Hik-ProConnect Portal

User Manual

Legal Information

About this Manual

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

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF 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 INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

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

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

Contents

Chapter 1 Introduction

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™ 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.

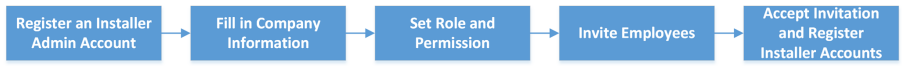

Figure 2-1 Flow Chart of Account Management

- **Register an Installer Admin Account:** The surveillance installation company should first register an Installer Admin account before accessing any functions of Hik-ProConnect. For details, refer to ***Register an Installer Admin Account*** .
- **Fill in Company Information:** After registering an Installer Admin account, you should bind your company information (including company name, country, logo, business license number, etc.) with this account for better service. You can edit your company information and view the comparison of the basic package and health monitoring package provided by Hik-ProConnect in the Company Information page. For details, refer to ***Manage Company Information*** .
- **Set Role and Permission:** Before adding an employee to the system, you can create different roles with different permissions for accessing system resources. For details, refer to ***Manage Role and Permission*** .
- **Invite Employees:** You can invite employees to register Installer accounts and assign different roles to employees to grant the permissions to her/him. For details, refer to ***Invite Employee*** .
- **Accept Invitation and Register Installer Accounts:** The employees can accept the invitation and register Installer accounts to manage sites and devices. For details, refer to ***Accept Invitation and Register Installer Account*** .

2.1 Register an Installer Admin Account

The 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**.

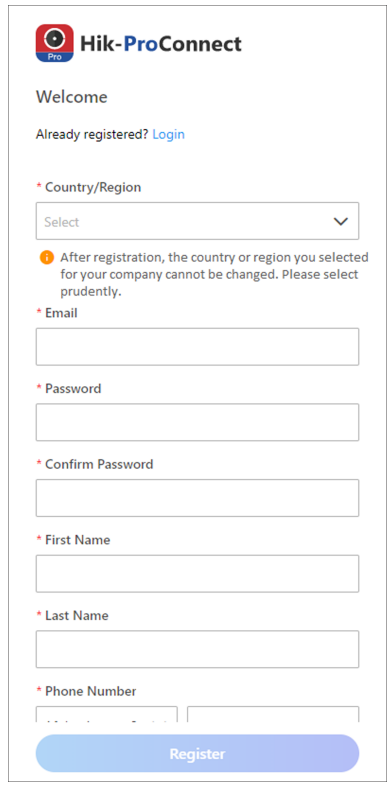

Figure 2-2 Register an Installer Admin Account

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. 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.

6. Enter your name and phone number.
7. Enter the authentication code which is used for authenticating that you are a professional installer.

Note

- Send your email address to the regional distributor or national distributor, and apply for an authentication code.
- If the authentication code is optional, you can leave it empty and authenticate your Installer Admin account later. For details about authenticating your account, refer to ***Authenticate Account*** .
- The authentication code should contain 10 digits.

8. **Optional:** Check **I would like to receive marketing communications by emails from Hik-ProConnect about services and activities. I understand that at any time I can unsubscribe.** 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 Hik-ProConnect activities, product updates, surveys, and special offers, to the email address which is used for your account registration.
9. Check **I agree to the Terms of Service and Privacy Policy** if you accept the details in these agreements.
10. Click **Register**.

    A registration confirmation email will be sent to the email address you entered in Step 4.
11. 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

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

Before You Start

Register an Installer Admin account first. For details, refer to ***Register an Installer Admin Account*** .

Steps

1. After Installer Admin registration and login, the following page will pop up.

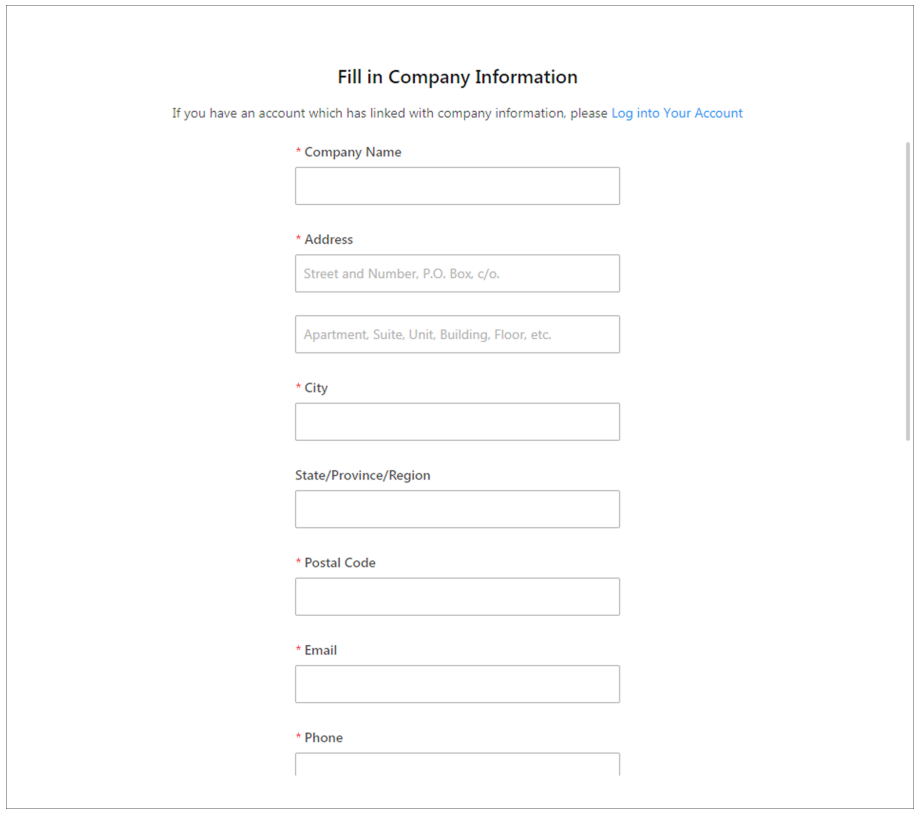

Figure 2-3 Fill in Company Information

2. Enter the name of your company.
3. Enter other information of your company, such as address, postal code, phone number, etc.
4. Enter the business license number and VAT number of your company which will be used for qualification verification.
5. Click **+** to upload a picture of the company's logo.

Note

- The picture should be in JPG, JPEG, or PNG format.
- Recommended picture size: Height = 200 px, 200 px ≤ Width ≤ 600 px.

6. **Optional:** Enter the website of your company if any.

7. Click **Bind**.

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

8. **Optional:** If you want to edit your company information, perform the following steps.
   1) In the Hik-ProConnect Portal, enter **Company → Company Information** .
   2) Click ✎ at the upper-right 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) Click **Save** to save the changes.
9. **Optional:** If you want to display the logo of your company on the Hik-Connect Mobile Client for brand promotion to the end users, in the Company Information page, set the switch near the **Co-Branding** area to on to enable it.

   Note

   Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

   After enabled, end users can view your company logo, address, and phone number via Hik-Connect Mobile Client.

10. **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.

    Basic Package

    Free package with up to totally 1,024 devices manageable and basic functions available (including adding devices in a batch, 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, device remote upgrading, 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. 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, contact the regional distributor or national distributor, send your **email address** (the one which is used when registering your Installer Admin account) or **company ID** (you can copy it in the **Company Information** page) to her/him, and apply for one authentication code.
After getting your authentication code, enter **Company → Company Information** page, click **Authenticate Now**, and enter the authentication code to authenticate your account.

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 two predefined roles in the system: Administrator and Site Manager. Employee with Administrator role has all the permissions of a role, while site manager has the permission of managing assigned site. And the two roles cannot be deleted by anyone. Different from Administrator role, the Installer Admin account can perform any operations on the company even if the account is assigned with no site.

1. Click **Company → Role and Permission** to display all the roles.
2. Add a role.
   1) Click **Add Role** to open the Add Role panel.
   2) Enter the role name and select permission(s) for the role.

      Manage Assigned Site

Manage the site(s) assigned to the employee. If one employee has the role of managing assigned site, he/she will have permission of all the operations and configuration in these site(s). This permission is an essential permission for site managers.

For example, he/she can edit site, invite site owner, apply for site information management permission, add existing site, add a new site, manage devices in the site (adding, deleting, editing, and upgrading devices), and delete site.

Note

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

Assign Site

Assign site to an employee.

Manage Account and Role

Access Employee and Role and Permission page, add and delete accounts and roles. Employee and Role and Permission page will not show without this permission.

Manage Company Information

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

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. Click **Company → Employee → Add Employee** to open the Add Employee panel.
2. Enter the email of the to-be-invited employee.
3. 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.
4. Click **Add**.

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

5. **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.

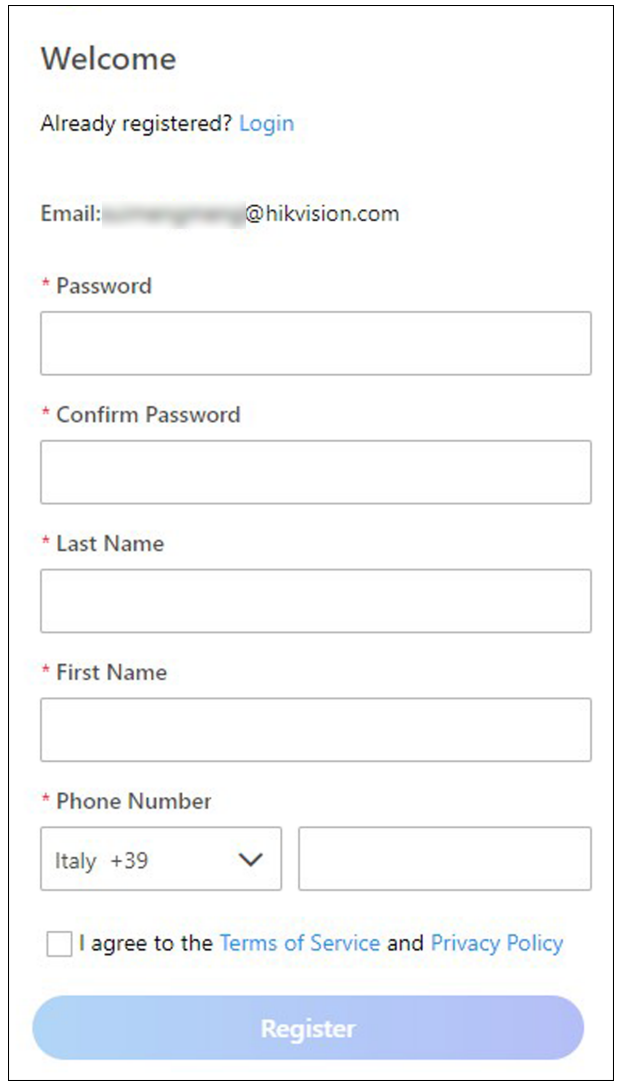

Figure 2-4 Register an Installer Account

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 necessary.

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. Check **I would like to receive marketing communications by emails from Hik-ProConnect about services and activities. I understand that at any time I can unsubscribe.** to subscribe to new services and activities of Hik-ProConnect.

   Note

   After subscription, we will send emails about latest Hik-ProConnect activities, product updates, surveys, and special offers, to the new email address.
7. 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**.

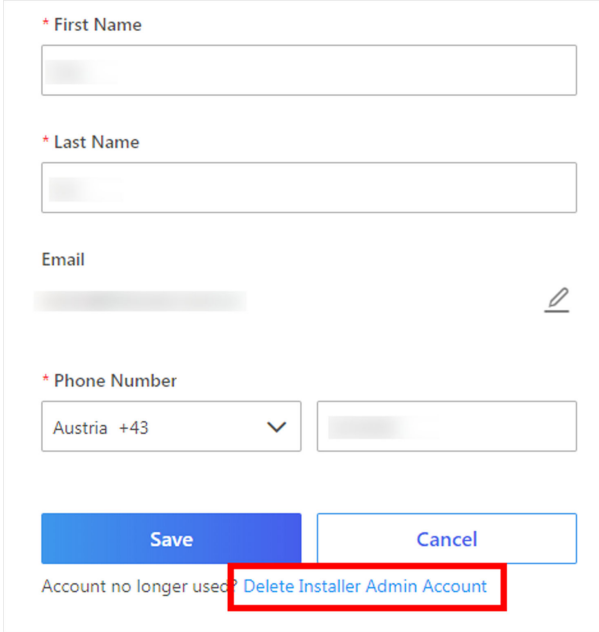

Figure 2-5 Delete Installer Admin Account

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*** / ***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. Enter the registered email and password.
3. **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.
4. Click **Login**.

   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 four 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, added employees, 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: • **Health Status:** Installer can view the devices overall, normal, and abnormal status, locate the abnormal devices, and perform troubleshooting quickly. • **Exception Center:** After setting the exception rules, when an exception occurs on the device, the device will push a notification to the Portal and you can view all the received notifications of exception in the Exception Center.
Company	The Company module deals with all the management and administration aspects of a single installation company. It contains the following four parts:

Module	Description
	• **Company Information:** You can manage your company information, purchase services and view available services. • **Employee:** Each company has only one Installer Admin but can have multiple Installers. The Installer Admin can invite the company's employees to register Installer accounts and assign different permissions to employees according to actual needs. Installer whose role contains permission of **Manage Account and Role** can also invite other employees to be Installers by registering Installer accounts. • **Role and Permission:** A role defines one employee's rights to the functions in the system. After creating a role and specifying the role's permission, you can assign it to the employees according to actual needs. • **Operation Log:** View the operation logs of all the accounts in the current company.

Home Page Introduction

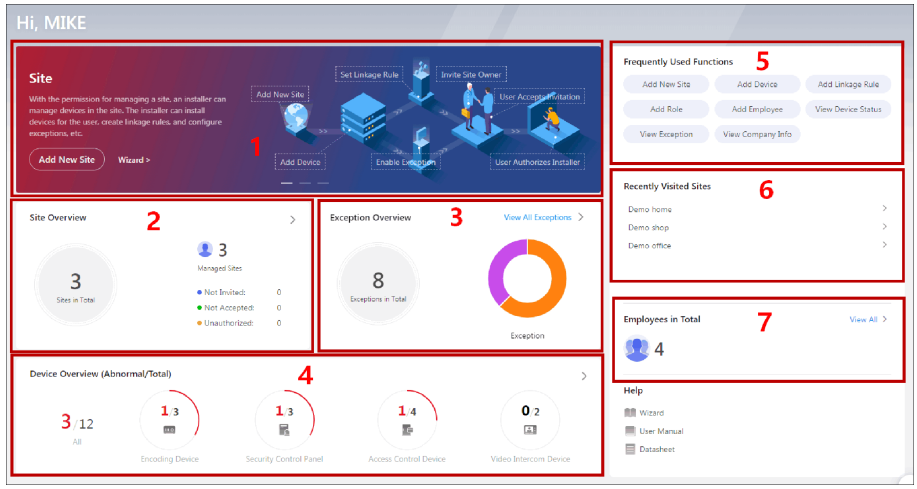

Figure 4-1 Home Page

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.

No.	Name	Introduction
		Note You can inform your end users to download or update the Hik-Connect Mobile Client (Version 4.3.0 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: • **Not Invited:** The number of sites for which no site owners are invited. • **Not Accepted:** The number of sites of which the site owner invitation are not accepted. • **Unauthorized:** The number of sites which are not authorized to you. **Note** 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. Hover the cursor to the pie chart to view the detailed proportions and amount. **Note** 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. **Note** 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*** .
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.

No.	Name	Introduction
		Click the site name to enter the site details page.
7	Employees in Total	You can view the number of added employees. **Note** For detailed instructions about inviting your employees, refer to ***Invite Employee*** .

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.

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.

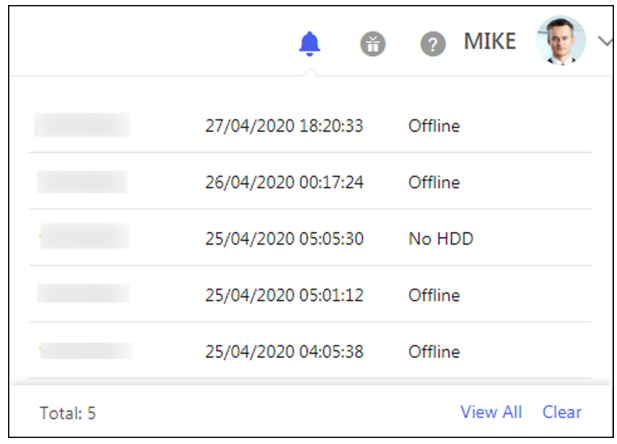

Figure 4-2 Recently Received Exceptions

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*** .

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 Marketing Communications

For Installer Admin, if you didn't subscribe marketing communications when account registration, you can click the name at the upper-right corner and select **Subscribe to Marketing**

Communications, or click  icon floating on the Home page to subscribe to the marketing communications about Hik-ProConnect.
After subscription, we will send emails about latest Hik-ProConnect activities, product updates, surveys, and special offers, to the email address which is used for your account registration.
You can unsubscribe at any time in the same way. After unsubscription, you will not receive any marketing communication 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.

View User Manual or Datasheet

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

Wizard

We provide you a wizard which guides you through the process of configurations and operations. There are three 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.
- Or click **Wizard** on the banner.

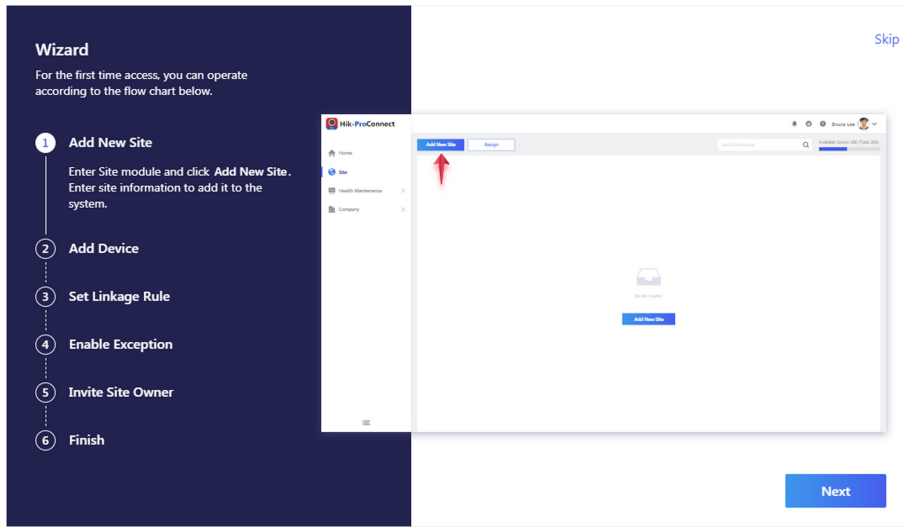

Figure 4-3 Wizard

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 **Logout** to log out of the current account and return to the login page.

Chapter 5 Site Management

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

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

5.1 Site Page Overview

On the Site page, you can view the sites that are assigned to you (the Installer Admin as well as Installers with Assign Site 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, etc.

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

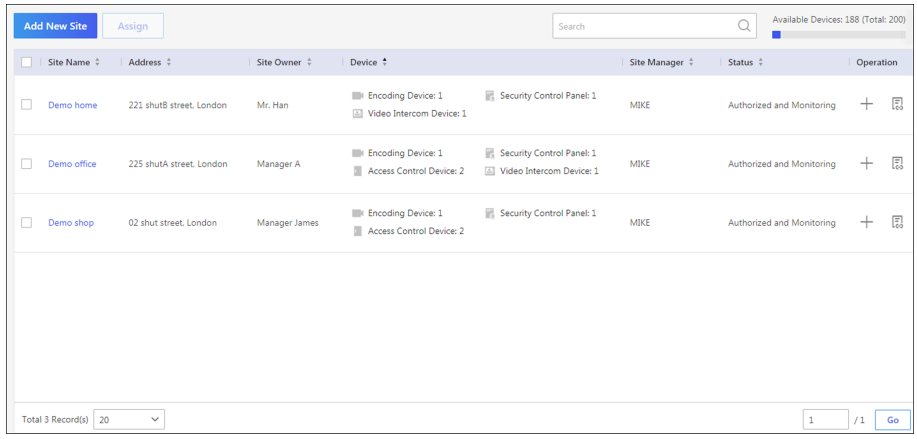

Figure 5-1 Site Page

There are different status for the sites in site list.

Not Invited

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

Not Registered

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

Not Accepted

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

Invited, Not Authorized

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

Authorized and Monitoring

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

Note

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

Table 5-1 Supported Operations in Different Status

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

5.2 Add New Site

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

Before You Start

Make sure you have the permission of adding new site.

Steps

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

   Note

   If an existing site of end user is not authorized to any installation company, you can click **Add 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, and add exception rule, etc. **Note** For more details, refer to ***Manage Device*** .

5.3 Add Existing Site

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

Steps

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

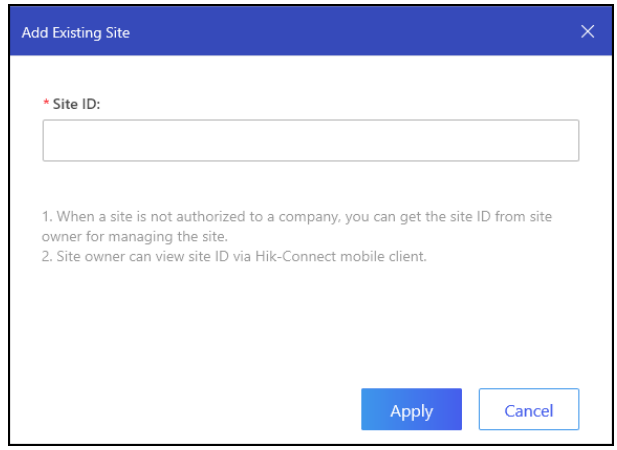

Figure 5-2 Add Existing Site

3. Enter the site ID provided.

Note

- You can get the site ID form the site owner, who can view the site ID via Hik-Connect Mobile Client.
- Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

4. Click **Apply**.

   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.

5.4 Assign Site to Installer

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

Before You Start

Make sure you have the permission of assigning site.

Steps

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

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

5.5 Invite Site Owner

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

Before You Start

Make sure the site status is **Not Invited** and you have the permission of site management.

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

   Note

   - If you have no device management permission or no devices are added in the site, the permissions of configuration and live view can not be selected.
   - 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.

7. Click **OK** to send the invitation.
   - If the invitee has registered a Hik-Connect account, he/she will receive the invitation via Hik-Connect Mobile Client. After accepting the invitation, the end user will become the site owner.
   - If the invitee has not registered a Hik-Connect account, he/she will receive the registration email or message in email box or via short message. 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 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

8. **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.

5.6 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.

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. 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.

   Note

   Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

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

Chapter 6 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 linkage rule, configuring exception rule, etc.

6.1 Add Device

You can add devices to sites in two ways, namely, adding manually or adding the detected online device.

6.1.1 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 seiral No., device IP address, activation status (activated or not), Hik-Connect status (connected to Hik-Connect service or not), etc.

Note

After adding the device, the Hik-ProConnect starts detecting whether the device firmware version is compatible with the Hik-ProConnect. Some functions (including health monitoring, linkage rule, 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.

After selecting the displayed device(s) and clicking **Next**, you should perform part or all of the following 4 steps based on the status of the selected devices before you can add them to the Portal.

Table 6-1 Step Description

Step	Description
Activate Device	If there are inactivated device(s), activate them. See ***Activate Device*** for details. **Note** 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 Password	Enter admin password of the device. See ***Enter Admin Password*** for details.
Connect to Hik-Connect Service	Connect device(s) to the Hik-Connect service. See ***Connect to Hik-Connect Service*** for details.
Enter Device Verification Code	Enter the device verification code. See ***Enter Device Verification Code*** for details.

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

- Click the device name to edit it. Or move the cursor to the device and then click to edit device name.
- Click to configure linkage rule for the device.

Note

For details, see ***Add Custom Linkage Rule***

- Click ··· → to delete the device.

Note

Deleting device is not supported if the site is authorized.

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 Admin 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.

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

For devices which are not connected to the Hik-Connect service, you should create a device verification code for all of them to connect them to the service.

Note

- Before connecting devices to the Hik-Connect service, you should 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.

You can also enter the default verification code of one of the disconnected device(s) to set it as the device verification code for all of the disconnected device(s). The default verification code is usually printed on the device label.

Enter Device Verification Code

For devices which are connected to the Hik-Connect service, you should enter their device verification code on the pop-up window. The device verificaiton code is created when you connect device(s) to the Hik-Connect service.

6.1.2 Manually Add Device

You can manually add devices 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. 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.

4. Click **Add Device**.

   Note

   - After adding the device, the Hik-ProConnect starts 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.
   - Please inform your end users to download or update the Hik-Connect Mobile Client (Version 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

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

Edit Device Name	Click the device name to edit it. Or move the cursor to the device and then click to edit it.
Delete Device	Click ··· → 🗑 . **Note** Deleting device is not supported if the site is authorized.
Upgrade Device	Refer to ***Upgrade Device*** .

6.2 Apply for Live View and Configuration Permission

After handing over a site to the end user, if you need to view the live view of devices added to the site or configure the devices added to the site, you can apply for the live view permission and (or) configuration permission 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 Live View Permission** or **Apply for Configuration Permission**.
3. Select device(s) you want to apply for permission.
4. Click **Apply** to apply for the permission from end user.

   If the end user approves your application, you will be able to view the live video and (or) configure devices.

6.3 Add Linkage Rule

An 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... 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 only shows the process of the linkage when its data transmission is done via Cloud (server).

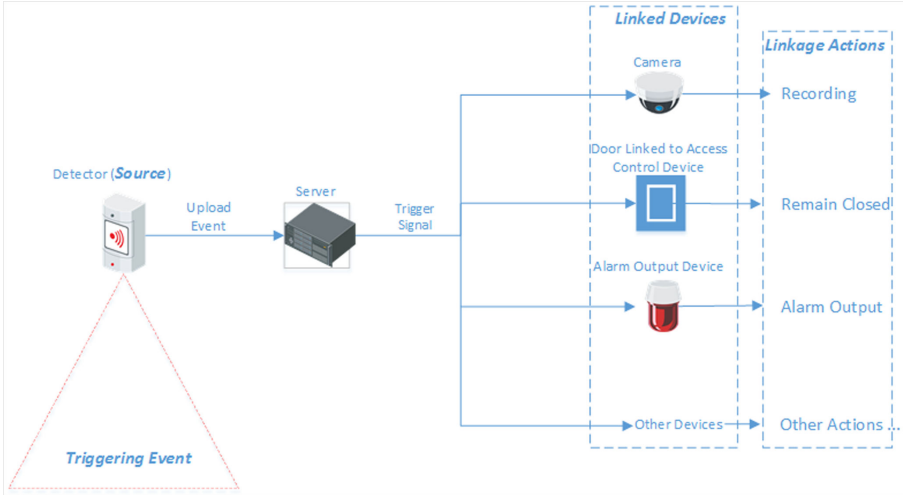

Figure 6-1 Linkage

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.

6.3.1 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.
- You should 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 Live View and Configuration 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.

1. Click **Site** to enter the site list page.
2. Open the Add Linkage Rule panel.
   - Select a site and click ··· → in the Operation column.
   - Click the name of a site to enter the site details page, and then click **Linkage Rule → Add Linkage Rule** .
   - Click the name of a site to enter the site details page, and then select a device and click .
3. Set the required information.

Linkage Rule Name

Create a linkage rule name.

Trigger

Define the trigger for the linkage action.

Select Source

Select a resource as the Source.

Set Triggering Event

Select an event as the triggering event.

Note

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

Table 6-2 Available Triggering Events for Different Resource Types

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

Linkage

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

Note

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

Linkage Action

Select linkage action(s).

Table 6-3 Linkage Action Description

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

Linked Resource	Linkage Action	Description
		Note You should have configured patrols for the PTZ camera. For details, see the user manual of the PTZ camera.
	Call Pattern	Select a pattern from the Pattern drop-down list tot specify it as the pattern which will be called when the Triggering Event is detected. A pattern is a predefined PTZ movement path with a certain dwell-time configured for a certain position. By calling a pattern, the PTZ camera moves according the predefined path. **Note** You should 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 Surveillance Center 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 Surveillance Center when the Triggering Event is detected.
	Enable Privacy Mask	Privacy mask will be displayed on the live images of the camera when the Triggering Event is detected. **Note** You should 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.

Linked Resource	Linkage Action	Description
	Disarm	The area of the security control panel will be disarmed when the Triggering Event is detected.
Door Linked to Access Control Device	Open Door	The door related to the access control device will be opened when the Triggering Event is detected.
	Remain Open	The door related to the access control device will remain open when the Triggering Event is detected.
	Remain Closed	The door related to the access control device will remain closed when the Triggering Event is detected.
Door Station	Open Door	The door linked to the door station will be automatically opened when the Triggering Event is detected.
Alarm Input	Arm Alarm Input	The alarm input will be armed and hence events related to it will be uploaded to the Surveillance Center 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 Surveillance Center 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 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page of Portal to them.

6.3.2 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 Live View and Configuration Permission*** .

Table 6-4 Template Description

Template	Description
Intrusion	The Intrusion Template: Used for improving security level by triggering the linkage actions including capture, recording, and alarm output, when the intrusion event (people, vehicles, or other objects enter a pre-defined area) occurs.
Forced Entry Alarm	The Forced Entry Alarm Template: Used for improving security level by triggering the linkage actions including capture, recording, remaining door closed, alarm output, and calling preset when 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.

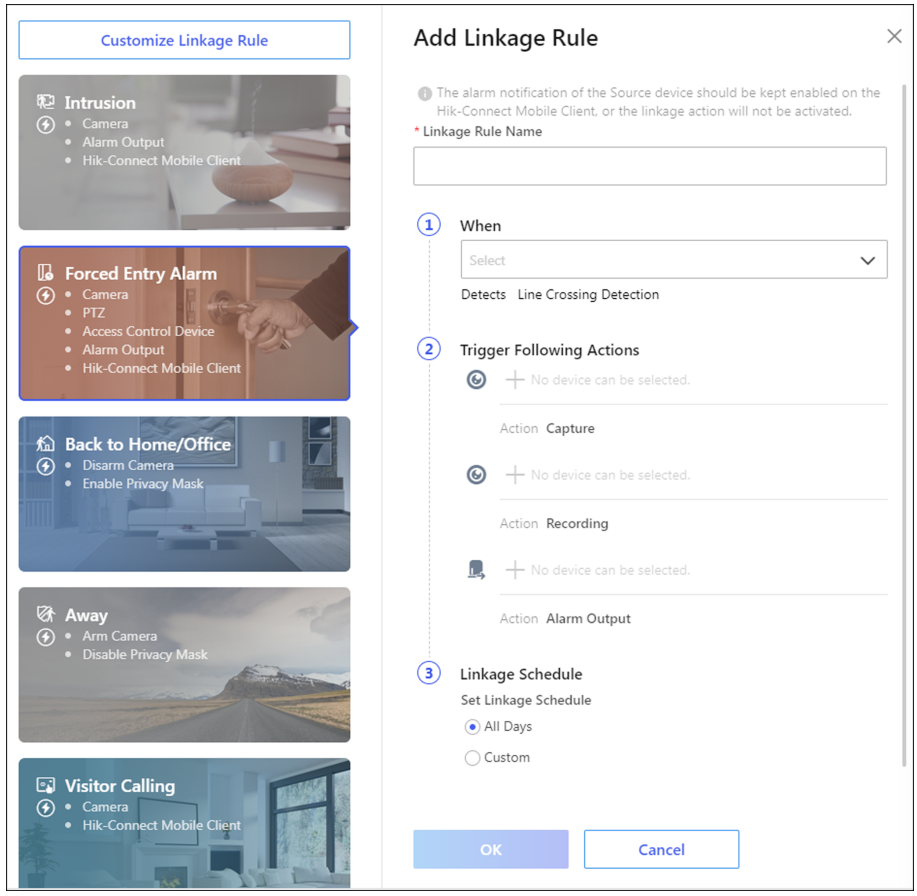

Figure 6-2 Add Linkage Rule by Template

3. Set the required information.

Linkage Rule Name

Create a linkage rule name.

When

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

Trigger the Following Actions

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

Note

- You can set only one linkage action.
- For details about the linkage actions, see ***Table 6-3*** .

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

6.4 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 Live View and Configuration Permission*** .
- Make sure you have enabled the device to send notifications to the system (if the device supports). For details, refer to ***Enable Device to Send Notifications*** .

You can add a rule to define such a notification. The rule contains five elements, including **Source** (device A or channel A), **Exception** (the exception occurred on device A or channel A), **Received by** (the source pushes a notification to notify the recipient via certain ways), **Recipient** (who can receive the notification), as well as **Schedule** (when the recipient can receive the notification).

Steps

1. Enter **Site** module.
2. Click the name of a site to enter the site details page, and then click **Exception**.

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

   Example

   For encoding devices, all the cameras will be displayed. For security control panels, all the zones and alarm outputs are displayed.
4. Set the types of exceptions which can trigger the notification.
   1) Move the cursor to the **Exception** field of the device or channel and click .

Figure 6-3 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 30 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.

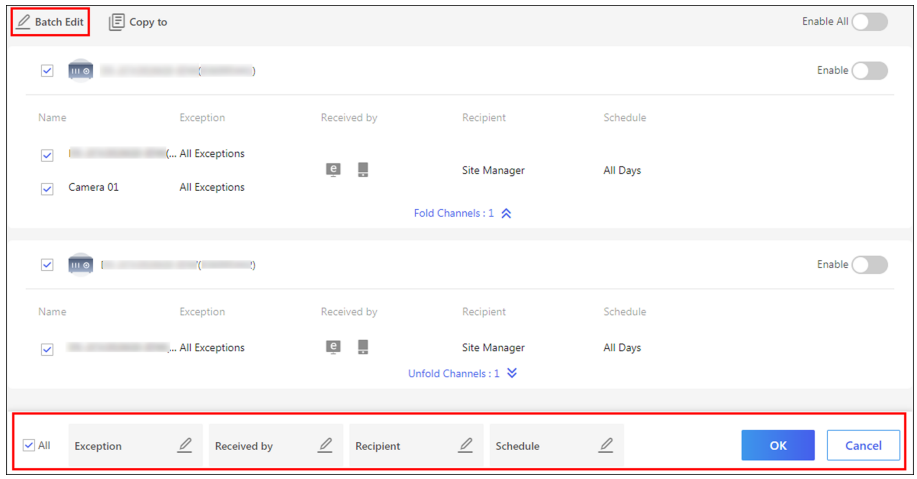

Figure 6-4 Batch Set/Edit Exception Rules

4) Click **OK** to save the settings.

9. **Optional:** After setting one rule, you can copy the rule settings to other devices or channels for quick settings.
   1) Click **Copy to**.
   2) In the **Copy Exception Settings from** field, select device(s) or channel(s) as the sources.
   3) In the **To** field, select the target resources of the same type as the selected sources.
   4) Click **Copy** to copy the rule settings of the sources to the target resources and back to the exception rule list. Or you can click **Copy and Continue** to copy the rule settings and continue to copy other settings.
10. After setting the exception rule, you need to set the **Enable** switch at the upper-right cornet of the rule to on to enable the device's exception rule, or set the **Enable All** switch to on to enable the all the devices' exception rules in the site.

    After enabling the rule, it will be active and when an exception occurs, the device will push a notification according to the settings in the rule.

6.5 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 4.3.0 and later). You can send the QR code or download link shown in the banner on the Home page to them.

6.6 Upgrade Device

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

Steps

Note

- The system supports upgrading an encoding device connected to the same LAN with the PC where the client runs.
- You can also upgrade devices in the Health Monitoring module. For details, see ***Health Monitoring*** .

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

Note

- Once started, the upgrade cannot be stopped. Make sure a power failure or network outage does not happen during the upgrade.
- You can enable EN50131 Compliant mode on device configuration page via a Web Client. See device user manual for details.

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

6.7 View Live View

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. 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

- 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 4.3.0 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.

6.8 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, 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 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.

Chapter 7 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 status information about the status of the devices added to the sites. The status information, which is of importance for maintenance of the Hik-ProConnect system as a whole, helps you locate the source of exceptions and determine methods for troubleshooting in time, thus 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.

7.1 View Status of Devices in All Sites

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

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

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

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

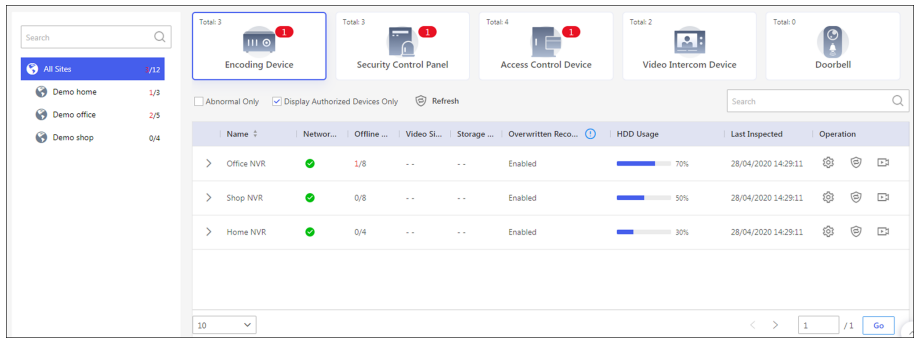

Figure 7-1 Status of Devices in All Sites

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 Live View and Configuration 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 Live View and Configuration Permission*** .

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 Live View and Configuration 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 7-1 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*** .
- 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 Live View and Configuration 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 Live View and Configuration 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 Live View and Configuration 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 Live View and Configuration 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*** .

7.2 View Status of Devices in Specific Site

You 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*** .
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.

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.

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 Live View and Configuration 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.

7.3 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.

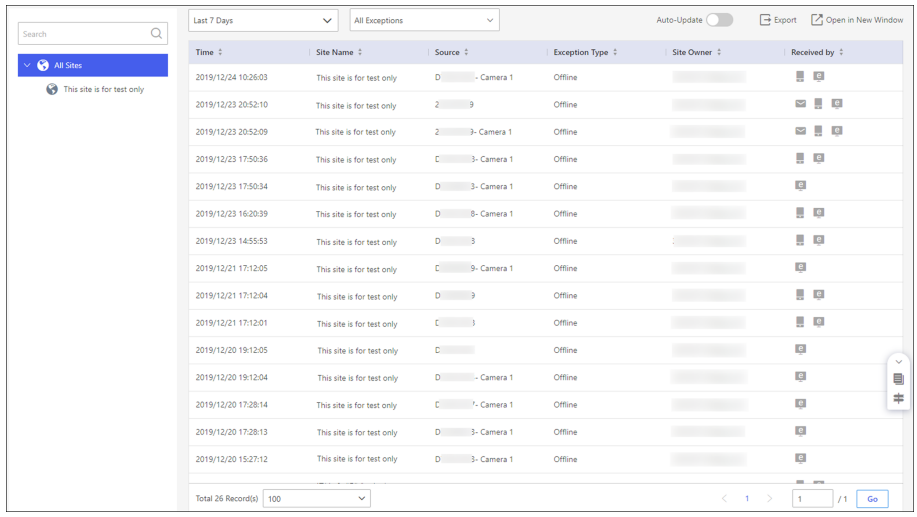

Figure 7-2 Exception Center

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 8 Search Operation Log

All operations information (including operator, operating time, 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 and selecting time. 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.

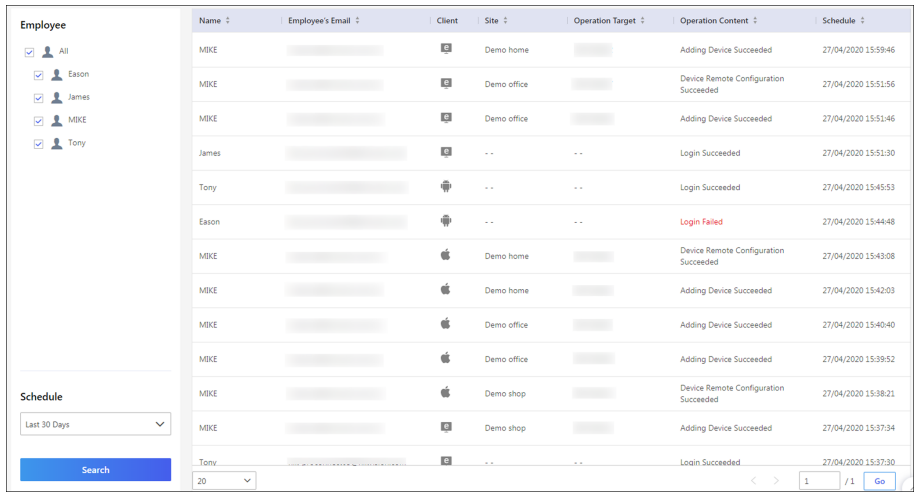

Figure 8-1 Search Operation Logs