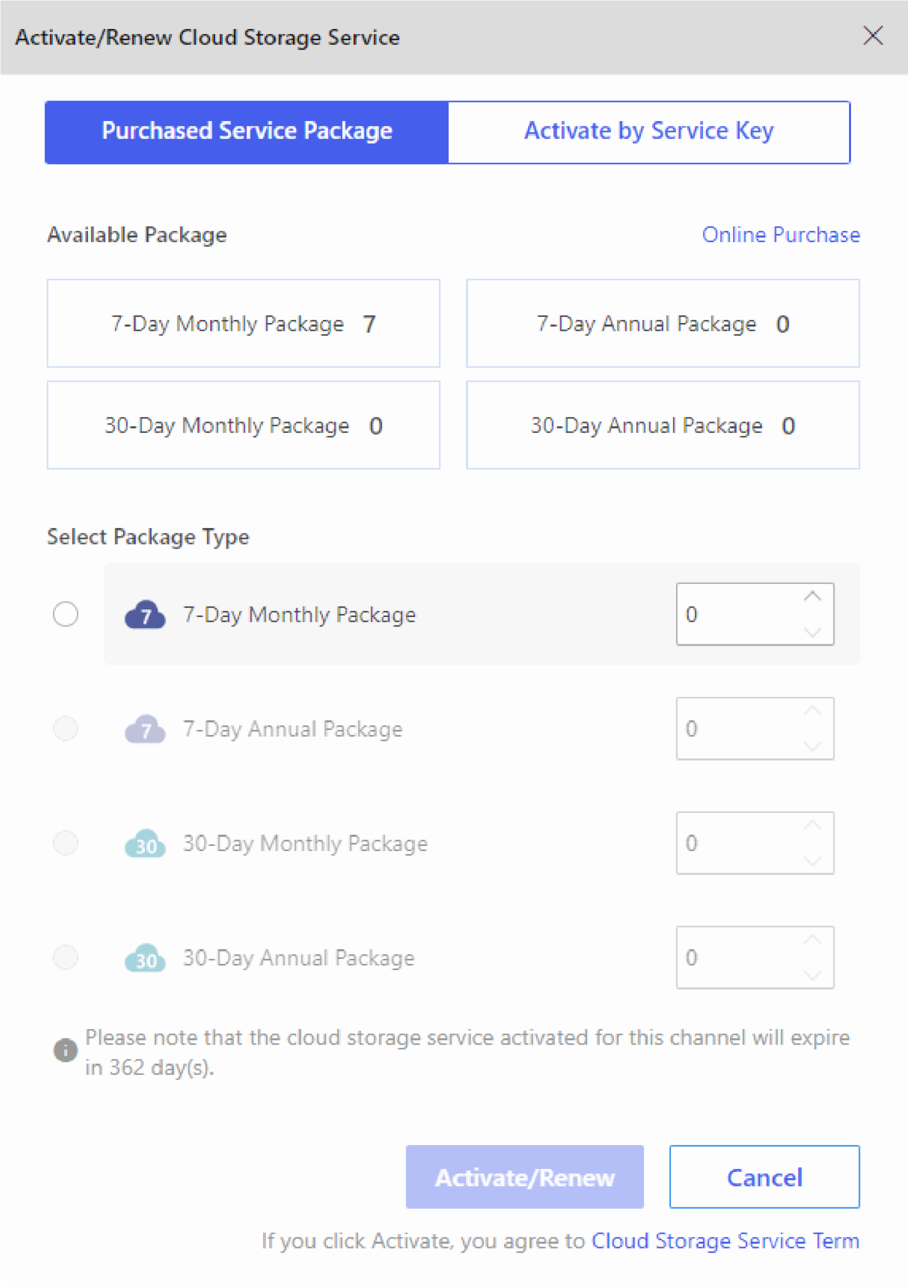
On the cloud storage service page, you can view the cloud storage details of different channels of a cloud storage device. If cloud storage service is not activated for a certain channel, you should activate the service before using it. For an activated service that will expire soon or has expired, you 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**

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.



Activate/Renew Cloud Storage Service

Purchased Service Package | Activate by Service Key

Available Package — Online Purchase

| | |
|---|---|
| 7-Day Monthly Package 7 | 7-Day Annual Package 0 |
| 30-Day Monthly Package 0 | 30-Day Annual Package 0 |

Select Package Type

○ 7-Day Monthly Package 0

○ 7-Day Annual Package 0

○ 30-Day Monthly Package 0

○ 30-Day Annual Package 0

Please note that the cloud storage service activated for this channel will expire in 362 day(s).

Activate/Renew | Cancel

If you click Activate, you agree to Cloud Storage Service Term

**Figure 8-3 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 **Purchased 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 get the service key from the distributor.

6. Click **Activate/Renew** to finish activating or renewing the cloud storage service.

**Note**

After activating or renewing the service, you can view the package type and expiry date of the service in each channel. When there are multiple unused service packages in a certain channel, these packages are listed according to the time they were purchased.

## 8.7 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*** .

# Chapter 9 Health Monitoring Service

Hik-ProConnect offers a permanent Free package containing a series of basic functions such as viewing device online status and remote device configuration once you complete account registration. In some cases, for the capacity and functionality limitation of the Free package, these basic functions are NOT sufficient for you to satisfy higher level demands of your customers (i.e., end users), such as their demand for the maintenance of large amount of devices. Compared with the Free package, the Health Monitoring service not only allows you to enjoy larger device capacity on Hik-ProConnect, but also monitor health status of customers' devices and configure other value-added functionality. You can access the Health Monitoring service by purchasing Health Monitoring packages from our Service Market.

**Note**

The Health Monitoring service is temporarily free in some countries and regions.

### Differences Between Free Package and Health Monitoring Package

The following table shows the differences between the Free package and 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 more details.

| Functionality | Free Package | Health Monitoring Package |
|---|---|---|
| Adding Devices | • Supported<br>• Manageable Devices: 1024 | • Supported<br>• Manageable Devices: More than 1024 based on the package you purchase. |
| Site & Device | | |
| Applying for Authorization | | |
| Viewing Device Online Status | | |
| Remote Configuration | | |
| Live View/Playback/ Downloading Video | | |
| Device Firmware Remote Upgrade | | |
| Health Monitoring | Supported | Supported |
| Exception Rule | Not Supported | Supported |

| Functionality | Free Package | Health Monitoring Package |
|---|---|---|
| Linkage Rule | Not Supported | Supported |
| Emplogee Management | Not Supported | Manageable Employees: 4 |
| Role/Permission Management | Not Supported | Supported |
| Searching Operation Logs of Employees | Not Supported | Supported |
| Co-Branding | Not Supported | Supported |

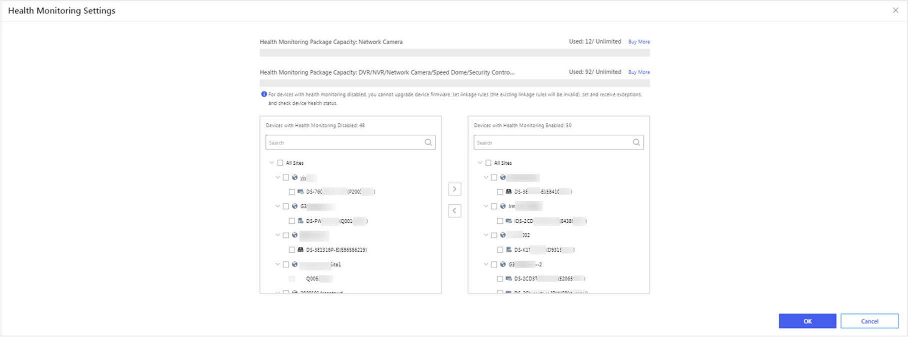
### Set Devices Covered by Health Monitoring Package

The devices that can access the Health Monitoring service is subject to the package your purchase. In particular scenarios, you might need to change the devices that can access the service. Perform the following operations to change the devices that can access value-added functions offered by the Health Monitoring package.

**Note**

This function is NOT currently available in every country and region.

1. Go to **Business → My Service → Health Monitoring Settings** .
2. Select device(s) from the Devices with Health Monitoring Disabled list, and then click › to enable Health Monitoring service for the selected device(s).
   Or select device(s) from the Devices with Health Monitoring Service Enabled list, and then click ‹ to disable Health Monitoring service for the selected device(s).
3. Click **OK**.



Health Monitoring Settings

Health Monitoring Package Capacity: Network Camera    Used: 12/ Unlimited

Health Monitoring Package Capacity: DVR/NVR/Network Camera/Speed Dome/Security Contro...    Used: 92/ Unlimited

For devices with health monitoring disabled, you cannot upgrade device firmware, set linkage rules (the existing linkage rules will be invalid), set and receive exceptions, and check device health status.

Devices with Health Monitoring Disabled: 48

Devices with Health Monitoring Enabled: 50

×
Buy More
Buy More
Search
□ All Sites
□ yjy[redacted]
□ DS-760[redacted](P200[redacted])
□ G3[redacted]
□ DS-PW[redacted](Q001[redacted])
□ [redacted]
□ DS-3E1318P-EI(E86586219)
□ [redacted]ite1
Q005[redacted]
›
‹
Search
□ All Sites
□ [redacted]
□ DS-3E[redacted]-EI(E8410[redacted])
□ Irr[redacted]
□ iDS-2CD[redacted](E438[redacted])
□ [redacted]02
□ DS-K1T[redacted](D931[redacted])
□ G3[redacted]-2
□ DS-2CD3T[redacted](E2065[redacted])
OK
Cancel

Figure 9-1 Health Monitoring Settings

# Chapter 10 Health Monitoring

The portal provides Health Monitoring module for managing the resources in the system. There are two 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 check 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 the system.

  **Note**

  For Installer, you can only view the status information of the devices in the site which has been assigned to you. For Installer Admin, you can view the status information of the devices in 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.

## 10.1 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 number of devices in total and number of abnormal devices of each device type.

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

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

**Table 10-1 Links of Different Device Type**

| | |
|---|---|
| Encoding Device | Refer to ***Encoding Device*** . |
| Access Control Device | Refer to ***Access Control Device*** . |
| Security Control Device | Refer to ***Security Control Device*** . |

| | |
|---|---|
| Video Intercom Device | Refer to ***Video Intercom Device*** . |
| Doorbell | Refer to ***Doorbell*** . |
| Hik-ProConnect Box | Refer to ***Hik-ProConnect Box*** . |
| Network Switch | Refer to ***Network Switch*** . |

### Encoding Device

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

**Note**

For analog camera, you can view 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 only.
- 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 onto 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 **Refresh** 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.
- 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.

The following table shows the description of each status icon.

**Table 10-2 Icon Description**

| Icon | Description |
|---|---|
| 🔋 | Sufficient battery power. |
| 🪫 | Insufficient battery power. |
| 🟢 | Normal strength of the communication signals between the peripheral device and the security control panel. |
| 🟢 | Medium 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. |
| 🔴 | Abnormal strength of the communication signals between the peripheral device and the security control panel. |
| 🚨 | Alarm triggered. |
| 🔨 | Device tampered. |
| 🔔 | Zone bypassed. |
| ⚠ | Trigger exception. |

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 **Refresh** 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 **Refresh** 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

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

You can also 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:

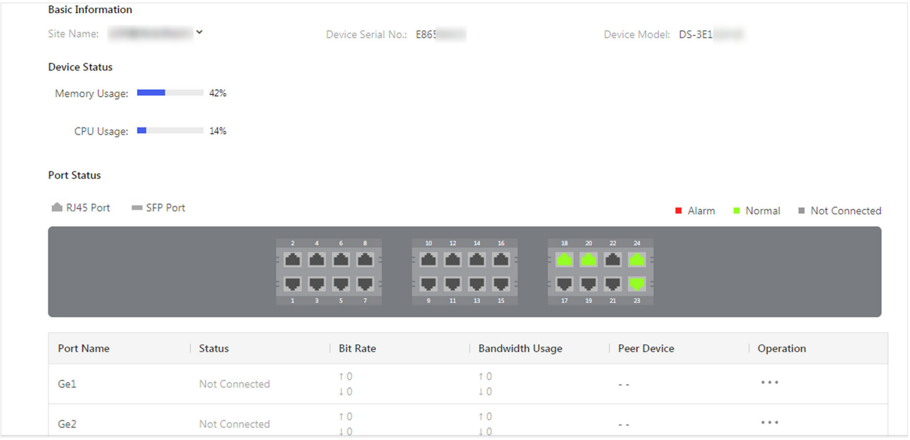
- Click ⚙ in the Operation column to remotely configure parameters of the device. For details, see the user manual of the device.
- Click 🛡 in the Operation column to inspect the device manually.

### Network Switch

You can 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, port status (alarm, normal, not connected), etc.



Basic Information

Site Name: [redacted]

Device Serial No.: E865[redacted]

Device Model: DS-3E1[redacted]

Device Status

Memory Usage: 42%

CPU Usage: 14%

Port Status

RJ45 Port SFP Port

🟥 Alarm 🟩 Normal ■ Not Connected

| Port Name | Status | Bit Rate | Bandwidth Usage | Peer Device | Operation |
|---|---|---|---|---|---|
| Ge1 | Not Connected | ↑0<br>↓0 | ↑0<br>↓0 | - - | ··· |
| Ge2 | Not Connected | ↑0<br>↓0 | ↑0<br>↓0 | - - | ··· |

**Figure 10-1 Switch Details**

Hover the cursor onto the switch picture to view the enlarged picture of the ports.

Click ··· → **Restart Port** to restart the port.

For the port with alarm, click **Clear Alarm** to clear the alarm of this port.

## 10.2 View Status of Devices in 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 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, port status(alarm, normal, not connected).

Hover the cursor onto the switch picture to view the enlarged picture of the switch.

Click ··· → **Restart Port** to restart the port.

Click **Topology** on 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 the port with alarm, click **Clear Alarm** to clear the alarm of this port.

## 10.3 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 enabled Health Monitoring service for the network switch, some topology functions (e.g., viewing device status on the topology) will be unavailable. For details about enabling Heath Monitoring service for devices, see ***Set Devices Covered by Health Monitoring Package*** for details.

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**.

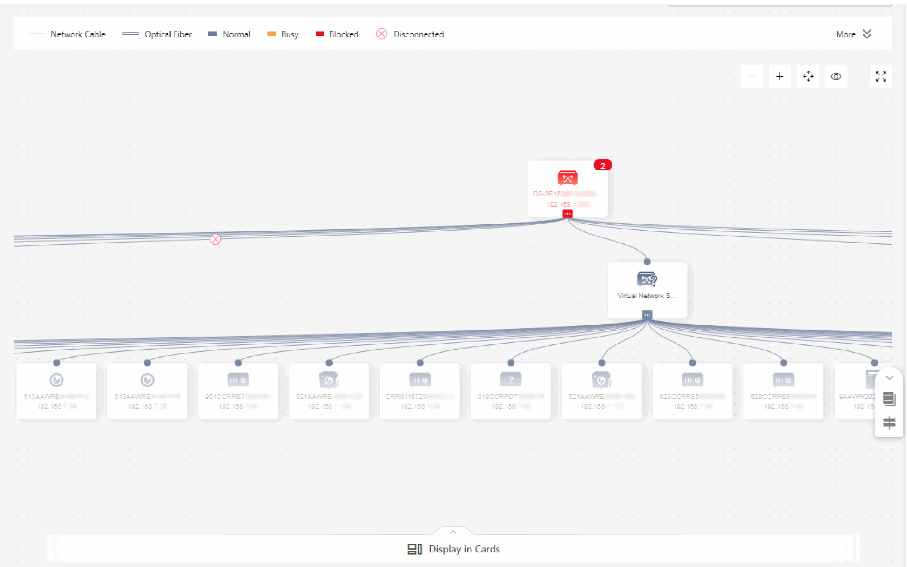
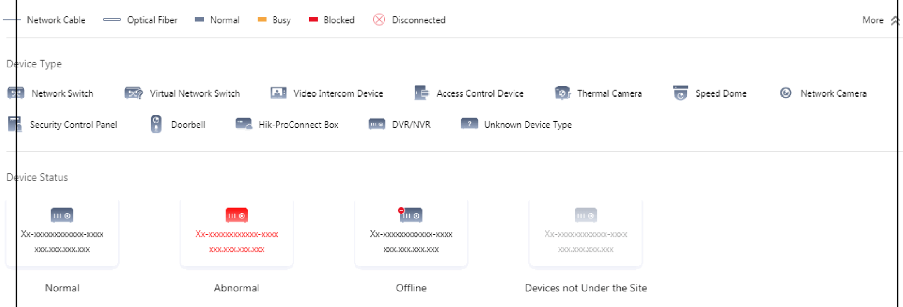
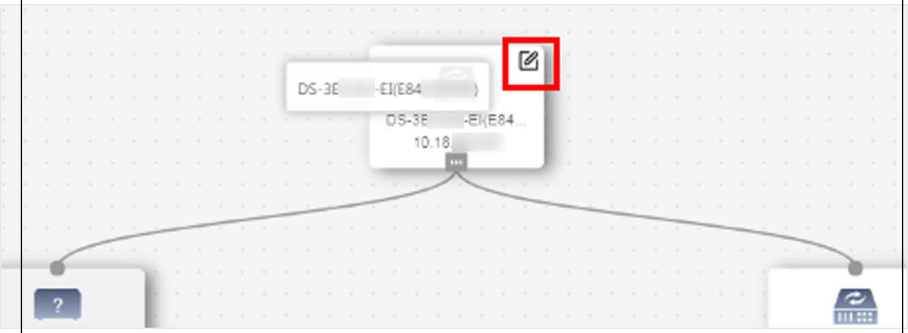


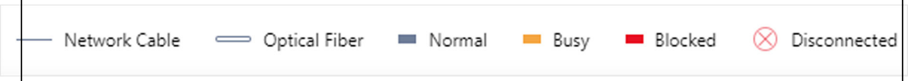
**Figure 10-2 Network Topology**

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

**Table 10-3 Available Operations**

| Operation | Description |
|---|---|
| View Legend | You can click ⌄ next to **More** to view the legends (see the figure below). |

| Operation | Description |
|---|---|
|  |  Network Cable<br>Optical Fiber<br>Normal<br>Busy<br>Blocked<br>Disconnected<br>More<br>Device Type<br>Network Switch<br>Virtual Network Switch<br>Video Intercom Device<br>Access Control Device<br>Thermal Camera<br>Speed Dome<br>Network Camera<br>Security Control Panel<br>Doorbell<br>Hik-ProConnect Box<br>DVR/NVR<br>Unknown Device Type<br>Device Status<br>Xx-xxxxxxxxxxxx-xxxx<br>xxx.xxx.xxx.xxx<br>Normal<br>Abnormal<br>Offline<br>Devices not Under the Site<br>**Figure 10-3 Legend** |
| Edit Root Node | When multiple network switches are added to a site, the platform will randomly select one of them as the root node by default for the network topology. If 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.<br> <br>**Figure 10-4 Edit Root Node** |
| Refresh Topology | Click **Refresh** to refresh the topology structure.<br>**Note**<br>The device status will not be refreshed. |
| Display in Cards | 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. |
| Move Network Topology | Drag the network topology to move it. |
| Zoom in/out | You can click + / − in the upper left corner to zoom in/out the topology. |
| Adjust Topology Size | You can click ✣ in the upper left corner to fit the topology size to the display window. |

| Operation | Description |
|---|---|
| | 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 | You can view link information based on the legends shown in the figure below.<br><br> Network Cable Optical Fiber Normal Busy Blocked Disconnected<br>**Figure 10-5 Link Information Legend** |
| 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 | 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.<br>**Note**<br>If you don't have the permission, the position of the device in the network topology might be incorrect. |
| View Network Switch Details and Control It | You can click a network switch on the topology to view the information about the network switch, including basic information, device status, and port status.<br>You can also perform operations such as rebooting the network switch and restarting port. For details, see ***Network Switch View Status of Devices in Specific Site*** .<br>**Note**<br>You cannot view details of a virtual network switch. |
| View Other Device's Details and Configure It | If an online device is connected to the network switch and added to the same site with the network switch, its device icon and device serial number will be displayed. And you can click the device to view information about it, including basic information (e.g., device model) and device status (e.g., network status). |

| Operation | Description |
|---|---|
| | You can also click ⚙ to configure device parameters.<br>**Note**<br>• If an unknown device (e.g., a PC) is connected to the network switch, it will be displayed as Xx-xxxxxxxxxxxx-xxxx xxx.xxx.xxx.xxx . And you cannot view its information.<br>• 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. |

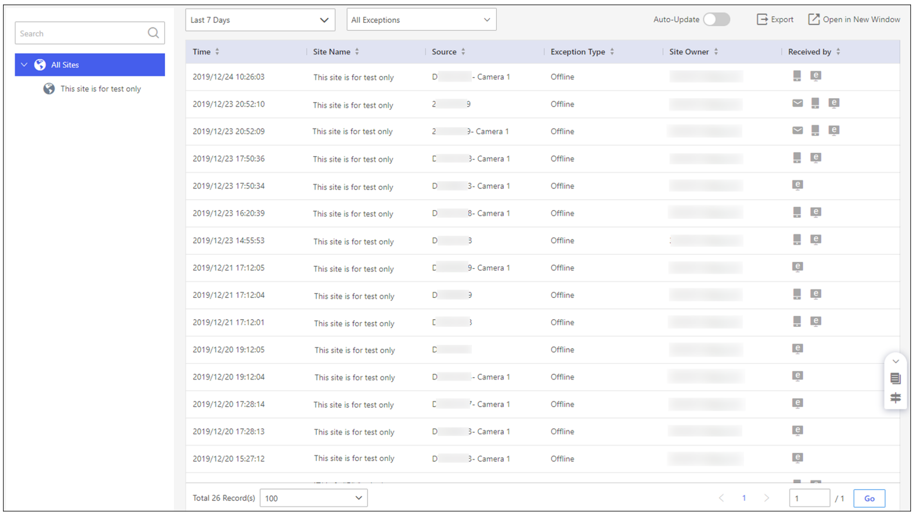
## 10.4 Exception Center

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.



| Time | Site Name | Source | Exception Type | Site Owner | Received by |
|---|---|---|---|---|---|
| 2019/12/24 10:26:03 | This site is for test only | D[redacted]- Camera 1 | Offline | [redacted] | ▯ ⓔ |
| 2019/12/23 20:52:10 | This site is for test only | 2[redacted]9 | Offline | [redacted] | ✉ ▯ ⓔ |
| 2019/12/23 20:52:09 | This site is for test only | 2[redacted]9- Camera 1 | Offline | [redacted] | ✉ ▯ ⓔ |
| 2019/12/23 17:50:36 | This site is for test only | D[redacted]3- Camera 1 | Offline | [redacted] | ▯ ⓔ |
| 2019/12/23 17:50:34 | This site is for test only | D[redacted]3- Camera 1 | Offline | [redacted] | ⓔ |
| 2019/12/23 16:20:39 | This site is for test only | D[redacted]8- Camera 1 | Offline | [redacted] | ▯ ⓔ |
| 2019/12/23 14:55:53 | This site is for test only | D[redacted]3 | Offline | [redacted] | ▯ ⓔ |
| 2019/12/21 17:12:05 | This site is for test only | D[redacted]9- Camera 1 | Offline | [redacted] | ⓔ |
| 2019/12/21 17:12:04 | This site is for test only | D[redacted]9 | Offline | [redacted] | ▯ ⓔ |
| 2019/12/21 17:12:01 | This site is for test only | D[redacted]3 | Offline | [redacted] | ▯ ⓔ |
| 2019/12/20 19:12:05 | This site is for test only | D[redacted] | Offline | [redacted] | ⓔ |
| 2019/12/20 19:12:04 | This site is for test only | D[redacted]- Camera 1 | Offline | [redacted] | ⓔ |
| 2019/12/20 17:28:14 | This site is for test only | D[redacted]7- Camera 1 | Offline | [redacted] | ⓔ |
| 2019/12/20 17:28:13 | This site is for test only | D[redacted]3- Camera 1 | Offline | [redacted] | ⓔ |
| 2019/12/20 15:27:12 | This site is for test only | D[redacted]3- Camera 1 | Offline | [redacted] | ⓔ |

Figure 10-6 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 are: 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.

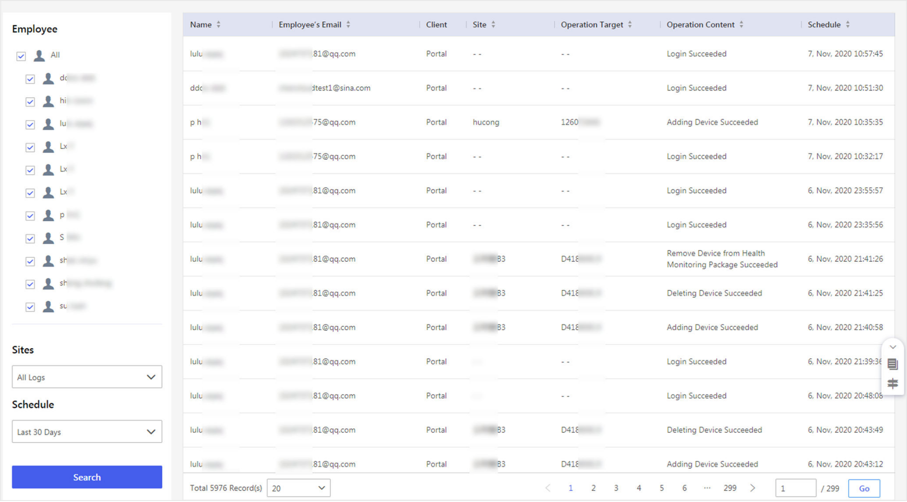
# Chapter 11 Search Operation Log

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.



Employee

- ☑ All
  - ☑ dc[redacted]
  - ☑ hi[redacted]
  - ☑ lu[redacted]
  - ☑ Lx[redacted]
  - ☑ Lx[redacted]
  - ☑ Lx[redacted]
  - ☑ p[redacted]
  - ☑ S[redacted]
  - ☑ sh[redacted]
  - ☑ sh[redacted]
  - ☑ su[redacted]

Sites: All Logs

Schedule: Last 30 Days

| Name | Employee's Email | Client | Site | Operation Target | Operation Content | Schedule |
|---|---|---|---|---|---|---|
| lulu[redacted] | [redacted]81@qq.com | Portal | - - | - - | Login Succeeded | 7, Nov, 2020 10:57:45 |
| ddc[redacted] | [redacted]dtest1@sina.com | Portal | - - | - - | Login Succeeded | 7, Nov, 2020 10:51:30 |
| p h[redacted] | [redacted]75@qq.com | Portal | hucong | 1260[redacted] | Adding Device Succeeded | 7, Nov, 2020 10:35:35 |
| p h[redacted] | [redacted]75@qq.com | Portal | - - | - - | Login Succeeded | 7, Nov, 2020 10:32:17 |
| lulu[redacted] | [redacted]81@qq.com | Portal | - - | - - | Login Succeeded | 6, Nov, 2020 23:55:57 |
| lulu[redacted] | [redacted]81@qq.com | Portal | - - | - - | Login Succeeded | 6, Nov, 2020 23:35:56 |
| lulu[redacted] | [redacted]81@qq.com | Portal | [redacted]B3 | D418[redacted] | Remove Device from Health Monitoring Package Succeeded | 6, Nov, 2020 21:41:26 |
| lulu[redacted] | [redacted]81@qq.com | Portal | [redacted]B3 | D418[redacted] | Deleting Device Succeeded | 6, Nov, 2020 21:41:25 |
| lulu[redacted] | [redacted]81@qq.com | Portal | [redacted]B3 | D418[redacted] | Adding Device Succeeded | 6, Nov, 2020 21:40:58 |
| lulu[redacted] | [redacted]81@qq.com | Portal | [redacted] | - - | Login Succeeded | 6, Nov, 2020 21:39:3 |
| lulu[redacted] | [redacted]81@qq.com | Portal | [redacted] | - - | Login Succeeded | 6, Nov, 2020 20:48:0 |
| lulu[redacted] | [redacted]81@qq.com | Portal | [redacted]B3 | D418[redacted] | Deleting Device Succeeded | 6, Nov, 2020 20:43:49 |
| lulu[redacted] | [redacted]81@qq.com | Portal | [redacted]B3 | D418[redacted] | Adding Device Succeeded | 6, Nov, 2020 20:43:12 |

Total 5976 Record(s) 20

Figure 11-1 Search Operation Logs

# Chapter 12 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.

UD21827N